
NetIQ Identity Manager Setup Guide

August 2014

Legal Notice

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, NETIQ CORPORATION PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

For purposes of clarity, any module, adapter or other similar material ("Module") is licensed under the terms and conditions of the End User License Agreement for the applicable version of the NetIQ product or software to which it relates or interoperates with, and by accessing, copying or using a Module you agree to be bound by such terms. If you do not agree to the terms of the End User License Agreement you are not authorized to use, access or copy a Module and you must destroy all copies of the Module and contact NetIQ for further instructions.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of NetIQ Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of NetIQ Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government's rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

© 2014 NetIQ Corporation. All Rights Reserved.

For information about NetIQ trademarks, see <https://www.netiq.com/company/legal/>.

Contents

About this Book and the Library	15
About NetIQ Corporation	17
Part I Introduction	19
1 Understanding the Architecture of Identity Manager	21
2 Creating and Maintaining Your Identity Manager Environment	23
2.1 Designer for Identity Manager	23
2.2 Analyzer for Identity Manager	23
2.3 Role Administration	24
2.4 iManager	25
3 Managing Data in the Identity Manager Environment	27
3.1 Understanding Data Synchronization	27
3.2 Understanding Auditing, Reporting, and Compliance	27
3.3 Understanding the Components for Synchronizing Your Identity Data	28
3.3.1 Identity Vault	28
3.3.2 Identity Manager Engine	28
3.3.3 Remote Loader	29
3.3.4 Identity Information Warehouse	29
4 Provisioning Users for Secure Access	31
4.1 Understanding the Attestation Process in Identity Manager	31
4.2 Understanding the Self-Service Process in Identity Manager	32
4.3 Understanding the Components for Managing User Provisioning	33
4.3.1 User Application and Roles Based Provisioning Module	33
4.3.2 Identity Manager Home and Provisioning Dashboard	34
Part II Planning to Install Identity Manager	37
5 Planning Overview	39
5.1 Planning Checklist	39
5.2 Understanding the Installation Process	40
5.2.1 Downloading the Installation Files	40
5.2.2 Installing Identity Manager in a Clustered Environment	41
5.3 Understanding Licensing and Activation	41
5.4 Understanding Identity Manager Communication	42
5.5 Understanding Language Support	42
5.5.1 Translated Components and Installation Programs	43
5.5.2 Special Considerations for Language Support	43

6 Considerations and Prerequisites for Installation 45

6.1	Installing Identity Manager on an RHEL 6.x Server	45
6.1.1	Using the Installation Wizard	45
6.1.2	Using the Command Line for Installation	45
6.2	Prerequisites and Requirements for Installing Designer	46
6.2.1	Prerequisites for Installing Designer	46
6.2.2	System Requirements for Installing Designer	46
6.3	Prerequisites and Requirements for Installing the Identity Vault	47
6.3.1	Considerations for Installing the Identity Vault	48
6.3.2	Considerations for Installing the Identity Vault as a Non-root User	49
6.3.3	Considerations for Installing Identity Vault on a Windows Server	50
6.3.4	Considerations for Installing the Identity Vault in a Clustered Environment.	50
6.3.5	Understanding Identity Manager Objects in eDirectory	51
6.3.6	Replicating the Objects that Identity Manager Needs on the Server	51
6.3.7	Using Scope Filtering to Manage Users on Different Servers	53
6.3.8	Understanding the Linux Packages in the Identity Vault Installation Kit	54
6.3.9	Improving Identity Vault Performance	57
6.3.10	System Requirements for Installing Identity Vault	57
6.4	Prerequisites and Requirements for Installing the Identity Manager Engine	58
6.4.1	Considerations for Installing Drivers with the Identity Manager Engine.	59
6.4.2	System Requirements for Installing the Identity Manager Engine	59
6.5	Prerequisites and Requirements for Installing iManager	61
6.5.1	Understanding the Server and Client Versions of iManager	61
6.5.2	Considerations for Installing iManager on a Linux Platform.	62
6.5.3	Considerations for Installing iManager on a Windows Platform.	63
6.5.4	Considerations for Installing iManager Workstation on Linux Clients	63
6.5.5	Considerations for Installing iManager Workstation on Windows Clients	64
6.5.6	System Requirements for iManager (Server Version)	64
6.5.7	System Requirements for iManager Workstation (Client Version).	66
6.6	Prerequisites and Requirements for Installing the Remote Loader	67
6.6.1	Prerequisites for Installing the Remote Loader	67
6.6.2	System Requirements for Installing the Remote Loader	68
6.7	Prerequisites and Requirements for Installing the User Application and Roles Based Provisioning Module.	69
6.7.1	Considerations for Installing the User Application and Roles Based Provisioning Module	69
6.7.2	Understanding the Installation Files for the Roles Based Provisioning Module	71
6.7.3	Understanding the Application Server Requirements	72
6.7.4	Understanding the User Application Database	73
6.7.5	Prerequisites for Installing the User Application in a Cluster Environment	75
6.7.6	System Requirements for Installing the User Application and Roles Based Provisioning Module	75
6.8	Prerequisites for Installing the Identity Information Warehouse	77
6.8.1	Prerequisites for the Event Auditing Service	78
6.8.2	Prerequisites for the Reporting Module	78
6.8.3	System Requirements for the Reporting Module.	78
6.8.4	System Requirements for the Event Auditing Service	80
6.9	Prerequisites and Requirements for Installing Role Administration	80
6.9.1	Prerequisites and System Requirements for Catalog Administrator	80
6.9.2	Prerequisites for Role Mapping Administrator	80
6.9.3	Understanding Permissions Required for Role Mapping Administrator Users	81
6.9.4	Understanding How Role Mapping Administrator Interacts with the Identity Vault	82
6.9.5	System Requirements for Installing Role Mapping Administrator	83
6.10	Prerequisites and Requirements for Installing Identity Manager Home and the Provisioning Dashboard	83
6.10.1	Prerequisites for Installing Identity Manager Home	84
6.10.2	System Requirements for Installing Identity Manager Home.	84
6.11	Prerequisites and Requirements for Installing Analyzer.	86

7	Installing Designer	89
7.1	Using the Installation Command on Linux	89
7.2	Running the Windows Executable File	90
7.3	Using the Silent Installation Process	90
Part III Installing the Identity Vault		91
8	Main Checklist for Installing Identity Vault	93
9	Preparing to Install the Identity Vault	95
9.1	Using Escape Characters when a Container Name Includes a Period (“.”)	95
9.2	Using OpenSLP or hosts.nds for Resolving Tree Names	95
9.2.1	Using a hosts.nds File to Resolve Tree Names	96
9.2.2	Understanding OpenSLP	97
9.2.3	Configuring SLP for the Identity Vault	99
9.3	Using IPv6 Addresses on the Identity Vault Server	100
9.3.1	Using IPv6 Addresses on Linux Servers	100
9.3.2	Using IPv6 Addresses on Windows Servers	102
9.4	Using LDAP to Communicate with the Identity Vault	102
9.5	Installing NICI Manually on Workstations that have Management Utilities	103
9.5.1	Installing NICI on Linux Servers	103
9.5.2	Installing NICI on Windows Servers	104
9.6	Installing NMAS Client Software	104
9.6.1	Installing and Configuring NMAS Client Software on Linux Servers	105
9.6.2	Installing NMAS Client Software on Windows Servers	106
10	Installing the Identity Vault on a Linux Server	107
10.1	Installing the Identity Vault as Root	107
10.2	Installing the Identity Vault as a Non-root User	109
11	Installing the Identity Vault on a Windows Server	111
11.1	Using the Wizard to Install the Identity Vault on a Windows Server	111
11.2	Silently Installing and Configuring the Identity Vault on a Windows Server	112
11.2.1	Editing the response.ni File	112
11.2.2	Performing a Silent or Unattended Installation	118
11.2.3	Performing a Silent Configuration	119
11.2.4	Performing a Silent Installation Combined with Configuration	119
12	Installing the Identity Vault in a Clustered Environment	121
12.1	Installing the Identity Vault in a Cluster on Linux	121
12.1.1	Installing and Configuring the Identity Vault on Linux	122
12.1.2	Configuring an SNMP Server in a Clustered Linux Environment	124
12.2	Installing the Identity Vault in a Cluster on Windows	124
12.2.1	Installing and Configuring the Identity Vault on Windows	124
12.2.2	Configuring an SNMP Server in Clustered Windows Environments	126
13	Configuring the Identity Vault after Installation	127
13.1	Modifying the eDirectory Tree and Replica Server with the ndsconfig Utility	127
13.1.1	Understanding the ndsconfig Utility Parameters	128
13.1.2	Configuring the Identity Vault in a Specific Locale	131

13.1.3	Adding a New Tree to the Identity Vault	131
13.1.4	Adding a Server to an Existing Tree	132
13.1.5	Removing the Identity Vault and its Database from the Server	132
13.1.6	Removing an eDirectory Server Object and Directory Services from a Tree	132
13.1.7	Configuring Multiple Instances of the Identity Vault	133
13.2	Managing Instances with the ndsmanage Utility	133
13.2.1	Listing Identity Vault Instances	133
13.2.2	Creating a New Instance in the Identity Vault	133
13.2.3	Configuring and Deconfiguring an Instance in the Identity Vault	134
13.2.4	Invoking a Utility for an Instance in the Identity Vault	134
13.2.5	Starting and Stopping Instances in the Identity Vault	134
Part IV Installing the Identity Manager Engine		137
14 Installing the Identity Manager Engine		139
14.1	Checklist for Installing the Identity Manager Engine	139
14.2	Verifying Environment Variables (UNIX / Linux) for the Identity Manager Installation	140
14.3	Using the Wizard to Install the Identity Manager Engine	140
14.3.1	Installing the Identity Manager Engine as a Root User	140
14.3.2	Installing the Identity Manager Engine as a Non-root User	142
14.4	Performing a Silent Installation of the Identity Manager Engine	143
14.5	Adding Support for Graphics in Email Notifications	144
Part V Installing iManager		145
15 Checklist for Installing iManager		147
16 Installing iManager Server and Workstation		149
16.1	Understanding Installation for iManager Plug-ins	149
16.2	Installing iManager and iManager Workstation on Linux	150
16.2.1	Installing iManager on Linux	150
16.2.2	Installing iManager Workstation on Linux Clients	152
16.3	Installing iManager and iManager Workstation on Windows	153
16.3.1	Installing iManager on Windows	154
16.3.2	Installing iManager Workstation on Windows	156
16.4	Installing iManager Silently	157
16.4.1	Editing the Properties File for a Customized Silent Installation	157
16.4.2	Running a Silent Installation for iManager	159
17 Post-Installation Tasks for iManager		161
17.1	Replacing the Temporary Self-Signed Certificates for iManager	161
17.1.1	Replacing the iManager Self-Signed Certificates on Linux	161
17.1.2	Replacing the iManager Self-Signed Certificates on Windows	163
17.2	Configuring iManager for IPv6 Addresses after Installation	164
17.3	Specifying an Authorized User for eDirectory	165
Part VI Installing the Remote Loader		167
18 Preparing to Install the Remote Loader		169
18.1	Checklist for Installing the Remote Loader	169
18.2	Using 32-bit and 64-bit Remote Loader on the Same Computer	170

18.3	Understanding the Java Remote Loader	170
18.4	Understanding Shims.	171
19	Installing Remote Loader	173
19.1	Installing the Remote Loader from the Console	173
19.2	Installing the Remote Loader Silently.	174
19.2.1	Creating the Properties File for a Silent Installation.	174
19.2.2	Running a Silent Installation for Remote Loader	175
19.3	Installing the Java Remote Loader on UNIX or Linux	176
20	Configuring the Remote Loader	177
20.1	Creating a Secure Connection to the Identity Manager Engine	177
20.1.1	Understanding the Communication Process	177
20.1.2	Managing Self-Signed Server Certificates.	178
20.1.3	Creating a Keystore File when Using SSL Connections	179
20.2	Configuring the Remote Loader for Driver Instances.	180
20.2.1	Understanding the Configuration Parameters for the Remote Loader.	180
20.2.2	Configuring the Remote Loader for Driver Instances on UNIX or Linux	188
20.2.3	Configuring the Remote Loader for Driver Instances on Windows	190
20.2.4	Configuring the Java Remote Loader for Driver Instances	192
20.3	Configuring Identity Manager Drivers to Work with the Remote Loader	193
21	Starting and Stopping the Remote Loader	195
21.1	Starting a Driver Instance in the Remote Loader	195
21.1.1	Starting Driver Instances on UNIX or Linux	195
21.1.2	Starting Driver Instances on Windows	196
21.2	Stopping a Driver Instance in the Remote Loader	197
Part VII	Installing the User Application and Roles Based Provisioning Module	199
22	Main Checklist for Installing RBPM and the User Application	201
23	Installing the Community Edition of JBoss	203
24	Installing the Roles Based Provisioning Module	205
24.1	Understanding the Roles Based Provisioning Module installation	205
24.1.1	Installation Checklist	205
24.1.2	Understanding Schema Extension.	206
24.2	Extending the eDirectory Schema Using the Wizard	206
24.2.1	Extending the Schema on a SUSE Server	206
24.2.2	Extending the Schema on a Windows Server	207
24.3	Extending the Schema Manually without Using the Wizard.	208
24.3.1	Extending the Schema on a Windows Server without the Wizard.	209
24.3.2	Extending the Schema on UNIX or Linux without the Wizard	209
24.3.3	Copying Additional JAR files	209
24.3.4	Adding the User Application Schema to your Audit Server as a Log Application	210
24.4	Installing RBPM with the Schema Extension Files.	210
25	Creating the Drivers for the Roles Based Provisioning Module	213
25.1	Creating the User Application Driver	213

25.2	Creating the Role and Resource Service Driver	214
25.3	Deploying the Drivers for the User Application	214
26	Configuring the Database Before Installing the User Application	215
26.1	Configuring a DB2 Database	215
26.1.1	Providing the Database Driver JARs	215
26.1.2	Tuning DB2 Databases to Prevent Deadlocks and Timeouts	216
26.2	Configuring a MySQL Database	217
26.2.1	Configuring INNODB Storage Engine and Table Types	217
26.2.2	Configuring the Character Set	218
26.2.3	Configuring Case Sensitivity	218
26.2.4	Configuring the ANSI Setting	218
26.2.5	Configuring the Admin User Account	219
26.3	Configuring an Oracle Database	219
26.3.1	Configuring the Character Set	219
26.3.2	Configuring the Admin User Account	220
26.4	Configuring a SQL Server Database	220
26.4.1	Configuring the Character Set	220
26.4.2	Configuring the Admin User Account	220
27	Preparing a Cluster Environment for Use with the User Application	221
27.1	Understanding Cluster Groups in JBoss and WebSphere Environments	221
27.2	Preparing a JBoss Cluster for the User Application	222
27.2.1	Setting JBoss System Properties	222
27.2.2	Specifying the Cluster Option	222
27.2.3	Configuring the Cluster for the User Application Database	223
27.2.4	Using the Same Master Key for Each User Application in the Cluster	223
27.2.5	Starting the User Application in a Cluster Group	223
27.3	Preparing a WebLogic Cluster for the User Application	224
27.4	Preparing a WebSphere Cluster for the User Application	224
28	Installing the User Application on an Application Server	227
28.1	Installing on a JBoss Application Server	227
28.1.1	Checklist for Installing the User Application on JBoss	227
28.1.2	Installing the JBoss Application Server	228
28.1.3	Installing the User Application on a JBoss Server	228
28.2	Installing on a WebLogic Application Server	239
28.2.1	Checklist for Installing the User Application on WebLogic	239
28.2.2	Configuring the Data Source for the User Application Database on WebLogic	240
28.2.3	Installing the User Application with the Installation Wizard	240
28.2.4	Configuring the WebLogic Environment for the User Application	244
28.2.5	Start the User Application on the WebLogic Server	246
28.3	Installing on a WebSphere Application Server	247
28.3.1	Checklist for Installing the User Application on WebSphere	247
28.3.2	Configuring a Data Source for the User Application Database on WebSphere	248
28.3.3	Installing the User Application on a WebSphere Server	249
28.3.4	Adding User Application Configuration Files and JVM System Properties	253
28.3.5	Creating and Applying a Shared Library	254
28.3.6	Importing the eDirectory Trusted Root to the WebSphere Keystore	255
28.3.7	Applying the Unrestricted Policy Files for the IBM JDK	256
28.3.8	Passing the preferIPv4Stack Property to JVM	256
28.3.9	Starting the User Application on the WebSphere Server	257

29	Installing RBPM Components from the Command Line	259
29.1	Performing a Guided Installation from the Command Line	260
29.2	Installing the User Application with a Single Command	263
29.2.1	Setting Passwords in the Environment for a Silent Installation	263
29.2.2	Editing the silent.properties File	264
29.2.3	Executing a Silent Installation of the User Application	272
29.3	Running the JBossPostgreSQL Utility in Silent or Command Mode	272
29.3.1	Setting Passwords in the Environment for a Silent Installation	273
29.3.2	Editing the silent.properties File	273
29.3.3	Performing a Silent or Command Installation for the JBossPostgreSQL Utility	274
29.4	Running the RIS Installation Program in Silent or Command Mode	275
29.4.1	Editing the silent.properties File	275
29.4.2	Performing a Silent or Command Installation for the RIS Facility	275
30	Completing the Roles Based Provisioning Module / User Application Installation	277
30.1	Recording the Master Key	277
30.2	Configuring the User Application	277
30.2.1	Identity Vault Settings	278
30.2.2	Identity Vault DNSs	279
30.2.3	Identity Vault User Identity	281
30.2.4	Identity Vault User Groups	282
30.2.5	Identity Vault Certificates	283
30.2.6	Email Server Configuration	283
30.2.7	Trusted Key Store	284
30.2.8	Novell Audit Digital Signature Certificate & Key	285
30.2.9	Access Manager Settings	285
30.2.10	Password Management	285
30.2.11	Miscellaneous	286
30.2.12	Container Object	287
30.3	Configuring Identity Vault for the User Application	288
30.3.1	Creating Indexes in eDirectory	288
30.3.2	Installing and Configuring SAML Authentication Method	288
30.4	Reconfiguring the User Application WAR File	289
30.5	Configuring External Forgot Password Management	290
30.5.1	Specifying an External Forgot Password Management WAR File	290
30.5.2	Specifying an Internal Password WAR File	291
30.5.3	Testing the External Forgot Password WAR Configuration	291
30.5.4	Configuring SSL Communication between JBoss Servers	291
30.6	Updating Forgot Password Settings	291
30.7	Defining the Java Heap Size for the Role and Resource Service Driver	292
Part VIII	Installing the Identity Information Warehouse	293
31	Preparing to Install the Information Warehouse	295
31.1	Checklist for Installing the Identity Information Warehouse	295
31.2	Understanding the Users Created during the Installation Process	296
32	Installing the Event Auditing System	297
32.1	Preparing the Environment for Event Auditing Service	297
32.2	Using the Wizard to Install Event Auditing Service	298
32.3	Installing Event Auditing Service Silently	299

33	Installing the Reporting Module	301
33.1	Using the Wizard to Install the Reporting Module	301
33.2	Installing the Reporting Module Silently	304
33.3	Configuring the Reporting Module	305
33.3.1	Defining User Preferences	305
33.3.2	Setting System Properties	306
33.4	Configuring the Reporting Module for WebLogic and WebSphere	307
33.4.1	Preparing WebSphere and WebLogic Environments	307
33.4.2	Configuring the WebLogic Environment	307
33.4.3	Configuring the WebSphere Environment	308
33.4.4	Configuring WebLogic and WebSphere for SSL Connections	309
34	Managing the Drivers for Reporting	311
34.1	Configuring Drivers for the Reporting Module	311
34.1.1	Installing the Driver Packages for the Reporting Module	311
34.1.2	Configuring the Managed System Gateway Driver	311
34.1.3	Configuring the Driver for Data Collection Service	313
34.2	Deploying and Starting Drivers for the Reporting Module	315
34.2.1	Deploying the Drivers	315
34.2.2	Verifying that the Managed Systems are Working	316
34.2.3	Starting the Drivers for the Reporting Module	318
34.3	Backing up the Schema for the Drivers	320
34.3.1	Backing Up and Restoring the idm_rpt_data and idm_rpt_cfg Schemas	320
34.3.2	Backing Up and Restoring the public Schema	320
34.4	Configuring the Runtime Environment	321
34.4.1	Migrating the Data Collection Service Driver	321
34.4.2	Adding Support for Custom Attributes and Objects	323
34.4.3	Adding Support for Multiple Driver Sets	326
34.4.4	Configuring the Drivers to Run in Remote Mode with SSL	327
34.5	Setting Auditing Flags for the Drivers	328
34.5.1	Setting Audit Flags in Identity Manager	328
34.5.2	Setting Audit Flags in eDirectory	329
Part IX	Installing a Role Administrator Component	333
35	Preparing and Installing Catalog Administrator	335
35.1	Checklist for Installing Catalog Administrator	335
35.2	Installing Catalog Administrator	336
36	Preparing to Install Role Mapping Administrator	337
36.1	Checklist for Installing Role Mapping Administrator	337
36.2	Setting Permissions for Role Mapping Administrator	338
36.2.1	Assigning Administrator Rights to Specific Roles	338
36.2.2	Assigning Administrator Rights to Specific Users or Groups	339
37	Installing Role Mapping Administrator	341
37.1	Using the Wizard to Install Role Mapping Administrator	341
37.2	Installing Role Mapping Administrator Silently	342
38	Configuring Role Mapping Administrator	345
38.1	Starting and Stopping Role Mapping Administrator	345

38.1.1	Automatically Starting Role Mapping Administrator on Linux	345
38.1.2	Automatically Starting Role Mapping Administrator on Windows	345
38.2	Logging in to the Administrator Configuration Page for Role Mapping Administrator	346
38.3	Connecting Role Mapping Administrator to the Identity Vault	346
38.4	Configuring the Drivers for Role Mapping Administrator	347
38.5	Loading Authorizations into the Database	348
38.6	Enabling TLS/SSL Communications for Role Mapping Administrator	348
38.6.1	Enabling Role Mapping Administrator to Use SSL for Connecting to the Identity Vault	348
38.6.2	Enabling SSL for a Browser to Access Role Mapping Administrator	349
38.7	Changing Role Mapping Administrator Settings	350
38.7.1	Changing Port Numbers for Role Mapping Administrator	350
38.7.2	Changing the Password for Role Mapping Administrator	351
38.7.3	Changing the Java Heap Size for the Role Mapping Administrator	351
38.8	Tuning Session Timeouts for Role Mapping Administrator	352

39 Configuring Authentication to Role Mapping Administrator 353

39.1	Configuring Single Sign-on through the Roles Based Provisioning Module	353
39.1.1	Enabling the Roles Based Provisioning Module for Single Sign-on	353
39.1.2	Creating a Shared Page for Role Mapping Administrator	354
39.1.3	Assigning Permissions for Single Sign-on to Role Mapping Administrator	354
39.1.4	Specifying the Content for the Page that Links to Role Mapping Administrator	355
39.2	Configuring Single Sign-on through Access Manager	356
39.2.1	Understanding Single Sign-on through Access Manager	356
39.2.2	Configuring Active Directory to Assign Kerberos Tickets	356
39.2.3	Configuring Access Manager Identity Server to Consume the Kerberos Tickets	358
39.2.4	Configuring the User's Web Browser	364

40 Auditing Role Mapping Administrator 367

40.1	Enabling Auditing of Role Mapping Administrator	367
40.2	Understanding the Audit Events Generated by Role Mapping Administrator	368
40.2.1	Event ID 00031550	368
40.2.2	Event ID 00031551	368
40.2.3	Event ID 00031630	369
40.2.4	Event ID 00031631	370
40.2.5	Event ID 00031632	371
40.2.6	Event ID 00031633	371
40.2.7	Event ID 00031634	372
40.2.8	Event ID 000361635	373
40.2.9	Event ID 00031670	373
40.2.10	Event ID 00031671	374
40.2.11	Event ID 00031674	375
40.2.12	Event ID 00031675	376
40.2.13	Event ID 00031676	376
40.2.14	Event ID 00031677	377
40.2.15	Event ID 0003167A	378
40.2.16	Event ID 0003167B	378

Part X Installing Identity Manager Home and the Provisioning Dashboard 381

41 Installing Identity Manager Home 383

41.1	Checklist for Installing Identity Manager Home	383
41.2	Preparing Your Environment	384
41.3	Installing Identity Manager Home	384

41.3.1	Installing Identity Manager Home	384
41.3.2	Updating User Application Files in an Environment that Uses a Non-Default Context . . .	386
42	Configuring Your Identity Manager Environment for Identity Manager Home	389
42.1	Checklist for Configuring Your Environment for Identity Manager Home	389
42.2	Configuring the Identity Vault for Identity Manager Home	389
42.3	Configuring the Information Warehouse for Identity Manager Home	391
42.3.1	Configuring the Event Auditing System for Identity Manager Home	391
42.3.2	Updating the WAR File for Event Auditing Service	391
42.3.3	Configuring the Data Collection Services Driver for OAuth Protocol with Identity Manager Home	392
42.3.4	Reconfiguring Auditing and Logging	393
42.4	Configuring Single Sign-on Access for Identity Manager Home	394
42.4.1	Creating a Keystore for One SSO Provider	394
42.4.2	Configuring Single Sign-on Settings	394
42.5	Configuring RBPM and the User Application for Identity Manager Home	396
42.5.1	Updating the User Application Driver Package for Identity Manager Home	396
42.5.2	Configuring the User Application Database for Identity Manager Home	397
42.5.3	Modifying SSO Clients and Authentication Settings with the RBPM Configuration Utility	399
42.6	Reconfiguring Forgotten Password Self-Service	400
43	Verifying Installation of Identity Manager Home	401
44	Installing Analyzer	403
44.1	Checklist for Installing Analyzer	403
44.2	Using the Wizard to Install Analyzer	404
44.3	Installing Analyzer Silently	404
44.4	Adding XULrunner to Analyzer.ini on Linux Platforms	405
44.5	Installing an Audit Client for Analyzer	406
45	Activating Identity Manager	407
45.1	Installing a Product Activation Credential	407
45.2	Reviewing Product Activations for Identity Manager and Drivers	408
45.3	Activating Identity Manager Drivers	408
45.4	Activating Specific Identity Manager Components	409
45.4.1	Activating Designer and Role Mapping Administrator	409
45.4.2	Activating Analyzer	409
Part XI	Upgrading or Migrating Identity Manager	411
46	Preparing to Upgrade or Migrate Identity Manager	413
46.1	Understanding Upgrade and Migration	413
46.2	Backing Up the Current Configuration	414
46.2.1	Exporting the Designer Project	414
46.2.2	Exporting the Configuration of the Drivers	415
46.3	Stopping and Starting Identity Manager Drivers during Upgrade and Migration	416
46.3.1	Stopping the Drivers	416
46.3.2	Starting the Drivers	417

47 Upgrading Identity Manager	419
47.1 Checklist for Upgrading Identity Manager	419
47.2 Upgrading to a New Version of Advanced Edition	420
47.3 Upgrading to Advanced Edition from Standard Edition	422
47.3.1 Upgrading the Identity Manager Engine Server	422
47.3.2 Upgrading the User Application	422
47.3.3 Upgrading the Identity Reporting Module	423
47.4 Upgrading to a New Version of Standard Edition	424
47.5 Upgrading Individual Components of Identity Manager	425
47.5.1 Upgrading Designer	425
47.5.2 Upgrading iManager	426
47.5.3 Upgrading the Remote Loader	430
47.5.4 Upgrading the Identity Information Warehouse	431
47.5.5 Upgrading Analyzer	432
47.6 Upgrading the Identity Manager Drivers	433
47.6.1 Creating a New Driver	433
47.6.2 Replacing Existing Content with Content from Packages	433
47.6.3 Keeping the Current Content and Adding New Content with Packages	434
47.7 Restoring Custom Policies and Rules to the Driver	434
47.7.1 Using Designer to Restore Custom Policies and Rules to the Driver	434
47.7.2 Using iManager to Restore Custom Policies and Rules to the Driver	435
48 Performing a Migration	437
48.1 Checklist for Performing a Migration	437
48.2 Preparing For Mixed-case Searches on Roles and Resources	438
48.2.1 How NrfCaseUpdate Affects the Schema	438
48.2.2 Creating a Backup of the User Application Drivers	439
48.2.3 Running NrfCaseUpdate	439
48.2.4 Verifying the NrfCaseUpdate Process	441
48.2.5 Enabling the JRE for SSL Connections	441
48.2.6 Restoring Invalidated User Application Drivers	442
48.3 Updating the User Application	443
48.4 Adding the New Server to the Driver Set	444
48.5 Copying Server-Specific Information for the Driver Set	444
48.5.1 Copying the Server-specific Information in Designer	444
48.5.2 Changing the Server-specific Information in iManager	445
48.5.3 Changing the Server-specific Information for the User Application	446
48.6 Removing the Old Server from the Driver Set	446
48.6.1 Using Designer to Remove the Old Server from the Driver Set	446
48.6.2 Using iManager to Remove the Old Server from the Driver Set	446
48.6.3 Decommissioning the Old Server	447
49 Uninstalling Identity Manager Components	449
49.1 Removing Objects from the Identity Vault	449
49.2 Uninstalling the Identity Manager Engine	449
49.2.1 Uninstalling the Identity Manager Engine on Linux/UNIX	450
49.2.2 Uninstalling the Identity Manager Engine as a Non-root User	450
49.2.3 Uninstalling the Identity Manager Engine on Windows	450
49.3 Uninstalling the Remote Loader	450
49.3.1 Uninstalling the Remote Loader on Linux/UNIX	450
49.3.2 Uninstalling the Remote Loader as a Non-root User	451
49.3.3 Uninstalling the Remote Loader on Windows	451
49.4 Uninstalling the Roles Based Provisioning Module	451
49.4.1 Deleting the Drivers for the Roles Based Provisioning Module	451
49.4.2 Uninstalling the User Application on Linux/UNIX	452

49.4.3	Uninstalling the User Application on Windows	452
49.5	Uninstalling the Identity Information Warehouse	453
49.5.1	Deleting the Reporting Drivers	453
49.5.2	Uninstalling the Identity Reporting Module	453
49.5.3	Uninstalling the Event Auditing Service	454
49.6	Uninstalling Role Mapping Administrator	454
49.7	Uninstalling Catalog Administrator	454
49.8	Uninstalling eDirectory	455
49.9	Uninstalling Analyzer	456
49.10	Uninstalling iManager.	456
49.10.1	Uninstalling iManager on Linux	457
49.10.2	Uninstalling iManager on Windows	457
49.10.3	Uninstalling iManager Workstation	457
49.11	Uninstalling Designer	457

50 Troubleshooting 459

50.1	Troubleshooting the User Application and RBPM Installation	459
------	--	-----

A Sample Identity Manager Cluster Deployment Solution 461

A.1	Prerequisites	461
A.2	Installation Procedure.	462
A.2.1	Configuring the iSCSI Server	462
A.2.2	Configuring the iSCSI initiator on all Nodes.	462
A.2.3	Partitioning the Shared Storage.	463
A.2.4	Installing the HA Extension	463
A.2.5	Configuring the HA Cluster	464
A.2.6	Configuring Global Cluster Options	465
A.2.7	Configuring the OCFS Resources	466
A.2.8	Configuring IP Resource	469
A.2.9	Installing and Configuring eDirectory and Identity Manager on Cluster Nodes	469
A.2.10	Configuring the eDirectory Resource	470

About this Book and the Library

The *Setup Guide* provides instructions for installing the NetIQ Identity Manager (Identity Manager) product. This guide describes the process for installing individual components in a distributed environment. To install Identity Manager on a single server, see the [Identity Manager 4.0.2 Integrated Installation Guide](#).

Intended Audience

This book provides information for identity architects and identity administrators responsible for installing the components necessary for building an identity management solution for their organization.

Other Information in the Library

For more information about the library for Identity Manager, see the [Identity Manager documentation Web site \(https://www.netiq.com/documentation/idm402/\)](#).

About NetIQ Corporation

We are a global, enterprise software company, with a focus on the three persistent challenges in your environment: Change, complexity and risk—and how we can help you control them.

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

In fact, of all the challenges you face, these are perhaps the most prominent variables that deny you the control you need to securely measure, monitor, and manage your physical, virtual, and cloud computing environments.

Enabling critical business services, better and faster

We believe that providing as much control as possible to IT organizations is the only way to enable timelier and cost effective delivery of services. Persistent pressures like change and complexity will only continue to increase as organizations continue to change and the technologies needed to manage them become inherently more complex.

Our Philosophy

Selling intelligent solutions, not just software

In order to provide reliable control, we first make sure we understand the real-world scenarios in which IT organizations like yours operate—day in and day out. That's the only way we can develop practical, intelligent IT solutions that successfully yield proven, measurable results. And that's so much more rewarding than simply selling software.

Driving your success is our passion

We place your success at the heart of how we do business. From product inception to deployment, we understand that you need IT solutions that work well and integrate seamlessly with your existing investments; you need ongoing support and training post-deployment; and you need someone that is truly easy to work with—for a change. Ultimately, when you succeed, we all succeed.

Our Solutions

- ◆ Identity & Access Governance
- ◆ Access Management
- ◆ Security Management
- ◆ Systems & Application Management
- ◆ Workload Management
- ◆ Service Management

Contacting Sales Support

For questions about products, pricing, and capabilities, contact your local partner. If you cannot contact your partner, contact our Sales Support team.

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	1-888-323-6768
Email:	info@netiq.com
Web Site:	www.netiq.com

Contacting Technical Support

For specific product issues, contact our Technical Support team.

Worldwide:	www.netiq.com/support/contactinfo.asp
North and South America:	1-713-418-5555
Europe, Middle East, and Africa:	+353 (0) 91-782 677
Email:	support@netiq.com
Web Site:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. The documentation for this product is available on the NetIQ Web site in HTML and PDF formats on a page that does not require you to log on. If you have suggestions for documentation improvements, click **comment on this topic** at the bottom of any page in the HTML version of the documentation posted at www.netiq.com/documentation. You can also email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

NetIQ Communities, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, NetIQ Communities helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, visit community.netiq.com.

Introduction

NetIQ Identity Manager helps you build an intelligent identity management framework to service your enterprise—both inside the firewall and into the cloud. Identity Manager centralizes the administration of user access and ensures that every user has one identity from your physical and virtual networks to the cloud.

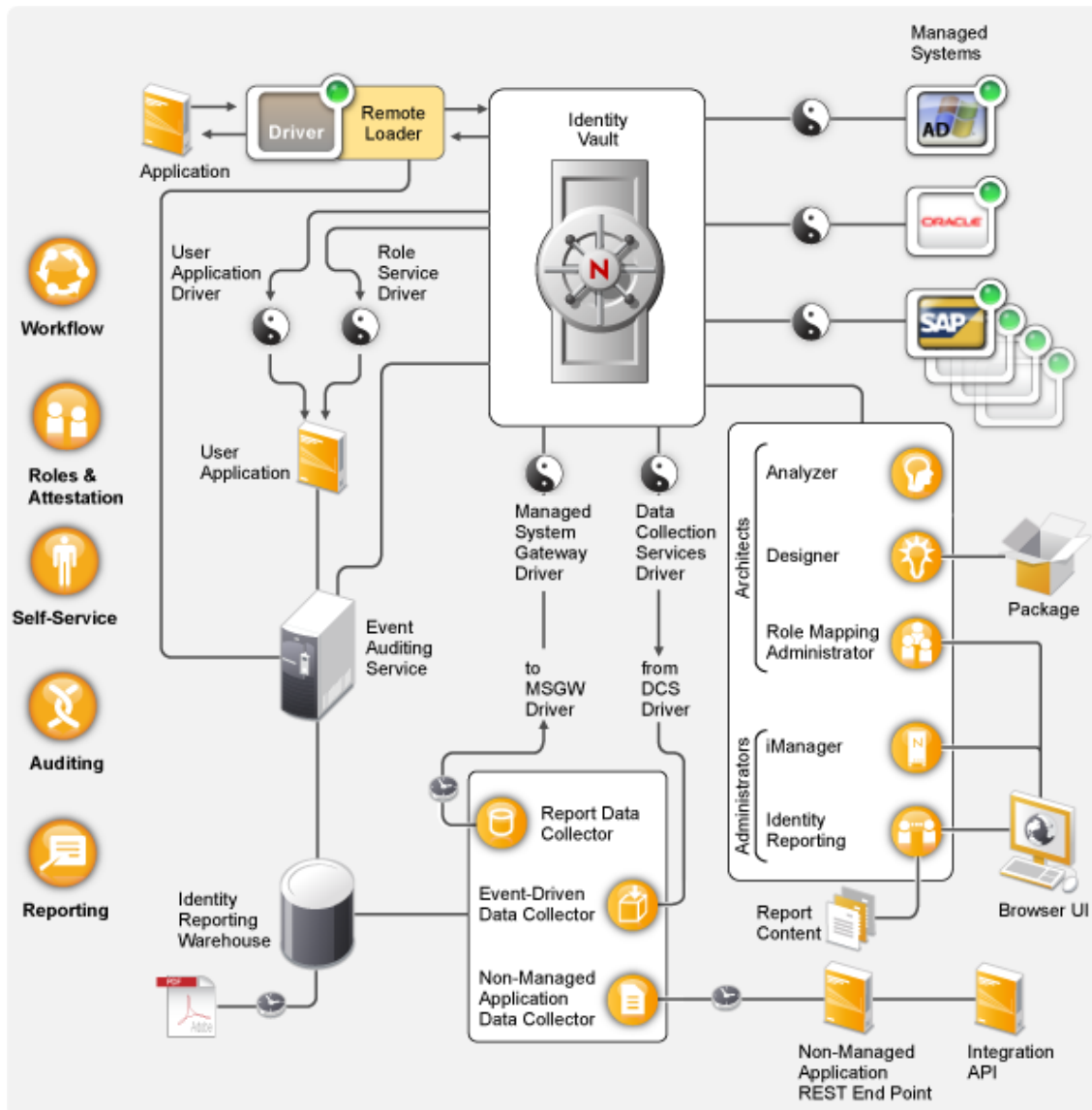
In general, you can group the components that comprise Identity Manager into the following functions:

- ♦ Creating and maintaining the Identity Manager environment. For more information, see [Chapter 2, “Creating and Maintaining Your Identity Manager Environment,” on page 23](#).
- ♦ Monitoring the Identity Manager environment, including the ability to audit and report user provisioning activities. You can then demonstrate compliance with business, IT, and corporate policies. For more information, see [Chapter 3, “Managing Data in the Identity Manager Environment,” on page 27](#).
- ♦ Managing user provisioning activities, such as roles, attestation, and self-service for individual users. For more information, see [Chapter 4, “Provisioning Users for Secure Access,” on page 31](#).

This section introduces you to the Identity Manager components that help you perform these activities. With this knowledge, you can begin planning to install the product. For a view of how these components interconnect, see [Chapter 1, “Understanding the Architecture of Identity Manager,” on page 21](#).

1 Understanding the Architecture of Identity Manager

Identity Manager ensures that every user has one identity from your physical and virtual networks to the cloud. The following diagram shows the high-level architecture of the components that support the Identity Manager capabilities. You install most of the components on servers. However, some components, such as Identity Manager Home, provide a browser-based interface that users access from workstations or mobile platforms.



In Identity Manager, a **managed system**, also called a **connected system** or **application**, is any system, directory, database, or operating system whose identity information you want to manage. For example, connected systems can be the PeopleSoft application or an LDAP directory. A **driver**, such

as the Data Collection Services Driver, provides the connection between a managed system and the Identity Vault. It also enables data synchronization and sharing between systems. Identity Manager stores drivers and library objects in a container called a **driver set**.

2 Creating and Maintaining Your Identity Manager Environment

Most organizations use separate environments to develop and stage Identity Manager, and then deploy to their production environment. To build and maintain your Identity Manager environment, you can use the following Identity Manager components:

- ♦ [Section 2.1, “Designer for Identity Manager,” on page 23](#)
- ♦ [Section 2.2, “Analyzer for Identity Manager,” on page 23](#)
- ♦ [Section 2.3, “Role Administration,” on page 24](#)
- ♦ [Section 2.4, “iManager,” on page 25](#)

These components also help you adapt Identity Manager to the changing needs of your business to ensure business continuity and improve user productivity enterprise-wide.

2.1 Designer for Identity Manager

Designer for Identity Manager (Designer) helps you design, test, document, and deploy Identity Manager solutions in a network or test environment. You can configure your Identity Manager project in an off-line environment, and then deploy to your live system. From a design perspective, Designer helps do the following:

- ♦ Graphically view all of the components that comprise your Identity Manager solution and observe how they interact.
- ♦ Modify and test your Identity Manager environment to ensure it performs as expected before you deploy part or all of your test solution to your production environment.

Designer keeps track of your design and layout information. With a click of a button, you can print that information in a format of your choice. Designer also enables teams to share work on enterprise-level projects.

For more information about using Designer, see the [Designer 4.0.2 for Identity Manager 4.0.2 Administration Guide](#).

2.2 Analyzer for Identity Manager

Analyzer for Identity Manager (Analyzer) provides data analysis, cleansing, reconciliation, and reporting to help you adhere to internal data quality policies. Analyzer lets you analyze, enhance, and control all data stores throughout the enterprise. Analyzer includes the following features:

- ♦ Analyzer’s schema map associates an application’s schema attributes to the corresponding schema attributes in Analyzer’s base schema. This lets you ensure that your data analysis and cleaning operations properly associate similar values between the disparate systems. To accomplish this, Analyzer leverages the schema mapping features in Designer.

- ♦ The Analysis Profile editor lets you configure a profile for analyzing one or more data set instances. Each analysis profile contains one or more metrics against which you can evaluate attribute values to see how the data conforms to your defined data format standards.
- ♦ The Matching Profile editor lets you compare values in one or more data sets. You can check for duplicate values within a specified data set and check for matching values between two data sets.

For more information about using Analyzer, see the [Analyzer 4.0.2 for Identity Manager Administration Guide](#).

2.3 Role Administration

In Identity Manager, a **role** defines a set of permissions related to one or more connected system. To maintain the permissions model, the Identity Manager drivers collect account IDs and permissions assignments from the connected systems. Identity Manager calls these permissions **entitlements**. Identity Manager uses entitlements to provide users with access to resources in connected systems. The Identity Manager roles system includes several different built-in roles that provide different levels of access rights to the role-based provisioning system. For example, someone assigned to administer the Roles Module has unlimited scope within the Roles system, but someone assigned to just manage roles is limited to specifically designated users, groups, and roles.

NetIQ provides the following Web-based components that allow your business and security analysts to manage user roles and resources:

- ♦ NetIQ Identity Manager Catalog Administrator
- ♦ NetIQ Identity Manager Role Mapping Administrator

Business analysts can use **Catalog Administrator** and **Role Mapping Administrator** to manage authorizations without needing to understand the overall IT infrastructure. These components let you discover roles, composite roles, and profiles (collectively referred to as **authorizations**), then map them to Identity Manager roles across different systems from one location. Authorizations can be business roles, composite roles, and profiles. For example, when you assign an Identity Manager role to a user in the Roles Based Provisioning Module, the user receives all authorizations mapped to that role.

While these components serve similar purposes, Catalog Administrator provides more functionality:

Functionality	Catalog Administrator	Role Mapping Administrator
Allows creation and deletion of roles	Yes	Yes
Allows mapping entitlements to roles	Yes	Yes
Allows mapping resources to roles	Yes	–
Allows configuring child roles	Yes	–
Allows editing role and resource attributes	Yes	–
Allows configuring Separation of Duties	Yes	–
Allows assigning grant and revoke processes for roles and resources	Yes	–
Exposes the resource model	Yes	–
Uses Identity Manager RBPM module permission model	Yes	–

Functionality	Catalog Administrator	Role Mapping Administrator
Supports custom entitlements	Yes	–
Leverages REST interfaces	Yes	–
Supports touch devices	Yes	–

Catalog Administrator and Role Mapping Administrator pull role information from the User Application driver and require access to the Identity Vault. Catalog Administrator also requires NetIQ Identity Manager Home and Provisioning Dashboard.

For more information about Catalog Administrator, see the [NetIQ Identity Manager Catalog Administrator User Guide](#). For more information about Role Mapping Administrator, see the [Novell Identity Manager Role Mapping Administrator 4.0.2 User Guide](#).

2.4 iManager

NetIQ iManager is a browser-based tool that provides a single point of administration for many Novell and NetIQ products, including Identity Manager. After you install the Identity Manager plug-ins for iManager, you can manage Identity Manager and receive real-time health and status information about your Identity Manager system.

With iManager, you can perform similar tasks as performed with Designer and also monitor the health of your system. NetIQ recommends that you use iManager for administrative tasks. Use Designer for configuration tasks that require changes to packages, modeling, and testing prior to deployment.

For more information about iManager, see the [NetIQ iManager Administration Guide](#).

3 Managing Data in the Identity Manager Environment

Identity Manager enforces consistent access controls across physical, virtual and cloud networks, and uses dynamic reports that let you prove compliance. In essence, Identity Manager synchronizes any type of data stored in a connected application or in the Identity Vault. The following components of the Identity Manager solution provide data synchronization, including password synchronization:

- ♦ Identity Vault
- ♦ Identity Manager engine
- ♦ Identity Manager Remote Loader
- ♦ Identity Manager drivers
- ♦ Connected Systems

3.1 Understanding Data Synchronization

Identity Manager lets you synchronize, transform, and distribute information across a wide range of connected systems, such as SAP, PeopleSoft, Microsoft SharePoint, Lotus Notes, Microsoft Exchange, Microsoft Active Directory, Novell eDirectory, and LDAP directories. Identity Manager lets you do the following activities:

- ♦ Control the flow of data among the connected systems.
- ♦ Determine what data is shared, which system is the authoritative source for a piece of data, and how the data is interpreted and transformed to meet the requirements of other systems.
- ♦ Synchronize passwords between systems. For example, if a user changes his or her password in Active Directory, Identity Manager can synchronize that password to Lotus Notes and Linux.
- ♦ Create new user accounts and remove existing accounts in directories such as Active Directory, systems such as PeopleSoft and Lotus Notes, and operating systems such as UNIX and Linux. For example, when you add a new employee to your SAP HR system, Identity Manager can automatically create a new user account in Active Directory, a new account in Lotus Notes, and a new account in a Linux NIS account management system.

3.2 Understanding Auditing, Reporting, and Compliance

Without Identity Manager, provisioning users can be a tedious, time-consuming, and costly effort. Then you must verify that your provisioning activities have complied with your organization's policies, requirements, and regulations. Do the right people have access to the right resources? Do you

ensure that unauthorized people are shut out of those same resources? Does the employee who started yesterday have access to the network, email, and the other systems required for the job? Has the access been canceled for the employee who left last week?

With Identity Manager, you can relax in your knowledge that all of your user provisioning activities, past and present, are being tracked and logged for auditing purposes. By querying the Identity Information Warehouse, you can retrieve all of the information you need to ensure that your organization is in full compliance with relevant business laws and regulations.

Identity Manager contains predefined reports that let you perform queries against the Identity Information Warehouse to demonstrate compliance for business, IT, and corporate policies. You can also create custom reports if the predefined reports do not meet your needs.

3.3 Understanding the Components for Synchronizing Your Identity Data

- ◆ [Section 3.3.1, “Identity Vault,” on page 28](#)
- ◆ [Section 3.3.2, “Identity Manager Engine,” on page 28](#)
- ◆ [Section 3.3.3, “Remote Loader,” on page 29](#)
- ◆ [Section 3.3.4, “Identity Information Warehouse,” on page 29](#)

3.3.1 Identity Vault

The **Identity Vault** contains all information that Identity Manager requires. The Identity Vault serves as a metadirectory of the data that you want to synchronize among the connected systems. For example, data synchronized from a PeopleSoft system to Lotus Notes is first added to the Identity Vault and then sent to the Lotus Notes system. The Identity Vault also stores information specific to Identity Manager, such as driver configurations, parameters, and policies.

By default, the Identity Vault uses a NetIQ eDirectory database. For more information about using eDirectory see the [NetIQ eDirectory 8.8 SP8 Administration Guide](#).

3.3.2 Identity Manager Engine

The **Identity Manager engine** processes all data changes that occur in the Identity Vault or a connected application. For events that occur in the Identity Vault, the engine processes the changes and issues commands to the application via the driver. For events that occur in the application, the engine receives the changes from the driver, processes the changes, and issues commands to the Identity Vault. **Drivers** connect the Identity Manager engine to the applications. A driver has two basic responsibilities: reporting data changes (events) in the application to the Identity Manager engine and carrying out data changes (commands) submitted by the Identity Manager engine to the application. Drivers must be installed on the same server as connected application.

The Identity Manager engine has also been referred to as the Metadirectory engine. The server on which the Identity Manager engine runs is referred to as the **Identity Manager server**. You can have more than one Identity Manager server in your environment, depending on server workload.

For more information about the Identity Manager engine, see the [Identity Manager 4.0.2 Overview Guide](#).

3.3.3 Remote Loader

The **Identity Manager Remote Loader** loads drivers and communicates with the Identity Manager engine on behalf of drivers installed on remote servers. If the application runs on the same server as the Identity Manager engine, you can install the driver on that server. However, if the application does not run on the same server as the Identity Manager engine, you must install the driver on the application's server. To help with the workload or configuration of your environment, you can install Remote Loader on a server separate from the application servers and the Identity Manager server.

For more information about Remote Loader, see the [Identity Manager 4.0.2 Remote Loader Guide](#).

3.3.4 Identity Information Warehouse

Identity Manager includes the **Identity Information Warehouse**, which is an intelligent repository of information about the actual and desired states of the Identity Vault and the connected systems within your organization. The Identity Information Warehouse gives you a 360-degree view of your business entitlements, providing the knowledge you need to see the past and present state of authorizations and permissions granted to identities in your organization.

When you query the Identity Information Warehouse, you can retrieve all of the information that you need to ensure that your organization is in full compliance with relevant business laws and regulations. With this knowledge, you can answer even the most sophisticated Governance Risk and Compliance (GRC) queries.

The infrastructure for the Identity Information Warehouse requires the following components:

- ♦ [“Identity Reporting Module for Identity Manager” on page 29](#)
- ♦ [“Data Collection Service” on page 30](#)
- ♦ [“Managed System Gateway Driver” on page 30](#)
- ♦ [“Event Auditing Service” on page 30](#)

Identity Reporting Module for Identity Manager

The Identity Information Warehouse stores its information in the SIEM database. The **Reporting Module** allows you to audit and create reports about your Identity Manager solution. You can use the reports to help meet compliance regulations for your business. You can run predefined reports to demonstrate compliance for business, IT, and corporate policies. You can also create custom reports if the predefined reports do not meet your needs. Use the Reporting Module to report critical business information about various aspects of your Identity Manager configuration, including information collected from Identity Vaults and connected systems. The user interface for the reporting module makes it easy to schedule reports to run at off-peak times for optimized performance. For more information about the Reporting Module, see the [Identity Reporting Module Guide](#).

Data Collection Service

The **Data Collection Service** uses the Data Collection Services driver to capture changes to objects stored in an Identity Vault, such as accounts, roles, resources, groups, and team memberships. The driver registers itself with the service and pushes change events (such as data synchronization, add, modify, and delete events) to the service.

The service includes three subservices:

- ♦ **Report Data Collector:** Uses a pull design model to retrieve data from one or more Identity Vault data sources. The collection runs on a periodic basis, as determined by a set of configuration parameters. To retrieve the data, the collector calls the Managed System Gateway driver.
- ♦ **Event-Driven Data Collector:** Uses a push design model to gather event data captured by the Data Collection Service driver.
- ♦ **Non-Managed Application Data Collector:** Retrieves data from one or more non-managed applications by calling a REST end point written specifically for each application. Non-managed applications are applications within your enterprise that are not connected to the Identity Vault.

Managed System Gateway Driver

The **Managed System Gateway Driver** queries the Identity Vault to collect the following type of information from managed systems:

- ♦ List of all managed systems
- ♦ List of all accounts for the managed systems
- ♦ Entitlement types, values, and assignments, and user account profiles for the managed systems

Event Auditing Service

To include auditing and reporting as part of your Identity Manager solution, you need a security information and event management service, such as NetIQ Event Auditing Service or NetIQ Sentinel. The installation package for the Identity Information Warehouse includes **Event Auditing Service** (EAS). EAS captures the following log events associated with the following types of actions:

- ♦ Actions performed within the RBPM and the role administration components
- ♦ Actions performed in the reporting module, such as the import, modification, deletion, or scheduling of a report

4 Provisioning Users for Secure Access

Identity Manager centralizes access administration and ensures that every user has one identity—from your physical and virtual networks to the cloud. Also, users often require access to resources based upon their roles in the organization. For example, a law firm's attorneys might require access to a different set of resources than the firm's paralegals.

Identity Manager lets you provision users based on their roles in the organization. You define the roles and make the assignments according to your organizational needs. When a user is assigned to a role, Identity Manager provisions the user with access to the resources associated with the role. Users that have multiple roles receive access to the resources associated with all of the roles.

You can have users automatically added to roles as a result of events that occur in your organization. For example, you might add to your SAP HR database a new user with the job title of Attorney. If approval is required for adding a user to a role, you can establish workflows to route role requests to the appropriate approvers. You can also manually assign users to roles.

In some cases, certain roles should not be assigned to the same person because the roles conflict. Identity Manager provides Separation of Duties functionality that lets you prevent users from being assigned to conflicting roles unless someone in your organization makes an exception for the conflict.

The Identity Manager solution provides the following components for provisioning users:

- ♦ NetIQ Identity Manager Roles Based Provisioning Module and User Application
- ♦ NetIQ Identity Manager Home and Provisioning Dashboard

Identity Manager Home and the Provisioning Dashboard provide a single access point for all Identity Manager users and administrators. They allow access to all existing Roles Based Provisioning Module and User Application functionality.

4.1 Understanding the Attestation Process in Identity Manager

Identity Manager helps you validate the correctness of your role assignments through an attestation process. Incorrect roles assignments might jeopardize compliance with both corporate and government regulations. Using the attestation process, responsible individuals within your organization certify the data associated with roles:

- ♦ **User profile attestation:** Selected users attest to their own profile information (first name, last name, title, department, e-mail, and so forth) and correct any incorrect information. Accurate profile information is essential to correct role assignments.
- ♦ **Separation of Duties violation attestation:** Responsible individuals review a Separation of Duties violation report and attest to the accuracy of the report. The report lists any exceptions that allow a user to be assigned conflicting roles.
- ♦ **Role assignment attestation:** Responsible individuals review a report listing selected roles and the users, groups, and roles assigned to each role. The responsible individuals must then attest to the accuracy of the information.
- ♦ **User assignment attestation:** Responsible individuals review a report listing selected users and the roles to which they are assigned. The responsible individuals must then attest to the accuracy of the information.

These attestation reports are designed primarily to help you ensure that role assignments are accurate and that there are valid reasons to allow exceptions for conflicting roles.

4.2 Understanding the Self-Service Process in Identity Manager

Identity Manager uses identity as the basis for authorizing users access to systems, applications, and databases. Each user's unique identifier and each user's roles come with specific access rights to identity data. For example, users who are identified as managers can access salary information about their direct reports, but not about other employees in their organization. With Identity Manager, you can delegate administrative duties to the people who should be responsible for them. For example, you can enable individual users to accomplish the following goals:

- ◆ Manage their own personal data in the corporate directory. Rather than having you change a cell phone number, they can change it in one place and have it changed in all the systems you have synchronized through Identity Manager.
- ◆ Change their passwords, set up a hint for forgotten passwords, and set up challenge questions and responses for forgotten passwords. Rather than asking you to reset a password because they've forgotten it, they can do it themselves after receiving a hint or responding to a challenge question.
- ◆ Request access to resources such as databases, systems, and directories. Rather than calling you to request access to an application, they can select the application from a list of available resources.

In addition to self-service for individual users, Identity Manager provides self-service administration for functions (management, Help Desk, and so forth) that are responsible for assisting, monitoring, and approving user requests. For example, John uses the Identity Manager self-service feature to request access to the documents that he needs. John's manager and the CFO receive the request through the self-service feature and can approve the request. The established approval workflow allows John to initiate and monitor the progress of his request and allows John's manager and CFO to respond to his request. Approval of the request by John's manager and the CFO triggers the provisioning of the Active Directory rights that John needs to access and view the financial documents.

Identity Manager also provides workflow capabilities to ensure that your provisioning processes involve the appropriate resource approvers. For example, assume that John, who has already been provisioned with an Active Directory account, needs access to some financial reports through Active Directory. This requires approval from both John's immediate manager and the CFO. Fortunately, you've set up an approval workflow that routes John's request to his manager and, after approval from his manager, to the CFO. Approval by the CFO triggers automatic provisioning of the Active Directory rights needed by John to access and view the financial documents.

You can initiate workflows automatically when a certain event occurs (for example, a new user is added to your HR system) or manually through a user request. To ensure that approvals take place in a timely manner, you can set up proxy approvers and approval teams.

4.3 Understanding the Components for Managing User Provisioning

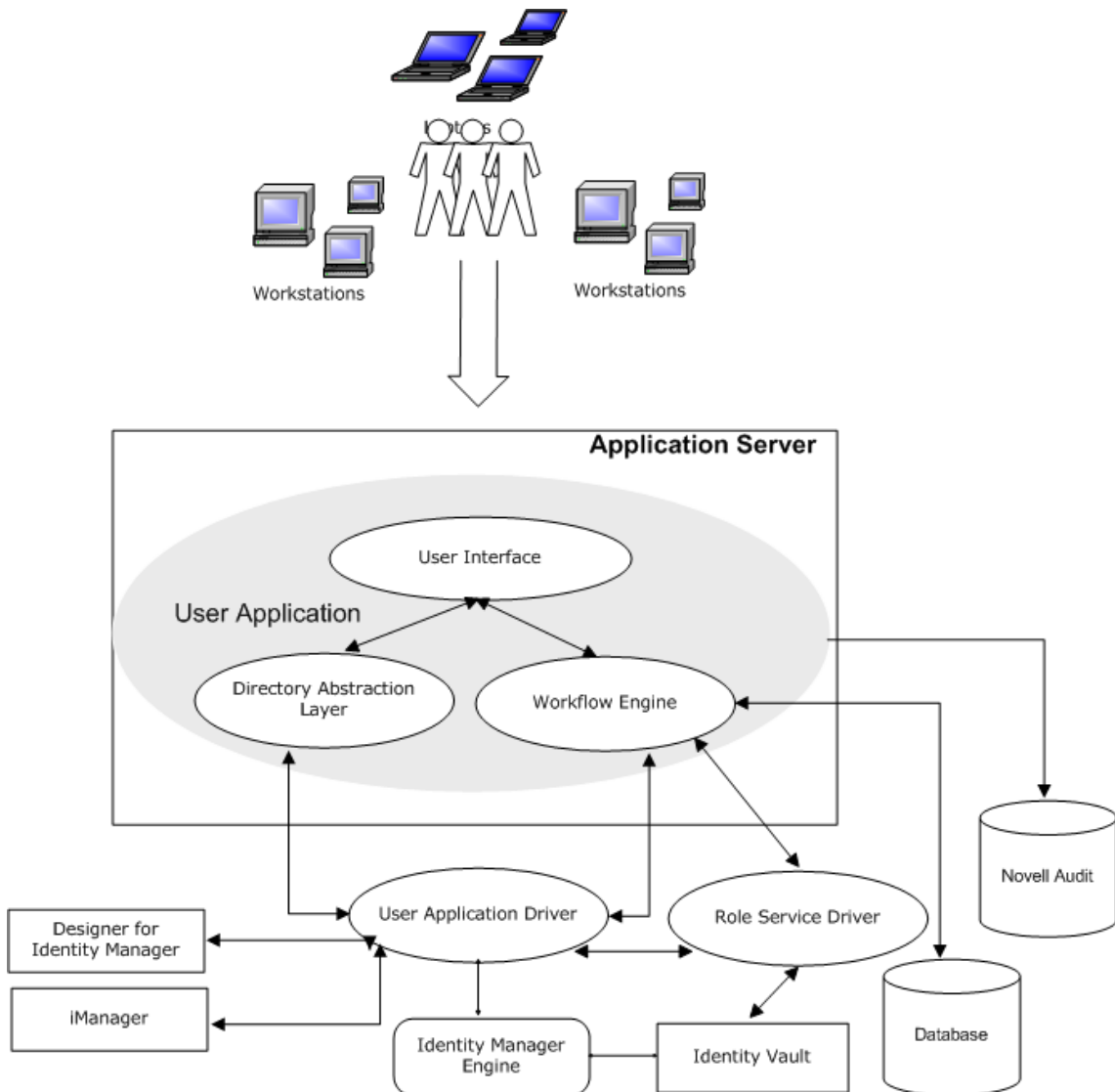
This section explains the purpose of the following components:

- ♦ [Section 4.3.1, “User Application and Roles Based Provisioning Module,”](#) on page 33
- ♦ [Section 4.3.2, “Identity Manager Home and Provisioning Dashboard,”](#) on page 34

4.3.1 User Application and Roles Based Provisioning Module

The Identity Manager **User Application** gives your users and business administrators a view into the information, resources, and capabilities of Identity Manager. The User Application is a browser-based Web application that gives the user the ability to perform a variety of identity self-service and roles provisioning tasks. Users can manage passwords and identity data, initiate and monitor provisioning and role assignment requests, manage the approval process for provisioning requests, and verify attestation reports.

The User Application relies on a number of independent components acting together.



The User Application runs on the **Roles Based Provisioning Module (RBPM)** framework, which includes the workflow engine that controls the routing of requests through the appropriate approval process. These components require the following drivers:

User Application driver

Stores configuration information and notifies the User Application whenever changes occur in the Identity Vault. You can configure the driver to allow events in the Identity Vault to trigger workflows. The driver can also report success or failure of a workflow's provisioning activity to the User Application so that users can view the final status of their requests.

Role and Resource Service driver

Manages all role and resource assignments. The driver starts workflows for role and resource assignment requests that require approval and maintains indirect role assignments according to group and container memberships. The driver also grants and revokes entitlements for users based on their role memberships. It performs cleanup procedures for completed requests.

Users can access the User Application from any supported Web browser. For more information about the User Application and RBPM, see the [NetIQ User Application: Administration Guide](#).

4.3.2 Identity Manager Home and Provisioning Dashboard

NetIQ Identity Manager Home (the Home page) provides a single access point for all Identity Manager users and administrators. It allows access to all existing functionality in RBPM and the User Application, as well as provides additional user-oriented features. When creating the content for the Home page, administrators have the following options:

- ◆ Customize the Home page to display only the items and links that are applicable to each user.
- ◆ Organize the links and items into categories that make sense. For example, add your company-specific links or REST endpoints.
- ◆ Configure items on the Home page to include **badges**. For example, badges can display how many items of a certain type a user has access to.

Users can access the Home page with any supported Web browser, from either a computer or a tablet. For more information, see the [NetIQ Identity Manager Home and Provisioning Dashboard User Guide](#).

The **Identity Manager Provisioning Dashboard** (the Dashboard) is a personalized view of each user's permissions, tasks, and requests. Identity Manager Home links to the appropriate location on each user's Dashboard.

The Dashboard focuses on the following basic areas of functionality:

I want something.

If users need an item, whether the item is a piece of equipment like a laptop or something intangible like access to a particular server or application, they can use the **Make a Request** option to request that item. To search for an item, the user enters all or part of a search term in the **Permissions** field.

I need to do something.

If users want to know what tasks they need to manage, **My Tasks** page shows all of a user's pending tasks in the Identity Manager system.

What do I have?

If users want to see everything they can currently access, the **My Permissions** page provides a list of the roles and resources to which they have access.

How did I get it?

If users want to see a list of past requests, the **History** page shows everything that they have requested recently, as well as the status of all their pending requests.

Users can access the Dashboard with any supported Web browser, from either a computer or a tablet. For more information, see the [NetIQ Identity Manager Home and Provisioning Dashboard User Guide](#).

|| Planning to Install Identity Manager

This section provides valuable information for planning your Identity Manager environment, including the prerequisites and system requirements for the computers where you want to install each Identity Manager component.

You do not need an activation code to install or initially run Identity Manager. However, without an activation code, Identity Manager stops functioning 90 days after installation. You can activate Identity Manager at any time during the 90 days or afterward.

5 Planning Overview

This section helps you plan the installation process for Identity Manager. Some components must be installed in a specific order because the installation process requires access to previously installed components. For example, you should install and configure the Identity Vault before installing the Identity Manager engine.

5.1 Planning Checklist

The following checklist provides high-level steps for planning an installation of Identity Manager in your environment. The sections for installing the Identity Manager components provide more specific checklists.

	Checklist Items
<input type="checkbox"/>	1. Review product architecture information to learn about Identity Manager components. For more information, see Chapter 1, “Understanding the Architecture of Identity Manager,” on page 21.
<input type="checkbox"/>	2. Ensure that you have the files for installing Identity Manager. For more information, see Section 5.2.1, “Downloading the Installation Files,” on page 40.
<input type="checkbox"/>	3. Ensure that you have a license for running Identity Manager. For more information, see Section 5.3, “Understanding Licensing and Activation,” on page 41.
<input type="checkbox"/>	4. Review the default ports for each Identity Manager component to determine whether you need to customize the installation settings. For more information, see Section 5.4, “Understanding Identity Manager Communication,” on page 42.
<input type="checkbox"/>	5. Determine whether you can run the installation programs in your preferred language. For more information, see Section 5.5, “Understanding Language Support,” on page 42.
<input type="checkbox"/>	6. Ensure that the computers on which you are installing the Identity Manager components meet the specified requirements. For more information, see Chapter 6, “Considerations and Prerequisites for Installation,” on page 45.
<input type="checkbox"/>	7. Ensure that you have the appropriate credentials required to install the Identity Manager components on your servers and the accounts that you might create during the installation.

	Checklist Items
<input type="checkbox"/>	<p>8. Install the Identity Manager components in the following order:</p> <ul style="list-style-type: none"> ◆ Designer: For more information, see “Installing Designer” on page 89 ◆ Identity Vault: For more information, see “Installing the Identity Vault” on page 91 ◆ Identity Manager Engine: For more information, see “Installing the Identity Manager Engine” on page 137 ◆ iManager: For more information, see “Installing iManager” on page 145 ◆ Remote Loader: For more information, see “Installing the Remote Loader” on page 167 ◆ RBPM and the User Application: For more information, see “Installing the User Application and Roles Based Provisioning Module” on page 199 ◆ EAS and the Reporting Module: For more information, see “Installing the Identity Information Warehouse” on page 293 ◆ Role Mapping Administrator: For more information, see “Installing a Role Administrator Component” on page 333 ◆ Identity Manager Home: For more information, see “Installing Identity Manager Home and the Provisioning Dashboard” on page 381 ◆ Analyzer: For more information, see “Installing Analyzer” on page 403 <p>NOTE: NetIQ recommends that you make a note of each account that you create during the installation process.</p>
<input type="checkbox"/>	<p>9. Activate your Identity Manager components. For more information, see Chapter 45, “Activating Identity Manager,” on page 407.</p>

5.2 Understanding the Installation Process

Several components, such as Designer, the Identity Manager engine, and Catalog Administrator, contribute to the Identity Manager environment. Since many of the Identity Manager components are data-intensive, such as the Identity Vault, NetIQ recommends installing them on separate servers. This guide provides instructions for installing each component, which provides you the opportunity to customize each installation.

Some installation programs can install more than one Identity Manager component. Also, most installation programs support a guided (GUI) installation mode and a silent installation process.

5.2.1 Downloading the Installation Files

NetIQ provides ISO files that contain all components for a full Identity Manager installation. Each file includes the 32-bit and 64-bit versions of the product. The name of the ISO file identifies the platform. For example, `Identity_Manager_version_Linux.iso`.

NOTE: The ISO images are large files. Ensure that you download them to a volume or DVD that supports the file size.

To download the Identity Manager installation files:

- 1 Go to the [NetIQ Downloads Web site \(https://dl.netiq.com/index.jsp\)](https://dl.netiq.com/index.jsp) .
- 2 In the **Product or Technology** menu, select **Identity Manager**, then click **Search**.

- 3 On the Novell Identity Manager Downloads page, click the **Download** button next to the ISO file that you want to download.
- 4 Follow the on-screen prompts to download the file to a directory on your computer.
- 5 Either mount the downloaded `.iso` file as a volume, or use the `.iso` file to create a DVD of the software.

5.2.2 Installing Identity Manager in a Clustered Environment

You can deploy some Identity Manager components in a clustered environment on servers running SUSE Linux Enterprise Server (SLES) 11 SP2 or later with the latest patches installed. Identity Manager is mostly a Java-based application that runs by default in the eDirectory process space. When you run eDirectory in a clustered environment, the Identity Manager engine is also clustered. You can also deploy the Remote Loader in a clustered environment. For more information about installing these components in a clustered environment, see the prerequisites and installation instructions for each component.

To determine whether you can install an Identity Manager component in a clustered environment, see the system requirements for that particular component in [Chapter 6, “Considerations and Prerequisites for Installation,” on page 45](#). For example, the User Application can run on an application server in a clustered environment. You cannot install the Reporting Module on a server in a clustered environment.

To manage the availability of your network resources for your Identity Manager environment, use the SUSE Linux Enterprise High Availability Extension. High Availability ensures efficient manageability of critical network resources including data, applications, and services. It also ensures that only one node is active at any given point of time. The High Availability Extension ships with Corosync/Pacemaker messaging and membership layer and uses Pacemaker as the Cluster Resource Manager (CRM). The Pacemaker manages the virtual IP addresses of eDirectory and assigns them dynamically to the most eligible node of a cluster. You must configure eDirectory to use these IP addresses.

To configure and enable the High Availability service, download the SUSE Linux Enterprise High Availability Extension ISO file from the [Novell Download](#) site. For more information about configuring and enabling High Availability on nodes, see [SUSE Linux Enterprise High Availability Extension 11 SP2 High Availability Guide](#).

5.3 Understanding Licensing and Activation

You can install an evaluation copy of Identity Manager and use it for 90 days free of charge. However, you must activate the Identity Manager components within 90 days of installation, or they will stop functioning. You can purchase a product license and activate Identity Manager either during the evaluation period of 90 days or later. For more information, see [Chapter 45, “Activating Identity Manager,” on page 407](#).

To purchase an Identity Manager product license, see the [NetIQ Identity Manager How to Buy Web page \(https://www.netiq.com/products/identity-manager/advanced/how-to-buy/\)](#). After you purchase a product license, NetIQ sends you a Customer ID. The email also contains a URL to the NetIQ Web site where you can obtain a Product Activation credential. If you do not remember your Customer ID or do not receive it, contact your sales representative.

5.4 Understanding Identity Manager Communication

For proper communication among the Identity Manager components, NetIQ recommends that you open the default ports listed in the following table.

Port Number	Component Computer	Port Use
389	Identity Vault	Used for LDAP communication in clear text
524	Identity Vault	Used for NetWare Core Protocol (NCP) communication
636	Identity Vault	Used for LDAP with TLS/SSL
1514	Role Mapping Administrator	Used by Role Mapping Administrator server to gather syslog auditing information
8000	Remote Loader	Used by the driver instance for TCP/IP communication
8028 and 8030	Identity Vault	Used for HTTP clear text communication with NetWare Core Protocol (NCP) communication
8080	iManager	Used by Tomcat for HTTP (non-secure) communication
8081	Role Mapping Administrator	Used by the server hosting Role Mapping Administrator Web portal for HTTP communication
8090	Remote Loader	Used by the Remote Loader to listen for TCP/IP connections from the remote interface shim
8180	RBPM	Used by the application server, such as JBoss, on which the User Application runs
8443	iManager Role Mapping Administrator	Used by Tomcat for HTTPS (SSL) communication Used by the server hosting Role Mapping Administrator Web portal for HTTPS communication
8543	User Application	Used by JBoss for HTTPS (SSL) communication
9009	iManager	Used by Tomcat for MOD_JK
15432	Identity Information Warehouse	Used for the PostgreSQL database of the Event Auditing Service
45654	User Application	Used by the server on which the database for the User Application is installed to listen for communications, when running JBoss with a cluster group

5.5 Understanding Language Support

NetIQ translates (localizes) the interface for Identity Manager and its installation programs to support the operating system language on your local computers. However, we cannot support all languages. During installation, some installation programs check the locale of the computer to determine the language for the installation process.

To run the installation program in a specific language, change the locale on Windows through the **Regional Settings** option. On Linux/Solaris, set the LANG variable in the profile or through the command line.

5.5.1 Translated Components and Installation Programs

The following table lists the available translations per component installation. Components not listed in the table are available in English only. Also, if the component is not translated to the language of the operating system, the program defaults to English.

Locale	Designer	Identity Manager Engine	iManager	iManager plug-ins	Reporting Module	RBPM
Chinese Simplified	Yes	Yes	Yes	Yes	Yes	Yes
Chinese Traditional	Yes	Yes	Yes	Yes	Yes	Yes
Czech	–	–	Yes	–	–	–
Danish	–	–	–	–	Yes	Yes
Dutch	Yes	–	–	–	Yes	Yes
English	Yes	Yes	Yes	Yes	Yes	Yes
French	Yes	Yes	Yes	Yes	Yes	Yes
German	Yes	Yes	Yes	Yes	Yes	Yes
Hungarian	–	–	Yes	–	–	–
Italian	Yes	–	Yes	–	Yes	Yes
Japanese	Yes	Yes	Yes	Yes	Yes	Yes
Polish	–	–	Yes	–	–	–
Portuguese (Brazilian)	Yes	–	Yes	–	Yes	Yes
Russian	–	–	Yes	–	Yes	Yes
Slovak	–	–	Yes	–	–	–
Spanish	–	–	Yes	–	Yes	Yes
Swedish	–	–	–	–	Yes	Yes

5.5.2 Special Considerations for Language Support

NetIQ recommends that you review the following considerations when deciding whether to use a translated version of Identity Manager.

- ♦ In general, if an Identity Manager component does not support the language of the operating system, the component's interface defaults to English. For example, the Identity Manager drivers are available in the same languages as the Identity Manager Engine. When Identity Manager does not support the driver language, the driver configuration defaults to English.
- ♦ The following iManager plug-ins are available in Spanish, Russian, Italian, and Portuguese, as well as in the languages listed in the previous table:

- ◆ When installing Designer on computers running a Linux operating system, you must install the gettext utilities. The GNU gettext utilities provide a framework for internationalized and multilingual messages.
- ◆ When you launch the installation program for an Identity Manager component, the following conditions apply:
 - ◆ If the operating system is in a language supported by the installation program, the program defaults to that language. However, you can specify a different language for the installation process.
 - ◆ If the installation program does not support the language of the operating system, the installation program defaults to English.
 - ◆ If the operating system uses a Latin-based language, the installation program allows you to specify any of the Latin-based languages.
 - ◆ If the operating system uses a supported Asian-based language or Russian, the installation program allows you to specify only the language matching the operating system or English.

6 Considerations and Prerequisites for Installation

This section lists the prerequisites and system requirements for the computers that you want to host your Identity Manager components. In general, you should install all of the components so you can provide full identity management in your environment. However, you do not need all of the components, such as Analyzer or iManager. For more information about the individual components, see the [Identity Manager 4.0.2 Overview Guide](#).

6.1 Installing Identity Manager on an RHEL 6.x Server

Before installing Identity Manager components on a server running a Red Hat Enterprise Linux 6.x operating system, you must install a set of libraries. The libraries vary according to your chosen method of installation.

6.1.1 Using the Installation Wizard

If you plan to use the installation wizard, which provides a guided installation, you must first install the following set of libraries in the listed order:

- ♦ **For a 64-bit RHEL:**
 1. `libXau-1.0.5-1.el6.i686.rpm`
 2. `libxcb-1.5-1.el6.i686.rpm`
 3. `libX11-1.3-2.el6.i686.rpm`
 4. `libXext-1.1-3.el6.i686.rpm`
 5. `libXi-1.3-3.el6.i686.rpm`
 6. `libXtst-1.0.99.2-3.el6.i686.rpm`
 7. `glibc-2.12-1.7.el6.i686.rpm`
 8. `libstdc++-4.4.4-13.el6.i686.rpm`
 9. `libgcc-4.4.4-13.el6.i686.rpm`
 10. `compat-libstdc++-33-3.2.3-69.el6.x86_64.rpm`
 11. `compat-libstdc++-33-3.2.3-69.el6.i686.rpm`
 12. `libXrender-0.9.7-2.el6.i686.rpm`
- ♦ **For a 32-bit RHEL,** install the `compat-libstdc++-33-3.2.3-69.el6.i686.rpm` library.

6.1.2 Using the Command Line for Installation

If you plan to use the command line for your installation method, you must first install the following set of libraries in the listed order:

- ♦ **For a 64-bit RHEL:**
 1. `glibc-2.12-1.7.el6.i686.rpm`

2. libstdc++-4.4.4-13.el6.i686.rpm
3. libgcc-4.4.4-13.el6.i686.rpm
4. compat-libstdc++-33-3.2.3-69.el6.x86_64.rpm
5. compat-libstdc++-33-3.2.3-69.el6.i686.rpm
6. libXrender-0.9.7-2.el6.i686.rpm

- ♦ For a 32-bit RHEL, install the `compat-libstdc++-33-3.2.3-69.el6.i686.rpm` library.

6.2 Prerequisites and Requirements for Installing Designer

6.2.1 Prerequisites for Installing Designer

Before installing or upgrading Designer, review the following considerations:

- ♦ To install Designer on a computer running an openSUSE 64-bit operating system, your environment must meet the following prerequisites:
 - ♦ Before installing Designer, you must install the 32-bit Novell International Cryptographic Infrastructure (NICI) Package.
 - ♦ You must install all libraries from [openSUSE.org \(http://www.opensuse.org/\)](http://www.opensuse.org), particularly `bug-buddy`, `gtk2 (32-bit)`, and `libgthread`.
 - ♦ You must install the `libgthread-2_0-0-32bit-2.17.2+2.17.3+20080708+r7171-3.1.x86_64.rpm` compat library before installing Designer.
 - ♦ You must install the 32-bit version of the `gtk2` RPM library, even if you install Designer on a computer running a 64-bit operating system.
- ♦ Before installing Designer on a computer running a Linux operating system, you must install the GNU gettext utilities. These utilities provide a framework for internationalized and multilingual messages. For more information about language support, see [Section 5.5, “Understanding Language Support,”](#) on page 42.
- ♦ You cannot use Designer 2.1x workspaces for Designer 3.0 or later because older workspace versions are not compatible with more recent versions of Designer. Designer stores projects and configuration information in **workspaces**. For example, Designer 4 workspaces are installed in the following directories by default:
 - ♦ **Linux:** `$HOME/designer_workspace`
 - ♦ **Windows XP:** `%UserProfile%\designer_workspace`
 - ♦ **Windows Vista and Windows 7:** `%UserProfile%\designer_workspace` directory for
- ♦ If you want to upgrade Designer and you are running workflow provisioning and provisioning with roles, review the upgrade procedure in [Migrating a 4.0 User Application Driver](#) in the [Migrating to the Roles Based Provisioning Module Version 4.0.2](#).

6.2.2 System Requirements for Installing Designer

This section provides requirements to help you set up the server hosting Designer.

Category	Requirement
Processor	1 GHz

Category	Requirement
Disk Space	1 GB
Memory	1024 MB
Operating System	<p>One of the following operating systems, at a minimum:</p> <ul style="list-style-type: none"> ◆ openSUSE 11.4 (32-bit or 64-bit) ◆ openSUSE 10.3 (32-bit or 64-bit) ◆ SUSE Linux Enterprise Server 11 SP1 (32-bit or 64-bit) ◆ SUSE Linux Enterprise Desktop 11 SP2 (32-bit or 64-bit) ◆ SUSE Linux Enterprise Server 10 SP4 (32-bit or 64-bit) ◆ SUSE Linux Enterprise Desktop 10 SP4 (32-bit or 64-bit) ◆ Windows 7 SP1 (32-bit and 64-bit) ◆ Windows Server 2008 R2 SP1 ◆ Windows Server 2008 SP2 (32-bit and 64-bit) ◆ Windows Vista Business (32-bit and 64-bit) ◆ Windows Server 2003 SP2 (32-bit) ◆ Windows XP Professional SP3
Virtualization Systems	<p>One of the following systems running a supported operating system unless otherwise noted:</p> <ul style="list-style-type: none"> ◆ VMware ESXi Workstation 6.5 running SLES 11 SP1 as the host operating system ◆ VMware ESXi 5.0 (32-bit or 64-bit) ◆ VMware ESXi 4.0 (32-bit or 64-bit) ◆ VMware ESX 4.0 (32-bit or 64-bit) ◆ Windows Server 2008 R2 Virtualization with Hyper-V (32-bit or 64-bit) ◆ Xen Virtual Machine running SLES 10, SLES 11, or Windows Server 2008 R2 as a guest operating system in para-virtualized mode and SLES 10 SP2 as the host operating system <p>NOTE: IThe VMware ESX and ESXi systems can also run the VMware version of SLES 11 SP2 (64-bit) as the guest operating system</p>

6.3 Prerequisites and Requirements for Installing the Identity Vault

Identity Vault uses a directory to store the objects that are synchronized through the Identity Manager solution. The follow sections contain guidelines that help you plan a deployment of NetIQ eDirectory to use as framework for the Identity Vault.

6.3.1 Considerations for Installing the Identity Vault

NetIQ recommends that you review the following considerations before you install eDirectory as the framework for the Identity Vault:

- ◆ Before installing eDirectory, you must have a method for resolving tree names to server referrals. NetIQ recommends using Service Location Protocol (SLP) services. Releases of Novell eDirectory before version 8.8 included SLP in the installation. However, after version 8.8, you must separately install SLP. You can also use the flat file `hosts.nds` to resolve tree names. For more information, see [Section 9.2, “Using OpenSLP or hosts.nds for Resolving Tree Names,” on page 95](#).
- ◆ When installing on a Linux server, you must enable the host for multicast routing, with 224.0.0.0 in the routing table. For example, enter the following command:

```
route add -net 224.0.0.0 netmask 240.0.0.0 dev interface
```

where *interface* represents a value such as `eth0`, `hme0`, `hme1`, or `hme2`, depending on the network interface card.

- ◆ You must configure a static IP address on the server for the eDirectory infrastructure to perform efficiently. If you use DHCP addresses on the server, eDirectory might have unpredictable results.
- ◆ Synchronize time across all network servers. NetIQ recommends using Network Time Protocol's (NTP) `ntp` option.
- ◆ (Conditional) To install a secondary server, all the replicas in the partition that you install the product on should be in the On state.
- ◆ (Conditional) To install a secondary server into an existing tree as a non-administrator user, create a container and then partition it. Ensure that you have the following rights:
 - ◆ Supervisor rights to the partition where you want to add the server.
 - ◆ (Windows) Supervisor rights to the container where you want to add the server.
 - ◆ All Attributes rights: read, compare, and write rights over the `W0.KAP.Security` object.
 - ◆ Attribute rights: read and compare rights over the Security container object.
 - ◆ Entry rights: browse rights over the Security container object.

These rights are required for adding the replica when the replica count is less than 3.

- ◆ (Conditional) To install a secondary server into an existing tree as a non-administrator user, ensure that at least one of the servers in the tree has the same or higher eDirectory version as that of the secondary being added as container admin. If the secondary being added is of later version, the administrator of the tree must extend the schema before adding the secondary using container admin.
- ◆ While configuring eDirectory, you must enable a NetWare Core Protocol (NCP) port (the default is 524) in the firewall to allow the secondary server addition. Also, you can enable the following default service ports based on your requirements:
 - ◆ LDAP clear text - 389
 - ◆ LDAP clear text - 636
 - ◆ HTTP clear text - 8028
 - ◆ HTTP clear text - 8030

- ♦ You must install Novell International Cryptographic Infrastructure (NICI) on every workstation using management utilities for eDirectory, such as iManager. NICI and eDirectory support key sizes up to 4096 bits.

On Linux, the Identity Vault installation program, `nds-install`, automatically installs NICI. However, you can install NICI manually. For more information, see “Installing NICI” (<https://www.netiq.com/documentation/edir88/edirin88/data/a79kg0w.html#bjtfrfr>) in the *NetIQ eDirectory Installation Guide*.

- ♦ (Conditional) NICI 2.7 and eDirectory 8.8 support key sizes up to 4096 bits. To use a 4 KB key size, you must upgrade every server to eDirectory 8.8. Also, you must also install NICI 2.7 on every workstation using the management utilities, such as iManager and ConsoleOne.

When you upgrade your Certificate Authority (CA) server to eDirectory 8.8, the key size will not change but will still be 2 KB. To create a 4 KB key size, you must recreate the CA on an eDirectory 8.8 server. In addition, during the CA creation, you must change the default from 2 KB to 4 KB for the key size.

- ♦ (Conditional) If the names of containers in your eDirectory tree include a period, you must use escape characters to specify the Admin name, admin context, and server context parameters during installation and when adding server in to an existing tree. For more information, see Section 9.1, “Using Escape Characters when a Container Name Includes a Period (.),” on page 95.

6.3.2 Considerations for Installing the Identity Vault as a Non-root User

To install the Identity Vault as a non-root user, your environment must meet the following conditions:

- ♦ You cannot install the Identity Vault in a cluster environment as a non-root user.
- ♦ NICI must be installed on the server by a root user. For more information, see Section 9.5, “Installing NICI Manually on Workstations that have Management Utilities,” on page 103.
- ♦ The SNMP subagent (`NOVsubag`) must be installed on the server by a root user and configured.

To install `NOVsubag`

Enter the following command: `rpm -ivh --nodeps NOVsubag_rpm_file_name_with_path`.

To configure SNMP:

Manually export the paths for the environment variables using the following command:

```
export LD_LIBRARY_PATH=custom_location/opt/novell/eDirectory/lib64:/opt/novell/eDirectory/lib64/nds-modules:/opt/novell/lib64:$LD_LIBRARY_PATH
export PATH=/opt/novell/eDirectory/bin:$PATH
export MANPATH=/opt/novell/man:$MANPATH
```

For example:

```
rpm -ivh --nodeps novell-NOVsubag-8.8.1-5.i386.rpm
```

- ♦ (Conditional) To use SLP and SNMP on the Identity Vault server, you must install the services as root.
- ♦ The non-root user account that installs Identity Vault must have Write rights to the directory where you want to install.

6.3.3 Considerations for Installing Identity Vault on a Windows Server

NetIQ recommends that you review the following considerations before you install the Identity Vault on a Windows server:

- ◆ You must have administrative rights to the Windows server and to all portions of the eDirectory tree that contain domain-enabled User objects. For an installation into an existing tree, you need administrative rights to the Tree object so that you can extend the schema and create objects.
- ◆ (Conditional) Before performing a silent installation (unattended), you must install the following software on the target server:
 - ◆ Microsoft Visual C++ 2005 and Microsoft Visual C++ 2012 Redistributable Packages. By default, the installation files, `vc redistrib_x86.exe` and `vc redistrib_x64.exe` are located in the `eDirectory\Windows\x64\redist_pkg` folder.
 - ◆ Novell International Cryptographic Infrastructure (NICI). By default, the installation files are located in the `eDirectory/Windows/x64/nici` folder.
- ◆ Because NTFS provides a safer transaction process than a FAT file system provides, you can install eDirectory only on an NTFS partition. Therefore, if you have only FAT file systems, do one of the following:
 - ◆ Use Disk Administrator. Refer to the Windows Server documentation for more information.
 - ◆ Create a new partition and format it as NTFS.
 - ◆ Convert an existing FAT file system to NTFS, using the CONVERT command.
 - ◆ Refer to the Windows Server documentation for more information.

If your server only has a FAT file system and you forget or overlook this process, the installation program prompts you to provide an NTFS partition.

- ◆ You must be running the latest version of the Windows SNMP service.
- ◆ Your Windows operating system must be running the latest service packs before you begin the installation process.
- ◆ To install on a virtual machine that has a DHCP address or on a physical or virtual machine in which SLP is not broadcast, ensure that the Directory Agent is configured in your network. For more information, see [Section 9.2.2, “Understanding OpenSLP,” on page 97](#).

6.3.4 Considerations for Installing the Identity Vault in a Clustered Environment

Before installing the Identity Vault in a clustered environment, NetIQ recommends reviewing the following considerations:

- ◆ You must have two or more Windows servers or Linux servers with clustering software.
- ◆ You must have external shared storage supported by the cluster software, with sufficient disk space to store all Identity Vault and NICI data:
 - ◆ The Identity Vault DIB must be located on the cluster shared storage. State data for the Identity Vault must be located on the shared storage so that it is available to the cluster node that is currently running the services.
 - ◆ The root Identity Vault instance on each of the cluster nodes must be configured to use the DIB on the shared storage.

- ◆ You must also share NCI (NetIQ International Cryptographic Infrastructure) data so that server-specific keys are replicated among the cluster nodes. NCI data used by all cluster nodes must be located on the cluster shared storage.
- ◆ NetIQ recommends storing all other eDirectory configuration and log data on the shared storage.
- ◆ You must have a virtual IP address.
- ◆ (Conditional) If you are using eDirectory as the support structure for the Identity Vault, the nds-cluster-config utility supports configuring the root eDirectory instance only. eDirectory does not support configuring multiple instances and non-root installations of eDirectory in a cluster environment.

For more information, see [Chapter 12, “Installing the Identity Vault in a Clustered Environment,”](#) on page 121.

6.3.5 Understanding Identity Manager Objects in eDirectory

The following list indicates the major Identity Manager objects that are stored in eDirectory and how they relate to each other. The installation process does not create objects. Instead, you create the Identity Manager objects when configuring the Identity Manager solution.

- ◆ **Driver Set:** A driver set is a container that holds Identity Manager drivers and library objects. Only one driver set can be active on a server at a time. However, more than one server might be associated to one driver set. Also, a driver can be associated with more than one server at a time. However, the driver should only be running on one server at a time. The driver should be in a disabled state on the other servers. Any server that is associated with a driver set must have the Metadirectory server installed on it.
- ◆ **Library:** The Library object is a repository of commonly used policies that can be referenced from multiple locations. The library is stored in the driver set. You can place a policy in the library so that every driver in the driver set can reference it.
- ◆ **Driver:** A driver provides the connection between an application and the Identity Vault. It also enables data synchronization and sharing between systems. The driver is stored in the driver set.
- ◆ **Job:** A job is automates a recurring task. For example, a job can configure a system to disable an account on a specific day, or initiate a workflow to request an extension of a person’s access to a corporate resource. The job is stored in the driver set.

6.3.6 Replicating the Objects that Identity Manager Needs on the Server

If your Identity Manager environment calls for multiple servers in order to run multiple Identity Manager drivers, your plan should make sure that certain eDirectory objects are replicated on servers where you want to run these Identity Manager drivers.

You can use filtered replicas, as long as all of the objects and attributes that the driver needs to read or synchronize are included in the filtered replica.

Keep in mind that you must give the Identity Manager Driver object sufficient eDirectory rights to any objects it is to synchronize, either by explicitly granting it rights or by making the Driver object security equivalent to an object that has the desired rights.

An eDirectory server that is running an Identity Manager driver (or that the driver refers to, if you are using the Remote Loader) must hold a master or read/write replica of the following:

- ◆ The Driver Set object for that server.

You should have one Driver Set object for each server that is running Identity Manager. Unless you have specific needs, don't associate more than one server with the same Driver Set object.

NOTE: When you create a Driver Set object, the default setting is to create a separate partition. Novell recommends creating a separate partition on the Driver Set object. For Identity Manager to function, the server is required to hold a full replica of the Driver Set object. If the server has a full replica of the location where the Driver Set object is installed, the partition is not required.

- ◆ The Server object for that server.

The Server object is necessary because it allows the driver to generate key pairs for objects. It is also important for Remote Loader authentication.

- ◆ The objects that you want this instance of the driver to synchronize.

The driver can't synchronize objects unless a replica of those objects is on the same server as the driver. In fact, an Identity Manager driver synchronizes the objects in *all* the containers that are replicated on the server unless you create rules for scope filtering to specify otherwise.

For example, if you want a driver to synchronize all user objects, the simplest way is to use one instance of the driver on a server that holds a master or read/write replica of all your users.

However, many environments don't have a single server that contains a replica of all the users. Instead, the complete set of users is spread across multiple servers. In this case, you have three choices:

- ◆ **Aggregate users onto a single server.** You can create a single server that holds all users by adding replicas to an existing server. Filtered replicas can be used to reduce the size of the eDirectory database if desired, as long as the necessary user objects and attributes are part of the filtered replica.

- ◆ **Use multiple instances of the driver on multiple servers, with scope filtering.** If you don't want to aggregate users onto a single server, you need to determine which set of servers holds all the users, and set up one instance of the Identity Manager driver on each of those servers.

To prevent separate instances of a driver from trying to synchronize the same users, you need to use scope filtering to define which users each instance of the driver should synchronize. Scope filtering means that you add rules to each driver to limit the scope of the driver's management to specific containers. See ["Using Scope Filtering to Manage Users on Different Servers"](#) on page 53.

- ◆ **Use multiple instances of the driver on multiple servers, without scope filtering.** If you want to have multiple instances of a driver running on different servers without using filtered replicas, you need to define policies on the different driver instances that enable the driver to process different sets of objects within the same Identity Vault.

- ◆ The Template objects you want the driver to use when creating users, if you choose to use templates.

Identity Manager drivers do not require you to specify eDirectory Template objects for creating users. However, if you specify that a driver should use a template when creating users in eDirectory, the Template object must be replicated on the server where the driver is running.

- ◆ Any containers you want the Identity Manager driver to use for managing users.

For example, if you have created a container named Inactive Users to hold user accounts that have been disabled, you must have a master or read/write replica (preferably a master replica) of that container on the server where the driver is running.

- ♦ Any other objects that the driver needs to refer to (for example, work order objects for the Avaya PBX driver).

If the other objects are only to be read by the driver, not changed, the replica for those objects on the server can be a read-only replica.

6.3.7 Using Scope Filtering to Manage Users on Different Servers

Scope filtering means adding rules to each driver to limit the scope of the driver's actions to specific containers. The following are two situations in which you would need to use scope filtering:

- ♦ You want the driver to synchronize only users that are in a particular container.

By default, an Identity Manager driver synchronizes objects in all the containers that are replicated on the server where it is running. To narrow that scope, you must create scope filtering rules.

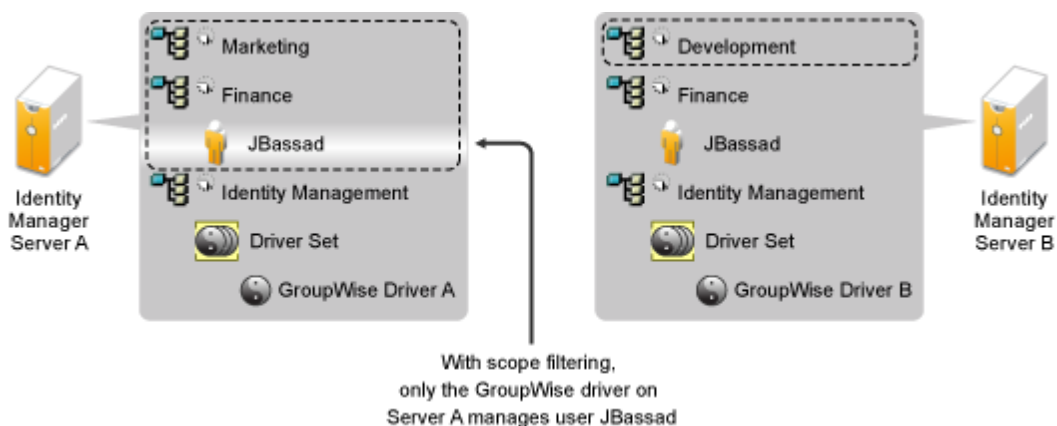
- ♦ You want an Identity Manager driver to synchronize all users, but you don't want all users to be replicated on the same server.

To synchronize all users without having them replicated on one single server, you need to determine which set of servers holds all the users, and then create an instance of the Identity Manager driver on each of those servers. To prevent two instances of the driver from trying to synchronize the same users, you need to use scope filtering to define which users each instance of the driver should synchronize.

NOTE: You should use scope filtering even if your server's replicas don't currently overlap. In the future, replicas could be added to your servers and an overlap could be created unintentionally. If you have scope filtering in place, your Identity Manager drivers do not try to synchronize the same users, even if replicas are added to your servers in the future.

Figure 6-1 on page 53 shows an example of an Identity Vault with three containers that hold users: Marketing, Finance, and Development. It also shows an Identity Management container that holds the driver sets. Each of these containers is a separate partition. In this example, the Identity Manager administrator has two Identity Vault servers, Server A and Server B. Neither server contains a copy of all the users. Each server contains two of the three partitions, so the scope of what the servers hold is overlapping.

Figure 6-1 Scope Filtering Defines Which Drivers Synchronize Each Container



The administrator wants all the users in the tree to be synchronized by the GroupWise driver, but does not want to aggregate replicas of the users onto a single server. He chooses instead to use two instances of the GroupWise driver, one on each server. He installs Identity Manager and sets up the GroupWise driver on each Identity Manager server.

Server A holds replicas of the Marketing and Finance containers. Also on the server is a replica of the Identity Management container, which holds the driver set for Server A and the GroupWise Driver object for Server A.

Server B holds replicas of the Development and Finance containers, and the Identity Management container holding the driver set for Server B and the GroupWise Driver object for Server B.

Because Server A and Server B both hold a replica of the Finance container, both servers hold the user JBassad, who is in the Finance container. Without scope filtering, both GroupWise Driver A and GroupWise Driver B would synchronize JBassad. Scope filtering prevents both instances of the driver from managing the same user, because it defines which drivers synchronize each container.

Identity Manager comes with predefined rules. There are two rules that help with scope filtering: “Event Transformation - Scope Filtering - Include Subtrees” and “Event Transformation - Scope Filtering - Exclude Subtrees”. For more information, see [Understanding Policies for Identity Manager 4.0.2](#).

For this example, you would use the Include Subtrees predefined rule for Server A and Server B. You would define the scope for each driver differently so that they would only synchronize the users in the specified containers. Server A would synchronize Marketing and Finance. Server B would synchronize Development.

6.3.8 Understanding the Linux Packages in the Identity Vault Installation Kit

NetIQ eDirectory includes a Linux package system, which is a collection of tools that simplify the installation and uninstallation of various eDirectory components. Packages contain makefiles that describe the requirements to build a certain component of eDirectory. Packages also include configuration files, utilities, libraries, daemons, and man pages that use the standard Linux tools installed with the OS.

Some packages depend on other packages or Identity Manager components such as NICE. You must install all dependent packages for proper functionality.

The following table provides information about the Linux packages that are included with eDirectory. All the packages are prefixed with *novell-*. For example, NDSserv is *novell-NDSserv*.

Package	Description
NOVLice	Contains the NetIQ Import Convert Export utility. This package depends on the NOVLmngnt, NOVLxis, and NLDAPbase packages.

Package	Description
NOVbase	<p>Represents the Directory User Agent. This package depends on the NICI package.</p> <p>This package contains the following items:</p> <ul style="list-style-type: none"> ◆ Authentication toolbox containing the RSA authentication needed for eDirectory. ◆ Platform-independent system abstraction library, a library containing all the defined Directory User Agent functions, and the schema extension library. ◆ Combined configuration utility and the Directory User Agent test utility. ◆ eDirectory configuration file and manual pages.
NDScommon	<p>Contains the man pages for the eDirectory configuration file, install, and uninstall utilities. This package depends on the NDSbase package.</p>
NDSmasv	<p>Contains the libraries required for mandatory access control (MASV).</p>
NDSserv	<p>Contains all the binaries and libraries that the eDirectory server needs. It also contains the utilities to manage the eDirectory Server on the system. This package depends on the NDSbase, NDScommon, NDSmasv, NLDAPsdk, NOVLpkia and NOVLpkit packages. Also contains the following items:</p> <ul style="list-style-type: none"> ◆ NDS install library, FLAIM library, trace library, NDS library, LDAP server library, LDAP install library, index editor library, DNS library, merge library, and LDAP extension library for LDAP SDK. ◆ eDirectory server daemon. ◆ Binary for DNS and a binary to load an unload LDAP. ◆ The utility needed to create the MAC address, the utility to trace the server and change some of the global variables of the server, the utility to back up and restore eDirectory, and the utility to merge eDirectory trees. ◆ Startup scripts for DNS, NDS, and NLDAP. ◆ Man pages.
NDSrepair	<p>Contains the runtime libraries and the utility that corrects problems in the eDirectory database. This package depends on the NDSbase package.</p>

Package	Description
NLDAPbase	<p>Contains LDAP libraries, extensions to LDAP libraries, and the following LDAP tools:</p> <ul style="list-style-type: none"> ◆ ldapdelete ◆ ldapmodify ◆ ldapmodrdn ◆ ldapsearch <p>This package is dependent on the NLDAPsdk package.</p>
NOVLnmas	<p>Contains all the NMAS libraries and the nmasinst binaries needed for NMAS server. This package depends on the NICI and NDSmasv packages.</p>
NLDAPsdk	<p>Contains NetIQ extensions to LDAP runtime and Security libraries (Client NICI).</p>
NOVLsubag	<p>Contains the runtime libraries and utilities for the eDirectory SNMP subagent. This package depends on the NICI, NDSbase, and NLDAPbase packages..</p>
NOVLpkit	<p>Provides PKI Services which do not require eDirectory. This package depend on the NICI and NLDAPsdk packages..</p>
NOVLpkis	<p>Provides PKI Server Service. This package depends on the NICI, NDSbase, and NLDAPsdk packages.</p>
NOVLsnmp	<p>The runtime libraries and utilities for SNMP. This package depends on the NICI package.</p>
NDSdexvnt	<p>Contains the library that manages events generated in NetIQ eDirectory to other databases..</p>
NOVLpkia	<p>Provides PKI services. This package depends on the NICI, NDSbase, and NLDAPsdk packages.</p>
NOVLembox	<p>Provides the eMBox infrastructure and eMTools..</p>
NOVLlmgmt	<p>Contains runtime libraries for NetIQ Language Management.</p>
NOVLxis	<p>Contains the runtime libraries for NetIQ XIS.</p>
NOVLsas	<p>Contains the NetIQ SAS libraries.</p>
NOVLntls	<p>Contains NetIQ TLS library. This package is also identified as ntls.</p>
NOVLldif2	<p>Contains the NetIQ Offline Bulkload utility and depends on the NDSbase, NDSserv, NOVLntls, NOVLlmgmt, and NICI packages.</p>
NOVLncp	<p>Contains the NetIQ Encrypted NCP Services for Linux. This package depends on the NDScommon package.</p>

6.3.9 Improving Identity Vault Performance

eDirectory, the underlying infrastructure for the Identity Vault, is I/O intensive application rather than being processor-intensive. Two factors increase performance of Identity Vault : more cache memory and faster processors. For best results, cache as much of the Directory Information Base (DIB) Set as the hardware allows.

While eDirectory scales well on a single processor, you might consider using multiple processors. Adding processors improves performance in areas such as logins. Also, having multiple threads active on multiple processors improves performance.

The following table provides a general guideline for server settings, based on the expected number of objects in your eDirectory.

Objects	Memory	Hard Disk
100.000	2+ GB (Linux)	300 MB (Linux)
	384 MB (Windows)	144 MB (Windows)
1 million	4 GB (Linux)	1.5 GB
	2 GB (Windows)	
10 million	4+ GB (Linux)	15 GB
	2+ GB (Windows)	

For example, a base installation of eDirectory with the standard schema requires about 74 MB of disk space for every 50,000 users. However, if you add a new set of attributes or completely fill in every existing attribute, the object size grows. These additions affect the disk space, processor, and memory needed. Also, requirements for processors depend on additional services available on the computer as well as the number of authentications, reads, and writes that the computer is handling. Processes such as encryption and indexing can be processor intensive.

6.3.10 System Requirements for Installing Identity Vault

This section provides requirements to help you set up the server hosting the Identity Vault.

Category	Minimum Requirement
Processor	1 GHz
Disk Space	<ul style="list-style-type: none">◆ 300 MB for the Identity Vault server◆ 150 MB of additional disk space for every 50,000 users
Memory	1 GB

Category	Minimum Requirement
Operating System	<p>One of the following operating systems:</p> <ul style="list-style-type: none"> ◆ Red Hat Enterprise Linux 5.7 (64-bit) ◆ Red Hat Enterprise Linux 6.2 (64-bit) ◆ SUSE Linux Enterprise Server 11 SP1 (64-bit) ◆ SUSE Linux Enterprise Server 10 SP4 (32-bit or 64-bit) ◆ SUSE Linux Enterprise Desktop 10 SP4 (32-bit or 64-bit) ◆ Windows Server 2012 ◆ Windows server 2008 R2 with the latest service pack ◆ Windows Server 2008 (64-bit) with the latest service pack <p>NOTE: To use Identity Vault with RHEL, the <code>glibc</code> library must be version 2.4 at a minimum.</p>
Virtualization Systems	<p>One of the following systems running a supported operating system unless otherwise noted:</p> <ul style="list-style-type: none"> ◆ VMware ESXi ◆ Windows Server 2008 R2 Virtualization with Hyper-V (64-bit) ◆ Xen Virtual Machine running SLES 10 or SLES 11 <p>NOTE: To use Identity Vault with SUSE Linux Enterprise Server 10, the minimum patch level for the SLES operating system must be 3.02_09763-0.8.</p>

6.4 Prerequisites and Requirements for Installing the Identity Manager Engine

Before installing the Identity Manager engine, review the following considerations:

- ◆ Before installing the Identity Manager engine, you must install the Identity Vault. Also, the Identity Vault must contain a tree with at least one organizational unit, one user, and an iManager server.
- ◆ (Conditional) To install the Remote Loader on the same computer as the Identity Manager engine, ensure that you select an operating system that supports both components. For more information about system requirements for the Remote Loader, see [Section 6.6, “Prerequisites and Requirements for Installing the Remote Loader,” on page 67](#).
- ◆ (Conditional) If you install the Identity Manager engine as a non-root user, the installation process does not install NetIQ Sentinel Platform Agent, UNIX/Linux Account Driver, or Remote Loader. You must install these components separately.

6.4.1 Considerations for Installing Drivers with the Identity Manager Engine

Many variables affect the performance of the server where you install the Identity Manager engine, including the number of drivers running on the server. When planning where to install the drivers, NetIQ provides the following recommendations:

- ◆ In general, have no more than 10 drivers running on the server.
- ◆ If you plan to synchronize millions of objects with each driver, reduce the number of drivers on the server.
- ◆ If you plan to synchronize 100 objects or fewer per driver, you might be able to run more than 10 drivers on the server.
- ◆ To create a baseline on server performance which helps you determine the optimum number of drivers, use the health monitoring tools in iManager. For more information about the health monitoring tools, see “[Monitoring Driver Health](#)” in the *NetIQ Identity Manager 4.0.2 Common Driver Administration Guide*.

For more information about activating Identity Manager drivers after installation, see [Chapter 45, “Activating Identity Manager,”](#) on page 407.

6.4.2 System Requirements for Installing the Identity Manager Engine

This section provides requirements to help you set up the server hosting the Identity Manager engine.

Category	Requirement
Processor	For servers running Red Hat and SUSE Linux Enterprise and Windows operating systems: <ul style="list-style-type: none">◆ AMD x86 32-bit◆ AMD Anthlon64◆ AMD Opteron◆ Intel x86 32-bit◆ Intel EM64T
Memory	<ul style="list-style-type: none">◆ 2048 MB◆ 200 MB for Identity Manager Drivers

Category	Requirement
Operating System	<p>One of the following operating systems, at a minimum:</p> <ul style="list-style-type: none"> ◆ Open Enterprise Server 2015 (64-bit) ◆ Open Enterprise Server 11 SP1 (64-bit) ◆ Red Hat 6.2 (32-bit or 64-bit) ◆ Red Hat 5.7 (32-bit or 64-bit) ◆ Oracle Solaris 10 (64-bit) ◆ SUSE Linux Enterprise Server 11 SP1 (32-bit or 64-bit) ◆ SUSE Linux Enterprise Server 10 SP4 (32-bit or 64-bit) ◆ Windows Server 2008 R2 SP2 (64-bit) ◆ Windows Server 2008 SP2 (32-bit or 64-bit) ◆ Windows Server 2003 (32-bit) <p>NOTE: You cannot use the integrated installation process on a system running Open Enterprise Server 11 SP1 (64-bit) or Open Enterprise Server 2015 (64-bit).</p>
Virtualization Systems	<p>One of the following systems running a supported operating system unless otherwise noted:</p> <ul style="list-style-type: none"> ◆ Red Hat Enterprise Linux 5 Virtualization ◆ VMware ESXi Workstation 6.5 ◆ VMware ESXi 5.0 (32-bit or 64-bit) ◆ VMware ESXi 4.1 (32-bit or 64-bit) ◆ VMware ESXi 4.0 (32-bit or 64-bit) ◆ VMware ESX 4.0 (32-bit or 64-bit) ◆ Windows Server 2008 R2 Virtualization with Hyper-V (32-bit or 64-bit) ◆ Xen Virtual Machine running SLES 10 or SLES 11 as a guest operating system in para-virtualized mode and SLES 10 SP2 as the host operating system <p>NOTE</p> <ul style="list-style-type: none"> ◆ The VMware ESX and ESXi systems can also run the VMware version of SLES 11 SP2 (64-bit) as the guest operating system. ◆ You must use the integrated installation process for the following virtualization systems: <ul style="list-style-type: none"> ◆ VMware Workstation 6.5 ◆ VMware ESXi 5.0 ◆ VMware ESXi 4.1 ◆ Xen Virtual Machine running Windows 8 R2 as a guest operating system in para-virtualized mode
Operating System Hotfixes	<p>Before installing Identity Manager, NetIQ recommends that you apply the latest operating system patches according to the manufacturer's automated update facility.</p>

Category	Requirement
Software	<p>All of the following products:</p> <ul style="list-style-type: none"> ◆ NetIQ eDirectory 8.8.7, at a minimum ◆ iManager 2.75, at a minimum

6.5 Prerequisites and Requirements for Installing iManager

Before installing the iManager, review the following considerations:

- ◆ If you previously installed the Identity Vault as a `root` user, you must install iManager as a `root` user.
- ◆ If you plan to have more than 10 administrators regularly working in iManager at the same time, do not install iManager on the same server as other Identity Manager components.
- ◆ If you plan to have only one administrator, you can install iManager on the same server as the Identity Manager engine.
- ◆ To install iManager on a server running a supported Open Enterprise Server platform, you must use the OES version's patch channel to upgrade to the latest iManager version.
- ◆ If the iManager 2.7.7 Server setup program detects a previously installed version of iManager 2.7.x, you can stop the installation process or remove the existing iManager, JRE, and Tomcat installations.
- ◆ Because iManager Workstation is a self-contained environment, you can install multiple versions on the same workstation, including older versions of Mobile iManager. However, you should not attempt to run them simultaneously. If you need to use different versions, run one version, close it, and then run the other version.
- ◆ You cannot run iManager Workstation from a path that includes spaces. For example, `C:\NetIQ\iManager Workstation\working`.
- ◆ You must have `root` access rights for Linux servers or Administrator access for Windows servers.
- ◆ To create a Role-Based Services (RBS) collection in the eDirectory tree, you must have admin-equivalent rights.
- ◆ To run the iManager RBS Configuration Wizard, you must have admin-equivalent rights.
- ◆ To manage the same eDirectory tree with multiple versions of iManager, you must update your RBS Collection(s) to the latest iManager version.

6.5.1 Understanding the Server and Client Versions of iManager

You must install iManager on a server that can access an eDirectory tree. To install iManager on a workstation instead of a server, you need the client-based version of iManager, the **iManager Workstation**. Use the following guidelines to decide which version fits best in your environment, or whether your eDirectory management policies would benefit from installing both versions:

- ◆ If you have a single administrator who always manages eDirectory from the same client workstation, you can take advantage of iManager Workstation. iManager Workstation is fully self-contained and requires little setup. It automatically starts and stops the resources it needs when

it loads or unloads. iManager Workstation installs and runs on various Linux or Windows client workstations, has no dependencies on server-based iManager, and it can coexist with any other versions of iManager installed on your network.

iManager plug-ins do not automatically synchronize between iManager instances. If you have multiple administrators and use customized plug-ins, iManager Workstation and these plug-ins must be installed on each administrator's client workstation.

- ♦ If you manage eDirectory from multiple client workstations, or have multiple administrators, install iManager Server so that it is available from any connected workstation. Additionally, customized plug-ins only need to be installed once per iManager Server.

6.5.2 Considerations for Installing iManager on a Linux Platform

Your Linux server must have specific packages already installed before you install iManager:

Red Hat Enterprise Linux

You must install the following packages. When you install iManager on 64-bit version of RHEL, ensure that the 32-bit versions of the RHEL libraries are also installed.

- ♦ `compat-libstdc++33` (RHEL 5)
- ♦ `compat-libstdc++-33-*.el6.i686.rpm` (RHEL 6 32-bit)
- ♦ `compat-libstdc++-33-*.el6.i686.rpm` (RHEL 6 64-bit)
- ♦ `compat-libstdc++-33-*.el6.x86_64.rpm` (RHEL 6 64-bit)
- ♦ `libstdc++-4.4.*.el6.i686.rpm` (RHEL 6 64-bit)
- ♦ `libstdc++-4.4.*.el6.x86_64.rpm` (RHEL 6 64-bit for GUI installation mode)
- ♦ `glibc-2.12-*.el6.i686` (RHEL 6 64-bit)
- ♦ `libXau-*.el6.i686.rpm` (RHEL 6 64-bit)
- ♦ `libxcb-*.el6.i686.rpm` (RHEL 6 64-bit)
- ♦ `libX11-*.el6.i686.rpm` (RHEL 6 64-bit)
- ♦ `libXext-*.el6.i686.rpm` (RHEL 6 64-bit)
- ♦ `libXi-*.el6.i686.rpm` (RHEL 6 64-bit)
- ♦ `libXtst-*.el6.i686.rpm` (RHEL 6 64-bit)
- ♦ `libstdc++-*.el6.i686.rpm` (RHEL 6 64-bit)
- ♦ `libgcc-*.el6.i686.rpm` (RHEL 6 64-bit)
- ♦ `libXrender-0.9.5-1.el6.i686.rpm` (RHEL 6 64-bit)

SUSE Linux Enterprise Server (64-bit)

You must install the following packages.

- ♦ `libstdc++33?32bit` (SLES 11, SLES 10 SP3, SLES 10 SP4)
- ♦ `libstdc++43?32bit` (for SLES 11 SP1)
- ♦ `libstdc++46?32bit` (for SLES 11 SP2)
- ♦ `compat?lsb` (SLES 10)

To use PKI plug-in, you must also install the following RPMs on the iManager server:

- ◆ **SLES 11 64-bit:** compat-32bit (compat-32bit-2009.1.19-2.1)
- ◆ **SLES 11 32-bit:** compat (compat-2009.1.19-2.1)
- ◆ **SLES 10 64-bit:** compat-32bit (compat-32-bit-2006.1.25-11.2)
- ◆ **SLES 10 32-bit:** compat (compat-2006.1.25-11.2)

SUSE Linux Enterprise Server (32-bit)

You must install the following packages.

- ◆ libstdc++33 (SLES 11)
- ◆ libstdc++43 (SLES 11)

To use PKI plug-in, you must also install the following RPMs on the iManager server:

- ◆ **SLES 11 64-bit:** compat-32bit (compat-32bit-2009.1.19-2.1)
- ◆ **SLES 11 32-bit:** compat (compat-2009.1.19-2.1)
- ◆ **SLES 10 64-bit:** compat-32bit (compat-32-bit-2006.1.25-11.2)
- ◆ **SLES 10 32-bit:** compat (compat-2006.1.25-11.2)

6.5.3 Considerations for Installing iManager on a Windows Platform

If you are using Microsoft Internet Information Services (IIS) or Apache HTTP Server for Windows, you must manually integrate iManager with these Web server infrastructures. By default, iManager uses Tomcat on Windows servers.

6.5.4 Considerations for Installing iManager Workstation on Linux Clients

Your Linux clients must have the following packages already installed before you install iManager Workstation:

- ◆ GTK2
- ◆ GLIBC 2.3
- ◆ libstdc++33
 - ◆ SUSE Linux Enterprise Desktop (SLED) 11 32-bit
 - ◆ SLED 11 SP1 32-bit
 - ◆ openSUSE 11.0 32-bit
 - ◆ openSUSE 11.1 32-bit
 - ◆ openSUSE 11.2 32-bit
 - ◆ openSUSE 11.3 32-bit
 - ◆ openSUSE 12.1
- ◆ libstdc++33-32 bit
 - ◆ SLED 11 64-bit

- ◆ SLED 11 SP1 64-bit
- ◆ openSUSE 11.0 64-bit
- ◆ openSUSE 11.1 64-bit
- ◆ openSUSE 11.2 64-bit
- ◆ openSUSE 11.3 64-bit
- ◆ libgtk-2_0-0-32bit
 - ◆ openSUSE 12.2 (64-bit)
 - ◆ openSUSE 12.3 (64-bit)
- ◆ libXt6-32bit
 - ◆ openSUSE 12.2 (64-bit)
 - ◆ openSUSE 12.3 (64-bit)
- ◆ libgthread-2_0-0-32bit
 - ◆ openSUSE 12.2 (64-bit)
 - ◆ openSUSE 12.3 (64-bit)
- ◆ libXtst6-32bit
 - ◆ openSUSE 12.2 (64-bit)
 - ◆ openSUSE 12.3 (64-bit)

6.5.5 Considerations for Installing iManager Workstation on Windows Clients

Before installing iManager Workstation on your Windows clients, NetIQ recommends that you review the following considerations:

- ◆ To enable Internet Explorer to use a proxy server for your LAN, you must specify **Bypass Proxy Server for Local Addresses** under **Tools > Internet Options > Connections > LAN Settings**.
- ◆ To run a Novell Client earlier than version 4.91, the Novell Modular Authentication Service (NMAS) client must be installed on the workstation before you launch iManager Workstation.
- ◆ If you run iManager Workstation from a path where any directory contains `temp` or `tmp` in the name, such as `c:\programs\temp\imanager`, iManager plug-ins do not install. Instead, run iManager Workstation from `C:\imanager` or a non-temporary directory.
- ◆ The first time that you run iManager Workstation on a Windows workstation, use an account that is a member of the workstation's Administrators group.

6.5.6 System Requirements for iManager (Server Version)

This section provides requirements to help you set up the server that hosts iManager. For more information about the server version of iManager, see [Section 6.5.1, “Understanding the Server and Client Versions of iManager,”](#) on page 61.

Category	Requirement
Processor	Pentium* III 600MHz, at a minimum
Disk Space	Linux: 200 MB, at a minimum Windows: 500 MB, at a minimum

Category	Requirement
Memory	512 MB (1024 MB recommended) 80 MB for iManager Plug-ins
Operating System	<p>One of the following operating systems, at a minimum:</p> <ul style="list-style-type: none"> ◆ Open Enterprise Server 2015 (64-bit) ◆ Open Enterprise Server 11 ◆ Open Enterprise Server 2 ◆ Red Hat Enterprise Linux Server 6 (64-bit) ◆ Red Hat Enterprise Linux Server 5.7 (64-bit) ◆ SUSE Linux Enterprise Server 11 (64-bit) ◆ SUSE Linux Enterprise Server 10 SP1 (64-bit) ◆ Windows Server 2012 (64-bit) ◆ Windows Server 2008 R2 (64-bit) ◆ Windows Server 2008 SP2 (64-bit) <p>NOTE: You cannot install iManager on a Solaris platform. However, iManager can still manage and work with applications and resources, such as eDirectory, that run on Solaris.</p>
Web browsers	<p>Any of the following Web browsers:</p> <ul style="list-style-type: none"> ◆ Firefox 23, 22, and 21 ◆ Firefox 19, 16, 15, 14, 13, 12, 11, and 10 ◆ Firefox 9.0.1 ◆ Firefox 4.0.1 ◆ Google Chrome 28, 27, 26, 25, 23, and 22 ◆ Internet Explorer 10, 9, or 8 (Normal and Compatibility modes) ◆ Safari 6.0 ◆ Safari 5.1.4 <p>NOTE: You cannot access iManager through an iChain server with a path-based multihoming accelerator and with Remove Sub Path from URL enabled.</p>
Application Server	<p>Tomcat 7.0.42, or the version supplied with iManager</p> <p>NOTE: You can manually integrate an existing IIS or Apache Web server infrastructure with iManager on a Windows server.</p>
Directory Services	eDirectory 8.8
Default Ports	8080, 8443, and 9009

6.5.7 System Requirements for iManager Workstation (Client Version)

This section provides requirements to help you set up the server hosting iManager Workstation. For more information about the client version of iManager, see [Section 6.5.1, “Understanding the Server and Client Versions of iManager,”](#) on page 61

Category	Requirement
Processor	Pentium* III 600MHz, at a minimum
Disk Space	200 MB, at a minimum
Memory	256 MB (521 MB recommended)
Operating System	<p>One of the following operating systems, at a minimum:</p> <ul style="list-style-type: none"> ◆ OpenSUSE 10.3 (32-bit and 64-bit) ◆ Red Hat Enterprise Linux Server 6 (31-bit and 64-bit) ◆ Red Hat Enterprise Linux Server 5.7 (64-bit) ◆ SUSE Linux Enterprise Server 11 (32-bit) ◆ SUSE Linux Enterprise Desktop 11 SP1 (32-bit or 64-bit) ◆ Windows 8 (32-bit or 64-bit) ◆ Windows 7 (32-bit or 64-bit) ◆ Windows Server 2008 (32-bit) <p>NOTE: The following platforms must be running a 32-bit version of the supported operating system:</p> <ul style="list-style-type: none"> ◆ RHEL 5.9 ◆ RHEL 6.3.4
Web browsers	<p>Any of the following Web browsers:</p> <ul style="list-style-type: none"> ◆ Firefox 23, 22, and 21 ◆ Firefox 19, 16, 15, 14, 13, 12, 11, and 10 ◆ Firefox 9.0.1 ◆ Firefox 4.0.1 ◆ Google Chrome 28, 27, 26, 25, 23, and 22 ◆ Internet Explorer 10, 9, or 8 (Normal and Compatibility modes) ◆ Safari 6.0 ◆ Safari 5.1.4 <p>NOTE</p> <ul style="list-style-type: none"> ◆ You cannot access iManager through an iChain server with a path-based multihoming accelerator and with Remove Sub Path from URL enabled. ◆ You cannot use the user interface view in Internet Explorer 10 Metro on a computer running Windows 7 and 8.
Application Server	Tomcat 7.0.42, bundled with iManager Workstation
Software	Java 1.7.0_25, bundled with iManager Workstation

Category	Requirement
Default Ports	8080, 8443, and 9009

6.6 Prerequisites and Requirements for Installing the Remote Loader

This section provides the prerequisites and system requirements for installing the Remote Loader.

6.6.1 Prerequisites for Installing the Remote Loader

Before installing the Remote Loader, NetIQ recommends that you review the following considerations:

- ◆ You must install the Remote Loader on a server that can communicate with the managed systems. The driver for each managed system must be available with the relevant APIs.
- ◆ You can install the Remote Loader on the same computer where you installed the Identity Manager engine. If you have installed the engine as a 32-bit application on a 64-bit operating system, you can install both a 32-bit and a 64-bit Remote Loader on the same server.
- ◆ You can install Java Remote Loader on platforms that do not support the native Remote Loader.
- ◆ You can install .NET Remote Loader on .NET platform version 2.
- ◆ (Conditional) To connect Identity Manager to Active Directory, you must install Remote Loader and the driver for Active Directory on a server that is a member server or a domain controller. You do not need to install eDirectory and Identity Manager on the same server as the connected system. The Remote Loader sends all of the events from Active Directory to the Identity Manager server. The Remote Loader then receives any information from the Identity Manager server and passes that to the connected application.
- ◆ NetIQ recommends that you use the Remote Loader configuration with your drivers where possible. Use the Remote Loader even in cases where the connected system is on the same server as the Identity Manager server engine.

When you run the driver with the Remote Loader configuration, the following solutions apply:

- ◆ Protects eDirectory from any exceptions encountered by the driver shim.
- ◆ Offloads driver commands to the remote application or database, which improve performance of the server that hosts the Identity Manager engine.
- ◆ Allows you to run additional drivers on servers that do not host the Identity Manager engine.
- ◆ The following drivers support the Remote Loader capability:
 - ◆ Active Directory
 - ◆ Avaya PBX
 - ◆ Banner
 - ◆ Blackboard
 - ◆ Delimited Text
 - ◆ Google Apps
 - ◆ GroupWise (for 32-bit Remote Loader)
 - ◆ JDBC
 - ◆ JMS

- ◆ LDAP
- ◆ Linux/UNIX Settings
- ◆ Lotus Notes
- ◆ Managed System Gateway
- ◆ Manual Task Services
- ◆ PeopleSoft 5.2
- ◆ Remedy ARS
- ◆ RACF
- ◆ RSA SecureID
- ◆ Salesforce.com
- ◆ SAP Business Logic
- ◆ SAP GRC (CMP only)
- ◆ SAP HR
- ◆ SAP Portal
- ◆ SAP User Management
- ◆ Sentinel
- ◆ Integration Module V2.0 for Sentinel
- ◆ Scripting
- ◆ SharePoint
- ◆ SOAP
- ◆ Top Secret
- ◆ WorkOrder

For more information about the Identity Manager Remote Loader, see [this article \(http://www.novell.com/communities/node/2994/many-faces-remote-loaders-idm\)](http://www.novell.com/communities/node/2994/many-faces-remote-loaders-idm).

6.6.2 System Requirements for Installing the Remote Loader

This section provides requirements to help you set up the server hosting the Remote Loader.

Category	Requirement
Processor	Pentium* III 600MHz, at a minimum
Memory	256 MB

Category	Requirement
Operating System	<p>One of the following operating systems, at a minimum:</p> <ul style="list-style-type: none"> ◆ Open Enterprise Server 2015 (64-bit) ◆ Open Enterprise Server 11 SP1 (32-bit and 64-bit) ◆ Open Enterprise Server 2 SP3 (32-bit and 64-bit) ◆ Red Hat Enterprise Linux Server 6.2 (32-bit or 64-bit) ◆ Red Hat Enterprise Linux Server 5.7 (32-bit or 64-bit) ◆ Oracle Solaris 10 (64-bit) ◆ SUSE Linux Enterprise Server 11 SP1 (32-bit or 64-bit) ◆ SUSE Linux Enterprise Server 10 SP4 (32-bit or 64-bit) ◆ Windows Server 2008 R2 SP1 ◆ Windows Server 2008 SP2 (32-bit and 64-bit) ◆ Windows Server 2003 SP2 (32-bit and 64-bit)
Virtualization Systems	<p>One of the following systems running a supported operating system unless otherwise noted:</p> <ul style="list-style-type: none"> ◆ Red Hat Enterprise Linux 5 Virtualization (64-bit) ◆ Windows Server 2008 R2 Virtualization with Hyper-V (32-bit or 64-bit) ◆ Xen Virtual Machine running SLES 10 or SLES 11 as a guest operating system in para-virtualized mode

6.7 Prerequisites and Requirements for Installing the User Application and Roles Based Provisioning Module

NetIQ recommends that you review the prerequisites and computer requirements for both the User Application and RBPM before you begin the installation process. For more information about configuring the User Application environment, see the [User Application Administration Guide](#).

6.7.1 Considerations for Installing the User Application and Roles Based Provisioning Module

Before installing the User Application and RBPM, review the following considerations:

- ◆ During the installation process, the installation program writes log files to the installation directory. These files contain information about your configuration. After you configure your User Application and RBPM environment, you should consider deleting these log files or storing them in a secure location. During the installation process, you might choose to write the database schema to a file. Since this file contains descriptive information about your database, you should move the file to a secure location after the installation process is complete.
- ◆ Before installing the User Application and RBPM, you must install the Identity Manager engine. The installation process requires the location of the computer running the Identity Manager engine. For more information about the Identity Manager engine, see [Section 6.4, "Prerequisites and Requirements for Installing the Identity Manager Engine,"](#) on page 58.

- ◆ Before installing the User Application and RBPM, you must install Identity Manager Designer. The drivers for RBPM derive from a set of packages in Designer. For more information about installing Designer, see [Chapter 7, “Installing Designer,” on page 89](#). For more information about the drivers, see [Chapter 25, “Creating the Drivers for the Roles Based Provisioning Module,” on page 213](#).
- ◆ You must execute the RBPM installation program from the same computer where you installed the Identity Manager engine.
- ◆ (Conditional) If you installed the Identity Vault in a non-default location, you must manually extend the eDirectory schema before installing RBPM. The Identity Vault must be running on the default LDAP ports 389 and 636.

For more information about manually extending the schema, see [Section 24.2, “Extending the eDirectory Schema Using the Wizard,” on page 206](#) and [Section 24.3, “Extending the Schema Manually without Using the Wizard,” on page 208](#). For more information about installing Identity Vault, see [Chapter 10, “Installing the Identity Vault on a Linux Server,” on page 107](#).

- ◆ You must configure the Identity Vault to use NMAS Login as the process for a user’s first login to ensure that Identity Manager enforces Universal Password functionality.
 - ◆ **Linux:** Add the following commands to the end of the `/opt/novell/eDirectory/sbin/pre_ndsd_start` script:


```
NDSM_TRY_NMASLOGIN_FIRST=true
export NDSM_TRY_NMASLOGIN_FIRST
```
 - ◆ **Windows:** Add `NDSM_TRY_NMASLOGIN_FIRST` with the string value `true` to the `HKLM\SYSTEM\CurrentControlSet\Control\SessionManager\Environment` registry key.
- ◆ Before you make the User Application available to users, the indexes for the Identity Vault must be in Online mode. For more information about configuring an index during installation, see [Section 30.2.11, “Miscellaneous,” on page 286](#).
- ◆ You must create the User Application driver before creating the Role and Resource driver. The Role and Resource driver references the role vault container (`RoleConfig.AppConfig`) in the User Application driver.
- ◆ You cannot use the Role and Resource Service Driver with the Remote Loader because the driver uses `jClient`.
- ◆ You must install an application server on the local computer before installing the User Application. For more information, see [Section 6.7.3, “Understanding the Application Server Requirements,” on page 72](#).
- ◆ The installation process places the program files in the `C:\Novell\IDM` or `/opt/novell/idm` directory by default. If you plan to install the User Application in non-default location, the new directory must meet the following requirements before you begin the installation process:
 - ◆ The directory exists and is writable.
 - ◆ For Linux environments, the directory is writable by non-`root` users.
- ◆ Although NetIQ recommends that you use dedicated computers for the application server, you should install the User Application on the same server where you plan to install the Identity Reporting Module.
- ◆ You must install a database on the local computer or a connected server before installing the User Application. For more information, see [Section 6.7.4, “Understanding the User Application Database,” on page 73](#).
- ◆ Each User Application instance can service only one user container. For example, you can add users to, search, and query only the container associated with the instance. Also, a user container association with an application is meant to be permanent.

- ♦ (Conditional) If you plan to use external password management, your environment must meet the following requirements:
 - ♦ Enable Secure Sockets Layer (SSL) protocol for the JBoss servers on which you deploy the User Application and the `IDMPwdMgt.war` file.
 - ♦ Ensure that the SSL port is open on your firewall.

For more information about the `IDMPwdMgt.war` file, see [Section 30.5, “Configuring External Forgot Password Management,” on page 290](#).

6.7.2 Understanding the Installation Files for the Roles Based Provisioning Module

The installation files for the User Application and RBPM are located in the `products/RBPM` directory of the installation package.

File	Description
<code>IDMProv.war</code>	The Web Application Archive (WAR) file for RBPM. This file includes the User Application with Identity Self-Service and RBPM features.
<code>IDMUserApp.jar</code>	The User Application installation program.
<code>silent.properties</code>	Specifies the parameters required for a silent installation. These parameters correspond to the installation parameters that you set in the installation procedures.
<code>JBossPostgreSQL.bin</code> or <code>JBossPostgreSQL.exe</code>	A utility for installing the JBoss application server and PostgreSQL database. For more information about this utility, see Chapter 23, “Installing the Community Edition of JBoss,” on page 203 .
<code>nmassaml.zip</code>	Contains an eDirectory method to support SAML. Use this file if you are not using Access Manager. For more information, see “Installing the SAML method in your eDirectory tree” on page 288 .
<code>rbpm_driver_install.exe</code>	The Windows installation program for the primary components of the RBPM (Role and Resource Service Driver, User Application Driver, and eDirectory schema).
<code>rbpm_driver_install_linux.bin</code>	The Linux installation program for the primary components of the RBPM (Role and Resource Service Driver, User Application Driver, and eDirectory schema).

The User Application installation program does the following:

- ♦ Designates an existing version of an application server to use.
- ♦ Designates an existing version of a database to use. For example PostgreSQL, Oracle, DB2, Microsoft SQL Server, or MySQL. The database stores User Application data and configuration information.
- ♦ Configures the JDK’s certificates file so that the User Application (running on the application server) can communicate securely with the Identity Vault and the User Application driver.
- ♦ Configures and deploys the Java Web Application Archive (WAR) file for the User Application to the application server. On WebSphere and WebLogic, you must manually deploy the WAR.

- ◆ Enables logging through Novell or OpenXDAS auditing clients if you choose to do so.
- ◆ Enables you to import an existing master key to restore a specific RBPM installation and to support clusters.

6.7.3 Understanding the Application Server Requirements

The User Application requires that an application server be installed with the following considerations:

- ◆ The application server must be running with Java Development Kit (JDK) or Java Runtime Environment (JRE). For more information about supported versions, see [Section 6.7.6, “System Requirements for Installing the User Application and Roles Based Provisioning Module,” on page 75.](#)

You must set the `JAVA_HOME` environment variable to point to the JDK that you plan to use with the User Application. To override `JAVA_HOME`, manually specify the path during the User Application installation.

- ◆ (Conditional) When installing on a SUSE Linux Enterprise Server (SLES), do not use the IBM JDK that comes with SLES. This version is incompatible with some aspects of the User Application installation. Instead, download the Oracle JDK.
- ◆ (Conditional) If you plan to install more than one application server with a deployment of the User Application, you must have a separate User Application driver for each deployment unless you install the User Applications on sister nodes of the same JBoss cluster. For more information, see [Section 6.7.5, “Prerequisites for Installing the User Application in a Cluster Environment,” on page 75.](#) For more information about configuring a cluster environment, see [Chapter 27, “Preparing a Cluster Environment for Use with the User Application,” on page 221.](#)
- ◆ (Conditional) To preserve documents that you digitally sign, you must install the User Application on a JBoss application server and use Novell Identity Audit. Digital signature documents are not stored with workflow data in the User Application database, but are stored in the logging database. You must also enable logging to preserve these documents. For more information, see the [“Setting Up Logging”](#) section of the *User Application Administration Guide*.
- ◆ (Conditional) In environments where you log a large amount of user data or your directory-server contains a large number of objects, you might want more than one application server with a deployment of the User Application. For more information about configuring the User Application for optimal performance, see the [“Performance Tuning”](#) section of the *User Application Administration Guide*.
- ◆ (Conditional) If you use a JBoss application server, do not start the server until after you complete the installation process.
- ◆ (Conditional) If you use a JBoss application server with external password management, you must do the following to enable the Secure Sockets Layer (SSL) protocol:
 - ◆ Enable SSL for the JBoss servers on which you deploy RBPM and the `IDMPwdMgt.war` file.
 - ◆ Ensure that the SSL port is open on your firewall.

For more information about enabling SSL, see your JBoss documentation.

For more information about the `IDMPwdMgt.war` file, see [Section 30.5, “Configuring External Forgot Password Management,” on page 290](#) and the *User Application Administration Guide*.

6.7.4 Understanding the User Application Database

The database stores the User Application data and configuration information.

Before installing the database instance, review the following prerequisites:

- ◆ To configure a database for use with the application server, you must create a JDBC driver. The User Application uses standard JDBC calls to access and update the database. The User Application uses a JDBC data source file bound to the JNDI tree to open a connection to the database.
- ◆ You must have an existing data source file that points to the database. Depending on your installation environment, you might need to create or configure the file:
 - ◆ **JBoss:** The installation program for the User Applications creates an application server data source file named `IDM-ds.xml`, which points to the database. The program places this file in the deploy directory. For example, `server/IDMProv/deploy`. The installation program also places the appropriate JDBC driver for the database specified during installation in the `lib` directory. For example, `/server/IDMProv/lib`.

All nodes in the JBoss cluster must access the same database instance. When you use the User Application installation program, you are prompted to specify the database name, host, and port. For more information about setting up the User Application database for a cluster, see [Section 27.2.3, “Configuring the Cluster for the User Application Database,” on page 223](#).

- ◆ **WebLogic:** You must configure the data source manually before performing the installation. For more information, see [Section 28.2.2, “Configuring the Data Source for the User Application Database on WebLogic,” on page 240](#).
- ◆ **WebSphere:** You must configure the data source manually before performing the installation. For more information, see [Section 28.3.2, “Configuring a Data Source for the User Application Database on WebSphere,” on page 248](#).
- ◆ Ensure that you have the following information:
 - ◆ Host and port of the database server.
 - ◆ Name of the database to create. The default database for the User Application is `idmuserappdb`.
 - ◆ Database username and password. The database username must represent an Administrator account or must have enough permissions to create tables in the Database Server. The default administrator for the User Application is `idmadmin`.

(Conditional) For a MySQL database, the database user account must have full access to (be the owner of) the database. The account must also have access to the tables in the database. The minimum set of privileges is CREATE, INDEX, INSERT, UPDATE, DELETE, and LOCK TABLES. The user account must also have select rights to the `mysql.user` table. To grant the proper rights, specify the following syntax:

```
USE mysql;  
GRANT SELECT ON mysql.user TO username@host;
```

- ◆ The driver `.jar` file provided by the database vendor for the database that you are using. NetIQ does not support driver JAR files provided by third-party vendors.
- ◆ The database instance can be on the local computer or a connected server.
- ◆ The database character set must use Unicode encoding. For example, UTF-8 is an example of a character set that uses Unicode encoding, but Latin1 does not use Unicode encoding. For more information about specifying the character set, see [Section 26.2.2, “Configuring the Character Set,” on page 218](#) or [Section 26.3, “Configuring an Oracle Database,” on page 219](#).

- ◆ You must use case-sensitive collation. If you use case-insensitive collation, you might encounter duplicate key errors during migration. If a duplicate key error occurs, check the collation and correct it, then re-install the User Application.
- ◆ (Conditional) To use the same database instance both for auditing purposes and for the User Application, NetIQ recommends installing the database on a separate dedicated server from the server that hosts the application server running the User Application.
- ◆ (Conditional) If you are migrating to a new version of the User Application, you must use the same User Application database that you used for the previous installation.
- ◆ (Conditional) If you use a MySQL database, you must add the `ansi` entry to the configuration file, `my.cnf` on Linux or `my.ini` file on Windows. For more information, see [Section 26.2.4, “Configuring the ANSI Setting,” on page 218](#).
- ◆ (Conditional) When you install the MySQL Database, the user account that you specify for the User Application must have full access (be the owner of) the database. This account also needs access to the tables in the system. For more information, see [Section 26.2.5, “Configuring the Admin User Account,” on page 219](#).
- ◆ (Conditional) To use SQL Server 2008, you must have version 3.0 of the Microsoft SQL Server 2008 JDBC Driver. The User Application has been tested specifically with version 3.0.119.0 of the Microsoft SQL Server 2008 JDBC Driver.
- ◆ (Conditional) If you plan to use Microsoft SQL Server, NetIQ supports the JDBC driver and User Application only on the Red Hat Linux and Windows 2000 operating systems.
- ◆ (Conditional) The installation package includes a utility for installing the Community Edition of the JBoss PostgreSQL database server. JBoss supports the Community Edition only in their User Forums. NetIQ recommends that you use this version only in your test environment. For production environments, use a full edition of the JBoss database server. For more information, see [Chapter 23, “Installing the Community Edition of JBoss,” on page 203](#).
- ◆ Database clustering is a feature of each respective database server. NetIQ does not officially test with any clustered database configuration because clustering is independent of the product functionality. Therefore, we support clustered database servers with the following caveats:
 - ◆ Some features or aspects of your clustered database server might need to be disabled. For example, Transactional Replication must be disabled on certain tables due to constraint violations when trying to insert a duplicate key.
 - ◆ We do not provide assistance on the installation, configuration, or optimization of the clustered database server, including installation of our products into a clustered database server.
 - ◆ We exert our best effort to resolve any issues that might arise with the use of our products in a clustered database environment. Troubleshooting methods in a complex environment often require cooperative work to resolve issues. NetIQ provides expertise to analyze, plan, and troubleshoot the NetIQ products. The customer must provide expertise to analyze, plan and troubleshoot any third-party products. We ask customers to reproduce issues or analyze behavior of their components in a non-clustered environment to help isolate potential cluster setup issues from NetIQ product issues.

6.7.5 Prerequisites for Installing the User Application in a Cluster Environment

You can install the User Application database in an environment supported by JBoss, WebLogic, and WebSphere clusters with the following considerations:

- ◆ The cluster must have a unique cluster partition name, multicast address, and multicast port. Using unique identifiers separates multiple clusters to prevent performance problems and anomalous behavior.
 - ◆ For each member of the cluster, you must specify the same port number for the listener port of the User Application database.
 - ◆ For each member of the cluster, you must specify the same hostname or IP address of the server hosting the User Application database.
- ◆ You must synchronize the clocks of the servers in a User Application cluster. If server clocks are not synchronized, sessions might time out early, causing HTTP session failover not to work properly.
- ◆ NetIQ recommends to not use multiple log ons across browser tabs or browser sessions on the same host. Some browsers share cookies across tabs and processes, so allowing multiple logons might cause problems with HTTP session failover (in addition to risking unexpected authentication functionality if multiple users share a computer).
- ◆ (Conditional) For JBoss clusters, you must start each server using the same partition name and partition UDP group. Each server in the cluster should use a unique engine ID. Also, all nodes in the JBoss cluster must access the same database instance. For more information about configuring the JBoss system properties, see [Section 27.2, “Preparing a JBoss Cluster for the User Application,” on page 222](#).
- ◆ (Conditional) By default, MySQL sets the maximum number of connections to 100. This number might be too small to handle the workflow request load in a cluster. If the number is too small, you might see the following exception:

```
(java.sql.SQLException: Data source rejected establishment of connection, message from server: "Too many connections.")
```

To increase the maximum number of connections, set the `max_connections` variable in `my.cnf` to a number greater than 100.

For more information about configuring the User Application in a cluster environment, see [Chapter 27, “Preparing a Cluster Environment for Use with the User Application,” on page 221](#) and the “Clustering” section of the *User Application: Administration Guide*.

6.7.6 System Requirements for Installing the User Application and Roles Based Provisioning Module

This section provides requirements to help you set up the server hosting the User Application and RBPM.

Category	Requirement
Processor	Pentium* III 600MHz, at a minimum
Disk Space	<ul style="list-style-type: none">◆ 320 MB for data◆ Enough space for the content of supporting applications, such as the database and application server logs

Category	Requirement
Memory	512 MB for the JBoss Application Server
Operating System	<p>One of the following operating systems, at a minimum:</p> <ul style="list-style-type: none"> ◆ Red Hat Enterprise 6.2 (32-bit or 64-bit) ◆ Red Hat 5.7 (32-bit or 64-bit) ◆ SUSE Linux Enterprise Server 11 SP1 (32-bit or 64-bit) ◆ SUSE Linux Enterprise Server 10 SP4 (32-bit or 64-bit) ◆ Windows Server 2008 R2 SP1 (64-bit) ◆ Windows Server 2008 SP2 (32-bit or 64-bit) ◆ Windows Server 2003 (32-bit or 64-bit) <p>NOTE: (Conditional) If you run the JBoss application server, you can also use one of the following operating systems:</p> <ul style="list-style-type: none"> ◆ Open Enterprise Server 2015 (64-bit) ◆ Open Enterprise Server 11 (64-bit) ◆ Open Enterprise Server 2 SP3 (32-bit or 64-bit)
Virtualization Systems	<p>One of the following systems running a supported operating systems:</p> <ul style="list-style-type: none"> ◆ Red Hat Enterprise Linux Virtualization (64-bit) ◆ VMware ESXi Workstation 6.5 ◆ VMware ESXi 5.0 (32-bit or 64-bit) ◆ VMware ESXi 4.1 (32-bit or 64-bit) ◆ VMware ESXi 4.0 (32-bit or 64-bit) ◆ VMware ESX 4.0 (32-bit or 64-bit) ◆ Windows Sever 2008 R2 Virtualization with Hyper-V (32-bit or 64-bit) ◆ Xen Virtual Machine running SLES 10 or SLES 11 as a guest operating system in para-virtualized mode
Application Server	<ul style="list-style-type: none"> ◆ IBM WebSphere 7.0 with IBM J9 VM (build 2.4, J2RE 1.6.0) and Fix Pack 7 ◆ JBoss Enterprise 5.1.2 with Java Development Kit (JDK) or Java Runtime Environment (JRE) 1.6.0_31 ◆ JBoss Community Edition 5.10 with JDK or JRE 1.6.0_31 ◆ Oracle WebLogic 10.3 (11gR1) with JRockit JVM 1.6.0_17 <p>NOTE: NetIQ provides the JBossPostgreSQL utility for installing the Community Edition of JBoss Application Server and PostgreSQL in your test environment.</p>
Database	<ul style="list-style-type: none"> ◆ IBM DB2 9.5b (for use with the WebSphere application server) ◆ Microsoft SQL Server 2008 ◆ MySQL 5.1 (for use with the JBoss Enterprise application server) ◆ Oracle 11gR2 ◆ PostgreSQL 8.4.3 and 9 (for use in your test environment)
Port	8180

Category	Requirement
Browser	<p>One of the following Internet browsers:</p> <ul style="list-style-type: none"> ◆ FireFox 9 is certified on: <ul style="list-style-type: none"> ◆ Windows XP with SP3 ◆ Windows 7 ◆ SUSE Linux Enterprise Desktop 11 ◆ SUSE Linux Enterprise Server 11 ◆ Novell OpenSUSE 11.2 ◆ Apple Mac ◆ Internet Explorer 8 is certified on Windows XP with SP3 ◆ Internet Explorer 9 is certified on Windows 7 <p>NOTE: For Internet Explorer browsers, the XML DOM (ActiveX control) from Microsoft Corporation is required for the Identity Manager Roles Based Provisioning Module 4.01 to work correctly. The version number of the XML DOM depends on the version of Internet Explorer being used.</p>
OpenXDAS	<p>0.8.345</p> <p>NOTE: (Conditional) For servers running SLES 10, you must have the following versions:</p> <ul style="list-style-type: none"> ◆ openxdas-0.8.351-1.1.i586.rpm ◆ openxdas-0.8.351-1.1.x86_64.rpm
Domain Services for Windows	OES 2 SP1
Password Management Challenge Response	NMAS Challenge Response Login Method version: 2770 Build: 20080603, at a minimum

6.8 Prerequisites for Installing the Identity Information Warehouse

The Identity Information Warehouse consists of two components: the Reporting Module and an event auditing service. You can use any application for auditing, such as NetIQ Sentinel. However, this document lists the requirements for the NetIQ Event Auditing Service (EAS).

- ◆ Install and configure RBPM before installing the Information Warehouse. For more information, see [Chapter 22, “Main Checklist for Installing RBPM and the User Application,”](#) on page 201.
- ◆ Install the User Application driver. For more information, see [Section 25.1, “Creating the User Application Driver,”](#) on page 213.
- ◆ Assign the Report Administrator role to any users that you want to be able to access reporting functionality.
- ◆ Install the event auditing service before the Reporting Module or the reporting drivers.
- ◆ The reporting functionality relies on the following drivers:
 - ◆ Identity Manager Driver for Data Collection Service
 - ◆ Identity Manager Manged System Gateway Driver

For more information about installing these drivers, see [Chapter 34, “Managing the Drivers for Reporting,”](#) on page 311.

- ◆ Ensure that all servers in your Identity Manager environment are set to the same time, particularly the servers for the Warehouse and EAS components. If you do not synchronize the time on your servers, some reports might be empty when executed. For example, this issue can affect data related to new users when the servers hosting the Identity Manager engine and the Warehouse have different time stamps. If you create and then modify a user, the reports are populated with data.

6.8.1 Prerequisites for the Event Auditing Service

When installing EAS, consider the following prerequisites:

- ◆ You must have Openssl libraries, usually `libssl.so.0.9.8` and `libcrypto.so.0.9.8`. Also, the version of the `.so` files should match. If they do not match, create a soft-link.
 - ◆ (Conditional) On RHEL 6.x computers, by default these libraries are in either the `/usr/lib` or `/usr/lib64` directory. The system might also use a bundled upgrade version of the files. For example:
 - ◆ `libssl.so.1.0.0`
 - ◆ `ln -s libssl.so.1.0.0 libssl.so.0.9.8`
 - ◆ `ln -s libcrypto.so.1.0.0 libcrypto.so.0.9.8`
 - ◆ (Conditional) On RHEL 5.x computers, ensure that you have the following libraries, located by default in either the `/lib` or `/lib64` directory:
 - ◆ `ln -s libssl.so.0.9.8e libssl.so.0.9.8`
 - ◆ `ln -s libcrypto.so.0.9.8e libcrypto.so.0.9.8`
- ◆ KornShell must be installed because the EAS installation scripts use KornShell, which is located by default at `/bin/kshis`. KornShell is usually bundled with all of the Linux operating system environments.

6.8.2 Prerequisites for the Reporting Module

When installing the Reporting Module, consider the following prerequisites:

- ◆ You cannot install the Reporting Module on a server in a clustered environment.
- ◆ The Reporting Module must have an exclusive EAS running on a separate Linux computer. You cannot have multiple reporting instances communicating with a single EAS environment.
- ◆ You can install the Reporting Module on the same computer that runs the User Application. For more information about the User Application, see [Section 6.7.1, “Considerations for Installing the User Application and Roles Based Provisioning Module,”](#) on page 69.

6.8.3 System Requirements for the Reporting Module

The Reporting Module can run on a JBoss, WebSphere, and WebLogic application server.

Category	Requirement
Processor	Pentium* III 600MHz, at a minimum

Category	Requirement
Operating System	<p>One of the following operating systems, at a minimum:</p> <ul style="list-style-type: none"> ◆ Open Enterprise Server 2015 (64-bit) ◆ Open Enterprise Server 11 SP1 (32-bit and 64-bit) ◆ Open Enterprise Server 2 SP3 (32-bit and 64-bit) ◆ Red Hat Enterprise 6.0 (32-bit or 64-bit) ◆ Red Hat 5.7 (32-bit or 64-bit) ◆ SUSE Linux Enterprise Server 11 SP1 (32-bit or 64-bit) ◆ SUSE Linux Enterprise Server 10 SP4 (32-bit or 64-bit) ◆ Windows Server 2008 R2 SP1 (32-64-bit) ◆ Windows Server 2008 SP2 (32-bit or 64-bit) ◆ Windows Server 2003 SP2 (32-bit or 64-bit)
Virtualization Systems	<p>One of the following systems running a supported operating systems:</p> <ul style="list-style-type: none"> ◆ Red Hat Enterprise Linux Virtualization (64-bit) ◆ VMware ESXi Workstation 6.5 ◆ VMware ESXi 5.0 (32-bit or 64-bit) ◆ VMware ESXi 4.1 (32-bit or 64-bit) ◆ VMware ESXi 4.0 (32-bit or 64-bit) ◆ VMware ESX 4.0 (32-bit or 64-bit) ◆ Windows Sever 2008 R2 Virtualization with Hyper-V (32-bit or 64-bit) ◆ Xen Virtual Machine running SLES 10 or SLES 11 as a guest operating system in para-virtualized mode
Application Server	<ul style="list-style-type: none"> ◆ IBM WebSphere 7.0 with IBM J9 VM (build 2.4, J2RE 1.6.0) ◆ JBoss Enterprise 5.1.2 with Java Runtime Environment (JRE) 1.6.0_31 ◆ JBoss Community Edition 5.10 with JRE 1.6.0_31 ◆ Oracle WebLogic 10.3.5 (11gR1) with JRockit JVM 1.6.0_05 <p>NOTE: NetIQ provides the JBossPostgreSQL utility for installing the Community Edition of JBoss Application Server and PostgreSQL in your test environment.</p>
Software	<p>All of the following products:</p> <ul style="list-style-type: none"> ◆ PostgreSQL 8.4.3 ◆ eDirectory 8.8.7 with Identity Manager 4.0.2 ◆ Roles Based Provisioning Module 4.0.2
Web Browser	<ul style="list-style-type: none"> ◆ Firefox 9 ◆ Internet Explorer 9 ◆ Internet Explorer 8

6.8.4 System Requirements for the Event Auditing Service

This section provides requirements to help you set up the server hosting EAS.

Category	Requirement
Processor	Pentium* III 600MHz, at a minimum
Operating System	One of the following operating systems, at a minimum: <ul style="list-style-type: none">♦ Red Hat Enterprise 6.0 (32-bit or 64-bit)♦ SUSE Linux Enterprise Server 11 (32-bit or 64-bit) with the ksh installed

6.9 Prerequisites and Requirements for Installing Role Administration

NetIQ provides two Web-based components that allow your business and security analysts to manage user roles and resources:

- ♦ Identity Manager **Catalog Administrator**
- ♦ Identity Manager **Role Mapping Administrator**

6.9.1 Prerequisites and System Requirements for Catalog Administrator

When installing Catalog Administrator, consider the following prerequisites and system requirements:

- ♦ To use Catalog Administrator, you must install Identity Manager Home. For more information, see [Part X, “Installing Identity Manager Home and the Provisioning Dashboard,” on page 381](#).
- ♦ Catalog Administrator has the same hardware and software requirements as Identity Manager Home. For more information, see [Section 6.10.2, “System Requirements for Installing Identity Manager Home,” on page 84](#).

6.9.2 Prerequisites for Role Mapping Administrator

When installing Role Mapping Administrator, consider the following prerequisites:

- ♦ Install a supported version of the following Identity Manager components:
 - ♦ Identity Vault
 - ♦ Identity Manager engine
 - ♦ Roles Based Provisioning Module
- ♦ Role Mapping Administrator is a Web-based application. You can install the infrastructure for the application on the same server that hosts the Identity Manager engine or on a separate server.
- ♦ You must connect Role Mapping Administrator to the Identity Vault.
 - ♦ For more information about the ways that the two components interact, see [Section 6.9.4, “Understanding How Role Mapping Administrator Interacts with the Identity Vault,” on page 82](#).
 - ♦ For more information about connecting the two components, see [Section 38.3, “Connecting Role Mapping Administrator to the Identity Vault,” on page 346](#).

- ◆ You can install one or more of the Identity Manager drivers to retrieve authorizations from managed systems.
 - ◆ You must use drivers supported by Identity Manager 3.6.1, 4.0, or later. For more information about installing the drivers, see the appropriate driver guides in [the NetIQ documentation \(https://www.netiq.com/documentation/idm402drivers/\)](https://www.netiq.com/documentation/idm402drivers/).
 - ◆ To manage the drivers, you must have previously installed Designer and the appropriate plug-ins for iManager.
 - ◆ For more information about setting up the drivers, see [Section 38.4, “Configuring the Drivers for Role Mapping Administrator,” on page 347.](#)
- ◆ You must configure at least one user account that can log on to Role Mapping Administrator to manage and configure other users.
 - ◆ For more information about the required permissions, see [Section 6.9.3, “Understanding Permissions Required for Role Mapping Administrator Users,” on page 81.](#)
 - ◆ For more information about creating an authorized account, see [Section 36.2, “Setting Permissions for Role Mapping Administrator,” on page 338.](#)
- ◆ (Conditional) To use Access Manager as a single sign-on method for users logging in to Role Mapping Administrator, your environment must meet the following requirements:
 - ◆ Access Manager 3.1 or later installed. For more information, see [Novell Access Manager 3.1 SP2 Installation Guide \(http://www.novell.com/documentation/novellaccessmanager31/installation/data/bookinfo.html\)](http://www.novell.com/documentation/novellaccessmanager31/installation/data/bookinfo.html).
 - ◆ Time must be synchronized among the Access Manager Identity server, Role Mapping Administrator, and the Identity Vault.
 - ◆ Your DNS server must have a DNS record for Role Mapping Administrator. Access Manager uses the DNS name to handle requests.
- ◆ (Conditional) To audit Role Mapping Administrator, you must have the Identity Information Warehouse installed in your environment and configured to capture the events. For more information about configuring the Identity Information Warehouse, see the [Identity Manager Reporting Guide \(http://www.novell.com/documentation/idm40/pdfdoc/reporting.pdf\)](http://www.novell.com/documentation/idm40/pdfdoc/reporting.pdf).
 You must also configure Role Mapping Administrator for auditing. For more information, see [Section 40.1, “Enabling Auditing of Role Mapping Administrator,” on page 367.](#)

6.9.3 Understanding Permissions Required for Role Mapping Administrator Users

You must have at least one authorized account that can log on to Role Mapping Administrator to manage and configure other users. This administrative account needs the following minimal rights:

- ◆ Browse entry rights, which allows the user to select objects in the configuration panel of Role Mapping Administrator. For example, the Root User container, Driver Discovery DN, and the User Application driver DN.
- ◆ Browse entry and read rights on the users contained within the Root User container defined in the configuration panel of Role Mapping Administrator. The list of potential role owners is derived by these rights.
- ◆ Browse entry rights on the active Driver Set object that is located under the Driver Discovery DN as defined in Role Mapping Administrator configuration panel.
- ◆ Inherited browse rights and read attribute rights on the drivers that participate in role mapping. Role Mapping Administrator needs access to the entitlements and entitlement configuration objects that are contained within the drivers that participate in role mapping.

- ◆ Inherited browse entry and read attribute rights on the User Application driver. Role Mapping Administrator needs access to DAL category definitions, role configuration objects, and role definition containers.
- ◆ Inheritable supervisor rights to the RoleDefs.RoleConfig.AppConfig, ResourceDefs.RoleConfig.AppConfig, and ResourceAssociations.RoleConfig.AppConfig containers within the User Application driver. These rights allow the user to add, modify, and delete resources. Rights can be pared down as needed.

NetIQ recommends creating a specific user for managing Role Mapping Administrator. Basically, you create an authorized user that is a member of the Role Manager role or the Role Module Administrator role in RBPM. These roles grant the user a specific set of rights in the Identity Vault and specific role assignments in RBPM.

All other users that use Role Mapping Administrator should have their rights limited to match their job duties. You can restrict rights for all other users by assigning them to roles with restricted rights and restricting their rights in the Identity Vault.

Authorized users can perform only the tasks associated with their assigned roles:

Role	Allowed Operations in Role Mapping Administrator
roleAdministrator, resourceAdministrator	Unrestricted access to create, edit, and delete mappings
roleAdministrator, resourceManager roleManager, resourceAdministrator	Read-only access to roles and mappings in Role Mapping Administrator
roleManager, resourceManager	

For more information about creating an authorized account, see [Section 36.2, “Setting Permissions for Role Mapping Administrator,” on page 338](#).

6.9.4 Understanding How Role Mapping Administrator Interacts with the Identity Vault

Role Mapping Administrator requires access to the Identity Vault to perform the following types of operations in the Identity Vault:

- ◆ Authenticating users who log on to Role Mapping Administrator and establishing their authorization level. The users should have both Resource Administrator and Role Administrator roles.
- ◆ Retrieving roles information to display if the authenticated user is a Role Module Administrator. If the authenticated user is a Role Manager, Role Mapping Administrator uses the user’s credentials to display roles.
- ◆ Creating resources with the selected authorization/entitlement and mapping them with the Identity Vault role.
- ◆ Accessing information stored on the Identity Manager driver object to build the queries required to retrieve authorizations from managed systems.
- ◆ Sending the queries to the Identity Manager drivers.
- ◆ Creating, editing, and deleting roles.

Role Mapping Administrator database does not store Identity Manager roles. Instead, Role Mapping Administrator reads and displays the roles directly from the Identity Vault. For more information about connecting Role Mapping Administrator to the Identity Vault, see [Section 38.3, “Connecting Role Mapping Administrator to the Identity Vault,”](#) on page 346.

6.9.5 System Requirements for Installing Role Mapping Administrator

This section provides requirements to help you set up the server hosting Role Mapping Administrator.

Category	Requirement
Operating System for Role Mapping Administrator structure	<p>One of the following operating systems, at a minimum:</p> <ul style="list-style-type: none"> ◆ Open Enterprise Server 2015 (64-bit) ◆ Open Enterprise Server 11 SP1 (64-bit) ◆ Red Hat 6.2 (32-bit or 64-bit) ◆ Red Hat 5.4 (32-bit or 64-bit) ◆ SUSE Linux Enterprise Server 11 SP1 (32-bit or 64-bit) ◆ SUSE Linux Enterprise Server 10 SP4 (32-bit or 64-bit) ◆ Windows Server 2008 R2 (64-bit) ◆ Windows Server 2008 SP2 (32-bit or 64-bit) ◆ Windows Server 2003 SP2 (32-bit)
Operating System Hotfixes	<p>Before installing Identity Manager, NetIQ recommends that you apply the latest operating system patches according to the manufacturer’s automated update facility.</p>
Web Browser	<p>Any of the following Web browsers:</p> <ul style="list-style-type: none"> ◆ Firefox 10 ◆ Internet Explorer 9 ◆ Internet Explorer 8
Java	<p>Sun JRE 1.6</p>

6.10 Prerequisites and Requirements for Installing Identity Manager Home and the Provisioning Dashboard

Identity Manager Home (Home) is a Web-based application that allows Identity Manager users and administrators to access all existing functionality in RBPM and the User Application. The Provisioning Dashboard is browser-based interface that provides a personalized view of each user’s permissions, tasks, and requests. Identity Manager Home links to the locations on each user’s Dashboard.

6.10.1 Prerequisites for Installing Identity Manager Home

Before you install and use Home and the Provisioning Dashboard, consider the following prerequisites:

- ◆ Install a supported version of the following Identity Manager components:
 - ◆ Designer
 - ◆ Identity Vault
 - ◆ Identity Manager engine
 - ◆ Remote Loader
 - ◆ Roles Based Provisioning Module

For more information about required versions and patches for these components, see “[System Requirements](https://www.netiq.com/documentation/idm402/idmhome-releasenotes/data/idmhome-releasenotes.html#b149h4pv)” (<https://www.netiq.com/documentation/idm402/idmhome-releasenotes/data/idmhome-releasenotes.html#b149h4pv>) in the *NetIQ Identity Manager Home and Provisioning Dashboard 4.0.2 Release Notes*.

- ◆ Install Identity Manager Home on a server running a supported version of JBoss application server.
- ◆ Create a single sign-on access (SSO) process using One SSO Provider (OSP). Identity Manager Home requires SSO for authentication with Identity Manager. For more information, see [Section 42.4, “Configuring Single Sign-on Access for Identity Manager Home,” on page 394](#).

NOTE: After you enable SSO in your Identity Manager environment, users can no longer access the User Application as a guest or anonymous user. Users are instead prompted to log on to the user interface.

- ◆ (Conditional) To run reports from Home and the Provisioning Dashboard, you must have the components for the Information Warehouse installed in your environment. For more information, see [Part VIII, “Installing the Identity Information Warehouse,” on page 293](#).
- ◆ (Optional) NetIQ recommends that you enable Secure Sockets Layer (SSL) protocol for communication between the Identity Manager components, including Identity Manager Home. To use SSL protocol, you must enable SSL in your environment and specify HTTPS in the URL for Identity Manager Home. For information about enabling SSL, see “[Enabling SSL in a Production Environment](#)” in the *User Application: Administration Guide*.
- ◆ Ensure that you have all necessary Identity Manager drivers installed before running Home or the Provisioning Dashboard.
- ◆ For users to access Home and the Provisioning Dashboard, you must enable cookies on all browsers. The products do not work when cookies are disabled.

6.10.2 System Requirements for Installing Identity Manager Home

This section provides requirements to help you set up the server hosting Identity Home and Provisioning Dashboard Web services.

NOTE: These hardware and software requirements also apply to Catalog Administrator. For more information, see [Section 6.9.1, “Prerequisites and System Requirements for Catalog Administrator,” on page 80](#).

Category	Requirement
Processor	1 GHz, at a minimum
Disk Space	1 GB
Memory	512 MB (1 GB recommended)
Video Resolution	1024x768 (1280x1025 recommended)
Operating System	One of the following operating systems, at a minimum: <ul style="list-style-type: none"> ◆ Red Hat Enterprise Linux 6 (64-bit) ◆ Red Hat Enterprise Linux 5 (64-bit) ◆ SUSE Linux Enterprise Server 11 SP1 (32-bit or 64-bit)
Operating System Hotfixes	Before installing Identity Manager, NetIQ recommends that you apply the latest operating system patches according to the manufacturer's automated update facility.
Application Server	JBoss AS 5.1 (for Identity Manager Home)
Database	One of the following databases, at a minimum: <ul style="list-style-type: none"> ◆ Microsoft SQL Server 2008 R2 ◆ Microsoft SQL Server 2008 ◆ MySQL 5.1 ◆ Oracle 11gR2 ◆ PostgreSQL 9.0 ◆ PostgreSQL 8.4.3
Additional Software Components	Java 2 Platform Standard Edition Development version 1.7 or later (JDK or JRE) from Sun (Oracle)

Category	Requirement
Web Browser	<p>Desktop Computer:</p> <ul style="list-style-type: none"> ◆ Apple Safari 7.0.1 ◆ Google Chrome 31 or later ◆ Microsoft Internet Explorer 10 ◆ Microsoft Internet Explorer 9 ◆ Mozilla Firefox 21 or later <p>NOTE: If you use Internet Explorer 9 to access Identity Manager Home and the Provisioning Dashboard and set the Document Mode to Quirks Mode, the browser might not display the user interfaces correctly. For more information on this issue, see the NetIQ Identity Manager Home and Provisioning Dashboard Release Notes (https://www.netiq.com/documentation/idm402/idmhome-releasenotes/data/idmhome-releasenotes.html).</p> <p>iPad:</p> <ul style="list-style-type: none"> ◆ Apple Safari ◆ Google Chrome 31 or later <p>NOTE: To access Identity Manager Home and the Provisioning Dashboard, the browser must have cookies enabled. If cookies are disabled, the product does not work.</p>

6.11 Prerequisites and Requirements for Installing Analyzer

Analyzer is a thick client component that you install on a workstation. You can use Analyzer to examine and clean the data in the connected systems that you want to add to your Identity Manager solution. By using Analyzer during the planning phase, you can see what changes need to be made and how best to make those changes.

When you install Analyzer, ensure that you install an appropriate package that contains the `/usr/lib/libpng12.so.0` library. Also, the following requirements help you set up the server hosting Analyzer:

Category	Requirement
Processor	1 GHz, at a minimum
Memory	512 MB (1 GB recommended)
Video Resolution	1024x768 (1280x1025 recommended)

Category	Requirement
Operating System	<p>One of the following operating systems, at a minimum:</p> <ul style="list-style-type: none"> ◆ openSUSE 11.2 (32-bit or 64-bit) ◆ openSUSE 10.3 (32-bit or 64-bit) ◆ SUSE Linux Enterprise Server 11 SP1 (32-bit or 64-bit) ◆ SUSE Linux Enterprise Server 10 SP4 (32-bit or 64-bit) ◆ SUSE Linux Enterprise Desktop 11 SP2 (32-bit or 64-bit) ◆ SUSE Linux Enterprise Desktop 10 SP4 (32-bit or 64-bit) ◆ Windows Server 2008 R2 SP1 (64-bit) ◆ Windows Server 2008 SP2 (32-bit and 64-bit) ◆ Windows 7 SP1 (32-bit and 64-bit) ◆ Windows Server 2003 SP2 (32-bit) ◆ Windows XP Professional SP3 (32-bit)
Virtualization Systems	<p>One of the following systems running a supported operating system as the guest operating system unless otherwise noted:</p> <ul style="list-style-type: none"> ◆ VMware Workstation 6.5, supported on SLES 11 SP1 as the base operating system ◆ VMware ESXi 5.0 (32-bit or 64-bit), supported on SLES 11 SP2 as the base operating system ◆ VMware ESXi 4.0 (32-bit or 64-bit), supported on SLES 11 SP2 as the base operating system ◆ VMware ESX 4.0 (32-bit or 64-bit), supported on SLES 11 SP2 as the base operating system ◆ Windows Server 2008 R2 Virtualization with Hyper-V (32-bit or 64-bit) ◆ Xen Virtual Machine running SLES 10, SLES 11, or Windows 2008 R2 as a guest operating system in para-virtualized mode and SLES 10 SP2 as the host operating system
Operating System Hotfixes	<p>NetIQ recommends that you apply the latest operating system patches according to the manufacturer's automated update facility before you install Identity Manager.</p>
Additional Software Components	<ul style="list-style-type: none"> ◆ compat-2008.5.6-6.1.i586.rpm (32-bit system) or compat-32bit-2008.5.6-6.1.x86_64.rpm (64-bit system) ◆ Gettext Utility (on Linux computers only)

7 Installing Designer

You can install Identity Manager Designer using an executable file, binary file, or in text mode, depending on the target computer. You can also perform a silent installation. After you download and unzip or unpack the Designer installation kit, the following programs are available for installing Designer:

- ♦ **Linux computers:** `IDM4.0.2_Lin/products/Designer/install`
- ♦ **Windows computers:** `IDM4.0.2_Win:\products\Designer\install.exe`

This section provides information about installing Designer in a new environment. For more information about upgrading Designer, see [Section 47.5.1, “Upgrading Designer,” on page 425](#).

Several components of Identity Manager require packages in Designer. When you install Designer, the installation program automatically adds several packages to your new project.

NetIQ recommends that you perform the steps in the following checklist:

	Checklist Items
<input type="checkbox"/>	1. Review product architecture information to learn about the interaction among Identity Manager components. For more information, see Section 2.1, “Designer for Identity Manager,” on page 23 .
<input type="checkbox"/>	2. Review the considerations for installing Designer to ensure that the computer meets the prerequisites. For more information, see Section 6.2, “Prerequisites and Requirements for Installing Designer,” on page 46 .
<input type="checkbox"/>	3. Ensure that the computer on which you are installing Designer meets the specified software and hardware requirements. For more information, see Section 6.2.2, “System Requirements for Installing Designer,” on page 46 .
<input type="checkbox"/>	4. To install Designer, see one of the following sections: <ul style="list-style-type: none">♦ “Using the Installation Command on Linux” on page 89♦ “Running the Windows Executable File” on page 90♦ “Using the Silent Installation Process” on page 90
<input type="checkbox"/>	5. Install the rest of the Identity Manager components.
<input type="checkbox"/>	6. (Optional) To start a project for your Identity Manager solution, see the Designer 4.0.2 for Identity Manager 4.0.2 Administration Guide .

7.1 Using the Installation Command on Linux

You can run the installation in text mode or execute the binary file. Enter one of the following commands from the directory containing the installation program:

- ♦ **Binary file:** `./install`
- ♦ **Text mode:** `./install -i console`

7.2 Running the Windows Executable File

- 1 Log on with an administrator account to the computer on which you want to install Designer.
- 2 Run the `install.exe` file.
- 3 Follow the steps in the wizard until the installation process completes.

7.3 Using the Silent Installation Process

You can use scripts to silently install Designer without user interaction. The `-i silent` option uses default parameter values for the installation unless you edit the `designerInstaller.properties` file.

- 1 Log on with an administrator account to the computer where you want to install Designer.
- 2 Navigate to the directory containing the installation program.
- 3 (Optional) To configure the installation directory and the language for Designer, complete the following steps.

3a Open the `designerInstaller.properties` file, by default in the following directory:

```
Path_to_unzipped_Designer_files/designer_install/  
designerInstaller.properties
```

3b In the properties file, modify the values for the following parameters:

USER_INSTALL_DIR

Specifies the path to the location where you want to install Designer. For example:

```
USER_INSTALL_DIR=/home/user/designer
```

If you specify a path that does not end with the `designer` directory, the Designer installation program automatically appends a `designer` directory.

SELECTED_DESIGNER_LOCALE

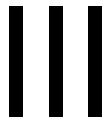
Specifies one of the following languages that you want Designer to launch after installation:

- ◆ `zh_CN` - Chinese Simplified
- ◆ `zh_TW` - Chinese Traditional
- ◆ `nl` - Dutch
- ◆ `en` - English
- ◆ `fr` - French
- ◆ `de` - German
- ◆ `it` - Italian
- ◆ `ja` - Japanese
- ◆ `pt_BR` - Portuguese Brazil
- ◆ `es` - Spanish

3c Save and close the properties file.

4 Run one of the following commands:

- ◆ **Linux:** `install -i silent -f Path\designerInstaller.properties`
- ◆ **Windows:** `install -i silent -f Path/designerInstaller.properties`



Installing the Identity Vault

This section guides you through the process of installing the required components for the Identity Vault, which stores information specific to Identity Manager, such as driver configurations, parameters, and policies. This section assumes that your Identity Vault uses a NetIQ eDirectory database. However, you can also use Active Directory or a similar directory service.

The installation files are located in the `products/eDirectory/processor_type/` directory within the `.iso` image file of the Identity Manager installation package. By default, the installation program installs the Identity Vault in the following locations:

- ♦ **Linux:** `/opt/novell/idm`
- ♦ **Windows:** `C:\Novell\IDM`

NetIQ recommends that you review the installation process before beginning. For more information, see [Chapter 8, “Main Checklist for Installing Identity Vault,”](#) on page 93.

8 Main Checklist for Installing Identity Vault

NetIQ recommends that you perform the steps in the following checklist:

	Checklist Items
<input type="checkbox"/>	1. Learn about the interaction among Identity Manager components. For more information, see Section 3.3.1, “Identity Vault,” on page 28.
<input type="checkbox"/>	2. Review the considerations for installing the Identity Vault to ensure that the computers meet the prerequisites. For more information, see Section 6.3, “Prerequisites and Requirements for Installing the Identity Vault,” on page 47.
<input type="checkbox"/>	3. Review the hardware and software requirements for the computers that will host the Identity Vault. For more information, see Section 6.3.10, “System Requirements for Installing Identity Vault,” on page 57.
<input type="checkbox"/>	4. Understand how to use escape characters when the names of containers in the Identity Vault include a period (“.”). For more information, see Section 9.1, “Using Escape Characters when a Container Name Includes a Period (“.”),” on page 95.
<input type="checkbox"/>	5. Understand how to use the Identity Vault in an environment that uses IPv6 addresses. For more information, see Section 9.3, “Using IPv6 Addresses on the Identity Vault Server,” on page 100.
<input type="checkbox"/>	6. Understand the ports required for LDAP communications. For more information, see Section 9.4, “Using LDAP to Communicate with the Identity Vault,” on page 102.
<input type="checkbox"/>	7. Ensure that you have installed a Service Location Protocol (SLP) service and that SLPDAs are stable or that you have configured a <code>hosts.nds</code> file. For more information, see Section 9.2, “Using OpenSLP or hosts.nds for Resolving Tree Names,” on page 95.
<input type="checkbox"/>	8. (Conditional) To install the Identity Vault as a non-root user, ensure that your environment meets the conditions for installation. For more information, see Section 6.3.2, “Considerations for Installing the Identity Vault as a Non-root User,” on page 49.
<input type="checkbox"/>	9. (Conditional) To install on a Linux server, see one of the following sections: <ul style="list-style-type: none">◆ To install as <code>root</code>, see Section 10.1, “Installing the Identity Vault as Root,” on page 107.◆ To install as a non-<code>root</code> user, see Section 10.2, “Installing the Identity Vault as a Non-root User,” on page 109.
<input type="checkbox"/>	10. (Conditional) To install on a Windows server, see one of the following sections: <ul style="list-style-type: none">◆ For a guided installation (wizard), see Section 11.1, “Using the Wizard to Install the Identity Vault on a Windows Server,” on page 111.◆ For a silent installation (unattended), see Section 11.2, “Silently Installing and Configuring the Identity Vault on a Windows Server,” on page 112.
<input type="checkbox"/>	11. (Optional) Exclude the DIB directory on your eDirectory server from any antivirus or backup software process.

	Checklist Items
<input type="checkbox"/>	12. (Optional) Back up your DIB directory. For more information, see “Backing Up and Restoring NetIQ eDirectory” (https://www.netiq.com/documentation/edir88/edir88/data/a2n4mb6.html) in the <i>NetIQ eDirectory 8.8 SP8 Administration Guide</i> .
<input type="checkbox"/>	13. Install the Identity Manager engine. For more information, see Chapter 14, “Installing the Identity Manager Engine,” on page 139.

9 Preparing to Install the Identity Vault

Your environment for the Identity Vault must be configured appropriately. For example, the server must have a method (a service or specified file) that can be used to resolve tree names in Identity Vault to server referrals. This section helps you prepare your environment before you install the Identity Vault.

9.1 Using Escape Characters when a Container Name Includes a Period (“.”)

You can add a Windows or Linux server that has a period in the server name to a directory tree. For example, `O=netiq.com` or `C=u.s.a.` However, if the names of your containers in the tree include a period (“.”), you must use escape characters. Review the following considerations:

- ◆ **Linux:**

- ◆ When specifying the Admin name, Admin context, and server context parameters, enclose the parameters in quotes.
- ◆ Escape the period in the container name with a backslash (“\”).
- ◆ For example, when installing the Identity Vault, enter the installation command:

```
ndsconfig new -a 'admin.netiq.com' -t netiq_tree -n  
'OU=servers.O=netiq\.com'
```

- ◆ **Windows:**

- ◆ Do not use a period at the beginning of a server name. For example, `.netiq`.
- ◆ Escape the period in the container name with a backslash (“\”). For example:

```
O=novell\.com
```

or

```
C=a\.b\.c
```

Include the escape characters when you enter a dotted admin name and context for utilities such as `iMonitor`, `iManager`, `DHost iConsole`, `DSRepair`, `Backup`, `DSMerge`, `DSLogin`, and `Idapconfig`. For example, when logging in to `iMonitor`, if the name of the O in your tree is `netiq.com`, enter `'admin.netiq\.com'` or `admin.netiq\.com`.

9.2 Using OpenSLP or hosts.nds for Resolving Tree Names

Before installing the Identity Vault infrastructure, the server should have a method (a service or specified file) that can be used to resolve tree names in Identity Vault to server referrals. NetIQ recommends using Service Location Protocol (SLP) services to resolve tree names. Previous versions of eDirectory included OpenSLP in the installation. However, starting with eDirectory 8.8, the

installation does not include OpenSLP. You must separately install an SLP service or use a `hosts.nds` file. If you use an SLP service, the directory agents for the service (SLPDAs) must be stable.

This section provides the following information:

- ♦ [Section 9.2.1, “Using a hosts.nds File to Resolve Tree Names,” on page 96](#)
- ♦ [Section 9.2.2, “Understanding OpenSLP,” on page 97](#)
- ♦ [Section 9.2.3, “Configuring SLP for the Identity Vault,” on page 99](#)

9.2.1 Using a hosts.nds File to Resolve Tree Names

The `hosts.nds` file is a static lookup table that Identity Vault applications use to search Identity Vault partitions and servers. It helps you avoid SLP multicast delays when SLP DA is not present in the network. For each tree or server, you must specify the following information in a single line in the `hosts.nds` file:

- ♦ **Server Name or Tree Name:** Tree names should end with a trailing dot (.).
- ♦ **Internet Address:** This can be a DNS name or IP address.
- ♦ **Server Port:** Optional, appended with a colon (:) to the Internet address.

You do not have to include an entry for the local server in the file, unless the server listens on a non-default NCP port.

To configure a hosts.nds file:

- 1 Create a new or open an existing `hosts.nds` file.
- 2 Add the following information:

```
partition_name.tree_name. host_name/ip-addr:port
server_name dns-addr/ip-addr:port
```

For example:

```
# This is an example of a hosts.nds file:
# Tree name Internet address/DNS Resolvable Name
CORPORATE. myserver.mycompany.com
novell.CORPORATE. 1.2.3.4:524

# Server name Internet address
CORPSEVER myserver.mycompany.com:524
```

- 3 (Optional) If you later decide to use SLP to resolve the tree name and ensure that the Identity Vault tree is available on the network, add the following text to the `hosts.nds` file:

```
/usr/bin/slptool findattrs services:ndap.novell///(svcname-ws==[treename or *]) "
```

For example, to search for the services whose `svcname-ws` attribute match with the value `SAMPLE_TREE`, enter the following command:

```
/usr/bin/slptool findattrs services:ndap.novell///(svcname-ws==SAMPLE_TREE) "
```

NOTE: Perform this action after you install SLP and the Identity Vault.

If you have a service registered with its `svcname-ws` attribute as `SAMPLE_TREE`, then the output will be similar to `service:ndap.novell:///SAMPLE_TREE`. Otherwise, you will not receive an output response.

9.2.2 Understanding OpenSLP

OpenSLP is an open-source implementation of the IETF Service Location Protocol Version 2.0 standard, which is documented in [IETF Request-For-Comments \(RFC\) 2608](http://www.ietf.org/rfc/rfc2608.txt?number=2608) (<http://www.ietf.org/rfc/rfc2608.txt?number=2608>).

The interface provided by OpenSLP source code is an implementation of another IETF standard for programmatically accessing SLP functionality, documented in [RFC 2614](http://www.ietf.org/rfc/rfc2614.txt?number=2614) (<http://www.ietf.org/rfc/rfc2614.txt?number=2614>).

To fully understand the workings of SLP, it is worth reading these documents and internalizing them. They are not necessarily light reading, but they are essential to the proper configuration of SLP on an intranet.

For more information on the OpenSLP project, see the [OpenSLP](http://www.OpenSLP.org) (<http://www.OpenSLP.org>) and the [SourceForge](http://sourceforge.net/projects/openslp) (<http://sourceforge.net/projects/openslp>) Web sites. The OpenSLP Web site provides several documents that contain valuable configuration tips. Many of these are incomplete at the time of this document's publication.

This section includes the following discussions about the use of SLP and how it relates to the Identity Vault:

- ♦ [“NetIQ Service Location Providers” on page 97](#)
- ♦ [“User Agents” on page 98](#)
- ♦ [“Service Agents” on page 98](#)
- ♦ [“Directory Agents” on page 99](#)

NetIQ Service Location Providers

The NetIQ version of SLP takes certain liberties with the SLP standard in order to provide a more robust service advertising environment, but it does so at the expense of some scalability.

For example, in order to improve scalability for a service advertising framework, you can limit the number of packets that are broadcast or multicast on a subnet. The SLP specification manages this by imposing restrictions on service agents and user agents regarding directory agent queries. The first directory agent discovered that services the desired scope is the one that a service agent (and consequently, local user agents) will use for all future requests on that scope.

The NetIQ SLP implementation actually scans all of the directory agents it knows about looking for query information. It assumes a 300-millisecond round trip time is too long, so it can scan 10 servers in about 3 to 5 seconds. This doesn't need to be done if SLP is configured correctly on the network, and OpenSLP assumes the network is in fact configured correctly for SLP traffic. OpenSLP's response timeout values are greater than that of NetIQ's SLP service provider, and it limits the number of directory agents to the first one that responds, whether or not that agent's information is accurate and complete.

User Agents

A user agent (UA) takes the physical form of a static or dynamic library that is linked to an application. It allows the application to query for SLP services. The user agent's job is to provide a programmatic interface for clients to query for services, and for services to advertise themselves. A user agent contacts a directory agent to query for registered services of a specified service class and within a specified scope.

User agents follow an algorithm to obtain the address of a directory agent to which queries will be sent. Once they obtain an address of a directory agent (DA) for a specified scope, they continue to use that address for that scope until it no longer responds, at which time they obtain another DA address for that scope. User agents locate a directory agent address for a specified scope by:

- 1 Checking to see if the socket handle on the current request is connected to a DA for the specified scope. If the request happens to be a multipart request, there may already be a cached connection present on the request.
- 2 Checking its local known DA cache for a DA matching the specified scope.
- 3 Checking with the local service agent (SA) for a DA with the specified scope (and adding new addresses to the cache).
- 4 Querying DHCP for network-configured DA addresses that match the specified scope (and adding new addresses to the cache).
- 5 Multicasting a DA discovery request on a well-known port (and adding new addresses to the cache).

The specified scope is "default," if not specified. That is, if no scope is statically defined in the SLP configuration file, and no scope is specified in the query, then the scope used is the word "default". It should also be noted that Identity Vault never specifies a scope in its registrations. If there is a statically configured scope, that scope becomes the default scope for all local UA requests and SA registrations in the absence of a specified scope.

Service Agents

Service agents take the physical form of a separate process on the host machine. In the case of Windows, `slpd.exe` runs as a service on the local machine. User agents query the local service agent by sending messages to the loop-back address on a well-known port.

The service agent's job is to provide persistent storage and maintenance points for local services that have registered themselves with SLP. The service agent essentially maintains an in-memory database of registered local services. In fact, a service cannot register with SLP unless a local SA is present. Clients can discover services with only a UA library, but registration requires an SA, primarily because an SA must reassert the existence of registered services periodically in order to maintain the registration with listening directory agents.

A service agent locates and caches directory agents and their supported scope list by sending a DA discovery request directly to potential DA addresses by:

- 1 Checking all statically configured DA addresses (and adding new ones to the SA's known DA cache).
- 2 Requesting a list of DA's and scopes from DHCP (and adding new ones to the SA's known DA cache).

- 3 Multicasting a DA discovery request on a well-known port (and adding new ones to the SA's known DA cache).
- 4 Receiving DA advertising packets that are periodically broadcast by DAs (and adding new ones to the SA's known DA cache).

Since a user agent always queries the local service agent first, this is important, as the local service agent's response will determine whether or not the user agent continues to the next stage of discovery (in this case DHCP-- see [Step 3](#) and [Step 4](#) in "User Agents" on page 98).

Directory Agents

The directory agent's job is to provide a long-term persistent cache for advertised services, and to provide a point of access for user agents to look up services. As a cache, the DA listens for SAs to advertise new services, and caches those notifications. Over a short time, a DA's cache becomes more full or more complete. Directory agents use an expiration algorithm to expire cache entries. When a directory agent comes up, it reads its cache from persistent storage (generally a hard drive), and then begins to expire entries according to the algorithm. When a new DA comes up, or when a cache has been deleted, the DA detects this condition and sends out a special notification to all listening SAs to dump their local databases so the DA can quickly build its cache.

In the absence of any directory agents, the UA will resort to a general multicast query that SAs can respond to, building a list of the requested services in much the same manner that DAs use to build their cache. The list of services returned by such a query is an incomplete and much more localized list than that provided by a DA, especially in the presence of multicast filtering, which is done by many network administrators, limiting broadcasts and multicasts to only the local subnet.

In summary, everything hinges on the directory agent that a user agent finds for a given scope.

9.2.3 Configuring SLP for the Identity Vault

The following parameters in the `%systemroot%/slp.conf` file control directory agent discovery:

```
net.slp.useScopes = comma-delimited scope list
net.slp.DAAddresses = comma-delimited address list
net.slp.passiveDADetection = <"true" or "false">
net.slp.activeDADetection = <"true" or "false">
net.slp.DAActiveDiscoveryInterval = <0, 1, or a number of seconds>
```

useScopes

Indicates which scopes the SA will advertise into, and which scopes queries will be made to in the absence of a specific scope on the registration or query made by the service or client application. Because Identity Vault always advertises into and queries from the default scope, this list will become the default scope list for all Identity Vault registrations and queries.

DAAddresses

Represents a comma-delimited list of dotted decimal IP addresses of DAs that should be preferred to all others. If this list of configured DAs does not support the scope of a registration or query, then SAs and UAs will resort to multicast DA discovery, unless such discovery is disabled.

passiveDADetection

Is `True` by default. Directory agents will periodically broadcast their existence on the subnet on a well-known port if configured to do so. These packets are termed DAAdvert packets. If this option is set to `False`, all broadcast DAAdvert packets are ignored by the SA.

activeDADetection

Is `True` by default. This allows the SA to periodically broadcast a request for all DAs to respond with a directed DAAvert packet. A directed packet is not broadcast, but sent directly to the SA in response to these requests. If this option is set to `False`, no periodic DA discovery request is broadcast by the SA.

DAActiveDirectoryInterval

Represents a try-state parameter. The default value is `1`, which is a special value meaning that the SA should only send out one DA discovery request upon initialization. Setting this option to `0` has the same effect as setting the `activeDADetection` option to `false`. Any other value is a number of seconds between discovery broadcasts.

These options, when used properly, can ensure an appropriate use of network bandwidth for service advertising. In fact, the default settings are designed to optimize scalability on an average network.

9.3 Using IPv6 Addresses on the Identity Vault Server

Identity Vault supports both IPv4 and IPv6 addresses. You can enable IPv6 addresses when you install the Identity Vault. If you upgrade from a previous version, you must manually enable IPv6 addresses.

Identity Vault also supports Dual IP stack, Tunneling, and Pure IPv6 transition methods. It supports only the global IP addresses. For example:

- ◆ `[::]`
- ◆ `[::1]`
- ◆ `[2015::12]`
- ◆ `[2015::12]:524`

You must specify IPv6 addresses within square braces `[]`. To use hostname instead of an IP address, you must specify the name in the `etc/hosts` file and associate it with the IPv6 address.

9.3.1 Using IPv6 Addresses on Linux Servers

You can use the `ndsconfig` utility to create trees with an IPv6 address, add servers with IPv6 addresses to existing trees, and specify LDAP URLs for IPv6. For more information about using the utility, see [Section 13.1, “Modifying the eDirectory Tree and Replica Server with the `ndsconfig` Utility,” on page 127](#).

In addition to the `ndsconfig` utility, you can perform other steps to configure the Identity Vault on a Linux computer that already supports IPv6 addresses:

- ◆ [“Enabling IPv6 Addresses on Existing or Upgraded eDirectory Servers” on page 101](#)
- ◆ [“Adding LDAP URLs for IPV6 on the LDAP Server Object” on page 101](#)

Enabling IPv6 Addresses on Existing or Upgraded eDirectory Servers

NOTE: You must add the IPv6 address to each configuration file, if the computer has multiple instances configured.

1 Open the `nds.conf` file, located by default in the `/etc/opt/novell/eDirectory/conf/` directory.

2 In the file, add the IPv6 interface address with the port number. For example:

```
n4u.server.interfaces=164.99.90.148@524, [2015::4]@524, [2015:1234:2345:3456:abcd:bcde:cdef:aaaa]@524
```

```
http.server.interfaces=164.99.90.148@8028, [2015::4]@8028, [2015:1234:2345:3456:abcd:bcde:cdef:aaaa]@8028
```

```
https.server.interfaces=164.99.90.148@8030, [2015::4]@8030, [2015:1234:2345:3456:abcd:bcde:cdef:aaaa]@8030
```

3 Restart `nds` using the following commands:

```
ndsmanage stopall  
ndsmanage startall
```

Adding LDAP URLs for IPV6 on the LDAP Server Object

If you do not specify the LDAP URLs when you initially configure the Identity Vault, you can use the `ldapconfig` command or `iManager` to add them to the `ldapInterfaces` attribute.

To add LDAP URLs from the command line:

You can use either the `ldapconfig set` or the `ldapconfig -s` command. Enter text similar to the following examples:

```
ldapconfig set "ldapInterfaces=ldap://[2015::3]:389,ldaps://[2015::3]:636"
```

```
ldapconfig -s  
"ldapInterfaces=ldap://[2015::3]:389,ldapInterfaces=ldaps://[2015::3]:636"
```

To add LDAP URLs in iManager:

- 1 In `iManager`, click **Roles and Tasks**.
- 2 Click **LDAP > LDAP Options**.
- 3 Click **View LDAP Server**, and then click the name of the LDAP Server object that you want to configure.
- 4 For **LDAP Interfaces**, click **Connections**, add **LDAP URLs**.
- 5 Click **Apply**, and then click **OK**.

9.3.2 Using IPv6 Addresses on Windows Servers

To use IPv6 addresses on a Windows server, you must select the **Enable IPv6** check box under **IPv6 Preference** during the installation. This option enables the NCP, HTTP, and HTTPS protocols for the IPv6 addresses. If you do not enable IPv6 addresses during the installation process, and then decide to use them later, you must run the setup program again. For more information, see [Chapter 11, "Installing the Identity Vault on a Windows Server,"](#) on page 111.

You can access iMontior over IPv6 addresses using the following link: `http://[2015::3]:8028/nds`.

9.4 Using LDAP to Communicate with the Identity Vault

When you install the Identity Vault, you must specify the ports that the LDAP server monitors so that it can service LDAP requests. As part of default configuration, the ports numbers for clear text and SSL/TLS are set to 389 and 636.

An LDAP Simple Bind requires only a DN and a password. The password is in clear text. If you use port 389, the entire packet is in clear text. Because port 389 allows clear text, the LDAP server services Read and Write requests to the Directory through this port. This openness is adequate for environments of trust, where spoofing does not occur and no one inappropriately captures packets. By default, this option is disabled during the installation.

The connection through port 636 is encrypted. TLS (formerly SSL) manages the encryption. A connection to port 636 automatically instantiates a handshake. If the handshake fails, the connection is denied.

NOTE: The installation program selects port 636 by default for SSL/TLS communications. This default selection might cause a problem for your LDAP server. If a service already loaded on the host server (before eDirectory was installed) uses port 636, you must specify another port. Installations earlier than eDirectory 8.7 treated this conflict as a fatal error and unloaded `nldap.nlm`. After eDirectory 8.7.3, the installation program loads `nldap.nlm`, places an error message in the `dstrace.log` file, and runs without the secure port.

During the installation process, you can configure Identity Vault to disallow clear passwords and other data. The **Require TLS for Simple Bind with Password** option discourages users from sending observable passwords. If you do not select this setting, users are unaware that others can observe their passwords. This option, which does not allow the connection, only applies to the clear-text port. If you make a secure connection to port 636 and have a simple bind, the connection is already encrypted. No one can view passwords, data packets, or bind requests.

Consider the following scenarios:

Require TLS for Simple Bind with Password Is Enabled

Olga is using a client that asks for a password. After Olga enters a password, the client connects to the server. However, the LDAP server does not allow the connection to bind to the server over the clear-text port. Everyone is able to view Olga's password, but Olga is unable to get a bound connection.

Port 636 Is Already Used

Your server is running Active Directory. Active Directory is running an LDAP program, which uses port 636. You install eDirectory. The installation program detects that port 636 is already used and doesn't assign a port number for the NetIQ LDAP server. The LDAP server loads and appears to run. However, because the LDAP server does not duplicate or use a port that is already open, the LDAP server does not service requests on any duplicated port.

To verify whether port 389 or 636 is assigned to the NetIQ LDAP server, run the ICE utility. If the *Vendor Version* field does not specify NetIQ, you must reconfigure LDAP Server for eDirectory and select a different port. For more information, see ["Verifying That the LDAP Server is Running"](https://www.netiq.com/documentation/edir88/edir88/data/ai8wt35.html) (<https://www.netiq.com/documentation/edir88/edir88/data/ai8wt35.html>) in the *NetIQ eDirectory 8.8 SP8 Administration Guide*.

Active Directory Is Running

When Active Directory is running and clear-text port 389 open, you can run the ICE command to port 389 and ask for the vendor version. The report displays **Microsoft***. You then reconfigure the NetIQ LDAP server by selecting another port, so that the eDirectory LDAP server can service LDAP requests.

iMonitor can also report whether port 389 or 636 is already open. If the LDAP server is not working, use iMonitor to identify details. For more information, see ["Verifying That the LDAP Server is Running"](https://www.netiq.com/documentation/edir88/edir88/data/ai8wt35.html) (<https://www.netiq.com/documentation/edir88/edir88/data/ai8wt35.html>) in the *NetIQ eDirectory 8.8 SP8 Administration Guide*.

9.5 Installing NCI Manually on Workstations that have Management Utilities

You must install NCI on every workstation that uses a management utility such as iManager. For more information about using NCI with the Identity Vault, see [Section 6.3.1, "Considerations for Installing the Identity Vault,"](#) on page 48.

9.5.1 Installing NCI on Linux Servers

Use `nds-install` and select the NCI option. By default, you can find the installation file in the `products\eDirectory\processor_type\setup\` directory. NetIQ recommends installing NCI as `root` because the required NCI packages are used system-wide. However, if necessary you can delegate access to a different account using `sudo` and use that account to install the NCI packages.

NOTE: Since eDirectory 8.8 Service Pack 3, NetIQ has allowed you to install both 32-bit and 64-bit versions of eDirectory on a single system. If you installed both versions on a server, you must also install the 32-bit and 64-bit versions of NCI.

This section describes the following activities:

- ♦ ["Installing NCI as Root User" on page 103](#)
- ♦ ["Installing NCI as a Non-root User" on page 104](#)

Installing NCI as Root User

To install NCI, enter both of the following commands:

```
32-bit: rpm -ivh NCI_rpm_absolute_path/nici-2.7.7-0.02.i586.rpm
64-bit: rpm -ivh NCI_rpm_absolute_path/nici64-2.7.7-0.02.x86_64.rpm
```

NOTE: Since eDirectory 8.8 Service Pack 3, NetIQ has allowed you to install both 32-bit and 64-bit versions of eDirectory on a single system. If you installed both versions on a server, you must also install the 32-bit and 64-bit versions of NICI.

Installing NICI as a Non-root User

Non-`root` users can use the `sudo` utility to install NICI. `sudo` (superuser do) allows a root user to give certain users the ability to run some commands as `root`. A `root` user can do this by editing the `/etc/sudoers` configuration file and adding appropriate entries in it.

WARNING: `sudo` enables you to give limited root permissions to non-`root` users.

- 1 Log on with a `sudo` account to the server where you want to install NICI.
- 2 Execute the following command:

```
sudo rpm -ivh nici_rpm_file_name_with_path
```

- 3 Initialize NICI with the following command:

```
ln -sf /var/opt/novell/nici /var/novell/nici
```

- 4 (Optional) To verify that NICI is set to server mode, enter the following command:

```
/var/opt/novell/nici/set_server_mode
```

9.5.2 Installing NICI on Windows Servers

To install NICI on a Windows server, use the `NICI_wx64.msi` file, by default in the `products\eDirectory\processor_type\windows\processor_type\nici` folder. You can run the file as a guided process (wizard) or a silent installation.

9.6 Installing NMAS Client Software

You must install the NetIQ Modular Authentication Service (NMAS) client software on each client workstation where you want to use the NMAS login methods. You specify the login methods when installing the Identity Vault.

9.6.1 Installing and Configuring NMAS Client Software on Linux Servers

The Identity Vault installation utility (`nds-install`) includes NMAS as a component of the installation process. NetIQ provides two utilities that you can use to configure NMAS:

ndsconfig utility

Use this utility to configure both the Identity Vault and NMAS after you install Identity Vault. This utility does not install the NMAS login methods.

nmasinst utility

Use this utility if you have already configured Identity Vault and want to configure NMAS only. This utility installs the NMAS login methods.

NOTE: Before installing the NMAS login methods, you must configure the Identity Vault using the `ndsconfig` utility. Also, you must have administrative rights to the tree.

Configuring NMAS

This process creates objects in the Security container that NMAS needs, and installs the LDAP extensions for NMAS on the LDAP Server object in eDirectory.

The first time that you install NMAS in a tree, you must be logged in with enough rights to create objects in the Security container. However, subsequent installations can be done by container administrators with read-only rights to the Security container. `nmasinst` will verify that the NMAS objects exist in the Security container before it tries to create them.

The `nmasinst` utility does not extend the schema. Instead, the Identity Vault installation includes the NMAS schema as part of the base eDirectory schema.

To configure NMAS and create NMAS objects in eDirectory:

- 1 Enter the following at the server console command line:

```
nmasinst -i admin.context tree_name
```

- 2 Enter the password.

Installing NMAS Login Methods

You can use the `nmasinst` utility to install NMAS login methods. You must specify `config.txt` file for the login method that you want to install. Each login method has a `config.txt` file.

At the server console command line, enter the following command:

```
nmasinst -addmethod admin.context tree_name config.txt_path
```

For example, to use the `-addmethod` command, enter:

```
nmasinst -addmethod admin.netiq MY_TREE ./nmas-methods/novell/Simple Password/config.txt
```

If the login method already exists, the `nmasinst` utility will update it.

For more information, see “Managing Login and Post-Login Methods and Sequences” (<http://www.netiq.com/documentation/nmas33/admin/data/a53vj9a.html>) in the *NetIQ Modular Authentication Services Administration Guide*.

9.6.2 Installing NMAS Client Software on Windows Servers

- 1 Log on to the Windows client workstation with an administrator account.
- 2 Run the `nmasinstall.exe` program from the installation directory, by default `IDM4.0.2_Win:\products\edirectory\processor_type\nmas\`.
- 3 Click **NMAS Client Components**.
- 4 (Optional) Select the NICI option to install the NICI component.
- 5 Click **OK**.
- 6 After the installation process completes, restart the client workstation.

10 Installing the Identity Vault on a Linux Server

The installation utility can guide you through the configuration settings for the Identity Vault. Your choice of performing the installation as a `root` or a `non-root` user should match the method that you plan to use for installing the Identity Manager engine.

This section assumes that you want to use eDirectory as the base structure for the Identity Vault. For more information about the additional packages that you can use to support eDirectory on a Linux server, see “Linux Packages for NetIQ eDirectory” (<https://www.netiq.com/documentation/edir88/edir88/data/a7f7odf.html>) in the *NetIQ eDirectory 8.8 SP8 Administration Guide*.

WARNING: The `install_location/etc/opt/novell/eDirectory/conf` directory contains critical configuration information used for tracking and managing the eDirectory instances running on your server. Do not remove any contents from this directory.

10.1 Installing the Identity Vault as Root

This section describes the process for using the `nds-install` utility to install the Identity Vault as a `root` user. The utility adds the required packages based on what components you choose to install.

NOTE: To install as a `root` user and specify a custom installation path, you might want to use the tarball format for installation. For more information, see [Section 10.2, “Installing the Identity Vault as a Non-root User,”](#) on page 109.

To install the Identity Vault as `root`:

- 1 Log on as `root` to the computer where you want to install the Identity Vault.
- 2 Run the following command from the directory containing the `nds-install` utility, by default `IDM4.0.2_Lin/products/eDirectory/processor_type/setup`:

```
./nds-install parameters
```

Use the following parameters in the command line:

-h or --help

Displays help for `nds-install`.

-i

Prevents the `nds-install` script from invoking the `ndsconfig upgrade` command if a DIB is detected at the time of the upgrade.

-j

Jumps or overrides the health check option before installing eDirectory. For more information about health checks, see “Keeping eDirectory Healthy” (<https://www.netiq.com/documentation/edir88/edir88/data/a5ziqam.html>) in the *NetIQ eDirectory 8.8 SP8 Administration Guide*.

-m *module_name*

Specifies the name of the module that you want to install and configure. While configuring a new tree, you can configure only the ds module. After configuring the ds module, you can add the NMAS, LDAP, SAS, SNMP, HTTP services, and NetIQ SecretStore (ss) by using the `add` command. If you do not specify the module name, all the modules are installed.

-u

Specifies that you want to run in unattended (silent) installation mode.

- 3 (Optional) If the license file is not in the default directory, specify the complete path to the license file at the prompt.
- 4 Respond to all prompts until the installation process completes.
- 5 (Conditional) To manually update the following environment variables and export them, enter the following command:

```
export LD_LIBRARY_PATH=/opt/novell/eDirectory/lib64:/opt/novell/eDirectory/lib64/nds-modules:/opt/novell/lib64:$LD_LIBRARY_PATH
```

```
export MANPATH=/opt/novell/man:/opt/novell/eDirectory/man:$MANPATH
```

```
export TEXTDOMAINDIR=/opt/novell/eDirectory/share/locale:$TEXTDOMAINDIR
```

- 6 (Conditional) To use the `ndspath` script to update the following environment variables and export the paths, you must prefix the `ndspath` script to the utility. Complete the following steps:

- 6a From the `custom_location/eDirectory/` directory, run the utility with the following command:

```
eDirectory installation/bin/ndspath utility_name_with_parameters
```

- 6b Export the paths in the current shell with the following command:

```
. custom_location/eDirectory/opt/novell/eDirectory/bin/ndspath
```

NOTE: When you prefix the `ndspath` script to the commands with arguments, specify the arguments in double quotes.

For example:

```
/opt/novell/eDirectory/bin/ndspath ldapconfig "-s ldapTLSRequired=yes"
```

- 6c Export the paths in the current shell with the following command:

```
. /opt/novell/eDirectory/bin/ndspath
```

- 6d Run the utilities as normal.

- 6e Add the instructions for exporting the path to the end of `/etc/profile`, `~/bashrc`, or similar scripts.

This step allows you to start the utilities directly whenever you log on or open a new shell.

10.2 Installing the Identity Vault as a Non-root User

This section describes how to use the tarball, instead of the nds-install utility, to install the Identity Vault. When you untar the tar file, the system creates the `etc`, `opt`, and `var` directories.

For more information about prerequisites for a non-root installation, see [Section 6.3.2, “Considerations for Installing the Identity Vault as a Non-root User,”](#) on page 49.

NOTE: You can also use this process when you want to specify a custom path while installing as a `root` user.

To install the Identity Vault as a non-root user:

- 1 Log on as a `sudo` user with the appropriate rights to the computer where you want to install the Identity Vault.

NOTE: You can also log on as a `root` user, when you want to specify a custom installation path.

- 2 In the directory where you want to install the Identity Vault, use the following command to untar the tar file:

```
tar xvf /tar_file_name
```

- 3 (Conditional) To manually export the paths for environment variables, enter the following command:

```
export LD_LIBRARY_PATH=custom_location/eDirectory/opt/novell/eDirectory/  
lib64:custom_location/eDirectory/opt/novell/eDirectory/lib64/ndsmodules:  
custom_location/eDirectory/opt/novell/lib64:$LD_LIBRARY_PATH
```

```
export PATH=custom_location/eDirectory/opt/novell/eDirectory/  
bin:custom_location/eDirectory/opt/novell/eDirectory/sbin:/opt/novell/  
eDirectory/bin:$PATH
```

```
export MANPATH=custom_location/eDirectory/opt/novell/man:custom_location/  
eDirectory/opt/novell/eDirectory/man:$MANPATH
```

```
export TEXTDOMAINDIR=custom_location/eDirectory/opt/novell/eDirectory/  
share/locale:$TEXTDOMAINDIR
```

- 4 (Conditional) To use the `ndspath` script to export the paths for environment variables, you must prefix the `ndspath` script to the utility. Complete the following steps:

- 4a From the `custom_location/eDirectory/opt` directory, run the utility with the following command:

```
custom_location/eDirectory/opt/novell/eDirectory/bin/ndspath  
utility_name_with_parameters
```

- 4b Export the paths in the current shell with the following command:

```
. custom_location/eDirectory/opt/novell/eDirectory/bin/ndspath
```

- 4c Run the utilities as normal.

- 4d Add the instructions for exporting the path to the end of `/etc/profile`, `~/bashrc`, or similar scripts.

This step allows you to start the utilities directly whenever you log on or open a new shell.

5 To configure the Identity Vault, complete one of the following steps:

5a To run the `ndsconfig` utility, enter the following text at the command line:

```
ndsconfig new [-t treename] [-n server_context] [-a admin_FDN] [-w  
admin password] [-i] [-S server_name] [-d path_for_dib] [-m module] [e] [-L  
ldap_port] [-l SSL_port] [-o http_port] -O https_port] [-p IP  
address:[port]] [-c] [-b port_to_bind] [-B interface1@port1,  
interface2@port2,..] [-D custom_location] [--config-file  
configuration_file]
```

For example:

```
ndsconfig new -t mary-tree -n novell -a admin.novell -S linux1 -d /home/  
mary/inst1/data -b 1025 -L 1026 -l 1027 -o 1028 -O 1029 -D /home/mary/  
inst1/var --config-file /home/mary/inst1/nds.conf
```

NOTE

- ◆ For more information about the parameters that you can specify with the `ndsconfig` utility, see [Section 13.1.1, “Understanding the ndsconfig Utility Parameters,” on page 128.](#)

- ◆ You must specify port numbers between 1024 and 65535. You cannot assume the default port 524 for any eDirectory applications.

This limitation on port specification might adversely affect the following types of applications:

- ◆ Applications that do not have an option to specify the target server port.
- ◆ Older applications that use NCP, and run as root for 524.
- ◆ You can specify IPv6 addresses in the `-B` and `-P` options. To specify an IPv6 address, you must contain the address within square braces []. For example, `-B [2015::4]@636.`

-
- 5b** Use the `ndsmanage` utility to configure a new instance. For more information, see [Section 13.2.2, “Creating a New Instance in the Identity Vault,” on page 133.](#)

11 Installing the Identity Vault on a Windows Server

The installation program (wizard) can guide you through the configuration settings for the Identity Vault. The installation program automatically defaults to wizard mode. However, you can also perform a silent installation.

This section assumes that you want to use eDirectory as the base structure for the Identity Vault.

When you start the installation program, it checks for Novell International Cryptographic Infrastructure (NICI) and Novell Client for Windows. The installation program will install or update these components as needed. If you install the Identity Vault on a computer already containing the Novell Client, eDirectory will use the existing Novell Client. You can install the Identity Vault for Windows without the Novell Client.

For more information about NICI, see the *Novell International Cryptographic Infrastructure 2.7 Administration Guide* (<https://www.netiq.com/documentation/nici27x/>). For more information on the Client, see the *Novell Client for Windows* (<http://www.novell.com/documentation/lg/noclienu/index.html>) online documentation.

The installation program can install the server components for NetIQ Module Authentication Service (NMAS). During the installation, you must specify the login methods to use with NMAS. You must also install the NMAS client software on each client workstation where you want to use the NMAS login methods.

NOTE

- ♦ Starting with eDirectory 8.8, you can use case-sensitive passwords for all the utilities.
 - ♦ Your container names can include a period (dot). For information on using dots in container names, see [Section 6.3.3, “Considerations for Installing Identity Vault on a Windows Server,” on page 50.](#)
-

11.1 Using the Wizard to Install the Identity Vault on a Windows Server

- 1 Log on as administrative user to the computer where you want to install eDirectory.
- 2 Navigate to the `Setup.exe` program in the installation directory, by default `IDM4.0.2_Win:\products\edirectory\processor_type\windows\`.
- 3 Run the `Setup.exe` program.
- 4 Follow the steps in the installation wizard.
- 5 (Conditional) If the NICI or Novell Client for Windows is not already installed on the computer, the installation program will prompt you to install these components.

The computer will restart after the program installs NICI. The Identity Vault installation wizard should open after the computer restarts. If it does not open, run the `Setup.exe` program.

6 In the Identity Vault installation program, complete the steps in the wizard with the following considerations:

- ◆ (Optional) To use IPv6 addresses on the Identity Vault server, click **Enable IPv6** under **IPv6 Preference**.

NOTE: NetIQ recommends that you enable this option. To enable IPv6 addressing after installation, you must run the setup program again.

- ◆ Ensure that the ports for HTTP stack are different than the HTTP stack ports you have used or will use for NetIQ iManager. For more information, see the *iManager Administration Guide* (http://www.netiq.com/documentation/imanager27/imanager_admin_275/data/hk42s9ot.html).
 - ◆ (Conditional) If a service already loaded on the host server (before eDirectory was installed) uses port 636, you must specify a different port for SSL/TLS.
 - ◆ (Optional) To disallow clear passwords and other data, select **Require TLS for Simple Bind with Password** when specifying the LDAP ports. For more information, see [Section 9.4, “Using LDAP to Communicate with the Identity Vault,”](#) on page 102.
 - ◆ Specify the login methods that you want to install for NetIQ Module Authentication Service (NMAS). For more information, see “[Managing Login and Post-Login Methods and Sequences](https://www.netiq.com/documentation/nmas33/admin/data/a53vj9a.html)” (<https://www.netiq.com/documentation/nmas33/admin/data/a53vj9a.html>) in the *NetIQ Modular Authentication Services 3.3 Administration Guide*.
- 7 Follow the instructions in the wizard until you finish installing the Identity Vault.
- 8 To use the NMAS login methods, install the NMAS client software on each client workstation. For more information, see [Section 9.6, “Installing NMAS Client Software,”](#) on page 104.
- 9 (Optional) Exclude the DIB directory on your eDirectory server from any antivirus or backup software processes. Use the eDirectory Backup Tool to back up your DIB directory. For more information about backing up eDirectory, see “[Backing Up and Restoring NetIQ eDirectory](https://www.netiq.com/documentation/edir88/edir88/data/a2n4mb6.html)” (<https://www.netiq.com/documentation/edir88/edir88/data/a2n4mb6.html>) in the *NetIQ eDirectory 8.8 SP8 Administration Guide*.

11.2 Silently Installing and Configuring the Identity Vault on a Windows Server

To support a silent (or unattended) installation or configuration of the Identity Vault, you can use a `response.ni` file that contains sections and keys, similar to a `Windows.ini` file.

11.2.1 Editing the `response.ni` File

You can use an ASCII text edit to create and edit the `response.ni` file. The response file helps you:

- ◆ Perform a complete unattended installation with all required user inputs.
- ◆ Define the default configuration of components.
- ◆ Bypass all prompts during the installation.

NetIQ provides a `response.ni` file in the `products\edirectory\x64\windows\x64\NDSonNT` folder of the installation kit. The file contains default settings for essential parameters. You must edit the values for the eDirectory instance in the `NWI:NDS` section.

NOTE: When you edit the `response.ni` file, do not include blank spaces between the key and values along with the equal sign (“=”) in each key-value pair.

WARNING: You specify the administrator user credentials in the `response.ni` file for an unattended installation. To prevent the administrator credentials from being compromised, you should permanently delete the file after the installation or configuration.

The following sections describe the sections and keys required in the `response.ni` file:

- ◆ [“NWI:NDS” on page 113](#)
- ◆ [“NWI:NMAS \(NMAS Methods\)” on page 115](#)
- ◆ [“eDir:HTTP \(Ports\)” on page 116](#)
- ◆ [“Novell:Languages:1.0.0 \(Language Settings\)” on page 116](#)
- ◆ [“Initialization” on page 116](#)
- ◆ [“NWI:SNMP” on page 117](#)
- ◆ [“EDIR:SLP” on page 117](#)
- ◆ [“Novell:ExistingTree:1.0.0” on page 117](#)
- ◆ [“Selected Nodes” on page 118](#)
- ◆ [“Novell:NOVELL_ROOT:1.0.0” on page 118](#)

NWI:NDS

Upgrade Mode

Specifies whether to run the installation program as an upgrade. Valid values are `False`, `True`, and `Copy`.

Mode

Specifies the type of installation that you want to perform:

- ◆ **full** allows you to both install and configure the Identity Vault. Specify this value when you want to perform a fresh installation and configuration of the Identity Vault or an upgrade and configuration of only the required files.
- ◆ **install** allows you to install a fresh version of the Identity Vault or upgrade the required files.
- ◆ **configure** allows you to modify the Identity Vault settings. If you only perform an upgrade of the required files, then the installation program configures only the upgraded files.

NOTE

- ◆ If you specify *configure*, ensure that you do not change the `RestrictNodeRemove` value of the `ConfigurationMode` key in the `[Initialization]` section.
 - ◆ If you specify *full*, you cannot opt for individual deconfiguration and uninstallation option when you uninstall the Identity Vault.
-

New Tree

Specifies whether this installation is for a new tree or a secondary server. Valid values are `Yes` and `No`. For example, if you want to install a new tree, specify `Yes`. For more information about specifying values for an existing tree, see [“Novell:ExistingTree:1.0.0” on page 117](#).

Tree Name

If this is a new installation, specify the name of the tree that you want to install. To install a secondary server, specify the tree where you want to add the server.

Server Name

Specifies the name of the server that you want to install in the Identity Vault.

Server Container

Specifies the container object in the tree to which the server object will be added. The server object contains all the configuration details specific to the Identity Vault server. If you are installing a fresh version of the Identity Vault, the installation program creates this container with the server object.

Server Context

Specifies the complete distinguished name (DN) of the server object (server name), along with the container object. For example, if the Identity Vault server is EDIR-TEST-SERVER and the container is Netiq, specify `EDIR-TEST-SERVER.Netiq`.

Admin Context

Specifies the container object in the tree to which the Administrator object will be added. For example, `Netiq`. Any user added to a tree has a user object that contains all the user-specific details. If you are installing a fresh version of the Identity Vault, the installation program creates this container with the server object.

Admin Login Name

Specifies the relative distinguished name (RDN) of the Administrator object in the tree that has full rights, at least to the context to which this server is added. For example, `Admin`. The installation program uses this account to perform all operations in the tree.

Admin Password

Specifies the password for the Administrator object. For example, `netiq123`. If you are installing a fresh version of the Identity Vault, the installation program configures this password for the Administrator object.

NDS Location

Specifies the path in the local system where you want to install the Identity Vault libraries and binaries. When you configure the Identity Vault components, they refer to this installation location for relevant files. By default, the installation program places the files in `C:\Novell\NDS`.

DataDir

Specifies the path in the local system where you want to install the DIB files. By default, the installation program places the files in `C:\Novell\NDS\DIBFiles`.

You might want to specify a different path if the DIB data files for your environment will require more space that is available in the default location.

Installation Location

(Optional) Specifies a path that the installation program uses while copying files to the NDS Location. For example, `[Novell:DST:1.0.0_Location]` or `Path=file://C:\Novell\NDS`. The default value is `C:\Novell\NDS`, the same as the default for NDS Location. The installation program uses this path while copying files to the specified NDS and DataDir locations.

System Location

(Optional) Specifies a path to the system folder of the computer where you want to install the Identity Vault server. For example, [Novell:SYS32_DST:1.0.0_Location] or Path=file:/C:\Windows\system32. The installation program requires access to the system folder to copy DLLs and to access system-specific files during installation.

Require TLS

(Optional) Specifies whether the Identity Vault requires Transport Layer Security (TLS) protocol when receiving LDAP requests in clear text.

LDAP TLS Port

(Optional) Specifies the port on which the Identity Vault listens for LDAP requests in clear text.

LDAP SSL Port

(Optional) Specifies the port on which the Identity Vault should listen for LDAP requests using Secure Sockets Layer (SSL) protocol.

Install as Service

Instructs the installation program to install eDirectory as a service in Windows. You must specify Yes.

Prompt

Specifies whether the installation program prompts you for decisions such as tree name and server name. For example, in a silent or unattended installation, specify False.

NWI:NMAS (NMAS Methods)

The Identity Vault supports multiple NMAS methods, both during installation and upgrade. You must specify the NDS NMAS method in the `response.ni` file. If you do not specify any NMAS methods, the installation program installs the NDS method by default. However, if you are creating an explicit list, you must include NDS.

Choices

Specifies the number of NMAS methods that you want to install. For example, 5.

Methods

Specifies the types of NMAS methods that you want to install. Use commas to separate multiple types. For example, `CertMutual, Challenge Response, DIGEST-MD5, NDS`.

The installation program matches the exact string (with case) for choosing the NMAS methods to install, so you must specify the values exactly as listed:

- ◆ `CertMutual`
- ◆ `Challenge Response` - which represents the NetIQ challenge response NMAS method.
- ◆ `DIGEST-MD5`
- ◆ `Enhanced Password`
- ◆ `Entrust`
- ◆ `GSSAPI` - which represents the SASL GSSAPI mechanism for eDirectory. Authentication to the Identity Vault occurs through LDAP using a Kerberos ticket.
- ◆ `NDS` - the default login method. REQUIRED.
- ◆ `NDS Change Password`
- ◆ `Simple Password`

- ◆ Universal Smart Card
- ◆ X509 Advanced Certificate
- ◆ X509 Certificate

When you specify the NMAS methods in the response file, the Identity Vault shows a status message while installing without prompting for user input.

eDir:HTTP (Ports)

The Identity Vault listens on preconfigured HTTP ports for access through the Web. For example, iMonitor accesses the Identity Vault through Web interfaces. They need to specify certain ports to access the appropriate applications. The following options allow you to configure the Identity Vault for specific ports:

Clear Text HTTP Port

Specifies the number of the port for the HTTP operations in clear text.

SSL HTTP Port

Specifies the number of the port for the HTTP operations using SSL protocol.

Novell:Languages:1.0.0 (Language Settings)

During installation, you can specify the locale and displayed language for the Identity Vault: English, French, or Japanese. These values are mutually exclusive.

LangID4

Represents English. For example, `LangID4=true`.

LangID6

Represents French.

LangID9

Represents Japanese.

NOTE

- ◆ Do not specify `true` for more than one language.
 - ◆ You can also specify the language that the installation program uses to display messages throughout the installation. For more information, see [“Initialization” on page 116](#).
-

Initialization

The `[Initialization]` section of the `response.ni` file specifies the settings for the installation process.

DisplayLanguage

Specifies the language used for messages displayed during the installation process. For example, `DisplayLanguage=en_US`.

InstallationMode

Specifies how you want to run the installation process. For example, to perform a silent or unattended installation, specify `silent`.

SummaryPrompt

Specifies whether the installation program prompts you to review a summary of the installation settings. For example, in a silent or unattended installation, specify `false`.

prompt

Specifies whether the installation program prompts you for decisions. For example, in a silent or unattended installation, specify `false`.

NWI:SNMP

Most Windows servers have SNMP configured and running. When you install the Identity Vault, you must stop SNMP services and then restart after the process completes. During a manual installation, the program prompts you to stop the SNMP services before continuing the installation.

To stop SNMP services without a prompt during a silent or unattended installation, in the `[NWI:SNMP]` section of the `response.ni` file, specify `Stop Service=yes`.

EDIR:SLP

The Identity Vault uses Service Location Protocol (SLP) services to identify other servers or trees in the subnet during installation or upgrade. If SLP services are already installed on your server, you can replace them with the version that ships with the current version of the Identity Vault or use your own SLP services.

Need to uninstall service

Specifies whether to uninstall any SLP services already installed on your server. The default value is `true`.

Need to remove files

Specifies whether to remove the files for any SLP services already installed on your server. The default value is `true`.

Novell:ExistingTree:1.0.0

The installation program provides options for the unattended install of a primary or a secondary server into a network. The installation program uses three different keys to decide whether to install a new tree or a secondary server in an existing tree.

NOTE: The `New Tree` key resides in the `NWI:NDS` section. For more information, see [“NWI:NDS” on page 113](#).

ExistingTreeYes

Valid values are `True` and `False`. For example, if you want to install a new tree, specify `False`.

ExistingTreeNo

Valid values are `True` and `False`. For example, if you want to install a new tree, specify `True`.

To run a silent or unattended installation without prompts for decisions about primary or secondary server installation, in the `Existing Tree` section of the `response.ni` file, specify `prompt=false`.

Selected Nodes

This section in the `response.ni` file lists the components that are installed in the Identity Vault, along with information in the profile database that contains more information about the component, including source location, destination copy location, and component version. These details in the profile database are compiled into a `.db` file that is delivered in the Identity Vault release.

To run a silent or unattended installation without prompts for decisions such as the destination copy location or version details, in the `[Selected Nodes]` section of the `response.ni` file, specify `prompt=false`.

Your response file must include this section. Use the keys and values exactly as provided in the sample `response.ni` file.

Novell:NOVELL_ROOT:1.0.0

This section in the `response.ni` file contains the settings for image and status displays that occur during the installation process. For example, you can specify the settings for the way the installation program responds to scenarios such as file write conflicts and file copying decisions. You can also specify whether images are displayed. Most images contain information on what version of the Identity Vault is installed, what components are installed, a welcome screen, license files, customization options, a status message indicating the component currently being installed, percentage complete, etc. Some applications that intend to embed eDirectory might not want eDirectory displaying these images.

To run a silent or unattended installation without prompts for decisions such as the destination copy location or version details, in this section of the `response.ni` file, specify `prompt=false`.

Your response file should include this section. Use the keys and values provided in the sample `response.ni` file.

11.2.2 Performing a Silent or Unattended Installation

Before beginning, review the prerequisites for performing a silent or unattended installation on a Windows server. For more information, see [Section 6.3.3, “Considerations for Installing Identity Vault on a Windows Server,” on page 50](#). Also, create the `response.ni` file to use as a template for the installation. For more information, see [Section 11.2.1, “Editing the response.ni File,” on page 112](#).

NOTE: To ensure that the operating system does not display a status window for installation, upgrade, or configuration, use the `nopleasewait` option in the command.

- 1 Create a new `response.ni` file or edit an existing response file. For more information about the values in the response file, see [Section 11.2.1, “Editing the response.ni File,” on page 112](#).
- 2 Log on with an administrator account to the computer where you want to install the Identity Vault.
- 3 Open a command prompt with the **Run as administrator** option enabled.
- 4 At the command line, enter the following command:

```
path_to_installation_files\windows\eDirectory\x64\NDSonNT>install.exe /silent /nopleasewait /template=Response file
```

For example:

```
D:\builds\eDirectory\windows\eDirectory\x64\NDSonNT>install.exe /silent /nopleasewait /template=D:\builds\eDirectory\windows\x64\NDSonNT\response.ni
```

11.2.3 Performing a Silent Configuration

- 1 Create a new `response.ni` file or edit an existing response file. For more information about the values in the response file, see [Section 11.2.1, “Editing the response.ni File,” on page 112](#).
- 2 Log on with an administrator account to the computer where you want to install the Identity Vault.
- 3 Open a command prompt with the **Run as administrator** option enabled.
- 4 At the command line, enter the following command:

```
Windows Drive\Program Files\Common Files\novell>install.exe /silent /  
restrictnoderemove /noplasewait /template=Response file
```

For example:

```
c:\Program Files\Common Files\novell>install.exe /silent /restrictnoderemove /  
noplasewait /template=D:\builds\edirectory\windows\x64\NDSonNT\response.ni
```

11.2.4 Performing a Silent Installation Combined with Configuration

Before beginning, review the prerequisites for performing a silent or unattended installation on a Windows server. For more information, see [Section 6.3.3, “Considerations for Installing Identity Vault on a Windows Server,” on page 50](#). Also, create the `response.ni` file to use as a template for the installation.

- 1 Create a new `response.ni` file or edit an existing response file. For more information about the values in the response file, see [Section 11.2.1, “Editing the response.ni File,” on page 112](#).
- 2 Log on with an administrator account to the computer where you want to install the Identity Vault.
- 3 Open a command prompt with the **Run as administrator** option enabled.
- 4 At the command line, enter the following command:

```
Unzipped Location\windows\edirectory\x64\NDSonNT>install.exe /silent /  
noplasewait /template=Response file
```

For example:

```
D:\builds\edirectory\windows\edirectory\x64\NDSonNT>install.exe /silent /  
noplasewait /template=D:\builds\edirectory\windows\x64\NDSonNT\response.ni
```

12 Installing the Identity Vault in a Clustered Environment

Installing the Identity Vault in a clustered environment might be a viable alternative for achieving high availability in some environments.

This section provides guidelines for configuring the Identity Vault on high-availability clusters by using shared storage. The information in this section is generalized for shared storage high-availability clusters on supported Windows and Linux platforms, and the information is not specific to a particular cluster manager.

NetIQ recommends reviewing the considerations for a clustered environment before beginning. For more information, see [Section 6.3.4, “Considerations for Installing the Identity Vault in a Clustered Environment,” on page 50](#).

The procedures in this section are based on the following assumptions:

- ◆ You use eDirectory as the underlying structure for the Identity Vault.
- ◆ You are familiar with eDirectory installation procedures.
- ◆ You are using a two-node cluster.

NOTE: A two-node cluster is the minimum configuration used for high availability. However, the concepts in this section can easily be extended to a cluster with additional nodes. Note that eDirectory does not support load balancing by using multiple cluster nodes.

12.1 Installing the Identity Vault in a Cluster on Linux

This procedure assumes that you use eDirectory as the underlying structure for the Identity Vault in a Linux environment. NetIQ recommends that you review the following considerations:

- ◆ When configuring eDirectory, the default **NCP server name** represents the host server name of the computer on which you installed eDirectory. Because eDirectory is hosted on multiple hosts in a clustered environment, you specify an NCP server name that is unique to the cluster instead of using the default name. For example, you can specify the name `clusterserver` for the NCP server when you configure eDirectory on the primary cluster node.
- ◆ During the configuration process, ensure that you set the virtual IP address for your eDirectory installation. In a clustered environment, eDirectory only listens on the virtual IP address, not on the system IP address.

IMPORTANT: Ideally, the cluster manager checks that two or more nodes do not access the same DIB simultaneously. However, you must ensure that `ndsd` does not run from two or more cluster nodes simultaneously. This is because accessing the same DIB through two or more nodes leads to DIB corruption.

12.1.1 Installing and Configuring the Identity Vault on Linux

- 1 Install and configure the Identity Vault on the Linux server that you want to use as the primary cluster node.

For more information about installation, see [Chapter 10, “Installing the Identity Vault on a Linux Server,” on page 107](#).

- 2 In a text editor, open the `nds.conf` file, located by default in the `/etc/opt/novell/eDirectory/conf` directory.
- 3 Change the `n4u.nds.preferred-server` setting to the virtual IP address of the clustered installation.
- 4 Save and close the `nds.conf` file.
- 5 (Optional) To verify the eDirectory installation, use the `ndsstat` command.
eDirectory must be up and running on the primary cluster node.
- 6 Use the cluster manager to mount the shared file system.
- 7 Back up all data in the following directories:
 - ◆ `/var/opt/novell/nici`
 - ◆ `/var/opt/novell/eDirectory/data` (`n4u.server.vardir`)
 - ◆ `/var/opt/novell/eDirectory/data/` (`n4u.nds.dir`)
 - ◆ `/etc/opt/novell/eDirectory/conf` (`n4u.server.configdir`)
 - ◆ `/var/opt/novell/eDirectory/log`

NOTE: If you install eDirectory in a non-default location, you can use the `ndsconfig get` command to find the `vardir`, `dir` paths used in your installation.

- 8 To stop the eDirectory service on the primary cluster node server, open a terminal and run the following command:

```
ndsmanage stopall
```

- 9 In the terminal, navigate to the `nds-cluster-config` configuration utility, located by default in the `/opt/novell/eDirectory/bin` directory.
- 10 Run the following command:

```
nds-cluster-config -s /sharedfilesystem
```

Where `sharedfilesystem` represents the location that you want to use for the eDirectory shared cluster data.

NOTE: You can also run the utility in unattended mode by using the `-u` option. If you use this option, the utility does not ask for confirmation when configuring eDirectory on a cluster.

If you use the unattended option, you must also use the `-s` option and specify the shared cluster file system.

- 11 After the nds cluster configuration utility verifies that the cluster shared storage is valid, click **y** to continue with configuration on the cluster.

The configuration utility moves the data in the directories above to the following locations on the shared file system:

- ◆ *sharedfilesystem/nici*
- ◆ *sharedfilesystem/data*
- ◆ *sharedfilesystem/data/*
- ◆ *sharedfilesystem/conf*
- ◆ *sharedfilesystem/log*

- 12 To restart eDirectory services, run the following command:

```
ndsmanage startall
```

- 13 (Optional) To check the status of eDirectory, use the `ndsstat` command.

- 14 To prepare the secondary node of the cluster, complete the following steps:

- 14a To stop eDirectory services, run the following command:

```
ndsmanage stopall
```

- 14b Log on to the server that you want to use as the secondary node of the cluster.

- 14c Use the cluster manager to move the shared storage to the secondary node.

- 14d Install the same version of eDirectory on the secondary cluster node that you installed on the primary cluster node, but do not configure eDirectory.

- 14e In the terminal, navigate to the `nds-cluster-config` configuration utility on the secondary node, located by default in the `/opt/novell/eDirectory/bin` directory.

- 14f In the terminal, run the following command:

```
nds-cluster-config -s /sharedfilesystem
```

Where *sharedfilesystem* represents the cluster shared storage. The path of the *sharedfilesystem* should be same path that you specified for the primary node in [Step 10 on page 122](#).

The `nds-cluster-config` utility links the secondary cluster node to the shared eDirectory data located on the shared cluster file system.

- 14g To start the eDirectory service on the secondary cluster node server, run the following command:

```
ndsmanage startall
```

- 14h (Optional) To check the status of eDirectory, use the `ndsstat` command.

- 14i To stop eDirectory services on the secondary cluster node server, run the following command:

```
ndsmanage stopall
```

- 15 After successfully configuring eDirectory on both nodes of the cluster, you must use the following command to change the startup mode of the `nds` service on each node:

```
chkconfig -d ndsd
```

- 16 After the configuration utility finishes configuring the secondary node, you can use the cluster manager to add the eDirectory services in the cluster.

12.1.2 Configuring an SNMP Server in a Clustered Linux Environment

- 1 On each node in the cluster, modify the `snmpd.conf` file.
For more information, see [“Installing and Configuring SNMP Services for eDirectory”](#) in the *NetIQ eDirectory 8.8 SP8 Administration Guide*.
- 2 Start `ndssnmpsa`.
- 3 For **Remember password**, select **Yes**.
- 4 To start the `snmp` service, perform either of the following actions:
 - ♦ Add `/etc/init.d/ndssnmpsa start` to the `post_ndsd_start` script and `/etc/init.d/ndssnmpsa stop` to the `pre_ndsd_stop` script.
 - ♦ Add `ndssnmpsa` as a cluster resource with a dependency on eDirectory resource.

NOTE: Because eDirectory listens on a virtual IP address, traps have the IP address of the host, which is the Agent IP address.

12.2 Installing the Identity Vault in a Cluster on Windows

This section describes how to configure eDirectory by using high availability clustering on Windows.

12.2.1 Installing and Configuring the Identity Vault on Windows

- 1 Install and configure the Identity Vault on the Windows server that you want to use as the primary cluster node.
For more information about installation, see [Chapter 11, “Installing the Identity Vault on a Windows Server,”](#) on page 111.
- 2 Use the cluster manager to mount the shared file system.
- 3 Back up all DIB files and NICI data.
- 4 Open a terminal on the primary cluster node server.
- 5 In the terminal, navigate to the `NDSCons.exe` configuration utility, located by default in the eDirectory installation folder.
- 6 In the terminal, run the following command:

```
NDSCons.exe
```
- 7 In the NDS configuration utility, click **Shutdown** to stop all eDirectory services.
- 8 Click **Yes** to confirm.
- 9 In the terminal, navigate to the eDirectory shared cluster configuration utility, `dsclusterconfig.exe`, located by default in the eDirectory installation directory.

10 Run the following command:

```
dsclusterconfig.exe -s /sharedfilesystem
```

Where *sharedfilesystem* represents the location that you want to use for the eDirectory shared cluster data.

NOTE

- ◆ You can also run the utility in unattended mode by using -s with -u option.
- ◆ You must specify a folder within a shared drive mounted on the primary cluster node. You cannot specify only a drive name. For example, instead of specifying E:, you must specify E:\Novell.

11 After the cluster configuration utility verifies that the cluster shared storage is valid, click **y** to continue with configuration on the cluster.

12 The cluster configuration utility moves the data in the directories above to the following locations on the shared file system:

- ◆ *sharedfilesystem/nici*
- ◆ *sharedfilesystem/Files*

In addition to moving eDirectory data to the shared file system, the utility copies the eDirectory service registry key to the shared volume, saving the key as the file *ndsConfigKey*.

The utility also changes the Startup Type of the NDS *Server* service on the primary node computer from *Automatic* to *Manual*.

13 In the NDS configuration utility, *ndsconfig*, click **Startup** to start all eDirectory services.

14 Verify that all eDirectory services are running, and then use the NDS configuration utility to stop services again.

15 Close the NDS configuration utility.

16 To prepare the secondary node of the cluster, complete the following steps:

16a Log on to the server that you want to use as the secondary node of the cluster.

16b Use the cluster manager to move the shared storage to the secondary node.

16c Install eDirectory on the secondary node as a silent, unattended installation. Ensure that the mode of installation is *install*. For more information, see [Section 11.2, "Silently Installing and Configuring the Identity Vault on a Windows Server,"](#) on page 112.

16d Open a terminal on the secondary cluster node server.

16e In the terminal, navigate to the *NDSCons.exe* configuration utility, located by default in the eDirectory installation folder.

16f In the terminal, run the following command:

```
dsclusterconfig.exe -s /sharedfilesystem
```

Where *sharedfilesystem* represents the cluster shared storage. The path of the *sharedfilesystem* should be same as the path location specified when the primary node was configured.

The cluster configuration utility updates the registry on the secondary cluster node to the shared eDirectory data located on the shared cluster file system.

16g After the configuration utility finishes configuring the secondary node, open the NDS configuration utility.

16h In the NDS configuration utility, click **Startup**.

16i Click **Yes** to confirm.

- 16j** When NDS configuration utility starts all eDirectory services, verify eDirectory, and then click **Shutdown**.
- 16k** Click **Yes** to confirm.
- 17** To configure eDirectory in the Cluster Resource group, complete the following steps:
- 17a** Create a new resource in the Resource Group to be used for eDirectory.
- 17b** Specify the following details:
- ◆ Resource type - Generic Service
 - ◆ Dependent on - IP address and shared disk in the Resource Group
 - ◆ Service name - NDS Server0
 - ◆ No start parameters
 - ◆ Registry keys - SYSTEM\CurrentControlSet\Services\NDS Server0

12.2.2 Configuring an SNMP Server in Clustered Windows Environments

- 1** On the primary cluster node, configure the master agent and set the startup type to automatic. For more information, see [“Installing and Configuring SNMP Services for eDirectory”](#) in the *NetIQ eDirectory 8.8 SP8 Administration Guide*.
- 2** Save the eDirectory password when it prompts for the password.
- 3** Start the sub-agent.
- 4** Repeat the steps for each node in the cluster.

13 Configuring the Identity Vault after Installation

After installing the Identity Vault, you can use the `ndsconfig` utility to configure the directory and the `ndsmanage` utility to create, start, and stop server instances. You can also configure the Identity Vault to work with IPv6 addresses, if your server already supports IPv6 addressing.

13.1 Modifying the eDirectory Tree and Replica Server with the `ndsconfig` Utility

After installing Identity Vault, you can use the `ndsconfig` utility to configure Identity Vault. You must have Administrator rights to use the `ndsconfig` utility. When you use this utility with arguments, it validates all arguments and prompts for the password of the user having Administrator rights. If you use the utility without arguments, `ndsconfig` displays a description of the utility and available options.

You can also use this utility to remove the eDirectory Replica Server and change the current configuration of eDirectory Server. For more information, see [Chapter 13, “Configuring the Identity Vault after Installation,” on page 127](#).

When you use the `ndsconfig` utility, the following conditions apply:

- ♦ The maximum number of characters allowed for the `treename`, `admin_FDN`, and `server_FDN` variables are as follows:
 - ♦ `treename`: 32 characters
 - ♦ `admin_FDN`: 255 characters
 - ♦ `server_FDN`: 255 characters
- ♦ When you add a server to an existing tree and the context that you specify does not exist in the Server object, the `ndsconfig` utility creates the context while adding the server.
- ♦ You can add LDAP and security services to the existing tree after installing the Identity Vault.
- ♦ To enable encrypted replication in the server, include the `-E` option in the commands for adding a server to an existing tree. For more information about encrypted replication, see [“Encrypted Replication” \(https://www.netiq.com/documentation/edir88/edir88/data/bs6rydy.html\)](https://www.netiq.com/documentation/edir88/edir88/data/bs6rydy.html) in the *NetIQ eDirectory 8.8 SP8 Administration Guide*.

For more information about using the `ndsconfig` utility to modify eDirectory, see the *NetIQ eDirectory 8.8 SP8 Administration Guide*.

13.1.1 Understanding the ndsconfig Utility Parameters

The ndsconfig utility supports the following parameters:

new

Creates a new tree. If you do not specify the parameters in the command line, the utility prompts you to enter the values for each of the missing parameters.

def

Creates a new tree. If you do not specify the parameters in the command line, ndsconfig applies the default value for each of the missing parameters.

add

Adds a server to an existing tree. Also adds LDAP and SAS services, after you configure Identity Vault in the existing tree.

rm

Removes the Server object and directory services from a tree.

NOTE: This option does not remove the key material objects. You must remove these objects manually.

upgrade

Upgrades eDirectory to a later version.

-i

Instructs the utility to ignore checking whether a tree of the same name exists if you are configuring a new tree. Multiple trees of the same name can exist.

-S *server_name*

Specifies the server name. The server name can contain periods (for example, netiq.com). However, you must include escape character for the period. For more information about using escape characters, see [Section 9.1, “Using Escape Characters when a Container Name Includes a Period \(”.\),” on page 95](#).

-t *treename*

Specifies the name of the tree to which you want to add the server. It can have a maximum of 32 characters. If not specified, ndsconfig takes the tree name from the `n4u.nds.treename` parameter that is specified in the `/etc/opt/novell/eDirectory/conf/nds.conf` file. The default treename is `$LOGNAME-$HOSTNAME-NDStree`.

-n *server_context*

Specifies the context of the server in which the server object is added. It can have a maximum of 64 characters. If the context is not specified, ndsconfig takes the context from the configuration parameter `n4u.nds.server-context` specified in the `/etc/opt/novell/eDirectory/conf/nds.conf` file. The server context should be specified in the typed form. The default context is `org`.

-d *path_for_DIB*

Specifies the directory path where the database files will be stored.

-r

Forcefully adds the replica of the server regardless of the number of servers already added to the server.

-L *ldap_port*

Specifies the TCP port number on the LDAP server. If the default port 389 is already in use, it prompts you to specify a new port.

-l *ssl_port*

Specifies the SSL port number on the LDAP server. If the default port 636 is already in use, it prompts you to specify a new port.

-a *admin_FDN*

Specifies the fully distinguished name of the User object with Supervisor rights to the context in which the server object and Directory services are to be created. The admin name should be specified in the typed form. It can have a maximum of 64 characters. The default value is admin.org.

-e

Enables clear text passwords for LDAP objects.

-m *module_name*

Specifies the name of the module that you want to install or configure. If you are configuring a new tree, you can specify the ds module only. After configuring the ds module, you can add the NMAS, LDAP, SAS, SNMP, HTTP services, and NetIQ SecretStore (ss) using the add command. If the module name is not specified, all the modules are installed.

NOTE: If you do not want to configure the SecretStore during an upgrade of eDirectory through the `nds-install` command, pass the `no_ss` value to this option. For example, enter `ndsinstall '-m no_ss'`.

-o

Specifies the HTTP clear port number.

-O

Specifies the HTTP secure port number.

-p *IP_address:[port]*

Specifies the IP address of the remote host that holds a replica of the partition to which this server is being added. Use this option when adding a secondary server (add command) to a tree. The default port number is 524. This helps in faster lookup of the tree since it avoids SLP lookup.

-R

Replicates to the local server the partition to which the server is added. This option disallows adding replicas to the local server.

-c

Prevents prompts during `ndsconfig` operation, such as yes/no to continue the operation, or prompt to re-enter port numbers when there is a conflict, etc. The utility continues to prompt you for mandatory parameters if they are not passed on command line.

-w *admin_password*

This option allows passing the admin user password in clear text.

NOTE: NetIQ does not recommend using this option in an environment concerned about password security.

-E

Enables encrypted replication for the server you are trying to add.

-j

Instructs the utility to jump or override the health check option before installing the Identity Vault.

-b port_to_bind

Specifies the default port number on which a particular instance should listen on. This sets the default port number on `n4u.server.tcp-port` and `n4u.server.udp-port`. If you use the `-b` option to specify an NCP port, then the utility assumes that port is the default port and updates the TCP and UDP parameters accordingly.

NOTE: The `-b` and `-B` options are mutually exclusive parameters.

-B interface1@port1,interface2@port2,...

Specifies the port number along with the IP address or interface. For example, `-B eth0@524`, `-B 100.1.1.2@524`, `-B [2015::3]@524`.

NOTE

- ◆ The `-b` and `-B` options are mutually exclusive parameters.
 - ◆ To specify an IPv6 address, you must contain the address in braces (`[]`).
-

--config-file configuration_file

Specifies the absolute path and file name to store the `nds.conf` configuration file. For example, to store the configuration file in the `/etc/opt/novell/eDirectory/directory`, enter the following command:

```
--config-file /etc/opt/novell/eDirectory/nds.conf
```

-P LDAP_URL(s)

Allows the LDAP URLs to configure the LDAP interface on the LDAP Server object. Uses commas to separate multiple URLs. For example:

```
-P ldap://1.2.3.4:1389,ldaps://1.2.3.4:1636,ldap://[2015::3]:389
```

NOTE

- ◆ To specify an IPv6 address, you must contain the address in braces (`[]`). For example, `ldap://[2015::3]:389`.
 - ◆ If you do not specify the LDAP URLs during the initial configuration, you can add them in the `ldapInterfaces` attribute using the `ldapconfig` command or in iManager after the initial configuration. For more information, see [“Adding LDAP URLs for IPV6 on the LDAP Server Object” on page 101](#).
-

-D path_for_data

Creates the `data`, `dib`, and `log` directories in the specified path.

set valuelist

Sets the value for the configurable parameters that you specified for the Identity Vault. Use this option to set the bootstrapping parameters before configuring a tree.

When you change configuration parameters, you must restart `nds` for the new value to take effect. You do not need to restart `nds` for the following configuration parameters:

- ◆ `n4u.nds.inactivity-synchronization-interval`
- ◆ `n4u.nds.synchronization-restrictions`
- ◆ `n4u.nds.janitor-interval`
- ◆ `n4u.nds.backlink-interval`
- ◆ `n4u.nds.drl-interval`
- ◆ `n4u.nds.flatcleaning-interval`
- ◆ `n4u.nds.server-state-up-threshold`
- ◆ `n4u.nds.heartbeat-schema`
- ◆ `n4u.nds.heartbeat-data`

get help paramlist

Displays the help strings for the configurable parameters that you specified for the Identity Vault. If you do not specify a parameter list, the utility lists the help strings for all of the configurable parameters.

13.1.2 Configuring the Identity Vault in a Specific Locale

To configure the Identity Vault in a specific locale, you must export `LC_ALL` and `LANG` to that particular locale before performing the configuration. For example, enter the following commands in the `ndsconfig` utility:

```
export LC_ALL=ja
export LANG=ja
```

13.1.3 Adding a New Tree to the Identity Vault

When you create a new tree in the Identity Vault, the `ndsconfig` utility can walk you through the configuration or you can enter a single command to specify all the parameter values. You can specify an IPv6 address for the new tree, if your Identity Vault server already supports IPv6 addresses.

- 1 (Conditional) To have the `ndsconfig` utility prompt you for the parameters for a new tree in the Identity Vault, enter the following command:

```
ndsconfig new [-t tree_name] [-n server_context] [-a admin_FDN]
```

For example:

```
ndsconfig new -t corp-tree -n o=company -a cn=admin.o=company
```

- 2 (Conditional) To create a new tree in the Identity Vault by specifying all the parameters in the command line, enter the following text:

```
ndsconfig new [-t treename] [-n server_context] [-a admin_FDN] [-i] [-S server_name] [-d path_for_dib] [-m module] [e] [-L ldap_port] [-l SSL_port] [-o http_port] [-O https_port] [-p IP_address:[port]] [-R] [-c] [-w admin_password] [-b port_to_bind] [-B interface1@port1,interface2@port2,..] [-D custom_location] [--config-file configuration_file]
```

or

```
ndsconfig def [-t treename] [-n server_context] [-a admin_FDN] [-w admin_password] [-c] [-i] [-S server_name] [-d path_for_dib] [-m module] [-e] [-L ldap_port] [-l SSL_port] [-o http_port] [-O https_port] [-D custom_location] [--config-file configuration_file]
```

13.1.4 Adding a Server to an Existing Tree

To add a server to an existing tree, enter the following command:

```
ndsconfig add [-t treename] [-n server context] [-a admin_FDN] [-i] [-S server_name] [-d path_for_dib] [-m module] [e] [-L ldap_port] [-l SSL_port] [-o http_port] [-O https_port] [-p IP_address:[port]] [-R] [-c] [-w admin_password] [-b port_to_bind] [-B interface1@port1,interface2@port2,..] [-D custom_location] [--config-file configuration_file]
```

For example:

```
ndsconfig add -t corp-tree -n o=company -a cn=admin.o=company -S srv1
```

13.1.5 Removing the Identity Vault and its Database from the Server

- 1 Navigate to the dsreports directory, located by default in /var/opt/novell/eDirectory/data/.
- 2 Delete the HTML files that you previously created using iMonitor.
- 3 Using the ndsconfig utility, enter the following command:

```
ndsconfig rm [-a admin_FDN] [-w admin_password] [-p IP_address:[port]] [-c]
```

13.1.6 Removing an eDirectory Server Object and Directory Services from a Tree

To remove the server object and directory services from a tree, enter the following command:

```
ndsconfig rm -a Admin_FDN
```

13.1.7 Configuring Multiple Instances of the Identity Vault

You can configure multiple instances of the Identity Vault on a single host. The method to configure multiple instance with the `ndsconfig` utility is similar to configuring a single instance multiple times. Each instance should have unique instance identifiers, such as the following:

- ◆ Different data and log file location. Use the `--config-file`, `-d`, and `-D` options.
- ◆ Unique port number for the instance to listen to. Use the `-b` and `-B` options.
- ◆ Unique server name for the instance. Use the `-S server name` option.

For more information, see “Using `ndsconfig` to Configure Multiple Instances of eDirectory” (<https://www.netiq.com/documentation/edir88/edirin88/data/a79kg0w.html#bqs8mmt>) in the *NetIQ eDirectory Installation Guide*.

NOTE:

- ◆ During configuration of the Identity Vault, the default NCP server name is set as the host server name. When configuring multiple instances, you must change the NCP server name. Use the `ndsconfig` command line option, `-S server_name` to specify a different server name. When configuring multiple instances, either on the same tree or on different trees, the NCP server name should be unique.
 - ◆ All the instances share the same server key (NICI).
-

13.2 Managing Instances with the `ndsmanage` Utility

The `ndsmanage` utility enables you to create, start, and stop server instances in the Identity Vault. You can also view a list of configured instances.

13.2.1 Listing Identity Vault Instances

You can use the `ndsmanage` utility to view the configuration file path, fully distinguished name and port for the server instance, and the status of the instance (active or inactive) for specified users. The utility supports the following parameters:

`ndsmanage`

Lists all instances configured by you.

`ndsmanage -a|--all`

Lists instances of all the users who are using a particular installation of the Identity Vault.

`ndsmanage username`

Lists the instances configured by the specified user.

13.2.2 Creating a New Instance in the Identity Vault

- 1 At the command line, enter `ndsmanage`.
- 2 Enter `c`.
- 3 Follow the instructions at the command prompt to create the new instance.

13.2.3 Configuring and Deconfiguring an Instance in the Identity Vault

To configure an instance, enter the following command:

```
ndsconfig new -t treename -n server_context -a admin_FDN -b port_to_bind -D  
path_for_data
```

For example:

```
ndsconfig new -t mytree -n o=netiq -a cn=admin.o=company -b 1524 -D  
/home/mary/inst1/var --config-file /home/mary/inst1/nds.conf
```

NOTE: The Linux operating system restricts sockets creation on the mounted file system. With eDirectory, NetIQ recommends that you have the `var` directory on the local file system (-D option with `ndsconfig`) and the DIB directory can be of any file system (-d option with `ndsconfig`).

To deconfigure an instance:

- 1 At the command line, enter `ndsmanage`.
- 2 Select the instance that you want to deconfigure.
- 3 Enter `d`.

13.2.4 Invoking a Utility for an Instance in the Identity Vault

You can run utilities, such as DStTrace, against an instance. For example, you want to run the DStTrace utility for instance 1 that is listening on port 1524, with its configuration file in the `/home/mary/inst1/nds.conf` directory and its DIB file in the `/home/mary/inst1/var` directory. You can enter one of the following commands:

```
ndstrace --config-file /home/mary/inst1/nds.conf
```

or

```
ndstrace -h 164.99.146.109:1524
```

If you do not specify the instance identifiers, the utility displays all of your instances. You can then select an instance.

13.2.5 Starting and Stopping Instances in the Identity Vault

You can start or stop one or more instances that you configured.

- 1 (Conditional) For a guided process in starting or stopping a single instance, complete the following steps:
 - 1a At the command line, enter `ndsmanage`.
 - 1b Select the instance that you want to start or stop.
 - 1c Enter `s` or `k` to start or stop the instance, respectively.
- 2 (Conditional) To start or stop a single instance, enter:

```
ndsmanage start --config-file configuration_file_of_the_instance
```

or

```
ndsmanage stop --config-file configuration_file_of_the_instance
```

3 (Conditional) To start or stop all instances, enter:

```
ndsmanage startall
```

or

```
ndsmanage stopall
```

IV Installing the Identity Manager Engine

This section provides information about installing the Identity Manager engine, formerly known as the Metadirectory. NetIQ recommends that you review the installation process before beginning. For more information, see [Section 14.1, “Checklist for Installing the Identity Manager Engine,” on page 139](#).

14 Installing the Identity Manager Engine

The Identity Manager engine processes the data changes that occur in the Identity Vault and connected applications. The engine has also been called the Identity Manager Metadirectory engine.

This section guides you through the process of installing the required components for the Identity Manager engine. By default, the installation program installs these components in the following locations:

- ♦ **Linux and UNIX:** /opt/novell/idm
- ♦ **Windows:** C:\Novell\IDM

14.1 Checklist for Installing the Identity Manager Engine

Before beginning the installation process, NetIQ recommends that you review the following steps.

	Checklist Items
<input type="checkbox"/>	1. Learn about the interaction among Identity Manager components. For more information, see Section 3.3.2, "Identity Manager Engine," on page 28.
<input type="checkbox"/>	2. Ensure that the Identity Vault has been installed and that it contains a tree with at least one organizational unit, one user, and an iManager server. For more information, see Chapter 10, "Installing the Identity Vault on a Linux Server," on page 107.
<input type="checkbox"/>	3. Review the considerations for installing the Identity Manager engine to ensure that the computers meet the prerequisites. For more information, see Section 6.4, "Prerequisites and Requirements for Installing the Identity Manager Engine," on page 58.
<input type="checkbox"/>	4. Review the hardware and software requirements for the computers that will host the Identity Manager engine. For more information, see Section 6.5.6, "System Requirements for iManager (Server Version)," on page 64 and Section 6.5.7, "System Requirements for iManager Workstation (Client Version)," on page 66.
<input type="checkbox"/>	5. Learn which drivers automatically become activated after installing the Identity Manager engine. For more information, see Section 6.4.1, "Considerations for Installing Drivers with the Identity Manager Engine," on page 59.
<input type="checkbox"/>	6. (Conditional) For computers running an RHEL 6.x operating system, ensure that you have installed the appropriate set of libraries. For more information, see Section 6.1, "Installing Identity Manager on an RHEL 6.x Server," on page 45.
<input type="checkbox"/>	7. (Conditional) For a guided installation process (wizard) of the Identity Manager engine, see one of the following sections: <ul style="list-style-type: none">♦ Section 14.3.1, "Installing the Identity Manager Engine as a Root User," on page 140♦ Section 14.3.2, "Installing the Identity Manager Engine as a Non-root User," on page 142
<input type="checkbox"/>	8. (Conditional) To install the Identity Manager engine in a single command, see Section 14.4, "Performing a Silent Installation of the Identity Manager Engine," on page 143.

	Checklist Items
<input type="checkbox"/>	9. Install the Identity Manager engine. For more information, see Chapter 14, "Installing the Identity Manager Engine," on page 139.
<input type="checkbox"/>	10. Install the rest of the Identity Manager components, including the Roles Based Provisioning Module and the Identity Information Warehouse.

14.2 Verifying Environment Variables (UNIX / Linux) for the Identity Manager Installation

When installing the Identity Manager engine on Linux and UNIX servers, ensure that the system's environment variables set the path for the Identity Vault installation. To verify that the environment variables for eDirectory are exported, enter the following command at the command prompt:

```
set | grep PATH
```

If the environment variables are set, the system responds with the path to the Identity Vault installation. If the environment variables are not configured already, enter the following command for your current shell:

```
. /opt/novell/eDirectory/bin/ndspath
```

You must include the space between the . and the / for the command to work. For more information, see "Using the nds-install Utility to Install eDirectory Components" (<http://www.novell.com/documentation/edir88/edirin88/index.html?page=/documentation/edir88/edirin88/data/a79kg0w.html#ai39feq>).

14.3 Using the Wizard to Install the Identity Manager Engine

The installation program (wizard) guides you through the configuration settings for the Identity Manager engine. The program installs the Identity Manager engine, Web components, and utilities for the different platforms that Identity Manager supports.

On UNIX and Windows computers, the installation program automatically defaults to wizard mode. To perform a silent installation, see [Section 14.4, "Performing a Silent Installation of the Identity Manager Engine,"](#) on page 143.

NOTE: Your choice of performing the installation as a `root` or a non-`root` user should match the method that you used for installing the Identity Vault.

14.3.1 Installing the Identity Manager Engine as a Root User

This section describes the guided process for using the installation wizard to install the Identity Manager engine as a `root` user or as an administrator on a Windows computer. Use the following installation programs for your platform:

- ♦ **Linux:** `IDM4.0.2_Lin/products/IDM/install.bin`
- ♦ **Solaris:** `IDM4.0.2_Solaris/products/IDM/install.bin`
- ♦ **Windows:** `IDM4.0.2_Win:\products\IDM\windows\setup\idm_install.exe`

NOTE: The steps outlined in this procedure refer to the installation wizard as it appears in the console.

To install the Identity Manager engine as a root or administrative user:

- 1 Log on as `root` or administrator on the computer where you want to install the Identity Manager engine.
 - 2 (Conditional) To execute the binary files on Linux or Solaris computers, complete one of the following options:
 - ♦ For the guided process from the command line, enter `./install.bin -i console`.
 - ♦ For the wizard (GUI), enter `./install.bin [-i gui]`.
 - 3 (Conditional) On Windows computers, launch the `idm_install.exe` program.
 - 4 In the Welcome page of the installation program, specify the language that you want to use for installation, and then click **OK**.
 - 5 In the License Agreement window, click **I accept the terms of the License Agreement** and then click **Next**.
 - 6 In the Select Components window, complete the following steps:
 - 6a (Conditional) To install the Identity Manager engine on the same server where you installed the Identity Vault, select **Novell Identity Manager Metadirectory Server**.

This option requires that the Identity Vault be installed on the server. The installation program installs a 32-bit or a 64-bit Identity Manager based on the version of the Identity Vault (eDirectory). The installation process extends the schema for Identity Manager and installs the Identity Manager engine (Metadirectory server) and the Identity Manager drivers.
 - 6b To install the Remote Loader Service and its drivers, select one or more of the following components:
 - ♦ **Novell Identity Manager Connected System Server (32-bit)**

This option does not require the Identity Vault to be installed on this server. Select this option only if you are installing the 32-bit Remote Loader. For more information, see [Chapter 19, "Installing Remote Loader," on page 173](#).
 - ♦ **Novell Identity Manager Connected System Server (64-bit)**

This option does not require the Identity Vault to be installed on this server. Select this option only if you are installing the 64-bit Remote Loader. For more information, see [Chapter 19, "Installing Remote Loader," on page 173](#).
 - ♦ *Novell Identity Manager Connected System Server (.NET)*

(Windows only) This option installs the .NET Remote Loader service and the SharePoint driver on the server.
 - 6c (Optional) If you previously installed iManager on the server, select **Novell Identity Manager Plug-ins for Identity Manager**.
 - 6d (Optional) To configure the drivers for the connected systems, select **Utilities**.
-
- NOTE:** Not all drivers have utilities.
-
- 6e (Optional) To specify which components to install, select **Customize the selected components**.
 - 7 (Conditional) If you chose **Customize the selected components** in [Step 6e](#), select the utilities and other components that you want to install.

- 8 Specify a user account and its password with sufficient rights in eDirectory to extend the schema. Specify the user name in the LDAP format. For example, `cn=idmadmin,o=company`.
- 9 In the Activation Notice window, click **OK**. For more information, see [Chapter 45, “Activating Identity Manager,”](#) on page 407.
- 10 Specify the paths where you want to install the selected components.
- 11 In the Select Shortcuts to Create window, specify the shortcuts that you want to add to the server.
- 12 In the Pre-Installation Summary window, verify the settings.
- 13 Click **Install**.
- 14 Activate Identity Manager. For more information, see [Chapter 45, “Activating Identity Manager,”](#) on page 407.
- 15 To create and configure your driver objects, consult the specific guide for that driver. For more information, see [Identity Manager Drivers documentation \(http://www.novell.com/documentation/idm401drivers/\)](http://www.novell.com/documentation/idm401drivers/).
- 16 (Optional) For the default installation locations, see the `/tmp/idmInstall.log` file.

14.3.2 Installing the Identity Manager Engine as a Non-root User

You can install Identity Manager as a `non-root` user to enhance the security of your UNIX or Linux server. You cannot install Identity Manager as a `non-root` user if you installed the Identity Vault as `root`.

When you use this method, you cannot install the following components:

- ♦ **Remote Loader:** To install the Remote Loader as a `non-root` user, use the Java Remote Loader. For more information, see [Section 19.3, “Installing the Java Remote Loader on UNIX or Linux,”](#) on page 176.
- ♦ **UNIX/Linux Account Driver:** Requires `root` privileges to function.
- ♦ **Novell Audit Platform Agent:** Install Novell Audit Platform Agent by `root`. The platform agent reports events to the audit server (Novell Audit or Sentinel). You can configure the platform agent through the `logevent` configuration file in the `/etc/logevent.conf` location.

The `logevent` file provides the configuration information that the platform agent needs to communicate with the audit server. By default, the events are logged into the `/var/opt/novell/idm/audit` location. This location must have the write permission for a `non-root` user. To log events into a different location, specify it in the `logevent` file. For more information about the structure of the `logevent` configuration file, refer to [Configuring the Platform Agent](#) in the *Novell Audit Installation Guide*.

To install the Identity Manager engine as a non-root user:

- 1 Log on as the `non-root` user that you used to install the Identity Vault.
The user account must have write access to the directories and files of the `non-root` Identity Vault (eDirectory) installation.
- 2 Execute the installation program:
 - ♦ **Linux:** `IDM4.0.2_Lin/products/IDM/linux/setup/idm-nonroot-install`
 - ♦ **Solaris:** `IDM4.0.2_Solaris/products/IDM/solaris/setup/idm-nonroot-install`
- 3 Use the following information to complete the installation:

Base Directory for the non-root eDirectory Installation: Specify the directory where the `non-root` eDirectory installation is. For example, `/home/user/install/eDirectory`.

Extend eDirectory Schema: If this is the first Identity Manager server installed in this instance of eDirectory, enter `Y` to extend the schema. If the schema is not extended, Identity Manager cannot function.

You are prompted to extend the schema for each instance of eDirectory owned by the `non-root` user that is hosted by the `non-root` eDirectory installation.

If you select to extend the schema, specify the full distinguished name (DN) of the eDirectory user who has rights to extend the schema. The user must have the Supervisor right to the entire tree to extend the schema. For more information about extending the schema as a `non-root` user, see the `schema.log` file that is placed in the `data` directory for each instance of eDirectory.

Run the `/opt/novell/eDirectory/bin/idm-install-schema` program to extend the schema on additional eDirectory instances after the installation is complete.

Utilities: (Optional) If you need an Identity Manager driver utility, copy the utilities from the Identity Manager installation media to the Identity Manager server. All utilities are found in the `IDM4.0.2_platform/product/IDM/platform/setup/utilities` directory.

- 4 Activate Identity Manager. For more information, see [Chapter 45, “Activating Identity Manager,” on page 407](#).
- 5 To create and configure your driver objects, consult the specific guide for that driver. For more information, see [Identity Manager Drivers documentation \(http://www.novell.com/documentation/idm401drivers/\)](http://www.novell.com/documentation/idm401drivers/).

14.4 Performing a Silent Installation of the Identity Manager Engine

To run a silent installation of Identity Manager, create a properties file with the parameters required to complete the installation. The Identity Manager media includes a sample file included:

- ♦ **Linux:** `IDM4.0.2_Lin/products/IDM/linux/setup/silent.properties`
- ♦ **Solaris:** `IDM4.0.2_Solaris/products/IDM/solaris/setup/silent.properties`
- ♦ **Windows:** `IDM4.0.2_Win:\products\IDM\windows\setup\silent.properties`

Start the silent installation by using the correct program for your platform:

- ♦ **Linux:** `IDM4.0.2_Lin/products/IDM/install.bin -i silent -f filename.properties`
- ♦ **Solaris:** `IDM4.0.2_Solaris/products/IDM/install.bin -i silent -f filename.properties`
- ♦ **Windows:** `IDM4.0.2_Win:\products\IDM\windows\setup\idm_install.exe -i silent -f filename.properties`

Create a property file `filename.properties` with the following attributes, in the location from where you run the Identity Manager installer:

```
EDIR_USER_NAME=cn=admin,o=test
EDIR_USER_PASSWORD=test
METADIRECTORY_SERVER_SELECTED=true
CONNECTED_SYSTEM_SELECTED=false
X64_CONNECTED_SYSTEM_SELECTED=false
WEB_ADMIN_SELECTED=false
UTILITIES_SELECTED=false
```

For default installed locations, see the `/tmp/idmInstall.log` file.

If you have installed iManager, and you later want to install iManager plug-ins, you must set the `WEB_ADMIN_SELECTED` value to `true`.

If you want to do a silent installation of Identity Manager on multiple instances, ensure that the `filename.properties` file has the following lines:

```
EDIR_NCP_PORT=524
EDIR_NDS_CONF=/etc/opt/novell/eDirectory/conf
EDIR_IP_ADDRESS=xxx.xx.xx.xx
```

The password is stored in a file for the silent installation of Metadirectory. You can also use the `EDIR_USER_PASSWORD` environment variable to supply the password instead of writing it in a file. If the `EDIR_USER_PASSWORD` variable is not set in the properties file, the installer reads the value from the `EDIR_USER_PASSWORD` environment variable.

14.5 Adding Support for Graphics in Email Notifications

If you install the Identity Vault and the Identity Manager engine as a non-root user, email notifications might fail to include the graphics or images provided in the email template. For example, when running the `do-send-email-from-template` action, Identity Manager sends the email but the included images are blank. You must update the driverset to ensure graphic support.

- 1 Log into your project in Designer.
- 2 In the Outline pane, expand **Identity Vault**.
- 3 Right-click **Driver Set**.
- 4 Select **Properties > Java**.
- 5 For JVM options, enter the following content:

```
-Dcom.novell.nds.dirxml.util.mail.templatepath=path_to_graphics_files
```

For example:

```
-Dcom.novell.nds.dirxml.util.mail.templatepath=/prod/eDirectory/opt/novell/eDirectory/lib/dirxml/rules/manualtask/mt_files
```

- 6 Click **OK**.
- 7 Deploy the changes to the driverset:
 - 7a Right-click **Driver Set**.
 - 7b Select **Live > Deploy**.
 - 7c Select **Deploy**.
- 8 Restart eDirectory.

V Installing iManager

This section guides you through the process of installing the required components for iManager. The setup programs can install the following components:

- ♦ iManager (server version)
- ♦ iManager Workstation (client version)
- ♦ Java
- ♦ Novell International Cryptographic Infrastructure (NICI)
- ♦ Tomcat

The installation files are located in the `products/iManager/installs/server_platform/` directory within the `.iso` image file for the Identity Manager installation package. By default, the installation program installs the components in the following locations:

- ♦ **Linux:** `/opt/novell/idm`
- ♦ **Windows:** `C:\Novell\IDM`

NetIQ recommends that you review the installation process before beginning. For more information, see [Chapter 15, “Checklist for Installing iManager,” on page 147](#).

15 Checklist for Installing iManager

Before beginning the installation process, NetIQ recommends that you review the following steps.

	Checklist Items
<input type="checkbox"/>	1. Learn about the interaction among Identity Manager components. For more information, see Chapter 1, “Understanding the Architecture of Identity Manager,” on page 21.
<input type="checkbox"/>	2. Understand the difference between iManager and iManager Workstation. For more information, see Section 6.5.1, “Understanding the Server and Client Versions of iManager,” on page 61.
<input type="checkbox"/>	3. (Conditional) To ensure that Linux computers meet the prerequisites for installing iManager and iManager Workstation, review the following considerations: <ul style="list-style-type: none">◆ For iManager, see Section 6.5.2, “Considerations for Installing iManager on a Linux Platform,” on page 62◆ For iManager Workstation, see Section 6.5.4, “Considerations for Installing iManager Workstation on Linux Clients,” on page 63
<input type="checkbox"/>	4. (Conditional) To ensure that Windows computers meet the prerequisites for installing iManager and iManager Workstation, review the following considerations: <ul style="list-style-type: none">◆ For iManager, see Section 6.5.3, “Considerations for Installing iManager on a Windows Platform,” on page 63◆ For iManager Workstation, see Section 6.5.5, “Considerations for Installing iManager Workstation on Windows Clients,” on page 64
<input type="checkbox"/>	5. Review the hardware and software requirements for the computers that will host iManager: <ul style="list-style-type: none">◆ For iManager, see Section 6.5.6, “System Requirements for iManager (Server Version),” on page 64◆ For iManager Workstation, see Section 6.5.7, “System Requirements for iManager Workstation (Client Version),” on page 66
<input type="checkbox"/>	6. Access the installation files for iManager, located by default in the <code>products/iManager/installs/server_platform/</code> directory within the <code>.iso</code> image file for the Identity Manager installation package. Alternatively, download the installation files from the Novell Downloads Web site (http://download.novell.com) . Search for iManager products, select the iManager version that you want, then download the <code>.tgz</code> and <code>tar.bz2</code> or <code>win.zip</code> file to a directory on your server. For example, <code>iMan_277_linux.tgz</code> and <code>iMan_277_workstation_linux.tar.bz2</code> or <code>iMan_277_win.zip</code> .
<input type="checkbox"/>	7. (Optional) To learn more about the process for installing plug-ins, see Section 16.1, “Understanding Installation for iManager Plug-ins,” on page 149.
<input type="checkbox"/>	8. (Optional) To review actions that you can perform after installing iManager, see Chapter 17, “Post-Installation Tasks for iManager,” on page 161.

	Checklist Items
<input type="checkbox"/>	<p>9. To install iManager and iManager Workstation, see the following sections:</p> <ul style="list-style-type: none">◆ For Linux computers, see Section 16.2, “Installing iManager and iManager Workstation on Linux,” on page 150◆ For Windows computers, see Section 16.3, “Installing iManager and iManager Workstation on Windows,” on page 153◆ For a silent installation, see Section 16.4, “Installing iManager Silently,” on page 157

16 Installing iManager Server and Workstation

This chapter describes the process for installing iManager. To prepare for the installation, review the prerequisites and system requirements provided in [Section 6.5, “Prerequisites and Requirements for Installing iManager,”](#) on page 61 .

To review the full installation process, see the [“Checklist for Installing iManager”](#) on page 147.

16.1 Understanding Installation for iManager Plug-ins

By default, the plug-in modules are not replicated between iManager servers. You must install the plug-in modules that you want on each iManager server.

In a clean install, the setup program preselects the “typical” plug-ins. For an upgrade, only plug-ins that need to be updated are preselected. You can override the default selections and add new plug-ins to download. However, for an upgrade, NetIQ recommends that you do not unselect any plug-in that was pre-selected. As a general rule, you should always upgrade plug-ins that you installed with a previous version of iManager. Also, more recent plug-ins might not be compatible with previous versions of iManager.

The base plug-ins for iManager are available only as part of the complete iManager software download (for example, eDirectory administrative plug-ins). Unless there are specific updates to these plug-ins, you can only download and install them with the entire iManager product.

The installation program uses an XML descriptor file, `iman_mod_desc.xml`, to identify the plug-ins that are available for downloading. The default URL for the file is http://www.novell.com/products/containers/imanager/iman_mod_desc.xml. However, you can point the installation program to an alternative network URL. For example, you might be installing iManager behind a proxy or firewall that prevents the installation program from accessing the default URL.

IMPORTANT: You must use the latest iManager SDK to re-compile any custom plug-ins that you want to use with the newly installed version environment.

For instructions about downloading and installing plug-ins, see the steps in one of the following sections:

- ♦ **For Linux computers**, see [Section 16.2, “Installing iManager and iManager Workstation on Linux,”](#) on page 150
- ♦ **For Windows computers**, see [Section 16.3, “Installing iManager and iManager Workstation on Windows,”](#) on page 153
- ♦ **For a silent installation**, see [Section 16.4, “Installing iManager Silently,”](#) on page 157

For more information about customizing the process for downloading and installing plug-ins, see [“Downloading and Installing Plug-in Modules”](https://www.netiq.com/documentation/imanager/imanager_install/data/bs3h82n.html#bs3h82n) (https://www.netiq.com/documentation/imanager/imanager_install/data/bs3h82n.html#bs3h82n) in the *NetIQ iManager Installation Guide*.

16.2 Installing iManager and iManager Workstation on Linux

This section provides the steps for installing iManager and iManager Workstation on Linux servers and clients. To prepare for the installation, review the prerequisites and system requirements:

- ♦ For iManager, see [Section 6.5.2, “Considerations for Installing iManager on a Linux Platform,” on page 62](#) and [Section 6.5.6, “System Requirements for iManager \(Server Version\),” on page 64](#).
- ♦ For iManager Workstation, see [Section 6.5.4, “Considerations for Installing iManager Workstation on Linux Clients,” on page 63](#) and [Section 6.5.7, “System Requirements for iManager Workstation \(Client Version\),” on page 66](#).
- ♦ Also see the Release Notes accompanying the release.

16.2.1 Installing iManager on Linux

The following procedure describes how to install the server version of iManager on a Linux server using an installation wizard, either in GUI format or from the console. To perform a silent, unattended installation, see [Section 16.4, “Installing iManager Silently,” on page 157](#).

If the setup program for iManager Server detects a previously installed version of iManager, it might give you the option to stop the installation process or remove the existing iManager, JRE, and Tomcat installations.

After a successful installation, the setup program generates a configuration file, by default `/var/log/install.properties`, with values based on the questions asked during the installation. You can modify this file for use in a silent installation. For more information, see [Section 16.4, “Installing iManager Silently,” on page 157](#).

To install iManager on Linux:

- 1 Log on as `root` or `root`-equivalent to the computer where you want to run the installation program.
- 2 (Conditional) If you have the `.iso` image file for the Identity Manager installation package, navigate to the directory containing the iManager installation files, located by default in the `products/iManager/installs/Linux/` directory.
- 3 (Conditional) If you downloaded the iManager installation files from the [Novell Downloads Web site \(http://download.novell.com\)](http://download.novell.com), identify the `.tgz` file. For example, `iMan_277_linux.tgz`.
- 4 To extract the iManager folder, enter the following command:

```
tar -zxvf iMan_version_linux.tgz
```
- 5 In a shell, change to the `/extracted_directory/iManager/installs/linux` directory. This path is relative to the directory where you copied or extracted the iManager files.
- 6 (Conditional) To run a command-line (text) installation, enter the following command:

```
./iManagerInstallLinux.bin
```
- 7 (Conditional) To run the wizard for the installation program, enter the following command:

```
./iManagerInstallLinux.bin -i gui
```
- 8 At the splash screen, specify a language, and then click **OK**.
- 9 Read the Introduction, and then click **Next**.

- 10 Accept the License Agreement, and then click **Next**.
- 11 For the components that you want to install, specify **iManager, Tomcat, JVM**.

NOTE: You must select this option *only*. iManager will not work as expected if you select either of the other two options.

- 12 Click **Next**.
- 13 (Optional) To use IPv6 addresses with iManager, click **Yes** in the Enable IPv6 window.
You can enable IPv6 addresses after you install iManager. For more information, see [Section 17.2, "Configuring iManager for IPv6 Addresses after Installation," on page 164](#).
- 14 Click **Next**.
- 15 (Optional) To download and install plug-ins as part of the installation, complete the following steps:
 - 15a Specify that you want to download and install plug-ins, and then click **Next**.
 - 15b (Conditional) For a console install, enter a comma-separated list of the plug-in numbers that you want to download.
 - 15c (Conditional) If you are using the wizard program, select the check boxes of the plug-ins that you want to download.

(Optional) To download plug-ins from an different network location, specify an alternative **Network URL**.

When using an alternative URL for downloading plug-ins, you must verify the URL contents, and verify that the plug-in is appropriate for your use. By default, the installation program downloads plug-ins from http://www.novell.com/products/consoles/imanager/iman_mod_desc.xml. For more information, see [Section 16.1, "Understanding Installation for iManager Plug-ins," on page 149](#).
 - 15d Click **Next**.
 - 15e (Conditional)The setup program might display the following message:


```
No new or updated plug-ins found. All plug-ins are downloaded or updated or the iManager download server is unavailable.
```


If this occurs, one or more of the following conditions exist:
 - ◆ There are no updated plug-ins available from the download site.
 - ◆ There is a problem with your Internet connection. Verify your connection and try again.
 - ◆ Connection to the [Descriptor File \(http://www.novell.com/products/consoles/imanager/iman_mod_desc.xml\)](http://www.novell.com/products/consoles/imanager/iman_mod_desc.xml) was not successful. This URL refers to an XML descriptor file of available iManager plug-ins.
 - ◆ The iManager installation is behind a proxy that does not allow a connection to the above URL.
 - 15f Specify whether you want to install plug-ins from a local drive, and then click **Next**.
 - 15g (Conditional) To install plug-ins from a local directory, specify the directory path that contains the appropriate plug-in (.npm) files.

The default path is `/extracted location/iManager/installs/plugins`, but you can specify any valid mount point here.
 - 15h Click **Next**.
- 16 Specify the ports on which you want Tomcat to run.
The default ports are 8080 for HTTP, 8443 for HTTPS, and 9009 as the MOD_JK connector port.

- 17 Click **Next**.
- 18 (Optional) Specify an authorized user and the appropriate eDirectory tree name that this user will manage.

NOTE

- ◆ NetIQ does not recommend leaving these settings blank. If you leave these fields blank, iManager allows any user to install plug-ins and make changes to iManager server settings. You can specify an authorized user after completing the installation process. For more information, see [Section 17.3, “Specifying an Authorized User for eDirectory,”](#) on page 165.
 - ◆ The installation program does not validate the specified user credentials with eDirectory.
-

- 19 Click **Next**.
- 20 Read the Pre-Installation Summary page, and then click **Next**.
- 21 When the installation completes, click **Done**.
- 22 When the initialization of iManager finishes, click the first link in the Getting Started page, and then log on. For more information, see [“Accessing iManager” \(https://www.netiq.com/documentation/imanager/imanager_admin/data/bsxrjzp.html\)](https://www.netiq.com/documentation/imanager/imanager_admin/data/bsxrjzp.html) in the *NetIQ iManager 2.7.7 Administration Guide*.

NOTE: If you plan to run iManager Workstation as a non-root user in the future, do not run iManager as `root` the first time. For more information, see [Section 16.3, “Installing iManager and iManager Workstation on Windows,”](#) on page 153.

- 23 Use the `chmod` command to change the permissions on the following InstallAnywhere files to `644` (read) from `600` (write):

```
/var/opt/novell/tomcat7/webapps/nps/UninstallerData/.com.zerog.registry.xml  
  
/var/opt/novell/tomcat7/webapps/nps/UninstallerData/Uninstall_PluginName/  
.com.zerog.registry.xml
```

Do not modify the content in these files. Changing the content might affect other installations that use InstallAnywhere.

16.2.2 Installing iManager Workstation on Linux Clients

iManager Workstation is a self-contained environment. You can install multiple versions on the same workstation (including older versions of Mobile iManager). However, you should not attempt to run them concurrently. If you need to use different versions, run one version, close it, and then run the other version.

NOTE: You cannot run iManager Workstation from a path that includes spaces. For example, `products/NetIQ/iManager Workstation/working`.

To install iManager Workstation on Linux clients:

- 1 (Conditional) If you have the `.iso` image file for the Identity Manager installation package, navigate to the directory containing the iManager installation files, located by default in the `products/iManager/installs/Linux/` directory.
- 2 (Conditional) If you downloaded the iManager installation files from the [Novell Downloads Web site \(http://download.novell.com\)](http://download.novell.com), identify the `tar.bz2` file. For example, `iMan_277_workstation_linux.tar.bz2`.
- 3 To extract the `tar.bz2` file, enter the following command:


```
tar -xjvf iMan_277_workstation_linux.tar.bz2
```

The extraction creates an `imanager` folder in the same folder containing the `tar.bz2` file.

- 4 (Optional) To install or upgrade the Novell International Cryptography Infrastructure (NICI) software, complete the following steps:

- 4a Log on as `root` or a `root`-equivalent on the computer where you want to install or upgrade NICI.

- 4b From the `imanager/NICI/linux` directory, enter the following command:

```
rpm -Uvh nici.i586.rpm
```

This command installs NICI as a fresh install or upgrades an existing version of NICI.

- 5 (Conditional) To run iManager Workstation as a non-root user in the future, do not run iManager as `root` the first time. Navigate to the `imanager/bin` directory and execute the iManager Workstation startup script.

```
./iManager.sh
```

- 6 In the iManager login window, specify a user name, password, and an eDirectory tree.

For more information about accessing iManager, see “Accessing iManager” (https://www.netiq.com/documentation/imanager/imanager_admin/data/bsxrjzp.html) in the *NetIQ iManager 2.7.7 Administration Guide*.

- 7 (Optional) To enable IPv6 addresses, complete the following steps:

1. Open the `User_Install_Directory/Tomcat/conf/catalina.properties` file.
2. Set the following configuration entries in the `catalina.properties` file:

```
java.net.preferIPv4Stack=false
```

```
java.net.preferIPv4Addresses=true
```

3. Restart Tomcat.

16.3 Installing iManager and iManager Workstation on Windows

This section provides the steps for installing iManager and iManager Workstation on Windows servers and clients. To prepare for the installation, review the prerequisites and system requirements:

- ♦ **iManager:** [Section 6.5.2, “Considerations for Installing iManager on a Linux Platform,”](#) on page 62.
- ♦ **iManager Workstation:** [Section 6.5.4, “Considerations for Installing iManager Workstation on Linux Clients,”](#) on page 63.
- ♦ Also see the Release Notes accompanying the release.

16.3.1 Installing iManager on Windows

The following procedure describes how to install the server version of iManager on a Windows server using an installation wizard. To perform a silent, unattended installation, see [Section 16.4, “Installing iManager Silently,”](#) on page 157.

If the setup program for iManager Server detects a previously installed version of iManager, it might give you the option to stop the installation process or remove the existing iManager, JRE, and Tomcat installations. When the setup program removes the previously installed version of iManager, it backs up the directory structure to the old `TOMCAT_HOME` directory to preserve any previously created custom content.

To install iManager Server on Windows:

- 1 Log on as a user with administrator privileges on the computer where you want to install iManager.
- 2 (Conditional) If you have the `.iso` image file for the Identity Manager installation package, navigate to the directory containing the iManager installation files, located by default in the `products/iManager/installs/Win/` directory.
- 3 (Conditional) If you downloaded the iManager installation files from the [Novell Downloads Web site \(http://download.novell.com\)](http://download.novell.com), complete the following steps:
 - 3a Identify the `win.zip` file. For example, `iMan_277_win.zip`.
 - 3b Extract the `win.zip` file to a folder on the local computer.
- 4 Run `iManagerInstall.exe`, located by default in the `\iManager\installs\win` folder.
- 5 (Optional) To view the debug output of the installation program, hold the `Ctrl` key immediately after launching the installation program until a console window appears. For more information about debugging, see “[Troubleshooting](https://www.netiq.com/documentation/imanager/imanager_admin/data/bz4k320.html)” (https://www.netiq.com/documentation/imanager/imanager_admin/data/bz4k320.html) in the *NetIQ iManager 2.7.7 Administration Guide*.
- 6 In the iManager welcome window, select a language, and then click **OK**.
- 7 In the **Introduction** window, and then click **Next**.
- 8 Accept the License Agreement, and then click **Next**.
- 9 (Conditional) If your server already has a version of JVM or Tomcat or other supporting components that are installed as part of iManager, in the **Detection Summary** window, complete the following steps:
 - 9a Under **Install the following components**, verify that the versions listed for the components match the versions that you want to install.
 - 9b (Optional) If the setup program does not list the versions that you want to install, browse to the the appropriate components in the installation folder.
- 10 Click **Next**.
- 11 In the **Get PORT Input** window, specify the port numbers on which Tomcat server must run, and then click **Next**.

By default, the HTTP port and SSL port values are 8080 and 8443, respectively. However, if you have another service or Tomcat server using the default ports, you can specify different ports.
- 12 (Optional) To use IPv6 addresses with iManager, click **Yes** in the **Enable IPv6** window.

You can enable IPv6 addresses after you install iManager. For more information, see [Section 17.2, “Configuring iManager for IPv6 Addresses after Installation,”](#) on page 164.
- 13 Click **Next**.
- 14 In the **Choose Install Folder** window, specify the folder to store the installation files, and then click **Next**.

The default installation location is `C:\Program Files\Novell`.

- 15** (Optional) To download and install plug-ins as part of the installation, complete the following steps:

15a In the **Select Plug-ins to Download and Install** window, select the plug-ins that you want.

15b (Optional) To download plug-ins from an different network location, specify an alternative **Network URL**.

When using an alternative URL for downloading plug-ins, you must verify the URL contents, and verify that the plug-in is appropriate for your use. By default, the installation program downloads plug-ins from http://www.novell.com/products/consoles/imanager/iman_mod_desc.xml. For more information, see [Section 16.1, "Understanding Installation for iManager Plug-ins," on page 149](#).

15c Click **Next**.

15d (Conditional) The setup program might display the following message:

No new or updated plug-ins found. All plug-ins are downloaded or updated or the iManager download server is unavailable.

If you see this error, one or more of the following conditions exist:

- ◆ There are no updated plug-ins available from the download site.
- ◆ There is a problem with your Internet connection. Verify your connection and try again.
- ◆ Connection to the **Descriptor File** (http://www.novell.com/products/consoles/imanager/iman_mod_desc.xml) was not successful. This URL refers to an XML descriptor file of available iManager plug-ins.
- ◆ The iManager installation is behind a proxy that does not allow a connection to the above URL.

15e (Optional) To install plug-ins from a local directory, in the **Select Plug-ins to Install from Disk** window, specify the directory path that contains the appropriate `.npm` plug-in files.

This step allows you to install previously downloaded or custom plug-ins. The default path is `/extracted location/iManager/installs/plugins`. However, you can specify any valid path.

15f Click **Next**.

- 16** (Optional) In the **Get User and Tree Names** window, specify an authorized user and the name of the eDirectory tree that this user will manage.

NOTE

- ◆ If eDirectory uses a port other than the default port 524, you can specify the IP address or DNS name of the eDirectory server plus the port number. For example, to specify an IPv6 address, enter `https://[2001:db8::6]:1080/nps/servlet/webacc?taskId=fw.Startup&forceMaster=true`.
- ◆ NetIQ does not recommend leaving these settings blank. If you leave these fields blank, iManager allows any user to install plug-ins and make changes to iManager server settings. You can specify an authorized user after completing the installation process. For more information, see [Section 17.3, "Specifying an Authorized User for eDirectory," on page 165](#).
- ◆ The installation program does not validate the specified user credentials with eDirectory.

17 Click **Next**.

18 Read the Pre-installation summary page, and then click **Install**.

- 19 When the installation completes, the **Install Complete** window displays relevant messages about the success of the process.

NOTE: Despite a successful installation, the **Install Complete** window might display the following error message:

The installation of iManager *version* is complete, but some errors occurred during the install.
Please see the installation log *Log file path* for details. Press "Done" to quit the installer.

- 20 (Conditional) If the installer displays the error message shown in [Step 19](#), complete the following steps:

- 20a Note the path to the log file that the error message displays.

- 20b In the **Install Complete** window, click **Done**.

- 20c Open the log file.

- 20d (Conditional) If you find the following error in the log file, you can ignore the error message. The installation was successful, and iManager functions properly.

```
Custom Action: com.novell.application.iManager.install.InstallDLLs
Status: ERROR
Additional Notes: ERROR - class
com.novell.application.iManager.install.InstallDLLs
NonfatalInstallException C:\WINDOWS\system32\msvcr71.dll (The process
cannot access the file because it is being used by another process)
```

- 20e (Conditional) If the log file does not contain the error listed in [Step 20d](#), NetIQ recommends that you retry the installation.

- 21 Click **Done**.

- 22 When the initialization of iManager finishes, click the first link in the Getting Started page, and then log on. For more information, see ["Accessing iManager"](https://www.netiq.com/documentation/imanager/imanager_admin/data/bsxrjzp.html) (https://www.netiq.com/documentation/imanager/imanager_admin/data/bsxrjzp.html) in the *NetIQ iManager 2.7.7 Administration Guide*.

16.3.2 Installing iManager Workstation on Windows

iManager Workstation is a self-contained environment. You can install multiple versions on the same workstation (including older versions of Mobile iManager). However, you should not attempt to run them concurrently. If you need to use different versions, run one version, close it, and then run the other version.

NOTE: You cannot run iManager Workstation from a path that includes spaces. For example, `C:\NetIQ\iManager Workstation\working`.

To install iManager Workstation on Windows:

- 1 (Conditional) If you have the `.iso` image file for the Identity Manager installation package, navigate to the directory containing the iManager installation files, located by default in the `products/iManager/installs/win/` directory.
- 2 (Conditional) If you downloaded the iManager installation files from the [Novell Downloads Web site](http://download.novell.com) (<http://download.novell.com>), complete the following steps:
 - 2a Identify the `win.zip` file. For example, `iMan_277_workstation_win.zip`.
 - 2b Extract the `win.zip` file to a folder on the local computer.

- 3 From the `imanager\bin` folder, run the `iManager.bat` file.
- 4 In the iManager login window, specify the credentials for an authorized user and the eDirectory tree that this user manages.

For more information about accessing iManager, see “Accessing iManager” (https://www.netiq.com/documentation/imanager/imanager_admin/data/bsxrjzp.html) in the *NetIQ iManager 2.7.7 Administration Guide*.

- 5 (Optional) To enable IPv6 addresses, complete the following steps:
 1. Open the `User_Install_Directory/Tomcat/conf/catalina.properties` file.
 2. Set the following configuration entries in the `catalina.properties` file:

```
java.net.preferIPv4Stack=false  
  
java.net.preferIPv4Addresses=true
```

3. Restart the Tomcat service.

16.4 Installing iManager Silently

A silent (non-interactive) installation does not display a user interface or ask the user any questions. Instead, `InstallAnywhere` uses information from a default `install.properties` file. You can run the silent installation with the default file or edit the file to customize the installation process.

To prepare for the installation, review the prerequisites and system requirements:

- ♦ **iManager:** [Section 6.5.2, “Considerations for Installing iManager on a Linux Platform,” on page 62.](#)
- ♦ **iManager Workstation:** [Section 6.5.4, “Considerations for Installing iManager Workstation on Linux Clients,” on page 63.](#)
- ♦ Also see the Release Notes accompanying the release.

16.4.1 Editing the Properties File for a Customized Silent Installation

For more control over which modules are installed, you can customize the silent installation process.

- 1 Open the `install.properties` file, located by default in the `products/iManager` directory within the `.iso` image file for the Identity Manager installation package for each operating system environment directory.

NOTE: If you previously installed the current version of iManager on a server, you can use the `installer.properties` file that setup program generated. The file, located by default in the `/var/log` directory, contains the values that you specified during the installation.

- 2 In the properties file, add the following parameters and values:

`$PLUGIN_INSTALL MODE$`

Specifies the property that controls whether plug-ins are installed. Add one of the following values:

- ♦ `DISK` - (default) instructs the setup program to install the plug-ins from the local disk.
- ♦ `NET` - instructs the setup program to install the plug-ins from the network.

- ◆ BOTH - instructs the setup program to install the plug-ins from both disk and network.
- ◆ SKIP - does not install the plug-ins.

\$PLUGIN_DIR\$

Specifies an alternate path to plug-ins located on the local disk. The default path is *installer_root_directory/iManager/installs/platform_path/plugin*.

The installation program installs all modules in the plug-in directory, except for subdirectories.

\$PLUGIN_INSTALL_URL\$

Specifies the network URL where the installation program can download the plug-ins, by default http://www.novell.com/products/consoles/imanager/iman_mod_desc.xml. If you specify an alternative URL, you must verify the URL contents, and verify that the plug-in is appropriate for your use. For more information, see [Section 16.1, “Understanding Installation for iManager Plug-ins,”](#) on page 149.

\$LAUNCH_BROWSER\$

Specifies whether the installation program launches the *gettingstarted.html* file launches once the installation process completes.

\$USER_INSTALL_DIR\$

Specifies the path where you want iManager to be installed.

USER_INPUT_ENABLE_IPV6

Specifies whether to enable iManager to use IPv6 addresses. By default, the installation program sets this value to *yes*.

- 3 For each plug-in module that you want to download and install, specify the module ID and version from the *MANIFEST.MF* file, located in the *META-INF/* folder of the *.npm* (plug-in module). For example:

```
$PLUGIN_MODULE_ID_1$=eDirectoryBackupAndRestore
```

```
$PLUGIN_VERSION_1$=2.7.20050517
```

```
$PLUGIN_MODULE_ID_2$=ldap
```

```
$PLUGIN_VERSION_2$=2.7.20050517
```

NOTE

- ◆ If you do not specify any modules, the program installs the most commonly installed modules, tagged as “selected” in the *iman_mod_desc.xml* files on the download Web site.
 - ◆ If you do not define a version for a module, the setup program installs any module that matches the *.npm* name.
-

16.4.2 Running a Silent Installation for iManager

You can silently install iManager on a Linux or Windows server using the default values in the `install.properties` file, located by default in the `products/iManager` directory within the `.iso` image file for the Identity Manager installation package for each operating system environment directory. The `products/iManager` directory should also contain the installation executable file.

- 1 In a console window, go to the directory containing the `install.properties` file that you downloaded.
- 2 On the command line, enter one of the following commands:
 - ♦ **Linux:** `./iManagerInstallplatform.bin -i silent`
 - ♦ **Windows:** `iManagerInstall.exe -i silent`

17 Post-Installation Tasks for iManager

After you install iManager, you can modify the configuration settings, such as enabling IPv6 addressing or changing the authorized user for an eDirectory tree. Also, NetIQ recommends that you replace the self-signed certificates that the installation process created.

17.1 Replacing the Temporary Self-Signed Certificates for iManager

Standalone iManager installations include a temporary, self-signed certificate for use by Tomcat. It has an expiration date of one year. NetIQ provides this certificate to help you get your system up and running so you can securely use iManager immediately after you install the product. NetIQ and OpenSSL do not recommend using self-signed certificates except for testing purposes. Instead, you should replace the temporary certificate with a secure one.

Tomcat stores the self-signed certificate in a keystore that uses Tomcat (JKS) format file. Normally, you would import a private key to replace the certificate. However, the `keytool` that you use to modify the Tomcat keystore cannot import a private key. The tool only uses a self-generated key.

This section explains how to generate a public/private key pair in eDirectory using Novell Certificate Server and to replace the temporary certificate. If you are using eDirectory, you can use Novell Certificate Server to securely generate, track, store, and revoke certificates with no further investment.

NOTE: The information in this section does not apply to OES Linux, which installs both Tomcat and Apache. The OES Linux documentation includes information about replacing the self-signed Apache/Tomcat certificate.

17.1.1 Replacing the iManager Self-Signed Certificates on Linux

This section describes how to create a keypair in eDirectory and export the Public, Private, and Root Certificate Authority (CA) keys with a PKCS#12 file on the Linux platform. This includes modifying Tomcat's `server.xml` configuration file to use the PKCS12 directive and point the configuration to an actual P12 file rather than use the default JKS keystore.

This process uses the following files:

- ♦ `/var/opt/novell/novlwww/.keystore`, which holds the temporary keypair
- ♦ `/opt/novell/jdk1.7.0_25/jre/lib/security/cacerts`, which holds the trusted root certificates
- ♦ `/etc/opt/novell/tomcat7/server.xml`, which is used for configuring Tomcat's use of certificates

To replace the self-signed certificates on Linux:

- 1 To create a new certificate, complete the following steps:
 - 1a Log on to iManager.
 - 1b Click **Novell Certificate Server** > **Create Server Certificate**.

- 1c Select the appropriate server.
 - 1d Specify a nickname for the server.
 - 1e Accept the rest of the certificate defaults.
- 2 To export the server certificate to the Tomcat home directory, complete the following steps:
- 2a In iManager, select **Directory Administration > Modify Object**.
 - 2b Browse to and select the Key Material Object (KMO) object.
 - 2c Click **Certificates > Export**.
 - 2d Specify a password.
 - 2e Save the server certificate as a PKCS#12 (.pfx) in the /var/opt/novell/novlwww directory.
- 3 To convert the .pfx file to a .pem file, complete the following steps:
- 3a Enter a command, such as `openssl pkcs12 -in newtomcert.pfx -out newtomcert.pem`.
 - 3b Specify the same password for the certificate that you specified in [Step 2](#).
 - 3c Specify a password for the new .pem file.
You can use the same password, if desired.
- 4 To convert the .pem file to a .p12 file, complete the following steps:
- 4a Enter a command, such as `openssl pkcs12 -export -in newtomcert.pem -out newtomcert.p12 -name "New Tomcat"`.
 - 4b Specify the same password for the certificate that you specified in [Step 3](#).
 - 4c Specify a password for the new .p12 file.
You can use the same password, if desired.
- 5 To stop Tomcat, enter the following command:

```
/etc/init.d/novell-tomcat7 stop
```

- 6 To ensure that Tomcat uses the newly created .p12 certificate file, add `keystoreType`, `keystoreFile`, and `keystorePass` variables to the Tomcat configuration file, by default `/etc/opt/novell/tomcat7.0.42/server.xml`. For example:

```
<Connector className="org.apache.coyote.tomcat7.CoyoteConnector"
  port="8443" minProcessors="5" maxProcessors="75" enableLookups="true"
  acceptCount="100" debug="0" scheme="https" secure="true"
  useURValidationHack="false" disableUploadTimeout="true">
  <Factory className="org.apache.coyote.tomcat7.CoyoteServerSocketFactory"
    clientAuth="false" protocol="TLS" keystoreType="PKCS12"
    keystoreFile="/var/opt/novell/novlwww/newtomcert.p12" keystorePass="password"
  />
</Connector>
```

NOTE: When setting the keystore type to PKCS12, you must specify the entire path to the certificate file, as Tomcat will no longer default to using the Tomcat home path.

- 7 To ensure that the .p12 certificate file functions appropriately, complete the following steps:
 - 7a Change the file's ownership to the appropriate Tomcat user/group, by default novlwww. For example, `chown novlwww:novlwww newtomcert.p12`.
 - 7b Change the file permissions to `user=rw, group=rw, and others=r`. For example, `chmod 654 newtomcert.p12`.
- 8 To restart Tomcat, enter the following command:

```
/etc/init.d/novell-tomcat7 start
```

17.1.2 Replacing the iManager Self-Signed Certificates on Windows

This section describes how to create a keypair in eDirectory and export the Public, Private, and Root Certificate Authority (CA) keys with a PKCS#12 file on the Windows platform. This includes modifying Tomcat's `server.xml` configuration file to use the PKCS12 directive and point the configuration to an actual P12 file rather than use the default JKS keystore.

This process uses the following files:

- ♦ `C:\Program Files\Novell\Tomcat\conf\ssl\.keystore`, which holds the temporary keypair
- ♦ `C:\Program Files\Novell\jre\lib\security\cacerts`, which holds the trusted root certificates
- ♦ `C:\Program Files\Novell\Tomcat\conf\server.xml`, which is used for configuring Tomcat's use of certificates

To replace the self-signed certificates on Windows:

- 1 To create a new certificate, complete the following steps:
 - 1a Log on to iManager.
 - 1b Click **Novell Certificate Server > Create Server Certificate**.
 - 1c Select the appropriate server.
 - 1d Specify a nickname for the server.
 - 1e Accept the rest of the certificate defaults.
- 2 To export the server certificate, complete the following steps:
 - 2a In iManager, select **Directory Administration > Modify Object**.
 - 2b Browse to and select the Key Material Object (KMO) object.
 - 2c Click **Certificates > Export**.
 - 2d Specify a password.
 - 2e Save the server certificate as a PKCS#12 (.pfx).

- 3 To convert the `.pfx` file to a `.pem` file, complete the following steps:

NOTE: OpenSSL is not installed on Windows by default. However, you can download a version for the Windows platform from [OpenSSL Web site \(http://www.openssl.org/related/binaries.html\)](http://www.openssl.org/related/binaries.html). Alternatively, you can convert the certificate on a Linux platform, on which OpenSSL is installed by default. For more information about using Linux to convert the file, see [Section 17.1, “Replacing the Temporary Self-Signed Certificates for iManager,” on page 161.](#)

- 3a** Enter a command, such as `openssl pkcs12 -in newtomcert.pfx -out newtomcert.pem`.
 - 3b** Specify the same password for the certificate that you specified in [Step 2](#).
 - 3c** Specify a password for the new `.pem` file.
You can use the same password, if desired.
- 4 To convert the `.pem` file to a `.p12` file, complete the following steps:
 - 4a** Enter a command, such as `openssl pkcs12 -export -in newtomcert.pem -out newtomcert.p12 -name "New Tomcat"`.
 - 4b** Specify the same password for the certificate that you specified in [Step 3](#).
 - 4c** Specify a password for the new `.p12` file.
You can use the same password, if desired.
- 5 Copy the `.p12` file to the Tomcat certificate location, by default `C:\Program Files\Novell\Tomcat\conf\ssl\`.
- 6 To stop the Tomcat Service, enter the following command:

```
/etc/init.d/novell-tomcat7 stop
```
- 7 To ensure that Tomcat uses the newly created `.p12` certificate file, add `keystoreType`, `keystoreFile`, and `keystorePass` variables to the Tomcat `server.xml` file. For example:

```
<Connector className="org.apache.coyote.tomcat7.CoyoteConnector"
  port="8443" minProcessors="5" maxProcessors="75" enableLookups="true"
  acceptCount="100" debug="0" scheme="https" secure="true"
  useURISValidationHack="false" disableUploadTimeout="true">
  <Factory className="org.apache.coyote.tomcat7.CoyoteServerSocketFactory"
    clientAuth="false" protocol="TLS" keystoreType="PKCS12"
    keystoreFile="/conf/ssl/newtomcert.p12" keystorePass="password" />
```

When setting the keystore type to `PKCS12`, you must specify the entire path to the certificate file, as Tomcat will no longer default to using the Tomcat home path.
- 8 Start the Tomcat service.

17.2 Configuring iManager for IPv6 Addresses after Installation

After installing iManager, you can enable iManager to use IPv6 addresses.

1. Open the `catalina.properties` file in the installation directory, located by default in the following directories:
Linux: `/var/opt/novell/tomcat7/conf/` directory
Windows: `installation_directory\Tomcat\conf` folder
2. Set the following configuration entries in the properties file:

```
java.net.preferIPv4Stack=false  
java.net.preferIPv4Addresses=true
```

3. Restart Tomcat.

17.3 Specifying an Authorized User for eDirectory

After installing iManager, you can modify the credentials for the authorized user and the appropriate eDirectory tree name that this user manages. For more information, see “iManager Authorized Users and Groups” (https://www.netiq.com/documentation/manager/manager_admin/data/b7gginc.html) in the *NetIQ iManager 2.7.7 Administration Guide*.

- 1 Log on to iManager.
- 2 In the Configure view, select **iManager Server > Configure iManager > Security**.
- 3 Update the user credentials and tree name.

VI Installing the Remote Loader

In this section, you will install the Remote Loader or the Java Remote Loader and configure driver instances in the loader.

The installation files are located in the `products/IDM/` directory in the Identity Manager installation package. By default, the installation program installs the components in the following locations:

- ♦ **Linux:** `/opt/novell/idm`
- ♦ **Windows:** `C:\Novell\IDM`

NetIQ recommends that you review the installation process before beginning. For more information, see [Section 18.1, "Checklist for Installing the Remote Loader,"](#) on page 169.

18 Preparing to Install the Remote Loader

This section provides information that helps you prepare for installing the Remote Loader and the Java Remote Loader.

18.1 Checklist for Installing the Remote Loader

NetIQ recommends that you complete the steps in the following checklist:

	Checklist Items
<input type="checkbox"/>	1. Learn about the interaction among Identity Manager components. For more information, see Section 3.3.3, "Remote Loader," on page 29.
<input type="checkbox"/>	2. Ensure that the Identity Manager engine has been installed. For more information, see Chapter 14, "Installing the Identity Manager Engine," on page 139.
<input type="checkbox"/>	3. Review the considerations for installing the Remote Loader to ensure that the computers meet the prerequisites. For more information, see Section 6.6, "Prerequisites and Requirements for Installing the Remote Loader," on page 67.
<input type="checkbox"/>	4. Review the hardware and software requirements for the computers that will host the Remote Loader. For more information, see Section 6.6.2, "System Requirements for Installing the Remote Loader," on page 68.
<input type="checkbox"/>	5. Ensure that you can establish a secure connection to the Identity Manager engine. For more information, see Section 20.1, "Creating a Secure Connection to the Identity Manager Engine," on page 177.
<input type="checkbox"/>	6. Decide whether you want to install a 32-bit or 64-bit version of the Remote Loader. For more information, see Section 18.2, "Using 32-bit and 64-bit Remote Loader on the Same Computer," on page 170.
<input type="checkbox"/>	7. Decide whether you should use the Remote Loader or Java Remote Loader. For more information, see Section 18.3, "Understanding the Java Remote Loader," on page 170.
<input type="checkbox"/>	8. (Conditional) To perform a guided installation of the Remote Loader, see Section 19.1, "Installing the Remote Loader from the Console," on page 173.
<input type="checkbox"/>	9. (Conditional) To install the Remote Loader in a single command, see Section 19.2, "Installing the Remote Loader Silently," on page 174.
<input type="checkbox"/>	10. (Conditional) To install the Java Remote Loader, see Section 19.3, "Installing the Java Remote Loader on UNIX or Linux," on page 176.
<input type="checkbox"/>	11. (Conditional) If you perform a non-root install, update the driverset to support graphics in email notifications. For more information, see Section 14.5, "Adding Support for Graphics in Email Notifications," on page 144.
<input type="checkbox"/>	12. Review the parameters for configuring a driver instance. For more information, see Section 20.2.1, "Understanding the Configuration Parameters for the Remote Loader," on page 180.

	Checklist Items
<input type="checkbox"/>	13. To configure a driver instance in the Remote Loader, see one of the following sections: <ul style="list-style-type: none"> ◆ Section 20.2.2, “Configuring the Remote Loader for Driver Instances on UNIX or Linux,” on page 188 ◆ Section 20.2.3, “Configuring the Remote Loader for Driver Instances on Windows,” on page 190 ◆ Section 20.2.4, “Configuring the Java Remote Loader for Driver Instances,” on page 192
<input type="checkbox"/>	14. Prepare your drivers for the Remote Loader. For more information, see Section 20.3, “Configuring Identity Manager Drivers to Work with the Remote Loader,” on page 193.
<input type="checkbox"/>	15. Start the driver instance in the Remote Loader. For more information, see Section 21.1, “Starting a Driver Instance in the Remote Loader,” on page 195.
<input type="checkbox"/>	16. Install the rest of the Identity Manager components, including the Roles Based Provisioning Module and the Identity Information Warehouse.

18.2 Using 32-bit and 64-bit Remote Loader on the Same Computer

By default, the installation program detects the version of the operating system then installs the corresponding version of the Remote Loader. You can install both the 32-bit and 64-bit Remote Loader on a 64-bit operating system:

- ◆ If you are upgrading a 32-bit Remote Loader installed on a 64-bit operating system, the process upgrades the 32-bit Remote Loader to the latest version and also installs the 64-bit Remote Loader.
- ◆ If you choose to have both a 32-bit and a 64-bit Remote Loader on the same computer, the audit events are generated only with the 64-bit Remote Loader. If a 64-bit Remote Loader is installed before installing a 32-bit Remote Loader, the events are logged to the 32-bit cache.

18.3 Understanding the Java Remote Loader

The Remote Loader can host a remote interface shim (Identity Manager application shim) on the Identity Manager engine server. To control all the instances that host a Java remote interface shim, you must use Java Remote Loader. The Java Remote Loader is a Java application, which runs on any system with a compatible JRE (1.5.0 minimum) and Java Sockets. To open the application, run the shell script named `dirxml_jremote`.

IMPORTANT: The JRE 1.6 versions before update 24 ship with [CVE-2010-4476 security vulnerability](http://www.oracle.com/technetwork/topics/security/alert-cve-2010-4476-305811.html) (<http://www.oracle.com/technetwork/topics/security/alert-cve-2010-4476-305811.html>). This security vulnerability has been addressed in JRE 1.6.0-24. You must use the FPUUpdater tool from Sun to update your JRE to 1.6.0-24 version. For more information about installing the latest JRE, see the [JRE Patch Download Site](http://www.oracle.com/technetwork/java/javase/fpupdater-tool-readme-305936.html) (<http://www.oracle.com/technetwork/java/javase/fpupdater-tool-readme-305936.html>).

18.4 Understanding Shims

The Remote Loader uses shims to communicate with the application on a managed system. A *shim* is the file or files that contain the code to process the events that are synchronizing between the Identity Vault and the application. Before using the Remote Loader, you must configure the application shim to connect securely with the Identity Manager engine. You must also configure both the Remote Loader and the Identity Manager drivers.

For more information, see [Chapter 20, “Configuring the Remote Loader,”](#) on page 177.

19 Installing Remote Loader

The Remote Loader uses the following programs to communicate with the server that hosts the Identity Manager engine:

- ♦ **Linux and UNIX:** The `rdxml` executable enables the Identity Manager engine to communicate with the Identity Manager drivers running in Solaris or Linux environments.
- ♦ **Windows:** The Remote Loader Console uses `rlconsole.exe` to interface with `dirxml_remote.exe`, which is an executable that enables the Identity Manager engine server to communicate with the Identity Manager drivers running on Windows.

19.1 Installing the Remote Loader from the Console

The following procedure describes how to install the Remote Loader on a Linux or Windows platform using an installation wizard, either in GUI format or from the console. To perform a silent, unattended installation, see [“Installing the Remote Loader Silently” on page 174](#).

To prepare for the installation, review the prerequisites and system requirements listed in [Section 18.1, “Checklist for Installing the Remote Loader,” on page 169](#). Also see the Release Notes accompanying the release.

- 1 Log on as root or Administrator to the computer where you want to install the Remote Loader components.
- 2 To access the installation program, complete one of the following steps:
 - 2a (Conditional) If you have the `.iso` image file for the Identity Manager installation package, navigate to the directory containing the Remote Loader installation files:
 - ♦ **Linux and UNIX:** `products/IDM/`
 - ♦ **Windows:** `products/IDM/windows/setup`
 - 2b (Conditional) If you downloaded the Remote Loader installation files from the [Novell Downloads Web site \(http://download.novell.com\)](http://download.novell.com), complete the following steps:
 - 2b1 Navigate to the `.tgz` or `win.zip` file for the downloaded image.
 - 2b2 Extract the contents of the file to a folder on the local computer.
- 3 From the directory that contains the installation files, complete one of the following steps:
 - 3a **On Linux computers**, enter one of the following commands:
 - ♦ For the guided process from the command line: `./install.bin -i console`
 - ♦ For the GUI (wizard): `./install.bin`
 - 3b **On Solaris computers**, enter one of the following commands:
 - ♦ For the guided process from the command line: `./install.bin -i console`
 - ♦ For the GUI (wizard): `./install.bin]`
 - 3c **On Windows computers**, run `idm_install.exe`.
- 4 In the installation program, specify the language that you want to use for installation, and then click **OK**.
- 5 Review the Introduction text, and then click **Next**.

- 6 Accept the License Agreement, and then click **Next**.
- 7 For **Select Components**, specify the components that you want to install on the server.
For Windows computers, NetIQ recommends that you include **Novell Identity Manager Connected System Server (.NET)** in the selected components.
- 8 (Conditional) To specify which sub-components you want to install for the selected Remote Loader components, select **Customize the selected components**.
- 9 Click **Next**.
- 10 (Conditional) If you chose **Customize the selected components** in [Step 8](#), complete the following steps:
 - 10a For **Select Custom Components**, select the components that you want to install.

NOTE: NetIQ recommends the drivers that you should install. If you need to add another Remote Loader instance, you do not need to run the installation again.

 - 10b Click **Next**.
- 11 For the **Identity Manager Activation Notice**, click **OK**.
- 12 (Conditional) On Windows computers, specify a path where you would like to install each of the selected components, and then click **Next**.
- 13 (Optional) On Windows computers, select the shortcuts that you want to add to your system, and then click **Next**.
- 14 Read the **Pre-Installation Summary**, and then click **Install**.
- 15 When the installation completes, click **Done**.
- 16 Create and configure your driver objects to use the Remote Loader. This information is contained in each driver guide. For more information, see the [Identity Manager Drivers documentation \(http://www.novell.com/documentation/idm402drivers/\)](http://www.novell.com/documentation/idm402drivers/).
- 17 Create a Remote Loader configuration file to work with your connected system. For more information, see “[Configuring the Remote Loader for Linux/UNIX by Creating a Configuration File](#)” in the *Identity Manager 4.0.2 Remote Loader Guide*.

19.2 Installing the Remote Loader Silently

A silent (non-interactive) installation does not display a user interface or ask you any questions. Instead, InstallAnywhere uses information from a default `install.properties` file. You can run the silent installation with the default file or edit the file to customize the installation process. To perform a guided installation, see “[Installing the Remote Loader from the Console](#)” on page 173.

To prepare for the installation, review the prerequisites and system requirements listed in [Section 18.1, “Checklist for Installing the Remote Loader,”](#) on page 169. Also see the Release Notes accompanying the release.

19.2.1 Creating the Properties File for a Silent Installation

To run a silent installation of the Remote Loader you must create a properties file that specifies the parameters for the installation. The installation kit provides a sample `silent.properties` file in the following locations:

- ♦ **Linux:** `/products/IDM/linux/setup/silent.properties`

- ♦ **Solaris:** /products/IDM/solaris/setup/silent.properties
- ♦ **Windows:** /products/IDM/windows/setup/silent.properties

Create a silent.properties file:

- 1 Copy and rename the sample properties file to the directory that contains the executable file for installing Remote Loader:
 - ♦ **Linux and Solaris:** products/IDM/
 - ♦ **Windows:** products/IDM/windows/setup

NOTE: You can use any prefix to name the .properties file. This procedure uses the name install.properties.

- 2 In a text editor, open the install.properties file.
- 3 Add the following text to the file:

```
METADIRECTORY_SERVER_SELECTED=false
CONNECTED_SYSTEM_SELECTED=true
Installing Identity Manager 67
X64_CONNECTED_SYSTEM_SELECTED=true
WEB_ADMIN_SELECTED=false
UTILITIES_SELECTED=false
```
- 4 (Conditional) If you already installed iManager and you now want to install plug-ins for iManager, set the WEB_ADMIN_SELECTED value to true.
- 5 Close and save the file.

19.2.2 Running a Silent Installation for Remote Loader

You can silently install Remote Loader on a Linux, Solaris, or Windows server using the install.properties file that you created in [Section 19.2.1, “Creating the Properties File for a Silent Installation,”](#) on page 174.

To start the silent installation, enter one of the following commands from the directory that contains the installation files, including the install.properties file:

- ♦ **Linux and Solaris:** install.bin -i silent -f install.properties
- ♦ **Windows:** idm_install.exe -i silent -f install.properties

NOTE

- ♦ You can use any prefix to name the .properties file. This procedure uses the name install.properties.
 - ♦ For the default installation locations, see the /tmp/idmInstall.log file.
-

19.3 Installing the Java Remote Loader on UNIX or Linux

`dirxml_jremote` is a pure Java Remote Loader. Identity Manager uses the program to exchange data between the Identity Manager engine running on one server and the Identity Manager drivers running in another location, where `rdxml` does not run. You can install `dirxml_jremote` on any supported UNIX or Linux computer that has a compatible JRE (1.5.0 minimum) and Java Sockets.

- 1 Log on as root or Administrator to the computer where you want to install the Remote Loader components.
- 2 Verify that the host system has a supported version of Java JDK or JRE.
- 3 To access the installation program, complete one of the following steps:
 - 3a (Conditional) If you have the `.iso` image file for the Identity Manager installation package, navigate to the directory containing the Java Remote Loader installation files, located by default in `products/IDM/java_remoteloader`.
 - 3b (Conditional) If you downloaded the Java Remote Loader installation files from the [Novell Downloads Web site \(http://download.novell.com\)](http://download.novell.com), complete the following steps:
 - 3b1 Navigate to the `.tgz` file for the downloaded image.
 - 3b2 Extract the contents of the file to a folder on the local computer.
- 4 Copy the `dirxml_jremote_dev.tar.gz` file to the desired location on the remote server. For example, copy the file to `/usr/idm`.
- 5 Copy one of the following files to the desired location on the remote server:
 - ♦ `dirxml_jremote.tar.gz`
 - ♦ `dirxml_jremote_mvs.tar`For information about `mvs`, untar the `dirxml_jremote_mvs.tar` file, then refer to the `usage.html` document.
- 6 On the remote server, unzip and extract the `.tar.gz` files.

For example, enter `gunzip dirxml_jremote.tar.gz` or `tar -xvf dirxml_jremote_dev.tar`.
- 7 Copy the application shim `.jar` files from the Identity Manager engine server to the `lib` subdirectory that was created when you extracted the `dirxml_jremote.tar` file.

By default, the `.jar` files are located in the `/opt/novell/eDirectory/lib/dirxml/classes` directory on the Identity Manager engine server.
- 8 To customize the `dirxml_jremote` script so the Java executable is reachable through the `RDXML_PATH` environment variable, complete one of the following steps:
 - 8a Enter one of the following commands to set the environment variable `RDXML_PATH`:
 - ♦ `set RDXML_PATH=path`
 - ♦ `export RDXML_PATH`
 - 8b Edit the `dirxml_jremote` script and prepend the path to the Java executable on the script line that executes Java.
- 9 Configure the sample `config8000.txt` file for use with your application shim. The file is located by default in the `/opt/novell/dirxml/doc` directory. For more information, see “[Configuring the Remote Loader for Linux/UNIX by Creating a Configuration File](#)” in the *Identity Manager 4.0.2 Remote Loader Guide*.

20 Configuring the Remote Loader

Before using the Remote Loader, you must configure the application shim to connect securely with the Identity Manager engine. You must also configure both the Remote Loader and Identity Manager drivers. For more information about shims, see [Section 18.4, “Understanding Shims,” on page 171](#).

20.1 Creating a Secure Connection to the Identity Manager Engine

You must ensure that data transfers securely between the Remote Loader and the Identity Manager engine. NetIQ recommends using Transport Layer Security/Secure Socket Layer (TLS/SSL) protocols for communication. To support TLS/SSL connections, you need an appropriate self-signed certificate in a keystore file. This section explains how to create, export, and store that certificate.

NOTE: Use the same version of SSL on the servers hosting the Identity Manager engine and the Remote Loader. If the versions of SSL on the server and the Remote Loader do not match, the server returns a `SSL3_GET_RECORD:wrong version number` error message. This message is only a warning, and communication between the server and Remote Loader is not interrupted. However, the error might cause confusion.

20.1.1 Understanding the Communication Process

The Remote Loader opens a server socket and listens for connections from the remote interface shim. The remote interface shim and the Remote Loader perform an SSL handshake to establish a secure channel. Then the remote interface shim authenticates to the Remote Loader. If the authentication of the remote interface shim succeeds, the Remote Loader authenticates to the remote interface shim. Only when both sides are satisfied that they are communicating with an authorized entity does synchronization traffic occur.

The process for establishing SSL connections between a driver and the Identity Manager engine depends on the type of driver:

- ♦ **For a native driver**, such as the Active Directory driver, point to a base64 encoded certificate. For more information, see [Section 20.1.2, “Managing Self-Signed Server Certificates,” on page 178](#).
- ♦ **For a Java driver**, you must create a keystore. For more information, see [Section 20.1.3, “Creating a Keystore File when Using SSL Connections,” on page 179](#).

NOTE: The Remote Loader allows for custom connection methods between the Remote Loader and the remote interface shim that is hosted on the Identity Manager server. To configure a custom connection module, see the documentation that comes with the module for information regarding what is expected and allowed in the connection string.

20.1.2 Managing Self-Signed Server Certificates

You can create and export a self-signed server certificate to ensure secure communication between the Remote Loader and the Identity Manager engine. You can export a newly created certificate. Or, if an SSL server certificate already exists and you have experience with SSL certificates, you can use the existing certificate instead of creating and using a new one. You should use this process when you want to use a native driver, such as the Active Directory driver.

NOTE: When a server joins a tree, eDirectory creates the following default certificates:

- ◆ SSL CertificateIP
 - ◆ SSL CertificateDNS
-

- 1 Log on to Novell iManager.
- 2 To create a new certificate, complete the following steps:
 - 2a Click **Novell Certificate Server > Create Server Certificate**.
 - 2b Select the server to own the certificate.
 - 2c Specify a nickname for the certificate. For example, `remotecert`.

NOTE: NetIQ recommends that you avoid using spaces in the certificate nickname. For example, use `remotecert` instead of `remote cert`.

Also, make a note of the certificate nickname. This nickname is used for the KMO name in the driver's remote connection parameters.

- 2d Leave the Creation method set to **Standard**, then click **Next**.
- 2e Review the Summary, click **Finish**, then click **Close**.
- 3 To export a certificate, complete the following steps:
 - 3a In iManager, click **eDirectory Administration > Modify Object**.
 - 3b Browse to and select the Certificate Authority in the Security container, then click **OK**.
The Certificate Authority (CA) is named after the tree name (Treename-CA.Security).
 - 3c In the **Certificates** tab, select **Self-Signed Certificate** from the list of certificates.
 - 3d Click **Export**.
 - 3e In the Export Certificate Wizard, deselect **Export private key**.
 - 3f For the export format, select **BASE64**, then click **Next**.

NOTE: When the Remote Loader is running on a Windows 2003 R2 SP1 32-bit server, the certificate must be in Base64 format. If you use the DER format, the Remote Loader fails to connect to the Identity Manager engine.

- 3g Click **Save the exported certificate**, then specify a location in the local file system.
- 3h Click **Save**, then click **Close**.

20.1.3 Creating a Keystore File when Using SSL Connections

To use SSL connections between a Java driver and the Identity Manager engine, you must create a keystore. A keystore is a Java file that contains encryption keys and, optionally, certificates. If you want to use SSL between the Remote Loader and the Identity Manager engine, and you are using a Java shim, you need to create a keystore file. The following sections explain how to create a keystore file:

- ♦ [“Creating a Keystore on Any Platform” on page 179](#)
- ♦ [“Creating a Keystore on Solaris and Linux” on page 179](#)
- ♦ [“Creating a Keystore on Windows” on page 179](#)

Creating a Keystore on Any Platform

To create a keystore on any platform, you can enter the following at the command line:

```
keytool -import -alias trustedroot -file self-signed_certificate_name -keystore filename -storepass keystorepass
```

The filename can be any name. For example, `rdev_keystore`.

Creating a Keystore on Solaris and Linux

In Solaris and Linux environments, use the `create_keystore` file, which is a shell script that calls the Keytool utility. The file is installed with `rdxml`, located by default in the `install_directory/dirxml/bin` directory. The `create_keystore` file is also included in the `dirxml_jremote.tar.gz` file, found in the `\dirxml\java_remoteloader` directory.

NOTE: On UNIX computers, when the self-signed certificate is used to create the keystore, the certificate can be exported in Base64 or binary DER format.

Enter the following at the command line:

```
create_keystore self-signed_certificate_name keystorename
```

For example, type one of the following

```
create_keystore tree-root.b64 mystore
create_keystore tree-root.der mystore
```

The `create_keystore` script specifies a hard-coded password of “`dirxml`” for the keystore password. This is not a security risk because only a public certificate and public key are stored in the keystore.

Creating a Keystore on Windows

On Windows computers, run the Keytool utility, located by default in the `c:\novell\remoteloader\jre\bin` directory.

20.2 Configuring the Remote Loader for Driver Instances

The Remote Loader can host the Identity Manager application shims contained in `.dll`, `.so`, or `.jar` files. The Java Remote Loader hosts only Java driver shims. It does not load or host a native (C++) driver shim.

For the Remote Loader to run, the application needs a configuration file, such as `LDAPShim.txt`. On Windows computers, you can use a utility called the Remote Loader Console to create and edit the configuration file. However, on UNIX or Linux computers, you must manually create the file.

20.2.1 Understanding the Configuration Parameters for the Remote Loader

For the Remote Loader to work with a driver instance that hosts an Identity Manager application shim, you must configure the driver instance. For example, you must specify the connection and port settings for the instance. You can specify the settings from the command line, in a configuration file (UNIX or Linux), or in the Remote Loader Console (Windows). Once the instance is running, you can use the command line to modify the configuration parameters or instruct the Remote Loader to perform a function. For example, you might want to open the trace window or unload the Remote Loader.

This section provides information about the configuration parameters. The explanation specifies whether a parameter can be sent from the command line to updated the Remote Loader while the instance is running.

For more information about configuring a new driver instance, see the following sections:

- ♦ **Linux and UNIX:** [Section 20.2.2, “Configuring the Remote Loader for Driver Instances on UNIX or Linux,” on page 188](#)
- ♦ **Windows:** [Section 20.2.3, “Configuring the Remote Loader for Driver Instances on Windows,” on page 190.](#)

Configuration Parameters for the Driver Instances in the Remote Loader

To configure a driver instance from the command line or in the configuration file, use the following parameters:

-description *value* (-desc *value*)

(Optional) Specifies a short description in string format, such as `SAP`, which the application uses for the title of the trace window and for audit logging. For example:

```
-description SAP
```

```
-desc SAP
```

-class *name* (-cl *name*)

(Conditional) When using a Java driver, specifies the Java class name of the Identity Manager application shim that you want to host. This options tells the application to use a Java keystore to read certificates. For example:

```
-class com.novell.nds.dirxml.driver.ldap.LDAPDriverShim
-cl com.novell.nds.dirxml.driver.ldap.LDAPDriverShim
```

NOTE

- ◆ You cannot use this option if you specify a `-module` option.
 - ◆ If you use the `tab` character as a delimiter in the `-class` option, the Remote Loader does not start automatically. Instead, you must manually start it. For the Remote Loader to start properly, you can use a space character instead of a `tab`.
 - ◆ For more information about names that you can specify for this option, see [“Specifying Names for the Java -class Parameter” on page 187](#).
-

-commandport *port_number* (-cp *port_number*)

Specifies the TCP/IP port that the driver instance uses for control purposes. For example, `-commandport 8001` or `-cp 8001`. The default value is 8000.

To use multiple driver instances with the Remote Loader on the same server, specify different connection ports and command ports for each instance.

If the driver instance hosts an application shim, the command port is the port on which another instance communicates with the instance that is hosting the shim. If the driver instance sends a command to an instance that is hosting an application shim, the command port is the port on which the hosting instance is listening.

When you send this parameter from the command line to an instance that hosts an application shim, the command port represents the port on which the hosting instance is listening. You can send this command when the Remote Loader is running.

-config *filename*

Specifies a configuration file for the driver instance. For example:

```
-config config.txt
```

The configuration file can contain any command line options except `-config`. Options specified on the command line override options specified in the configuration file.

You can send this command when the Remote Loader is running.

-connection “*parameters*” (-conn “*parameters*”)

Specifies the settings for connecting to the server hosting the Identity Manager engine that runs the Identity Manager remote interface shim. The default connection method is TCP/IP using SSL.

To use multiple driver instances with the Remote Loader on the same server, specify different connection ports and command ports for each instance.

Enter the connection settings in the following syntax:

```
-connection "parameter parameter parameter"
```

For example:

```
-connection "port=8091 fromaddress=198.51.100.0 rootfile=server1.pem
keystore=ca.pem localaddress=198.51.100.0 hostname=198.51.100.0 kmo=remote
driver cert"
```

Use the following parameters for the specifying the settings for a TCP/IP connection:

address=*IP_address*

(Optional) Specifies whether the Remote Loader listens on a particular local IP address. This is useful if the server hosting the Remote Loader has multiple IP addresses and the Remote Loader must listen on only one of the addresses. The following values are valid:

- ◆ address=address number
- ◆ address='localhost'

For example:

```
address=198.51.100.0
```

If you do not specify a value, the Remote Loader listens on all local IP addresses.

fromaddress=*IP_address*

Specifies the server from which the Remote Loader accepts connections. The application ignores connections from other addresses. Specify an IP address or the DNS name of the server. For example:

```
fromaddress=198.51.100.0
```

```
fromaddress=testserver1.company.com
```

handshaketimeout=*milliseconds*

(Conditional) Applies when handshake timeouts occur with otherwise valid connections from the Identity Manager engine. Specifies the timeout period, in milliseconds, for the handshake between the Remote Loader and the Identity Manager engine. For example:

```
handshaketimeout=1000
```

You can specify an integer greater than or equal to zero. Zero means that the connection never times out. The default value is 1000 milliseconds.

hostname=*server*

Specifies the IP address or name of the server on which the Remote Loader runs. For example:

```
hostname=198.51.100.0
```

keystore=*filename*

(Conditional) Applies when Identity Manager application shims are contained in .jar files. Specifies the file name of the Java keystore that contains the trusted root certificate of the issuer of the certificate that the remote interface shim uses. For example:

```
keystore=ca.pem
```

Usually, you specify the Certificate Authority of the tree that is hosting the remote interface shim.

kmo=*name*

Specifies the key name of the Key Material Object containing the keys and certificate used for SSL connections. For example:

```
kmo=remote driver cert
```

localaddress=IP_address

Specifies the IP address to which you want to bind the socket for client connection. For example:

```
localaddress=198.51.100.0
```

port=port_number

Specifies the TCP/IP port on which the Remote Loader listens for connections from the remote interface shim. To specify the default port, enter `port=8090`.

rootfile=trusted_certname

(Conditional) Applies only when you use SSL and you want the Remote Loader to communicate with a native driver. Specifies the file that contains the trusted root certificate of the issuer of the certificate used by the remote interface shim. The certificate file must be in Base 64 format (PEM). For example:

```
rootfile=server1.pem
```

Usually, the file will be the Certificate Authority of the tree that is hosting the remote interface shim.

storepass=password

(Conditional) Applies only to the Java Remote Loader, when Identity Manager application shims are contained in `.jar` files. Specifies password for the Java keystore that you entered for the `keystore` parameter. For example:

```
storepass=mypassword
```

NOTE: If you use SSL and you want the Remote Loader to communicate with a Java driver, specify a key-value pair, using the following syntax:

```
keystore=keystorename storepass=password
```

-datadir directory (-dd directory)

Specifies the directory for data files that the Remote Loader uses. For example:

```
-datadir /var/opt/novell/dirxml/rdxml/data
```

When you use this command, the `rdxml` process changes its current directory to the specified directory. Trace files and other files that do not have an explicitly specified path will be created in this data directory.

-help (-h)

Instructs the application to display the Help.

-java (-j)

(Conditional) Specifies that you want to set passwords for a Java driver shim instance.

NOTE: Use this option with the `-setpasswords` option when you do not also specify a `-class` value.

-javadebugport *port_number* (-jdp *port_number*)

Instructs the instance to enable Java debugging on the specified port. For example:

```
-javadebugport 8080
```

Use this command when developing Identity Manager application shims. You can send this command when the Remote Loader is running.

-javaparam *parameters* (-jp *parameters*)

Specifies the parameters for the Java environment. Enter the Java environment parameters in the following syntax:

```
-javaparam parameter  
-jp parameter  
-jp parameter
```

To specify multiple values for an individual parameter, enclose the parameter in quotation marks. For example:

```
-javaparam DHOST_JVM_MAX_HEAP=512M  
-jp DHOST_JVM_MAX_HEAP=512M  
-jp "DHOST_JVM_OPTIONS=-Dfile.encoding=utf-8 -Duser.language=en"
```

Use the following parameters for setting the Java environment:

DHOST_JVM_ADD_CLASSPATH

Specifies additional paths for the JVM to search for package (*.jar*) and class (*.class*) files. To specify multiple class paths for a UNIX or Linux JVM, insert a colon between each path. For a Windows JVM, use a semicolon.

DHOST_JVM_INITIAL_HEAP

Specifies the initial (minimum) JVM heap size in decimal number of bytes. Use a numeric value followed by G, M, or K representing the byte type. For example:

```
100M
```

If you do not specify a byte type, the size defaults to bytes. Using this parameter is the same as using the `java -Xms` command.

This parameter has precedence over the driver set attribute option. Increasing the initial heap size can improve startup time and throughput performance.

DHOST_JVM_MAX_HEAP

Specifies the maximum JVM heap size in decimal number of bytes. Use a numeric value followed by G, M, or K representing the byte type. For example:

```
100M
```

If you do not specify a byte type, the size defaults to bytes.

This parameter has precedence over the driver set attribute option.

DHOST_JVM_OPTION

Specifies the arguments that you want to use when starting the JVM instance of the driver. Use a space to separate each option string. For example:

```
-Xnoagent -Xdebug -Xrunjdwp:transport=dt_socket,server=y,address=8000
```

The driver set attribute option has precedence over this parameter. This environment variable is tacked on to the end of driver set attribute option. For more information about valid options, see the JVM documentation.

-module "name" (-m "name")

(Conditional) When using a native drive, specifies the module containing the Identity Manager application shim that you want to host. This option tells the application to use a rootfile certificate. For example, for a native driver, type one of the following:

```
-module "c:\Novell\RemoteLoader\ADDriver.dll"
-m "c:\Novell\RemoteLoader\ADDriver.dll"
```

or

```
-module "usr/lib/dirxml/NISDriverShim.so"
-m "usr/lib/dirxml/NISDriverShim.so"
```

NOTE

- ◆ You cannot use this option if you specify a `-class` option.
 - ◆ If you use the `tab` character as a delimiter in the `-module` option, the Remote Loader does not start automatically. Instead, you must manually start it. For the Remote Loader to start properly, you can use a space character instead of a `tab`.
-

-password value (-p value)

Specifies the password for the driver instance when you issue commands that change settings or affect instance operation. You must specify the same password as the first password specified with `setpasswords` for the instance that you want to command. For example:

```
-password novell4
```

If you do not send the password when issuing commands, the driver instance prompts you for the password.

You can send this command when the Remote Loader is running.

-piddir directory (-pd directory)

Specifies the path to directory for the process id file (pidfile) used by the Remote Loader process. For example:

```
-piddir /var/opt/novell/dirxml/rdxml/data
```

The pidfile exists primarily for use by SysV-style init scripts. The default value is `/var/run`. Alternatively, the default value is the current directory, if the Remote Loader is run by a user without sufficient rights to open the pidfile for reading and writing in `/var/run`.

This parameter is similar to `-datadir`.

-service value (-serv value)

(Windows only) Specifies whether you want to configure an instance as a Win32 service on a Windows computer. Valid values are `install` and `uninstall` plus the other parameters necessary to host an application shim. For example, you must include `-module` and might also include `-commandport` and the connection settings.

This command simply installs or uninstalls the instance as a service. It does not start the service.

You can send this command when the Remote Loader is running. However, you cannot use this command on `rdxml` or the Java Remote Loader.

-setpasswords Remote_Loader_pwd optional_pwd (-sp Remote_Loader_pwd optional_pwd)

Specifies the password for the driver instance and the password of the Identity Manager Driver object of the remote interface shim with which the Remote Loader communicates.

You do not need specify a password. Instead, the Remote Loader prompts you for the passwords. However, if you specify the password for the Remote Loader, you must also specify the password for the Identity Manager Driver object associated with the remote interface shim on the Identity Manager engine server. To specify the passwords, use the following syntax:

```
-setpasswords Remote_Loader_password driver_object_password
```

For example:

```
-setpasswords novell14 idmobject6
```

NOTE: Using this option configures the driver instance with the passwords specified but does not load a Identity Manager application shim or communicate with another instance.

trace file settings

(Conditional) When hosting an Identity Manager application shim, specifies the settings for a trace file that contains informational messages from both the Remote Loader and the driver for this instance.

Add the following parameters to the configuration file:

-trace *integer* (-t *integer*)

Specifies the level of messages that you want displayed in a trace window. For example:

```
-trace 3
```

Trace levels for the Remote Loader correspond to those used on the server hosting the Identity Manager engine.

-tracefile *filepath* (-tf *filepath*)

Specifies the path to a file where trace messages are logged. You must specify a unique trace file for each driver instance running on a particular computer. For example:

```
-tracefile c:\temp\trace.txt
```

The application writes messages to the file if the `-trace` parameter is greater than zero. The trace window does not need to be open for messages to be written to the file.

-tracefilemax *size* (-tf *size*)

Specifies a limit to the size of the trace file for this instance. Specify the value in kilobytes, megabytes, or gigabytes, using the abbreviation for the byte type. For example:

- ◆ `-tracefilemax 1000K`
- ◆ `-tf 100M`
- ◆ `-tf 10G`

NOTE

- ◆ If the trace file data is larger than the specified maximum when the Remote Loader is started, the trace file data remains larger than the specified maximum until roll-over is completed through all 10 files.
 - ◆ When you add this option to the configuration file, the application uses the specified name for the tracefile and includes up to 9 “roll-over” files. The roll-over files are named using the base of the main trace filename plus `_n`, where `n` is 1 through 9.
-

-tracechange *integer* (-tc *integer*)

(Conditional) When you have an existing driver instance that hosts an application shim, specifies a new level of informational messages. Trace levels correspond to those used on the Identity Manager server. For example:

```
-trace 3
```

You can send this command when the Remote Loader is running.

-tracefilechange *filepath* (-tfc *filepath*)

(Conditional) When you have an existing driver instance that hosts an application shim, instructs that instance to use a trace file or to close a file already in use and change to this new file. For example:

```
-tracefilechange \temp\newtrace.txt
```

You can send this command when the Remote Loader is running.

-unload (-u)

Instructs the driver instance to unload. If the Remote Loader is running as a Win32 Service, this command stops the service.

You can send this command when the Remote Loader is running.

-window *value* (-w) *value*

(Windows only) Instructs the application to turn on or off the trace window for a driver instance on a Windows computer. Valid values are `on` and `off`. For example:

```
-window on
```

You can send this command when the Remote Loader is running. You cannot use this command with the Java Remote Loader.

-wizard (-wiz)

(Windows only) Launches the Configuration Wizard for the Remote Loader on a Windows computer. You can also launch the wizard by running `dirxml_remote.exe` with no command line parameters.

If you run this command and also specify a configuration file (`-config` option), the wizard starts with the values from the configuration file. You can use the wizard to change the configuration without editing the configuration file directly. For example:

```
-wizard -config config.txt
```

You cannot use this command with the Java Remote Loader.

Specifying Names for the Java -class Parameter

When you use the `-class` parameter to configure a driver instance for the Remote Loader and Java Remote Loader, you must specify the Java class name of the Identity Manager application shim that you want to host.

Java Class Name	Driver
com.novell.nds.dirxml.driver.avaya.PBXDriverShim	Avaya PBX Driver
com.novell.nds.dirxml.driver.dcsshim.DCSShim	Driver for Data Collection Service
com.novell.nds.dirxml.driver.delimitedtext.DelimitedTextDriver	Delimited Text Driver

Java Class Name	Driver
be.opns.dirxml.driver.ars.arsremedydrivershim.ARSDriverShim	Driver for Remedy ARS
com.novell.nds.dirxml.driver.entitlement.EntitlementServiceDriver	Entitlements Service Driver
com.novell.gw.dirxml.driver.gw.GWdriverShim	GroupWise Driver
com.novell.idm.drivers.idprovider.IDProviderShim	ID Provider Driver
com.novell.nds.dirxml.driver.jdbc.JDBCDriverShim	JDBC Driver
com.novell.nds.dirxml.driver.jms.JMSDriverShim	JMS Driver
com.novell.nds.dirxml.driver.Idap.LDAPDriverShim	LDAP Driver
com.novell.nds.dirxml.driver.loopback.LoopbackDriverShim	Loopback Driver
com.novell.nds.dirxml.driver.msggateway.MSGatewayDriverShim	Managed System Gateway Driver
com.novell.nds.dirxml.driver.manualtask.driver.ManualTaskDriver	Manual Task Driver
com.novell.nds.dirxml.driver.nisd.driver.NISDriverShim	NIS Driver
com.novell.nds.dirxml.driver.notes.NotesDriverShim	Notes Driver
com.novell.nds.dirxml.driver.psoftshim.PSOFTDriverShim	PeopleSoft Driver
com.novell.nds.dirxml.driver.salesforce.SFDriverShim	Salesforce Driver
com.novell.nds.dirxml.driver.SAPHRShim.SAPDriverShim	SAP HR Driver
com.novell.nds.dirxml.driver.sap.portal.SAPPortalShim	SAP Portal Driver
com.novell.nds.dirxml.driver.sapumshim.SAPDriverShim	SAP User Management Driver
com.novell.nds.dirxml.driver.soap.SOAPDriver	SOAP Driver
com.novell.idm.driver.ComposerDriverShim	User Application
com.novell.nds.dirxml.driver.workorder.WorkOrderDriverShim	WorkOrder Driver

20.2.2 Configuring the Remote Loader for Driver Instances on UNIX or Linux

For the Remote Loader to run on a UNIX or Linux computer, the application needs a configuration file such as `LDAPShim.txt` for each driver instance. You can also create or edit a configuration file by using command line options.

By default, the Remote Loader connects to the Identity Manager engine through TCP/IP using TLS/SSL protocols. The default TCP/IP port for this connection is 8090. You can run multiple driver instances with the Remote Loader on the same server. Each instance hosts a separate Identity Manager application shim instance. To use multiple instances of the Remote Loader on the same server, specify different connection ports and command ports for each instance.

NOTE

- ◆ The configuration file can contain any command line options except `-config`.

- ◆ When adding parameters to the configuration file, you can use the long form or a short form of the parameter. For example, `-description` or `-desc`.
 - ◆ The following procedure lists the long form first, followed by the short form in parentheses. For example `-description value (-desc value)`.
 - ◆ For more information about the parameters used in this section, see [“Understanding the Configuration Parameters for the Remote Loader” on page 180](#).
-

To create a configuration file:

- 1 In a text editor, create a new file.
- 2 Add the following configuration parameters to the file:

- ◆ `-description` (optional)
- ◆ `-commandport`
- ◆ connection parameters:
 - ◆ `port`
 - ◆ `address`
 - ◆ `fromaddress`
 - ◆ `handshaketimeout`
 - ◆ `rootfile`
 - ◆ `keystore` (conditional)
 - ◆ `storepass` (conditional)
 - ◆ `localaddress`
 - ◆ `hostname`
 - ◆ `kmo`
- ◆ trace file parameters (optional):
 - ◆ `-trace`
 - ◆ `-tracefile`
 - ◆ `-tracefilemax`
- ◆ `-javaparam`
- ◆ `-class` or `-module`

For more information about specifying values for these parameters, see [Section 20.2.1, “Understanding the Configuration Parameters for the Remote Loader,” on page 180](#).

- 3 Save the file.

For the Remote Loader to start automatically when your computer starts, save the file to the `/etc/opt/novell/dirxml/rdxml` directory.

20.2.3 Configuring the Remote Loader for Driver Instances on Windows

The Remote Loader Console utility (the Console) helps you manage all instances of Identity Manager drivers running on the Windows server. You can start, stop, add, remove, and edit each instance of a Remote Loader. The installation program for the Remote Loader also installs the Console.

If you are upgrading, the Console detects and imports existing driver instances. For a driver to be automatically imported, its configuration file must be stored in the Remote Loader directory, located by default at `c:\novell\remoteloader`. You can then use the Console to manage the remote drivers.

You can use the command line or the Remote Loader Console to configure the Remote Loader to recognize a driver on Windows. For more information about using the command line, see [Section 20.2.1, “Understanding the Configuration Parameters for the Remote Loader,” on page 180](#).

This section provides instructions for the following activities:

- ♦ [“Creating a New Driver Instance in the Remote Loader on Windows” on page 190](#)
- ♦ [“Modifying an Existing Driver Instance in the Remote Loader on Windows” on page 191](#)

Creating a New Driver Instance in the Remote Loader on Windows

- 1 Open the Remote Loader Console.

NOTE: During installation, if you selected to create a shortcut for the Console, use the Identity Manager Remote Loader Console icon on the desktop. Otherwise, run the `rlconsole.exe` located by default in `C:\novell\remoteloader\nnbit`.

- 2 To add an instance of your driver on this server, click **Add**.
- 3 For **Description**, provide a short name to represent the instance.
The Console uses this information in the default value for **Config File**.
- 4 For **Driver**, select the Java class name.

NOTE: To use the Active Directory drive, select **ADDriver.dll**. For more information about the class names for each driver, see [“Specifying Names for the Java -class Parameter” on page 187](#).

- 5 For **Config File**, specify the path to the file where Remote Loader stores its configuration parameters. The default value is `C:\novell\remoteloader\nnbit\Description-config.txt`.
- 6 Specify passwords for the Remote Loader and driver object.
- 7 (Optional) To use a TLS/SSL connection between the Remote Loader and the Identity Manager engine server, complete the following steps:
 - 7a Select **Use an SSL Connection**.

NOTE: NetIQ recommends using the same version of SSL on both the Identity Manager engine server and the Remote Loader. If the versions of SSL on the server and the Remote Loader do not match, the server returns a “`SSL3_GET_RECORD:wrong version number`” error message. This message is only a warning, and communication between the server and Remote Loader is not interrupted. However, the error might cause confusion.

- 7b For **Trusted Root File**, specify the exported self-signed certificate from the eDirectory tree’s Organization Certificate Authority. For more information, see [“Creating a Secure Connection”](#) in the *Identity Manager 4.0.2 Remote Loader Guide*.

- 8 (Optional) To configure the trace file for the Remote Loader, complete the following steps:

NOTE: NetIQ recommends using the trace functionality only for troubleshooting issues. Having the trace enabled reduces the performance of the Remote Loader. Do not leave the trace enabled in production.

- 8a For **Trace Level**, specify a value greater than zero that defines the level of informational messages from both the Remote Loader and the driver that you want display in a trace window. Values 1 to 4 are pre-defined by the Console. To create your own message types, specify a value of 5 or higher.

The most common setting is trace level 3, which provides general processing, XML documents, and Remote Loader messages.
 - 8b For **Trace File**, specify the path to a file where trace messages are logged. For example, `C:\netiq\remoteloader\64bit\Test-Delimited-Trace.log`.

You must specify a unique trace file for each driver instance running on a particular computer. Trace messages are written to the trace file only if the trace level is greater than zero.
 - 8c For **Maximum Disk Space Allowed for all Trace Logs (Mb)**, specify an approximate value for the most disk space that the trace file for this instance can occupy.
- 9 (Optional) To allow the Remote Loader to start automatically when the computer starts, select **Establish Remote Loader Service for this driver instance**.
- 10 (Conditional) To modify the parameters for Java configuration, complete the following steps:
 - 10a Select **Advanced**.
 - 10b For **Classpath**, specify the paths for the JVM to search for package (`.jar`) and class (`.class`) files. To specify multiple paths, separate the paths with a colon for UNIX or Linux JVM and a semicolon for Windows JVM.

This parameter functions the same as the `java -classpath` command.
 - 10c For **JVM Options**, specify the options that you want to use when starting the JVM instance of the driver.
 - 10d Specify the initial and maximum heap size for the JVM instance in MB.
 - 10e Click **OK**.
- 11 Click **OK**.

Modifying an Existing Driver Instance in the Remote Loader on Windows

- 1 In the Remote Loader Console, select the driver instance from the **Description** column.
- 2 Click **Stop**.
- 3 Enter the password for the Remote Loader, then click **OK**.
- 4 Click **Edit**.
- 5 Modify the configuration information. For more information about each parameter, see [“Creating a New Driver Instance in the Remote Loader on Windows” on page 190](#).
- 6 To save the changes, click **OK**.

20.2.4 Configuring the Java Remote Loader for Driver Instances

To configure a new instance for the Java Remote Loader on Linux and Solaris platforms, complete the following steps. For more information about the parameters used in this section, see [“Understanding the Configuration Parameters for the Remote Loader” on page 180](#).

- 1 In a text editor, create a new file.
- 2 Add the following parameters to the new configuration file:
 - ◆ -description (optional)
 - ◆ -class or -module
For example, `-class com.novell.nds.dirxml.driver.ldap.LDAPDriverShim`
 - ◆ -commandport
 - ◆ connection parameters:
 - ◆ port
 - ◆ address
 - ◆ fromaddress
 - ◆ handshaketimeout
 - ◆ rootfile
 - ◆ keystore (conditional)
 - ◆ storepass (conditional)
 - ◆ localaddress
 - ◆ hostname
 - ◆ kmo
 - ◆ -java (conditional)
 - ◆ -javadebugport (optional)
 - ◆ -password
 - ◆ -service (conditional)
 - ◆ -setpasswords
 - ◆ trace file parameters (optional):
 - ◆ -trace
 - ◆ -tracefile
 - ◆ -tracefilemax
- 3 Save the new configuration file.
For the Remote Loader to start automatically when your computer starts, save the file to the `/etc/opt/novell/dirxml/rdxml` directory.
- 4 Open a command prompt.
- 5 At the prompt, enter `-config filename`, where *filename* is the name of the new configuration file. For example:

```
-config config.txt
```


20.3 Configuring Identity Manager Drivers to Work with the Remote Loader

You can configure a new driver or enable an existing driver to communicate with the Remote Loader. This section provides general information on configuring drivers so that they communicate with the Remote Loader. For driver-specific information, refer to the relevant driver implementation guide at the [Identity Manager Driver Documentation Web page \(http://www.novell.com/documentation/idm40drivers/index.html\)](http://www.novell.com/documentation/idm40drivers/index.html).

To add a new or modify an existing Driver object in either Designer or iManager, you must configure settings that enable the driver instance for the Remote Loader. For more information about the parameters used in this section, see “[Understanding the Configuration Parameters for the Remote Loader](#)” on page 180.

- 1 In the properties of the Driver object, complete the following steps:
 - 1a For **Driver Module**, select **Connect to Remote Loader**.
 - 1b For **Driver Object Password**, specify the password that the Remote Loader uses to authenticate itself to the Identity Manager engine server.

This password must match the password for the driver object defined on the Remote Loader.
 - 1c For **Remote Loader Connection Parameters**, specify the information required to connect to the Remote Loader. Use the following syntax:

```
hostname=xxx.xxx.xxx.xxx port=xxxx kmo=certificatename  
localaddress=xxx.xxx.xxx.xxx
```

where

hostname

Specifies the IP address for the server that hosts the Remote Loader.

port

Specifies the port that the Remote Loader listens on. The default is 8090.

kmo

Specifies the key name of the Key Material Object containing the keys and certificate used for SSL connections.

localaddress

Specifies the source IP address if more than one IP addresses are configured on the server that hosts the Identity Manager engine.

- 1d For **Remote Loader Password**, specify the password required for the Identity Manager engine (or Remote Loader shim) to authenticate to the Remote Loader.
- 2 Define a security-equivalent user.
- 3 Click **Next**, then click **Finish**.

21 Starting and Stopping the Remote Loader

The Remote Loader is either a service or a daemon, which occasionally must be restarted. This chapter explains how to stop and start the Remote Loader.

21.1 Starting a Driver Instance in the Remote Loader

You can configure each platform to automatically start a driver instance when the host computer starts. You can also manually start an instance.

21.1.1 Starting Driver Instances on UNIX or Linux

NetIQ provides two ways that you can start a driver instance for the Remote Loader on UNIX or Linux computers:

- ♦ [“Starting Driver Instances Automatically on UNIX or Linux” on page 195](#)
- ♦ [“Using the Command Line to Start Driver Instances on UNIX or Linux” on page 195](#)

Starting Driver Instances Automatically on UNIX or Linux

You can configure a driver instance for the Remote Loader to start automatically when the computer starts. Place your configuration file in the `/etc/opt/novell/dirxml/rdxml` directory.

Using the Command Line to Start Driver Instances on UNIX or Linux

For Solaris and Linux platforms, the binary component `rdxml` supports command line functionality for the Remote Loader. This component is located by default in the `/usr/bin/` directory.

For more information about the parameters used in this section, see [“Understanding the Configuration Parameters for the Remote Loader” on page 180](#).

- 1 Open a command prompt.
- 2 To specify the passwords for authenticating the driver instance to the Identity Manager engine, enter one of the following commands:
 - ♦ **Solaris and Linux:** `rdxml -config filename -sp password password`
 - ♦ **HP-UX, AS/400, OS/390, and zOS:** `dirxml_jremote -config config_file -sp password password`
- 3 To start the driver instance, enter the following command:
 - ♦ **Solaris and Linux:** `rdxml -config filename`
 - ♦ **HP-UX, AS/400, OS/390, and zOS:** `dirxml_jremote -config filename`
- 4 Log on to iManager, then start the driver.

5 Confirm that the Remote Loader is working properly.

- ♦ **Solaris and Linux:** Use the `ps` command or a trace file to determine whether the command and connection ports are listening.
- ♦ **HP-UX, AS/400, OS/390, and zOS:** Monitor the Java Remote Loader by using the `tail` command on the tracefile:

```
tail -f trace filename
```

If the last line of the log shows the following text, the loader is successfully running and awaiting connection from the Identity Manager remote interface shim:

```
TRACE: Remote Loader: Entering listener accept()
```

The Remote Loader loads the Identity Manager application shim only when the Remote Loader is in communication with the remote interface shim on the Identity Manager engine server. This means, for example, that the application shim shuts down if the Remote Loader loses communication with the server.

21.1.2 Starting Driver Instances on Windows

NetIQ provides three ways that you can start a driver instance for the Remote Loader on Windows computers:

- ♦ [“Starting Driver Instances Automatically on Windows” on page 196](#)
- ♦ [“Using the Console to Start Driver Instances on Windows” on page 196](#)
- ♦ [“Using the Command Line to Start Driver Instances on Windows” on page 197](#)

Starting Driver Instances Automatically on Windows

You can configure a driver instance for the Remote Loader to start automatically when the Windows computer starts.

- 1 Open the Remote Loader Console.
- 2 Select a driver instance, then click edit.
- 3 Select **Establish a Remote Loader service for this driver instance**.
- 4 Save your changes.

Using the Console to Start Driver Instances on Windows

During installation, if you selected to create a shortcut for the Remote Loader Console, use the Identity Manager Remote Loader Console icon on the desktop. Otherwise, run the `rlconsole.exe` located by default in `C:\novell\remoteloader\mnbit`.

- 1 Open the Remote Loader Console.
- 2 Select a driver instance, then click **Start**.

Using the Command Line to Start Driver Instances on Windows

The `dirxml_remote.exe` file supports command line functionality for the Remote Loader. The executable is located by default in the `c:\novell\RemoteLoader` directory. For more information about the parameters used in this section, see [“Understanding the Configuration Parameters for the Remote Loader” on page 180](#).

- 1 Open a command prompt.
- 2 To specify the passwords for authenticating the driver instance for the Remote Loader to the Identity Manager engine, enter the following command:

```
dirxml_remote -config filename -setpasswords password password
```

For example:

```
dirxml_remote -config config.txt -sp Novell4 idmpwd6
```

- 3 To start the driver instance, enter the following command:

```
dirxml_remote -config filename
```

For example:

```
dirxml_remote -config config.txt
```

- 4 Log on to iManager, then start the driver.
- 5 Confirm that the Remote Loader is working properly.

The Remote Loader loads the Identity Manager application shim only when the Remote Loader is in communication with the remote interface shim on the Identity Manager engine server. This means, for example, that the application shim shuts down if the Remote Loader loses communication with the server.

- 6 (Conditional) If you did not previously install the Remote Loader as a Win32 service, enter the following command:

```
dirxml_remote -config filename -service install
```

For example:

```
dirxml_remote -config config.txt -service install
```

21.2 Stopping a Driver Instance in the Remote Loader

Each platform has a different method for stopping a driver instance in the Remote Loader. For more information about the parameters used in this section, see [“Understanding the Configuration Parameters for the Remote Loader” on page 180](#).

NOTE

- ♦ If you run multiple instances of the Remote Loader on a UNIX or Linux computer, include the `-cp command port` option to ensure that the Remote Loader can stop the appropriate instance.
- ♦ When you stop a driver instance, you must have sufficient rights or specify the Remote Loader password. For example, the Remote Loader is running as a Windows service. You have sufficient rights to stop it. You enter a password, but realize that it is incorrect. The Remote

Loader stops anyway, because the Remote Loader does not actually “accept” the password. Instead, it ignores the password because the password is redundant in this case. If you run the Remote Loader as an application rather than as a service, the password is used.

To stop a driver instance:

HP-UX, AS/400, OS/390, and zOS

Enter the `dirxml_jremote -config filename -u` command. For example:

```
dirxml_remote -config config.txt -u
```

Linux and Solaris

Enter the `rdxml -config filename -u` command. For example:

```
rdxml -config config.txt -u
```

Windows

Use the Remote Loader Console.

VII Installing the User Application and Roles Based Provisioning Module

This section guides you through the process of installing required components for the Roles Based Provisioning Module (RBPM) and the User Application. By default, the installation program installs these components in the following locations:

- ♦ **Linux:** /opt/novell/idm
- ♦ **Windows:** C:\Novell\IDM

RBPM and the User Application require access to other Identity Manager components during and after installation. NetIQ recommends that you review the installation process before beginning. For more information, see [Chapter 22, “Main Checklist for Installing RBPM and the User Application,”](#) on page 201.

22 Main Checklist for Installing RBPM and the User Application

Before beginning the installation process, NetIQ recommends that you review the following steps.

	Checklist Items
<input type="checkbox"/>	1. Learn about the interaction among Identity Manager components. For more information, see Section 4.3.1, “User Application and Roles Based Provisioning Module,” on page 33.
<input type="checkbox"/>	2. Ensure that the Identity Manager engine has been installed. For more information about installing the engine, see Chapter 14, “Installing the Identity Manager Engine,” on page 139.
<input type="checkbox"/>	3. Review the considerations for installing the User Application and RBPM to ensure that the computers meet the prerequisites. For more information, see Section 6.7, “Prerequisites and Requirements for Installing the User Application and Roles Based Provisioning Module,” on page 69.
<input type="checkbox"/>	4. Review the hardware and software requirements for the computers that will host RBPM and the User Application. For more information, see Section 6.7.6, “System Requirements for Installing the User Application and Roles Based Provisioning Module,” on page 75.
<input type="checkbox"/>	5. (Optional) Create a test environment using the Community Edition of JBoss Application Server and PostgreSQL database server. NetIQ provides this version of JBoss in the installation kit. For more information, see Chapter 23, “Installing the Community Edition of JBoss,” on page 203.
<input type="checkbox"/>	6. Install and configure a database for the User Application on the local computer or a connected server. <ul style="list-style-type: none">◆ To learn about the database, see Section 6.7.4, “Understanding the User Application Database,” on page 73.◆ To install the database, see Chapter 26, “Configuring the Database Before Installing the User Application,” on page 215.
<input type="checkbox"/>	7. Prepare an application server on the local computer or in a cluster. <ul style="list-style-type: none">◆ To understand the requirements, see Section 6.7.3, “Understanding the Application Server Requirements,” on page 72.◆ To prepare the cluster, see Chapter 27, “Preparing a Cluster Environment for Use with the User Application,” on page 221.◆ To install an application server, see Chapter 28, “Installing the User Application on an Application Server,” on page 227.
<input type="checkbox"/>	8. Review the contents of the User Application installation kit to determine which files are needed for your environment. For more information, see Section 6.7.2, “Understanding the Installation Files for the Roles Based Provisioning Module,” on page 71.
<input type="checkbox"/>	9. Install the RBPM component. For more information, see Chapter 24, “Installing the Roles Based Provisioning Module,” on page 205.
<input type="checkbox"/>	10. Create and deploy the User Application driver and the Roles and Resource Service driver. For more information, see Chapter 25, “Creating the Drivers for the Roles Based Provisioning Module,” on page 213.

	Checklist Items
<input type="checkbox"/>	<p>11. (Conditional) For a guided installation process (wizard) of the User Application, see one of the following sections:</p> <ul style="list-style-type: none"> ◆ Section 28.1, “Installing on a JBoss Application Server,” on page 227 ◆ Section 28.2, “Installing on a WebLogic Application Server,” on page 239 ◆ Section 28.3, “Installing on a WebSphere Application Server,” on page 247
<input type="checkbox"/>	<p>12. (Conditional) To install the User Application from the command line (console) either as a guided process or in a single command (silent installation), see Chapter 29, “Installing RBPM Components from the Command Line,” on page 259.</p> <p>NOTE: Silent installation can be performed on Linux computers only.</p>
<input type="checkbox"/>	<p>13. To perform the final tasks in the installation process, see Chapter 30, “Completing the Roles Based Provisioning Module / User Application Installation,” on page 277.</p>
<input type="checkbox"/>	<p>14. Install the rest of the Identity Manager components, including the Identity Information Warehouse.</p>
<input type="checkbox"/>	<p>15. (Optional) To begin using the User Application and RBPM, see the NetIQ User Application Administration Guide.</p>

23 Installing the Community Edition of JBoss

NetIQ provides the JBossPostgreSQL utility as a convenience for installing the Community Edition of JBoss Application Server and PostgreSQL database server, which are Open Source components.

- ♦ NetIQ recommends that you use this utility for creating test environments only. JBoss supports the Community Edition of the JBoss Application Server only in their User Forums. If you need support for these components, you must go to the third party provider of the component. NetIQ does not provide updates for these components, or administration, configuration, or tuning information for these components, beyond what it is outlined in the RBPM documentation.
- ♦ The JBossPostgreSQL utility does not secure the JMX Console or the JBoss Web Console. This leaves the JBoss environment vulnerable to security risks. You must lock down the environment as soon as you complete your installation. For more information about securing the JMX Console and JBoss Web Console, see (<http://community.jboss.org/wiki/SecureTheJmxConsole>).
- ♦ The installation program creates a new user with the name `novlua`. The `jboss_init` script runs JBoss as this user, using the permission defined in the JBoss files.

For more information about the database requirements, see [Section 6.7.4, “Understanding the User Application Database,” on page 73](#). For more information about the application server requirements, see [Section 6.7.3, “Understanding the Application Server Requirements,” on page 72](#).

To install JBoss PostgreSQL

- 1 Log on to the computer as the root user (Linux) or with an Administrator account (Windows).
- 2 Execute `JBossPostgreSQL.exe` or `JBossPostgreSQL.bin`, located by default in the `RBPM` folder of the installation kit.
- 3 Complete the steps in the installation wizard.
- 4 Shut down the JBoss server until you complete the installation for the User Application.
- 5 Lock down the JBoss environment to eliminate security risks.

For more information about securing the JMX Console and JBoss Web Console, see (<http://community.jboss.org/wiki/SecureTheJmxConsole>).

24 Installing the Roles Based Provisioning Module

This chapter describes the process for installing the core runtime infrastructure of RBPM:

Component	Description
Roles Based Provisioning Module	Installs the User Application Driver and the Role and Resource Driver.
Schema Extensions	Installs the eDirectory schema extensions.
Configuration Files	Installs driver configuration files.

NetIQ provides a wizard that guides you through the installation process.

24.1 Understanding the Roles Based Provisioning Module installation

This section provides a checklist to guide you through the installation process, as well as a description of the circumstances under which you might need to extend the schema for eDirectory.

24.1.1 Installation Checklist

	Checklist Items
<input type="checkbox"/>	1. Ensure that your servers meet the prerequisites for installing RBPM. For more information, see Section 6.7, "Prerequisites and Requirements for Installing the User Application and Roles Based Provisioning Module," on page 69.
<input type="checkbox"/>	2. Ensure that your servers meet the hardware and software requirements for installing RBPM. For more information, see Section 6.7.6, "System Requirements for Installing the User Application and Roles Based Provisioning Module," on page 75.
<input type="checkbox"/>	3. Ensure that eDirectory is running on the default LDAP ports 389 and 636 to avoid getting an error message about invalid schema. You can manually extend the eDirectory schema after installation. For more information, see Section 24.1.2, "Understanding Schema Extension," on page 206.
<input type="checkbox"/>	4. Identify a user account with rights to administer the Identity Vault server. You must know the LDAP format for the account's credentials.
<input type="checkbox"/>	5. Determine whether you can install RBPM with the schema extension files or you must manually extend the eDirectory schema. For more information, see Section 24.1.2, "Understanding Schema Extension," on page 206.
<input type="checkbox"/>	6. (Conditional) Manually extend the eDirectory schema. For more information, see Section 24.2, "Extending the eDirectory Schema Using the Wizard," on page 206 and Section 24.3, "Extending the Schema Manually without Using the Wizard," on page 208.

	Checklist Items
<input type="checkbox"/>	7. Install RBPM. For more information, see Section 24.4, “Installing RBPM with the Schema Extension Files,” on page 210.

24.1.2 Understanding Schema Extension

The RBPM installation wizard automatically installs the schema extension files for eDirectory to interact with RBPM. However, in the following circumstances you must manually extend the schema rather than use the wizard to install the extension files:

- ♦ You installed the Identity Vault in a non-default location. For more information, see [Section 24.2, “Extending the eDirectory Schema Using the Wizard,”](#) on page 206.
- ♦ You installed the Identity Vault and the Identity Manager engine as a non-root user. For more information, see [Section 24.3, “Extending the Schema Manually without Using the Wizard,”](#) on page 208.
- ♦ You do not want to use the RBPM installation wizard to perform the schema extension. For more information, see [Section 24.3, “Extending the Schema Manually without Using the Wizard,”](#) on page 208.

24.2 Extending the eDirectory Schema Using the Wizard

This section provides instructions for installing the RBPM runtime infrastructure files and then manually extending the eDirectory schema. Complete these steps only if the following circumstances are true:

- ♦ You want to use the RBPM installation wizard.
- ♦ You installed the Identity Vault in a non-default location.

If these circumstances are not true, you might need to use a different process for extending the eDirectory schema or you might not need to extend the schema at all. For more information, see [Section 24.1, “Understanding the Roles Based Provisioning Module installation,”](#) on page 205.

24.2.1 Extending the Schema on a SUSE Server

To extend the schema, you must copy the driver files to the non-default location and then run the `ndssch` command against both the `srvprv.sch` and `nrf-extensions.sch` schema files.

To extend the schema on SUSE:

- 1 Log on to the computer where you installed the Identity Manager engine.
- 2 To copy the driver and driver configuration files to the non-default location of Identity Vault, complete the following steps:
 - 2a Launch `rbpm_driver_install_linux.bin`, located by default in the `products/RBPM` directory within the `.iso` image file for the Identity Manager installation package for each operating system environment directory.
 - 2b In the Select Components window, select *Roles Based Provisioning Module and Configuration Files*. Click **Next**.

- 2c For installing the drivers, specify the same location path where you installed Identity Vault. Click **Next**.
 - 2d For installing the driver configuration files, specify the same location path where you installed Identity Vault. Click **Next**.
 - 2e Complete the installation wizard.
- 3 To extend the schema, run the following command against the `srvprv.sch` file:
- ```
ndssch -h hostname:port -t tree_name -p password admin-FDN path/srvprv.sch
```
- For example:
- ```
ndssch -h 172.16.1.137:524 -t TESTTREE -p PASSWORD
.cn=admin.o=novell.T=TESTTREE.
/opt/novell/eDirectory/lib/nds-schema/srvprv.sch
```
- 4 Repeat [Step 3](#) against the `nrf-extensions.sch` file.
 - 5 Continue to the process for creating the RBPM drivers. For more information, see [Chapter 25, "Creating the Drivers for the Roles Based Provisioning Module,"](#) on page 213.

24.2.2 Extending the Schema on a Windows Server

To extend the eDirectory schema on a Windows server, you must run `schemaStart.bat` against the `sch_nt.cfg`, `srvprv.sch`, and `update-nrf-case.sch` files.

To extend the schema on Windows:

- 1 Log on to the computer where you installed the Identity Vault.
- 2 Stop eDirectory.
- 3 Run the following command to extend the schemas listed in the `sch_nt.cfg` file, located by default in the eDirectory installation location:

```
eDirLocation\schemastart.bat eDirLocation yes admin name
with tree password yes 6 " " "schemafilename"
"servername" dibPathLocation
```

For example:

```
C:\eDir\NDS\schemastart.bat "C:\eDir\NDS" yes
.cn=admin.o=n.T=IDM-INSTALLISSUE." "n" yes 6 " "
"C:\eDir\NDS\vrschema.sch" ".CN=WIN2008-64-NDS.O=n.T=IDMINSTALLISSUE."
"C:\DIB\NDS\DIBFiles"
```

NOTE

- ♦ The `dibPathLocation` must contain the DIBFiles folder.
 - ♦ The above command does not use `sch_nt.cfg` file to extend all the schema files, but instead manually extends each and every schema file mentioned in the `sch_nt.cfg` file.
-

- 4 Log on to the computer where you installed the Identity Manager engine.

- 5 To copy the driver and driver configuration files to the non-default location of Identity Vault, complete the following steps:
 - 5a Launch the `rbpm_driver_install.exe`, located by default in the `products/RBPM` directory within the `.iso` image file for the Identity Manager installation package for each operating system environment directory.
 - 5b In the Select Components window, select *Roles Based Provisioning Module and Configuration Files*. Click **Next**.
 - 5c For installing the drivers, specify the same location path where you installed Identity Vault. Click **Next**.
 - 5d For installing the driver configuration files, specify the same location path where you installed Identity Vault. Click **Next**.
 - 5e Complete the installation wizard.
- 6 To extend the `SrvPrv` schema, run the command listed in [Step 3 on page 207](#) against the `srvprv.sch` file.
- 7 To extend the `NrfCaseupdate` schema, run the command listed in [Step 3 on page 207](#) against the `update-nrf-case.sch` file.
- 8 Start eDirectory.
- 9 Continue to the process for creating the RBPM drivers. For more information, see [Chapter 25, "Creating the Drivers for the Roles Based Provisioning Module," on page 213](#).

24.3 Extending the Schema Manually without Using the Wizard

This section provides instructions for installing the RBPM runtime infrastructure files and manually extending the eDirectory schema. Complete these steps only if all of the following circumstances are true:

- ◆ You do not want to use the RBPM installation wizard.
- ◆ You installed the Identity Vault in a non-default location.
- ◆ You installed the Identity Vault and Identity Manager engine as a non-root user.

If these circumstances are not true, you might need to use a different process for extending the eDirectory schema or you might not need to extend the schema at all. For more information, see [Section 24.1, "Understanding the Roles Based Provisioning Module installation," on page 205](#).

For these steps, you should copy the following additional files from the `prerequisites.zip` archive within the `.iso` image for Identity Manager to a location on the Identity Vault server:

File	Location
<code>nrf-extensions.sch</code>	<code>./schema</code>
<code>nrfdriver.jar</code>	<code>./lib</code>
<code>srvprvUAD.jar</code>	<code>./lib</code>
<code>xcd-all.jar</code>	<code>./lib</code>
<code>dirxml.lsc</code>	top-level folder
tmp folder	<code>./lib</code>

24.3.1 Extending the Schema on a Windows Server without the Wizard

Use `NDSCons.exe` to extend the schema on Windows servers. Schema files (*.sch) that come with eDirectory are installed by default into the `C:\Novell\NDS` directory.

- 1 Log on as a user with administrative rights to the computer where you installed the Identity Manager engine.
- 2 Click **Start > Settings > Control Panel > Novell eDirectory Services**.
- 3 Click **install.dlm**, then click **Start**.
- 4 Click **Install Additional Schema Files**, then click **Next**.
- 5 Specify the path to and name of the schema file. For example, enter `c:\Novell\NDS\nrf-extensions.sch`.

NOTE: You can copy this file from the `./schema` folder within the `prerequisitefiles.zip` archive within the `.iso` image for Identity Manager.

- 6 Click **Finish**.

24.3.2 Extending the Schema on UNIX or Linux without the Wizard

To extend the eDirectory schema for RBPM on a UNIX or Linux platform, you must add the RBPM schema file `nrf-extensions.sch`. To add the file, enter the following command from the command line:

```
ndssch [-h hostname[:port]] [-t tree_name] admin-FDN schemafilename.sch
```

24.3.3 Copying Additional JAR files

To ensure a successful installation, RBPM requires the following additional files be added to the server for the Identity Manager engine:

- ♦ `nrfdriver.jar`
- ♦ `srvprvUAD.jar`
- ♦ `xcd-all.jar`

For more information about the location of these files, see [Section 24.3, “Extending the Schema Manually without Using the Wizard,” on page 208](#).

Copy these files to the following directory on the server:

- ♦ **Linux and UNIX** (eDirectory 8.8.x): `/opt/novell/eDirectory/lib/dirxml/classes`
- ♦ **Windows:** `drive:\novell\nds\lib`

24.3.4 Adding the User Application Schema to your Audit Server as a Log Application

If your Audit server will use the User Application as a log application, you must copy the `dirxml.lsc` file to the server. This section applies to Novell Identity Audit only.

- 1 Locate the `dirxml.lsc` file.

This file is located in the Identity Manager User Application installation directory after the install, for example `/opt/novell/idm`. For more information about the location of the `dirxml.lsc` file, see [Section 24.3, “Extending the Schema Manually without Using the Wizard,” on page 208](#).

- 2 Use a Web browser to access an iManager with the Novell Identity Audit plug-in installed, and log on as an administrator.
- 3 Go to **Roles and Tasks > Auditing and Logging** and then select **Logging Server Options**.
- 4 Browse to the Logging Services container in your tree and select the appropriate Audit Secure Logging Server. Then click **OK**.
- 5 In the **Log Applications** tab, select the appropriate Container Name, and then click the **New Log Application** link.
- 6 In the New Log Application dialog box, complete the following steps:
 - 6a For Log Application Name, specify any name that is meaningful for your environment.
 - 6b For Import LSC File, browse to the `dirxml.lsc` file.
 - 6c Click **OK**.
- 7 Click **OK** to complete your Audit server configuration.
- 8 Ensure that the status on the Log Application is set to **ON**. (The circle under the status should be green.)
- 9 Restart the Audit server to activate the new log application settings.

24.4 Installing RBPM with the Schema Extension Files

This section provides the steps for installing RBPM and the eDirectory schema extension files by using an installation wizard.

NOTE: In some circumstances, you might not want to install the extension files. For more information, see [Section 24.1.2, “Understanding Schema Extension,” on page 206](#).

To install RBPM with the wizard:

- 1 Log on to the computer where you installed the Identity Manager engine.
- 2 Launch the installation program, located by default in the `products/RBPM` directory within the `.iso` image file for the Identity Manager installation package for each operating system environment directory.
 - ♦ **Linux:** `rbpm_driver_install_linux.bin`
 - ♦ **Windows:** `rbpm_driver_install.exe`
- 3 Complete the steps in the wizard.

NetIQ recommends that you select all of the components for installation, including the Schema Extensions component.

- 4 Continue to the process for creating the RBPM drivers. For more information, see [Chapter 25, "Creating the Drivers for the Roles Based Provisioning Module,"](#) on page 213.

25 Creating the Drivers for the Roles Based Provisioning Module

The process for installing RBPM adds the files for creating the RBPM drivers to the server. The driver configuration support allows you to do the following:

- ♦ Associate one User Application driver with a Role and Resource Service driver.
- ♦ Associate one User Application with a User Application driver.

Before you attempt to configure the drivers, ensure that you have all of the necessary packages in the Package Catalog on Identity Manager Designer. When you create a new Identity Manager project, the user interface automatically prompts you to import several packages into the new project.

25.1 Creating the User Application Driver

The User Application driver serves both as a runtime component and as a storage wrapper for directory objects (comprising the User Application's runtime artifacts). It is responsible for storing application-specific environment configuration data. The driver also notifies the directory abstraction layer when important data values change in the Identity Vault. This notification causes the directory abstraction layer to update its cache.

- 1 Open your project in Designer.
- 2 Under **Provisioning** in the **Modeler** view, select **User Application** in the palette.
- 3 Drag the icon for **User Application** onto the **Modeler** view.
- 4 In the Driver Configuration Wizard, select **User Application Base**, and then click **Next**.

NOTE: For the 4.0.2 release, you must have version 2.2.0.20120516011608 of the User Application Base package.

- 5 At the prompt for installing several additional packages, click **OK**.
- 6 (Optional) Specify the name of the driver.
Click **Next**.
- 7 In the connection parameters window, specify the ID and password for the User Application Administrator.
- 8 Specify the host and port for the User Application server.
- 9 Specify the application context for the User Application server.
- 10 (Optional) To allow the Provisioning Administrator to start workflows in the name of another person for whom the Provisioning Administrator is designated as proxy, select **Yes** for **Allow Initiator Override**.
- 11 In the Confirm Installation Tasks window, click **Finish**.

25.2 Creating the Role and Resource Service Driver

The User Application uses the Role and Resource Service Driver to manage back-end processing of resources. For example, it manages all resource requests, starts workflows for resource requests, and initiates the provisioning process for resource requests.

- 1 Open your project in Designer.
- 2 Under **Provisioning** in the **Modeler** view, select **Role Service** in the palette.
- 3 Drag the icon for **Role Service** onto the **Modeler** view.
- 4 In the Driver Configuration Wizard, select **Role and Resource Service Base**, and then click **Next**.

NOTE: For the 4.0.2 release, you must have version 2.0.0.20120509191258 of the Role and Resource Service Base package.

- 5 (Optional) Specify the name of the driver.
- 6 Click **Next**.
- 7 In the connection parameters window, specify the domain names for the base container and the User Application Driver that you just created.
Since the driver has not yet been deployed, the browse function will not show the User Application Driver that you just configured. You might need to type the DN for the driver.
- 8 Specify the URL for the User Application.
- 9 Specify the ID and password for the User Application Administrator.
- 10 Click **Next**.
- 11 In the Confirm Installation Tasks window, click **Finish**.

25.3 Deploying the Drivers for the User Application

The User Application and the Role and Resource Service drivers will not be available for use until you deploy them.

NOTE: When replicating an eDirectory environment, you must ensure that the replicas contain the NCP Server object for Identity Manager. Identity Manager is constrained to the local replicas of a server. For this reason, the Role and Resource Service Driver might not start properly if a secondary server does not include the server object.

To deploy the drivers:

- 1 Open your project in Designer.
- 2 In either the **Modeler** or the **Outline** view, select the Driver Set.
- 3 Click **Live > Deploy**.

26 Configuring the Database Before Installing the User Application

The database for the User Application supports tasks such as storing configuration data and data for workflow activities. Before you can install the User Application, you must have a database installed and configured. For more information about supported databases, see [Section 6.7.6, “System Requirements for Installing the User Application and Roles Based Provisioning Module,”](#) on page 75. For more information about considerations for the User Application database, see [Section 6.7.4, “Understanding the User Application Database,”](#) on page 73.

NOTE: If you are migrating to a new version of RBPM, you must use the same User Application database that you used for the previous installation (that is, the installation from which you are migrating).

26.1 Configuring a DB2 Database

This section helps you configure a DB2 database to be used with the User Application on a WebSphere Application Server.

26.1.1 Providing the Database Driver JARs

When configuring a DB2 database, the window allows you to specify only one database driver JAR file. However, the User Application requires two database driver JAR files:

- ♦ `db2jcc.jar`
- ♦ `db2jcc_license_cu.jar`

To specify two JAR files for a DB2 database:

- 1 Create the DB2 database.
- 2 In the **Database Username and Password** window of the wizard to install the User Application, manually enter the path to and names of both JAR files.

To separate the names, use the correct file separator for the operating system on which you want to install the database.

For example, on Windows, enter:

```
c:\db2jars\db2jcc.jar;c:\db2jars\db2jcc_license_cu.jar
```

On Linux, enter:

```
/home/lab/db2jars/db2jcc.jar:/home/lab/db2jcc_license_cu.jar
```

For more information, see [Step 14 on page 250](#).

26.1.2 Tuning DB2 Databases to Prevent Deadlocks and Timeouts

When using a DB2 database, if you see an error indicating that the current transaction has been rolled back because of a deadlock or timeout, the problem might be caused by a high level of user and database concurrency. DB2 provides many techniques for resolving lock conflicts, including tuning of the cost-based optimizer. The *Performance Guide* included in the DB2 Administration documentation is an excellent source that contains much information on the topic of tuning.

There are no prescribed tuning values that can be used for all installations since the level of concurrency and size of data varies. However, the following statements provide some DB2 tuning tips that might be relevant for your installation:

- ♦ Run the `reorgchk update statistics` command to update the statistics that the optimizer uses. Periodically updating these statistics might be enough to alleviate the problem.
- ♦ Use the DB2 registry parameter `DB2_RR_TO_RS` to improve concurrency. This parameter prevents locking the next key of the row that was inserted or updated.
- ♦ Increase the `MAXLOCKS` and `LOCKLIST` parameters on the database.
- ♦ Increase the `currentLockTimeout` property on the database connection pool.
- ♦ Use the Database Configuration Advisor and optimize for faster transactions.
- ♦ Alter all the User Application tables to be `VOLATILE` to indicate to the optimizer that cardinality of the table will vary significantly. For example, to make the `AFACTIVITY` table `VOLATILE`, you might issue the command: `ALTER TABLE AFACTIVITY VOLATILE`

The `ALTER TABLE` commands need to be run after the User Application has been started once and the database tables have been created. Refer to the `ALTER TABLE` documentation for more information on this statement. Here are the SQL statements for all the User Application tables:

```
ALTER TABLE AFACTIVITY VOLATILE
ALTER TABLE AFACTIVITYTIMERTASKS VOLATILE
ALTER TABLE AFBRANCH VOLATILE
ALTER TABLE AFCOMMENT VOLATILE
ALTER TABLE AFDOCUMENT VOLATILE
ALTER TABLE AFENGINE VOLATILE
ALTER TABLE AFENGINESTATE VOLATILE
ALTER TABLE AFMODEL VOLATILE
ALTER TABLE AFPROCESS VOLATILE
ALTER TABLE APPROVISIONINGSTATUS VOLATILE
ALTER TABLE AFQUORUM VOLATILE
ALTER TABLE AFRESOURCEREQUESTINFO VOLATILE
ALTER TABLE AFWORKTASK VOLATILE
ALTER TABLE AF_ROLE_REQUEST_STATUS VOLATILE
ALTER TABLE ATTESTATION_ATTESTER VOLATILE
ALTER TABLE ATTESTATION_ATTRIBUTE VOLATILE
ALTER TABLE ATTESTATION_QUESTION VOLATILE
ALTER TABLE ATTESTATION_REPORT VOLATILE
ALTER TABLE ATTESTATION_REQUEST VOLATILE
ALTER TABLE ATTESTATION_RESPONSE VOLATILE
ALTER TABLE ATTESTATION_SURVEY_QUESTION VOLATILE
ALTER TABLE ATTESTATION_TARGET VOLATILE
ALTER TABLE AUTHPROPS VOLATILE
ALTER TABLE DATABASECHANGELOG VOLATILE
ALTER TABLE DATABASECHANGELOGLOCK VOLATILE
ALTER TABLE DSS_APPLET_BROWSER_TYPES VOLATILE
ALTER TABLE DSS_APPLET_CFG VOLATILE
ALTER TABLE DSS_APPLET_CFG_MAP VOLATILE
ALTER TABLE DSS_BROWSER_TYPE VOLATILE
ALTER TABLE DSS_CONFIG VOLATILE
```



```

ALTER TABLE DSS_EXT_KEY_USAGE_RESTRICTION VOLATILE
ALTER TABLE DSS_USR_POLICY_SET VOLATILE
ALTER TABLE JBM_COUNTER VOLATILE
ALTER TABLE JBM_DUAL VOLATILE
ALTER TABLE JBM_ID_CACHE VOLATILE
ALTER TABLE JBM_MSG VOLATILE
ALTER TABLE JBM_MSG_REF VOLATILE
ALTER TABLE JBM_POSTOFFICE VOLATILE
ALTER TABLE JBM_ROLE VOLATILE
ALTER TABLE JBM_TX VOLATILE
ALTER TABLE JBM_USER VOLATILE
ALTER TABLE PORTALCATEGORY VOLATILE
ALTER TABLE PORTALPORTLETHANDLES VOLATILE
ALTER TABLE PORTALPORTLETSETTINGS VOLATILE
ALTER TABLE PORTALPRODUCERREGISTRY VOLATILE
ALTER TABLE PORTALPRODUCERS VOLATILE
ALTER TABLE PORTALREGISTRY VOLATILE
ALTER TABLE PROFILEGROUPPREFERENCES VOLATILE
ALTER TABLE PROFILEUSERPREFERENCES VOLATILE
ALTER TABLE PROVISIONING_CODE_MAP VOLATILE
ALTER TABLE PROVISIONING_CODE_MAP_LABEL VOLATILE
ALTER TABLE PROVISIONING_VIEW_VALUE VOLATILE
ALTER TABLE PROVISIONING_VIEW_VALUE_LABEL VOLATILE
ALTER TABLE SECURITYACCESSRIGHTS VOLATILE
ALTER TABLE SECURITYPERMISSIONMETA VOLATILE
ALTER TABLE SECURITYPERMISSIONS VOLATILE
ALTER TABLE SEC_DELPROXY_CFG VOLATILE
ALTER TABLE SEC_DELPROXY_SRV_CFG VOLATILE
ALTER TABLE SEC_SYNC_CLEANUP_QUEUE VOLATILE

```

26.2 Configuring a MySQL Database

This section provides configuration options for using a MySQL database. You can modify the options in the database configuration file:

Linux: `my.cnf` file

Windows: `my.ini` file

26.2.1 Configuring INNODB Storage Engine and Table Types

By default, a MySQL database uses the MyISAM table type. However, the User Application uses the INNODB storage engine, which requires the INNODB table types. You can either modify the configuration file or edit the SQL script for your database:

Modify the configuration file

In the database configuration file, change the default table statement to `default-table-type=innodb`. Also, remove any statement that contains the `skip-innodb`.

Edit the SQL scripts

In the SQL script for your database, append the `ENGINE=InnoDB` option to the Create Table statements.

26.2.2 Configuring the Character Set

Your User Application database must use UTF-8 as the character set. You can configure this setting for the whole server or just for a database:

On a server-wide basis

In the database configuration file, specify `character_set_server=utf8`.

When creating a database

To specify the character set for a database, complete the following steps:

1. When creating the database, enter the following command: `create database databasename character set utf8 collate utf8_bin;`
2. In the `IDM-ds.xml` file, specify the character set in the JDBC URL. For example,

```
connection-urljdbc:mysql://localhost:3306/  
databasename?useUnicode=true&characterEncoding=utf8&connectionColl  
ation=utf8_bin/connection-url
```

26.2.3 Configuring Case Sensitivity

If you plan to back up and restore data across servers or platforms, case sensitivity must be consistent across those servers or platforms.

Linux

In the `my.cnf` files for all platforms on which you plan to back up and restore a database, specify `0` for `lower_case_table_names`. For example, `lower_case_table_names=0`.

Windows

In the `my.ini` files for all platforms on which you plan to back up and restore a database, specify `1` for `lower_case_table_names`. For example, `lower_case_table_names=1`.

26.2.4 Configuring the ANSI Setting

When you create RBPM tables in your database, the system checks whether it should use ANSI mode to initially load data in the tables. If the database configuration file does not have an entry for ANSI mode, you might see a “Guest Container Page definition not found” error message.

Modify the configuration file

In the database configuration files, add the following statements:

```
# These variables are required for IDM User Application  
character_set_server=utf8  
default-table-type=innodb  
  
# Put the server in ANSI SQL mode.  
#See http://www.mysql.com/doc/en/ANSI\_mode.html  
ansi
```

Verify ANSI mode

To confirm that ANSI mode has taken effect, execute the following SQL command on your MySQL server:

```
mysql> select @@global.sql_mode;
+-----+
| @@global.sql_mode |
+-----+
| REAL_AS_FLOAT,PIPES_AS_CONCAT,ANSI_QUOTES,IGNORE_SPACE,ANSI |
+-----+
1 row in set (0.00 sec)
```

26.2.5 Configuring the Admin User Account

When you install the MySQL Database, the user account that you specify for the User Application must have full access to (be the owner of) the database. This account also needs access to the tables in the system.

Create a user to log on to the MySQL server and grant privileges to the user. For example, enter:

```
GRANT ALL PRIVILEGES ON dbname.* TO username@host IDENTIFIED BY 'password'
```

The minimum set of privileges should include the following:

- ◆ CREATE
- ◆ DELETE
- ◆ INDEX
- ◆ INSERT
- ◆ LOCK TABLES
- ◆ UPDATE

For more information about the GRANT command, see <http://www.mysql.org/doc/refman/5.0/en/grant.html> (<http://www.mysql.org/doc/refman/5.0/en/grant.html>).

IMPORTANT: The user account must also have select rights to the `mysql.user` table. To grant the proper rights, use the following SQL syntax:

```
USE mysql;
GRANT SELECT ON mysql.user TO username@host;
```

26.3 Configuring an Oracle Database

This section provides configuration options for using an Oracle database for the User Application. For information about supported versions of Oracle, see [Section 6.7.6, “System Requirements for Installing the User Application and Roles Based Provisioning Module,”](#) on page 75.

26.3.1 Configuring the Character Set

Your User Application database must use a Unicode-encoded character set. When creating the database, use AL32UTF8 to specify this character set.

To confirm that an Oracle 11g database is set for UTF-8, issue the following command:

```
select * from nls_database_parameters;
```

If the database is not configured for UTF-8, the system responds with the following information:

```
NLS_CHARACTERSET  
WE8MSWIN1252
```

Otherwise, the system responds with the following information that confirms the database is configured for UTF-8:

```
NLS_CHARACTERSET  
AL32UTF8
```

For more information about configuring a character set, see “[Choosing an Oracle Database Character Set](http://docs.oracle.com/cd/B28359_01/server.111/b28298/ch2charset.htm)” (http://docs.oracle.com/cd/B28359_01/server.111/b28298/ch2charset.htm).

26.3.2 Configuring the Admin User Account

The User Application requires that the Oracle database user account have `CONNECT` and `RESOURCE` privileges. In the SQL Plus utility, enter the following commands:

```
CREATE USER idmuser IDENTIFIED BY password
```

```
GRANT CONNECT, RESOURCE to idmuser
```

where *idmuser* represents the user account.

26.4 Configuring a SQL Server Database

This section provides configuration options for using an SQL Server database for the User Application. For information about supported versions of SQL Server, see [Section 6.7.6, “System Requirements for Installing the User Application and Roles Based Provisioning Module,”](#) on page 75.

26.4.1 Configuring the Character Set

SQL Server does not allow you to specify the character set for databases. The User Application stores SQL Server character data in a `NCHAR` column type, which supports UTF-8.

26.4.2 Configuring the Admin User Account

After installing Microsoft SQL Server, create a database and database user using an application such as SQL Server Management Studio. The database user account must have the following privileges:

- ♦ `CREATE TABLE`
- ♦ `DELETE`
- ♦ `INSERT`
- ♦ `SELECT`
- ♦ `UPDATE`

27 Preparing a Cluster Environment for Use with the User Application

The User Application benefits from higher availability when running in a cluster. In addition, the User Application supports HTTP session replication and session failover. This means that if a session is in process on a node and that node fails, the session can be resumed on another server in the cluster without intervention.

This chapter provides instructions for preparing a cluster environment to function with the User Application. You must complete the steps in this chapter in conjunction with the instructions in one of the following sections:

- ◆ [Section 28.1, “Installing on a JBoss Application Server,” on page 227](#)
- ◆ [Section 28.2, “Installing on a WebLogic Application Server,” on page 239](#)
- ◆ [Section 28.3, “Installing on a WebSphere Application Server,” on page 247](#)

For more information about the requirements for a cluster environment, see [Section 6.7.5, “Prerequisites for Installing the User Application in a Cluster Environment,” on page 75](#) and [Section 6.7.6, “System Requirements for Installing the User Application and Roles Based Provisioning Module,” on page 75](#).

27.1 Understanding Cluster Groups in JBoss and WebSphere Environments

The JGroups communications module provides communication among groups that share a common name, multicast address, and multicast port. JGroups is installed with JBoss, but you can use it without JBoss. The User Application includes a JGroups module in the User Application WAR file to support caching in a cluster environment.

JBoss uses the JGroups communications module to implement JBoss clusters. JBoss defines the configuration of JGroups and session replication which depends on the version of JBoss you are using.

The User Application uses an additional cluster group solely to coordinate User Application caches in a clustered environment in JBoss and WebSphere clusters. The **User Application cluster group** is independent of the two JBoss cluster groups and does not interact with them. By default, the User Application cluster group and the two JBoss groups use different group names, multicast addresses, and multicast ports, so no reconfiguration is necessary. The following table lists the default settings for the User Application cluster group.

Setting	Default Value
Name	c373e901aba5e8ee9966444553544200
Multicast address	228.8.8.8
Port	45654

The User Application cluster group uses a UUID name to minimize the risk of conflicts with other cluster groups that users might add to their servers. You can modify the configuration settings for User Application cluster group using the User Application administration features. Changes to the cluster configuration take effect for a server node only when you restart that node.

For more information about prerequisites for installing in a cluster environment, see [Section 6.7, “Prerequisites and Requirements for Installing the User Application and Roles Based Provisioning Module,”](#) on page 69.

27.2 Preparing a JBoss Cluster for the User Application

JBoss comes with three different ready-to-use server configurations: **minimal**, **default** and **all**. You can enable clustering in the *all* configuration only. A `cluster-service.xml` file in the `/deploy` folder describes the configuration for the default cluster partition. When you install the User Application and indicate to the installation program that you want to install into a cluster, the installation program makes a copy of the **all** configuration, names the copy IDM by default, and installs the User Application into this configuration.

27.2.1 Setting JBoss System Properties

To ensure performance of the cluster and the workflow engine, every server in the cluster should use the same partition name and partition UDP group. Also, each server in the cluster must be started with a unique ID for the workflow engine, because clustering for the workflow engine works independently of the User Application cache framework.

- 1 Open the JBoss startup script, by default located in the directory where you downloaded the User Application files.
 - ♦ **Linux:** `start-jboss.sh`
 - ♦ **Windows:** `start-jboss.bat`
- 2 Add the following text to the script:

```
start run.bat -c IDM -Djboss.partition.name=PartitionName-  
Djboss.partition.udpGroup=UDP_Group -Dcom.novell.afw.wf.engine-id=Engine_ID
```

where

- ♦ *PartitionName* represents the name of the partition, such as `Example_Partition`.
 - ♦ *UDP_Group* represents the User Datagram Protocol (UDP) group for the partition, such as `228.3.2.1`.
 - ♦ *Engine_ID* represents the unique ID of the workflow engine, such as `Engine1`.
- 3 Close and save the setup script.

27.2.2 Specifying the Cluster Option

When you install the User Application, you must specify the Identity Manager server name and workflow engine ID. Ensure that you also click **all** for **Single node (Default) or cluster (All)?** in the IDM Configuration window. For more information, see [Step 25](#) and [Step 27](#) on page 231.

27.2.3 Configuring the Cluster for the User Application Database

All nodes in the JBoss cluster must access the same database instance. Each time that you install the User Application to a cluster node, specify the same database name, host name or IP address, and port of the server on which the database for the User Application is installed.

27.2.4 Using the Same Master Key for Each User Application in the Cluster

The Identity Manager User Application encrypts sensitive data using a master key. All User Applications in a cluster must use the same master key. This section helps you ensure that all User Applications in a cluster use the same master key.

For more information about creating the master key, see [Step 31 on page 232](#). For more information about encrypting sensitive data in the User Application, see “[Encryption of Sensitive User Application Data](https://www.netiq.com/documentation/idm402/agpro/data/b2gx72y.html#b7z12vr)” (<https://www.netiq.com/documentation/idm402/agpro/data/b2gx72y.html#b7z12vr>) in the *User Application Administration Guide*.

- 1 Install the User Application on the first node in the cluster.
- 2 In the Security - Master Key window of the installation program, note the location of the `master-key.txt` file that will contain the new master key for the User Application. By default, the file is in the installation directory.
- 3 Install the User Application on the other nodes in the cluster.
- 4 In the Security - Master Key window, click **Yes** and then click **Next**.
- 5 In the Import Master Key window, copy the master key from the text file that was created in [Step 2 on page 223](#).

27.2.5 Starting the User Application in a Cluster Group

After you install the User Applications in your cluster, you must enable the cluster in the User Application cluster configuration.

- 1 Ensure that all servers are stopped.
- 2 Start the first User Application in the cluster.
- 3 Log on as the User Application administrator.
- 4 Click **Administration**.
- 5 In the Application Configuration portal, click **Caching**.
- 6 In the Caching Management window, select **True** for **Cluster Enabled**.
- 7 Click **Save**.
- 8 Restart the server.
- 9 (Conditional) To use local settings, repeat this procedure for each server in the cluster.

27.3 Preparing a WebLogic Cluster for the User Application

The process of installing the User Application in a WebLogic cluster is essentially the same as the process of installing the User Application on a single WebLogic server. The key difference is that you must explicitly identify the engine ID for each server when running in a clustered environment.

Complete the following steps to ensure that all of the components are configured correctly for a WebLogic clustered environment.

- 1 Install a WebLogic server (AdminServer) according to the instructions in the WebLogic documentation.
- 2 Configure a domain and add a managed Server1 with the Server1 IP address in the same domain.
- 3 Configure the additional managed servers in the same domain.
- 4 Configure the cluster and add the managed servers in the same cluster in the domain.
- 5 Install, configure, and deploy the User Application on the first WebLogic server (Server1).

For more information about installing and configuring the User Application on a single WebLogic server, see [Section 28.2, “Installing on a WebLogic Application Server,” on page 239](#).

- 6 Install, configure, and deploy the User Application on each additional server.
- 7 To specify the engine ID for each server, complete the following steps:
 - 7a Open the `C:\Oracle\Middleware\wlserver_10.3\common\bin\commEnv.cmd` file.
 - 7b Add an entry for the engine-id property (for example, `-Dcom.novell.afw.wf.engine-id=Engine1`).

27.4 Preparing a WebSphere Cluster for the User Application

This section outlines the process for preparing a WebSphere cluster for use with the User Application. This section assumes that you are an experienced user of the WebSphere Application Server (WAS).

- 1 Install and configure your WebSphere Application Servers and cluster according to the manufacturer's instructions.
- 2 Install, configure, and deploy the User Application on a WebSphere Application Server.

For more information about installing and configuring the User Application on a single server, see [Section 28.3, “Installing on a WebSphere Application Server,” on page 247](#).

NOTE: The installer writes the `sys-configuration-xmldata.xml` file to the directory that you specify during installation.

- 3 While performing the steps in [Section 28.3.4, “Adding User Application Configuration Files and JVM System Properties,” on page 253](#), you must complete the following additional steps:
 - 3a Create a new JVM system property for each User Application server in the cluster.
 - 3b Name the system property `com.novell.afw.wf.engine-id` where the engine ID is a unique value.
Each User Application server runs a workflow engine, and each engine requires a unique engine ID.

- 4 (Conditional) To use session failover with RBPM, complete the following steps:
 - 4a In the IBM Admin Console, navigate to **Application servers > clustermember1 > Session management > Distributed environment settings > Tuning parameters > Custom tuning parameters**.
 - 4b Specify **All session attributes** mode, which controls the write content for session failover.
- 5 Start the application server, and then access the User Application portal using the context that you specified during deployment.

28 Installing the User Application on an Application Server

This chapter provides instructions for installing and configuring an application server for the User Application and RBPM. You must have the correct version of the Java environment for your application server.

For more information about the requirements for the application server and Java, see [Section 6.7.6, “System Requirements for Installing the User Application and Roles Based Provisioning Module,”](#) on page 75.

28.1 Installing on a JBoss Application Server

This section describes how to install the User Application for RBPM on a JBoss Application Server by using the graphical user interface version of the installer.

28.1.1 Checklist for Installing the User Application on JBoss

Use the following checklist to guide you through the process of installing the User Application on a JBoss application server.

	Checklist Items
<input type="checkbox"/>	1. (Conditional) Review considerations for installing the User Application on JBoss in a cluster environment. For more information, see Section 27.1, “Understanding Cluster Groups in JBoss and WebSphere Environments,” on page 221.
<input type="checkbox"/>	2. Install a supported version of JBoss application server and Java development kit or runtime environment. For more information, see Section 6.7.6, “System Requirements for Installing the User Application and Roles Based Provisioning Module,” on page 75 and Section 28.1.2, “Installing the JBoss Application Server,” on page 228.
<input type="checkbox"/>	3. Ensure that the JBoss application server has the correct settings. For more information, see Section 27.2.1, “Setting JBoss System Properties,” on page 222.
<input type="checkbox"/>	4. Install the User Application. For more information, see “Installing the User Application with the Installation Wizard” on page 229.
<input type="checkbox"/>	5. (Conditional) To deploy the User Application on JBoss 5.1.2 Enterprise Application Platform (EAP), replace the <code>messaging-jboss-beans.xml</code> file. For more information, see “Deploying the User Application on JBoss 5.1.2 EAP” on page 233.
<input type="checkbox"/>	6. Deploy and start the User Application. For more information, see “Starting the User Application on a JBoss Server” on page 237.

28.1.2 Installing the JBoss Application Server

To install a JBoss Application Server, you can use one of the following scenarios:

- ◆ Download and install the JBoss Application Server according to manufacturer's instructions. For more information about supported versions, see [Section 6.7.6, "System Requirements for Installing the User Application and Roles Based Provisioning Module,"](#) on page 75.
- ◆ (Conditional) Use the JBossPostgreSQL utility provided with the RBPM download to install a JBoss Application Server (and optionally PostgreSQL). For more information, see ["Installing the Community Edition of JBoss" on page 203.](#) NetIQ recommends using this version of JBoss in your test environment only.

NOTE

- ◆ Do not start the JBoss server until after you install RBPM. On Linux, JBoss starts as a service by default. The installation program downloads a script called `/etc/init.d/jboss_init start/stop` to start JBoss at system reboot.
 - ◆ You can use a JavaServiceWrapper to install, start, and stop the JBoss Application Server as a Windows service or a Linux or UNIX daemon process. For more information, see the directions from JBoss at <http://www.jboss.org/community/wiki/RunJBossAsAServiceOnWindows>. One such wrapper is at <http://wrapper.tanukisoftware.org/doc/english/integrate-simple-win.html>. Manage it by JMX (<http://wrapper.tanukisoftware.org/doc/english/jmx.html#jboss>).
-

28.1.3 Installing the User Application on a JBoss Server

This section describes how to install the User Application for RBPM on a JBoss Application Server by using the graphical user interface version of the installation program. The installation process includes the following activities:

- ◆ ["Installing the User Application with the Installation Wizard" on page 229](#)
- ◆ ["Deploying the User Application on JBoss 5.1.2 EAP" on page 233](#)
- ◆ ["Starting the User Application on a JBoss Server" on page 237](#)

For more information about ...	See ...
Prerequisites for installing on a JBoss application server	Section 6.7, "Prerequisites and Requirements for Installing the User Application and Roles Based Provisioning Module," on page 69
Hardware and software requirements for installing on a JBoss application server	Section 6.7.6, "System Requirements for Installing the User Application and Roles Based Provisioning Module," on page 75
Using the console to install the User Application	Section 29.1, "Performing a Guided Installation from the Command Line," on page 260
Using a single command to install the User Application	Section 29.2, "Installing the User Application with a Single Command," on page 263

Installing the User Application with the Installation Wizard

This section explains how to use the User Application installation wizard. The following considerations apply to this process:

- ♦ You must use the Sun Java Runtime Environment (JRE) to launch the installation program.
- ♦ The installation program does not save the values that you enter as you progress through the windows in the wizard. If you click **Previous** to return to an earlier window, you must re-enter the configuration values.
- ♦ The installation program creates the **novlua** user account and sets the permissions in the JBoss files to this user. The `jboss_init` script uses this user account to run JBoss.

To install the User Application with the installation wizard:

- 1 Log on as a root user to the computer where you want to install the User Application.
- 2 Stop the JBoss application server.
- 3 (Conditional) If you are installing the User Application on JBoss 5.1.2 Enterprise Application Platform (EAP), copy the `jbossex.jar` file from the `%jboss-root%/lib` directory to the `%jboss-root%/common/lib` directory. Complete the installation steps in this section, and then continue to [“Deploying the User Application on JBoss 5.1.2 EAP” on page 233](#).
- 4 In the JRE, enter one of the following commands to start the `.jar` file, by default in the `products/RBPM/user_app_install` folder within the `.iso` image file for Identity Manager. For example:

Linux

```
$ /opt/novell/jre/bin/java -jar IdmUserApp.jar  
or  
$ /opt/novell/idm/jre/bin/java -jar IdmUserApp.jar
```

Windows

```
C:\Novell\InstallFiles\> "C:\Program Files\Java\jdk1.6.0_31\bin\java.exe"  
-jar IdmUserApp.jar
```

- 5 In the Welcome page of the User Application installation program, specify the language that you want to use for installation, and then click **OK**.
- 6 In the License Agreement window, click **I accept the terms of the License Agreement** and then click **Next**.
- 7 In the Application Server Platform window, click **JBoss** and then click **Next**.
- 8 In the Install Folder window, specify the folder where you want to place the installation files and then click **Next**.
- 9 In the Database Platform window, specify the platform of the User Application database. For example, Oracle. Click **Next**.
- 10 In the Database Host and Port window, specify the hostname or IP address of the server hosting the User Application database.
- 11 For **Port**, specify the number of the listener port for the database.
For a cluster, you must specify the same port for each member of the cluster.
- 12 Click **Next**.

- 13 In the Database Username and Password window, specify the name of the database according to the database platform. By default, the database name is `idmuserappdb`.
 - ◆ For a PostgreSQL, My SQL, or SQL Server database, specify the name.
 - ◆ For an Oracle database, specify the Security Identifier (SID) that you created with the database instance.
 - ◆ For a cluster, you must specify the same database name or SID for each member in the cluster.
- 14 Specify the name for the database user account to use with the User Application and the password associated with the user account.

In a cluster environment, you must use the same user account and password for each member in the cluster.
- 15 Specify the JAR file for the database platform.

The database vendor provides the driver JAR file, which represents the Thin Client JAR for the database server. For example, for PostgreSQL, specify `postgresql-8.4-701.jdbc4.jar`, by default in the `novell\idm\Postgres` folder. NetIQ does not support driver JAR files from third-party vendors.
- 16 Click **Next**.
- 17 (Optional) In the Database Administrator window, specify the name and password for the database administrator.

This field automatically lists the same user account and password that you specified in [Step 14](#). To use that account, do not make any changes.
- 18 Click **Next**.
- 19 In the Create Database Tables window, select one of the following options:
 - Create Tables Now**

The installation program creates the database tables as part of the installation process.
 - Create Tables at Application Startup**

The installation program leaves instructions to create the tables when the User Application starts for the first time.
 - Write SQL to File**

Create a schema file at installation time for the database administrator to use later to create the tables. When selecting this option, you must also specify a name for the file in the Schema Output File window.
- 20 Click **Next**.
- 21 (Conditional) If you chose **Create Tables Now** or **Write SQL to File** in [Step 19](#), specify whether the database is a new or empty database or it already exists from a previous installation. Click **Next**.

- 22 To verify that the User Application can connect to the specified database, click **Test Database Connection** and then click **Next**.

This step enables the installer to connect to the database for creating tables directly or for creating the .sql file.

NOTE: You can continue with installation if the database connection fails. However, after installation, you must manually create the tables and connect to the database. For more information, see “[Recreating the Database after Installation](http://www.netiq.com/documentation/idm402/agpro/?page=/documentation/idm402/agpro/data/bncf7rj.html)” (<http://www.netiq.com/documentation/idm402/agpro/?page=/documentation/idm402/agpro/data/bncf7rj.html>) in the *User Application Administration Guide*.

- 23 In the Java Install window, specify the path to the JRE file used to launch the installation program and then click **Next**.
- 24 In the JBoss Configuration window, specify the path to the installation files for the JBoss server and then click **Next**.
- 25 In the IDM Configuration window, specify the configuration for the JBoss application server:
- default**

Specifies that this installation is on a single node that is not part of a cluster.

If you select this option and decide later than you need a cluster, you must reinstall the User Application.
 - all**

Specifies that this installation is on a node within a cluster.
- 26 For **Application Context**, specify a name that represents the application server configuration, the application WAR file, and the name in the URL context.
- The installation script creates a server configuration, then names the configuration according to the name that you created when installing the application server. For example, `IDMProv`.
- IMPORTANT:** NetIQ recommends that you make a note of the specified **Application Context**. You will use this application name in the URL when you start the User Application from a browser.
- 27 (Optional) When installing the provisioning WAR file on a node in a cluster, you must also specify the **Workflow Engine ID**. The engine ID cannot exceed 32 characters. For more information about workflow engine IDs, see the section on configuring workflows for clustering in the *User Application Administration Guide*.
- 28 Click **Next**.
- 29 (Optional) To send log events to an auditing server, complete the following steps in the Select Audit Logging Type window:
- 29a Click **Yes** and then click **Next**.
 - 29b In the Audit Logging window, specify the type(s) of logging that you want to enable:
 - Novell Identity Audit or NetIQ Sentinel**

Enables logging through a Novell or NetIQ client for the User Application.
 - OpenXDAS**

Enables the User Application to send events to your OpenXDAS logging server.
 - 29c Click **Next**.

- 29d** (Conditional) If you chose in [Step 29](#) to send log events through a Novell client, in the Novell Identity Audit or Novel Sentinel window, specify the hostname or IP address for the client server and the path to the log cache.
- For more information about setting up loggin, see the [User Application Administration Guide](#).
- 30** Click **Next**.
- 31** (Optional) To import an existing master key, complete the following steps in the Security - Master Key window:

NOTE:

- ◆ The User Application uses the master key to access encrypted data.
- ◆ You must complete these steps after installing the first instance of the User Application in a cluster. Every instance of the User Application in a cluster must use the same master key. For more information, see [Section 27.2.4, “Using the Same Master Key for Each User Application in the Cluster,”](#) on page 223.
- ◆ Complete these steps if you are moving your installation from a staging system to a production system and want to keep access to the database you used with the staging system.
- ◆ Complete these steps also if you are restoring your User Application and you want to access the encrypted data stored by your previous version of the User Application.
- ◆ By default, the installation procedure writes the encrypted master key to the `master-key.txt` file in the installation directory.

-
- 31a** Click **Yes** and then click **Next**.
- 31b** In the Import Master Key window, copy and paste the master key from the `master-key.txt` file.
- 32** Click **Next**.
- 33** (Conditional) If, at this time, you do not want to specify the settings for the User Application to interact with RBPM, click **No** in the Configure IDM window.

NOTE: After installing the User Application, you can modify most of the settings in the `configureupdate.sh` or `configureupdate.bat` files. For more information about specifying the values for the settings, see the tables in [Section 30.2, “Configuring the User Application,”](#) on [page 277](#). The tables also explain which settings are required, and whether you can edit them with the configuration update files.

- 34** (Conditional) To immediately configure the User Application to interact with RBPM, complete the following steps in the Configure IDM window:
- 34a** Click **Yes** and then click **Next**.
 - 34b** In the Roles Based Provisioning Module Configuration window, click **Show Advanced Options**.
 - 34c** Modify the settings as needed.

NOTE

- ♦ For more information about specifying the values, see the tables in [Section 30.2, “Configuring the User Application,”](#) on page 277. The tables also explain which settings are required, and whether you can edit them with the configuration update files.
- ♦ In production environments, all administrator assignments are restricted by licensing. NetIQ collects monitoring data in the audit database to ensure that production environments comply. Also, NetIQ recommends that only one user be given the permissions of the Security Administrator.

-
- 34d** Click **OK**.
 - 35** Click **Next**.
 - 36** In the Pre-Installation Summary window, click **Install**.
 - 37** (Optional) Review the installation log files. For results of the basic installation, see the `Identity_Manager_User_Application_InstallLog.log` file. For information about the User Application configuration performed in Step 33, see the `Novell-Custom-Install.log` file.

Deploying the User Application on JBoss 5.1.2 EAP

To deploy RBPM on JBoss 5.1.2 Enterprise Application Platform (EAP), you need to perform several manual setup steps.

This procedure includes instructions for replacing the `messaging-jboss-beans.xml` file, which is part of JBoss 5.1.2 EAP. If you do not replace this file, you might see multiple warnings and errors in the startup log. This problem occurs because the RBPM installation uses the community version of the `messaging-jboss-beans.xml` file as a template to generate its own version of the file. Unfortunately, the EAP version is very different in many aspects, including the definitions of `QueueMODefinition` and `TopicMODefinition`.

- 1** Install JBoss 5.1.2 EAP.
- 2** Before launching the User Application installation program, copy the `jbossx.jar` file from the `%jboss-root%/lib` directory to the `%jboss-root%/common/lib` directory.
- 3** Install the User Application as described in [“Installing the User Application with the Installation Wizard”](#) on page 229.

4 Create a new messaging-jboss-beans.xml file with the following content:

```
<?xml version="1.0" encoding="UTF-8"?>

<!--
=====

Copyright (c) 2014 NetIQ Corporation. All Rights Reserved.

THIS WORK IS SUBJECT TO U.S. AND INTERNATIONAL COPYRIGHT LAWS AND TREATIES
NO PART OF THIS WORK MAY BE USED, PRACTICED, PERFORMED COPIED, DISTRIBUTED,
REVISED, MODIFIED, TRANSLATED, ABRIDGED, CONDENSED, EXPANDED, COLLECTED,
COMPILED, LINKED, RECAST, TRANSFORMED OR ADAPTED WITHOUT THE PRIOR WRITTEN
CONSENT OF NOVELL, INC. ANY USE OR EXPLOITATION OF THIS WORK WITHOUT
AUTHORIZATION COULD SUBJECT THE PERPETRATOR TO CRIMINAL AND CIVIL
LIABILITY.

=====
-->

<!--
    Messaging beans
    $Id: messaging-jboss-beans.xml 88672 2009-05-11 20:49:47Z
    anil.saldhana@jboss.com $
-->
<deployment xmlns="urn:jboss:bean-deployer:2.0">

    <!-- messaging application-policy definition -->
    <application-policy xmlns="urn:jboss:security-beans:1.0" name="messaging">
        <authentication>
            <login-module
code="org.jboss.security.auth.spi.DatabaseServerLoginModule" flag="required">
                <module-option name="unauthenticatedIdentity">guest</module-option>
                <module-option name="dsJndiName">java:/IDMUADDataSource</module-
option>
                <module-option name="principalsQuery">SELECT PASSWD FROM JBM_USER
WHERE USER_ID=?</module-option>
                <module-option name="rolesQuery">SELECT ROLE_ID, 'Roles' FROM
JBM_ROLE WHERE USER_ID=?</module-option>
            </login-module>
        </authentication>
    </application-policy>

    <bean name="SecurityStore"
class="org.jboss.jms.server.jbossxx.JBossASSecurityMetadataStore">
        <!-- default security configuration -->
        <property name="defaultSecurityConfig">
            <![CDATA[
                <security>
                    <role name="guest" read="true" write="true" create="true"/>
                </security>
            ]]>
        </property>
        <property name="suckerPassword">changeit</property>
        <property name="securityDomain">messaging</property>
        <property name="securityManagement"><inject
bean="JNDIBasedSecurityManagement"/></property>
        <!-- @JMX annotation to export the management view of this bean -->
        <annotation>@org.jboss.aop.microcontainer.aspects.jmx.JMX(name="jboss.messagin
```

```

g:service=SecurityStore",exposedInterface=org.jboss.jms.server.jbossx.JBossAS
SecurityMetadataStoreMBean.class)/annotation>
    <!-- Password Annotation to inject the password from the common password
utility
<annotation>@org.jboss.security.integration.password.Password(securityDomain="
messaging",methodName="setSuckerPassword")</annotation>
    -->
</bean>

    <bean name="MessagingDeploymentTemplateInfoFactory"
        class="org.jboss.managed.plugins.factory.DeploymentTemplateInfoFactory"/>

    <bean name="QueueTemplate"
class="org.jboss.profileservice.management.templates.JmsDestinationTemplate">
        <property name="info"><inject bean="QueueTemplateInfo"/></property>
    </bean>
    <bean name="QueueTemplateInfo"
class="org.jboss.profileservice.management.templates.JmsDestinationTemplateInf
o">
        <constructor factoryMethod="createTemplateInfo">
            <factory bean="DSDeploymentTemplateInfoFactory"/>
            <parameter
class="java.lang.Class">org.jboss.profileservice.management.templates.JmsDesti
nationTemplateInfo</parameter>
            <parameter
class="java.lang.Class">org.jboss.jms.server.destination.QueueServiceMO</
parameter>
            <parameter class="java.lang.String">QueueTemplate</parameter>
            <parameter class="java.lang.String">A template for JMS queue *-
service.xml deployments</parameter>
        </constructor>
        <property name="destinationType">QueueTemplate</property>
    </bean>

    <bean name="TopicTemplate"
class="org.jboss.profileservice.management.templates.JmsDestinationTemplate">
        <property name="info"><inject bean="TopicTemplateInfo"/></property>
    </bean>
    <bean name="TopicTemplateInfo"
class="org.jboss.profileservice.management.templates.JmsDestinationTemplateInf
o">
        <constructor factoryMethod="createTemplateInfo">
            <factory bean="DSDeploymentTemplateInfoFactory"/>
            <parameter
class="java.lang.Class">org.jboss.profileservice.management.templates.JmsDesti
nationTemplateInfo</parameter>
            <parameter
class="java.lang.Class">org.jboss.jms.server.destination.TopicServiceMO</
parameter>
            <parameter class="java.lang.String">TopicTemplate</parameter>
            <parameter class="java.lang.String">A template for JMS topic *-
service.xml deployments</parameter>
        </constructor>
        <property name="destinationType">TopicTemplate</property>
    </bean>
</deployment>

```

- 5 Replace the existing `messaging-jboss-beans.xml` file in the `IDMProv/deploy/messaging` folder with the file that you created in [Step 4](#).
- 6 Locate the persistence service configuration file for JBoss. For example, for PostgreSQL databases, the file is the `postgresql-persistence-service.xml` in the `novell\idm\jboss\docs\examples\jms` directory.
- 7 Replace the existing persistence service configuration file with the file in the database examples folder. For example for PostgreSQL, the `%jboss-root%/docs/examples/jms/postgresql-persistence-service.xml` file.
- 8 Add a copy of the new persistence service configuration file to the `%jboss-root%/server/IDMProv/deploy/messaging/` directory.
- 9 Open the persistence service configuration file, and then complete the following steps:
 - 9a Replace the text `DefaultDS` with the text `IDMUADataSource`.
 - 9b Within the `Clustered` attribute, comment out the following lines:

```

<attribute name="Clustered">false</attribute>

    <!-- All the remaining properties only have to be specified if the
post
office is clustered.
    You can safely comment them out if your post office is non
clustered
-->

    <!-- The JGroups group name that the post office will use -->

    <!--attribute
name="GroupName">${jboss.messaging.groupname:MessagingPostOffice}</
attribute>-->

    <!-- Max time to wait for state to arrive when the post office joins
the
cluster -->

    <!--attribute name="StateTimeout">30000</attribute>-->

    <!-- Max time to wait for a synchronous call to node members using the
MessageDispatcher -->

    <!--attribute name="CastTimeout">30000</attribute>-->

    <!-- Set this to true if you want failover of connections to occur
when a
node is shut down -->

    <!--<attribute name="FailoverOnNodeLeave">false</attribute>

    <depends
optional-attribute-
name="ChannelFactoryName">jboss.jgroups:service=ChannelFactory</depends>
    <attribute name="ControlChannelName">jbm-control</attribute>
    <attribute name="DataChannelName">jbm-data</attribute>
    <attribute
name="ChannelPartitionName">${jboss.partition.name:DefaultPartition}-JMS</
attribute>-->
    </mbean>

```

9c Replace the following lines with the specified text:

Replace this text	With this text
POPULATE.TABLES.3 = INSERT INTO JBM_USER (USER_ID, PASSWD, CLIENTID) VALUES ('john', 'needle', 'DurableSubscriberExample')	POPULATE.TABLES.3 = INSERT INTO JBM_USER (USER_ID, PASSWD, CLIENTID) VALUES ('p_user', 'changeit', 'IDMNotificationDurableTopic')
POPULATE.TABLES.8 = INSERT INTO JBM_ROLE (ROLE_ID, USER_ID) VALUES ('john', 'guest')	POPULATE.TABLES.8 = INSERT INTO JBM_ROLE (ROLE_ID, USER_ID) VALUES ('p_user', 'guest')
POPULATE.TABLES.9 = INSERT INTO JBM_ROLE (ROLE_ID, USER_ID) VALUES ('subscriber', 'john')	POPULATE.TABLES.9 = INSERT INTO JBM_ROLE (ROLE_ID, USER_ID) VALUES ('subscriber', 'p_user')
POPULATE.TABLES.10 = INSERT INTO JBM_ROLE (ROLE_ID, USER_ID) VALUES ('publisher', 'john')	POPULATE.TABLES.12 = INSERT INTO JBM_ROLE (ROLE_ID, USER_ID) VALUES ('durpublisher', 'p_user')

9d Close and save the persistence service configuration file.

10 Start JBoss.

11 Add the JBoss administrator account to the `stop-jboss.sh` script by completing the following steps:

11a Open the `stop-jboss.sh` script.

11b At the end of the `shutdown.sh` command, append the user account and password of the JBoss administrator. Use the following syntax:

```
shutdown.sh -s jnp://localhost:1199 -u %user_account% -p %password%
```

For example:

```
shutdown.sh -s jnp://localhost:1199 -u admin -p novell
```

11c Close and save the script.

12 (Optional) To verify proper configuration, ensure that the server log contains the following information:

```
INFO [ServerPeer] JBoss Messaging 1.4.7.GA server [0] started

INFO [TopicService] Topic[/topic/IDMNotificationDurableTopic] started,
fullSize=200000, pageSize=2000, downCacheSize=2000

INFO [RBPM] [com.novell.soa.notification.impl.jms.JMSConnectionMediator:init]
Starting JMS notification system
INFO [STDOUT] INFO [RBPM]
[com.novell.soa.notification.impl.NotificationThread:run] Starting
asynchronous notification system
```

Starting the User Application on a JBoss Server

This section provides instructions for starting the User Application and logging in the first time. This section requires one of the following JBoss startup scripts:

- ♦ **Linux:** `etc/init.d/jboss_init start`
- ♦ **Windows:** `start-jboss.bat`

If your browser does not display the User Application page after you complete these steps, check the terminal console for error messages and refer to [Chapter 50, “Troubleshooting,” on page 459](#).

To start the User Application on a JBoss Server:

- 1 Start your database. For more information, see your database documentation.
- 2 For the User Application to run reports, add the `Djava.awt.headless=true` flag to the startup script for the JBoss application server. For example:

```
JAVA_OPTS="-Djava.awt.headless=true -Dfile.encoding=UTF-8 -  
Dsun.jnu.encoding=UTF-8 -server -Xms1024m -Xmx1024m -XX:MaxPermSize=512m
```

NOTE: You do not need to perform this step if you are running on an X11 Windows system.

- 3 Start the JBoss application server where you installed the User Application.
- 4 At the command line, make the installation directory your working directory.
- 5 Execute the JBoss startup script.
- 6 To enable communication with the User Application driver, complete the following steps:
 - 6a Log on to iManager.
 - 6b Under **Identity Manager** in the Roles and Tasks display in the left navigation frame, select **Identity Manager Overview**.
 - 6c In the content view, specify the driver set that contains the User Application driver, then click **Search**.
 - 6d In the graphic showing the driver set with its associated drivers, click the red-and-white icon for the User Application driver.
 - 6e Select **Start Driver**.

Upon start, the driver attempts a “handshake” with the User Application. If your application server is not running or if the WAR was not deployed successfully, the driver returns an error. Otherwise, the driver status changes to the yin-yang symbol, indicating that the driver is now started.
- 7 To start the Role and Resource Service driver, repeat the procedure in [Step 6](#).
- 8 To launch and log on to the User Application, enter the following URL in your Web browser:
`http://hostname:port/ApplicationName`
 - hostname**

Represents the name of the application server. For example, `myserver.domain.com`
 - port**

Represents the port number of the application server. For example, `8180`.
 - ApplicationName**

Represents the name that you specified during the installation for the application when you provided application server configuration information.
- 9 In the upper right corner of the User Application landing page, click **Login**.

28.2 Installing on a WebLogic Application Server

This section describes how to install the User Application for RBPM on a WebLogic Application Server by using the graphical user interface version of the installation program.

For more information about ...	See ...
Prerequisites for installing on a WebLogic application server	Section 6.7, “Prerequisites and Requirements for Installing the User Application and Roles Based Provisioning Module,” on page 69
Hardware and software requirements for installing on an application server	Section 6.7.6, “System Requirements for Installing the User Application and Roles Based Provisioning Module,” on page 75
Using the console to install the User Application	Section 29.1, “Performing a Guided Installation from the Command Line,” on page 260
Using a single command to install the User Application	Section 29.2, “Installing the User Application with a Single Command,” on page 263

28.2.1 Checklist for Installing the User Application on WebLogic

Use the following checklist to guide you through the process of installing the User Application on a WebLogic application server.

	Checklist Items
<input type="checkbox"/>	1. Install a supported version of WebLogic application server and Java development kit or runtime environment. For more information, see Section 6.7.6, “System Requirements for Installing the User Application and Roles Based Provisioning Module,” on page 75.
<input type="checkbox"/>	2. Configure a data source file. For more information, see Section 28.2.2, “Configuring the Data Source for the User Application Database on WebLogic,” on page 240.
<input type="checkbox"/>	3. Create a WebLogic-enabled WAR for the User Application. For more information, see Section 28.2.3, “Installing the User Application with the Installation Wizard,” on page 240.
<input type="checkbox"/>	4. Prepare the WebLogic application server environment for running the User Application. For more information, see Section 28.2.4, “Configuring the WebLogic Environment for the User Application,” on page 244.
<input type="checkbox"/>	5. Deploy and log on to the User Application. For more information, see Section 28.2.5, “Start the User Application on the WebLogic Server,” on page 246.

28.2.2 Configuring the Data Source for the User Application Database on WebLogic

Before installing the User Application, you must have an existing data source file that points to the database. For WebLogic environments, you must manually create the data source file.

- 1 Copy the JAR files for your User Application database to the domain where you will deploy the User Application.
- 2 Create the data source file according to the instructions in the WebLogic documentation.
- 3 Change the JNDI name for the data source file to `jdbc/IDMUADataSource`, regardless of what name you specify for the data source file or for the database when you create the User Application WAR file.

28.2.3 Installing the User Application with the Installation Wizard

This section explains how to use the User Application installation wizard. The following considerations apply to this process:

- ◆ You must install a supported version of WebLogic Application Server before installing the User Application.
- ◆ You must use a supported version of the JRockit Java environment to launch the installation program.
- ◆ The installation program does not save the values that you enter as you progress through the windows in the wizard. If you click **Previous** to return to an earlier window, you must re-enter the configuration values.
- ◆ The installation program creates the `novlua` user account and sets the permissions in the JBoss files to this user. The `jboss_init` script uses this user account to run JBoss.

To install the User Application with the installation wizard:

- 1 Log on as a root user to the computer where you want to install the User Application.
- 2 In the JRockit Java environment, enter one of the following commands to start the `.jar` file, by default in the `products/RBPM/user_app/install` folder within the `.iso` image file for Identity Manager. For example:

Linux

```
$ /opt/WL/boa/jrockit_160_17/bin/java -jar IdmUserApp.jar
```

Windows

```
C:\WL\boa\jrockit_160_17\bin\java -jar IdmUserApp.jar
```

- 3 In the Welcome page of the User Application installation program, specify the language that you want to use for installation, and then click **OK**.
- 4 In the License Agreement window, click **I accept the terms of the License Agreement** and then click **Next**.
- 5 In the Application Server Platform window, click **WebLogic** and then click **Next**.
- 6 In the Install Folder window, specify the folder where you want to place the installation files and then click **Next**.
- 7 In the Database Platform window, specify the platform of the User Application database. For example, Oracle. Click **Next**.
- 8 In the Database Host and Port window, specify the hostname or IP address of the server hosting the User Application database.

For a cluster, you must specify the same name or IP address for each member of the cluster.

- 9 For **Port**, specify the number of the listener port for the database.

For a cluster, you must specify the same port for each member of the cluster.

- 10 Click **Next**.

- 11 In the Database Username and Password window, specify the name of the database according to the database platform. By default, the database name is `idmuserappdb`.

- ◆ For a PostgreSQL, My SQL, or SQL Server database, specify the name.
- ◆ For an Oracle database, specify the Security Identifier (SID) that you created with the database instance.
- ◆ For a cluster, you must specify the same database name or SID for each member in the cluster.

- 12 Specify the name for the database user account to use with the User Application and the password associated with the user account.

In a cluster environment, you must use the same user account and password for each member in the cluster.

- 13 Specify the JAR file for the database platform.

The database vendor provides the driver JAR file, which represents the Thin Client JAR for the database server. For example, for PostgreSQL, specify `postgresql-8.4-701.jdbc4.jar`, by default in the `novell\idm\Postgres` folder. NetIQ does not support driver JAR files from third-party vendors.

- 14 Click **Next**.

- 15 (Optional) In the Database Administrator window, specify the name and password for the database administrator.

This field automatically lists the same user account and password that you specified in [Step 14](#). To use that account, do not make any changes.

- 16 Click **Next**.

- 17 In the Create Database Tables window, select one of the following options:

Create Tables Now

The installation program creates the database tables as part of the installation process.

Create Tables at Application Startup

The installation program leaves instructions to create the tables when the User Application starts for the first time.

Write SQL to File

Create a schema file at installation time for the database administrator to use later to create the tables. When selecting this option, you must also specify a name for the file in the Schema Output File window.

- 18 Click **Next**.

- 19 (Conditional) If you chose **Create Tables Now** or **Write SQL to File** in [Step 19](#), specify whether the database is a new or empty database or it already exists from a previous installation). Click **Next**.

- 20 To verify that the User Application can connect to the specified database, click **Test Database Connection** and then click **Next**.

This step enables the installer to connect to the database for creating tables directly or for creating the .sql file.

NOTE: You can continue with installation if the database connection fails. However, after installation, you must manually create the tables and connect to the database. For more information, see “[Recreating the Database after Installation](http://www.netiq.com/documentation/idm402/agpro/?page=/documentation/idm402/agpro/data/bncf7rj.html)” (<http://www.netiq.com/documentation/idm402/agpro/?page=/documentation/idm402/agpro/data/bncf7rj.html>) in the *User Application Administration Guide*.

- 21 In the Java Install window, specify the path to the Java root installation folder and then click **Next**.

- 22 For **Application Context** in the IDM Configuration window, specify a name that represents the application server configuration, the application WAR file, and the name in the URL context.

The installation script creates a server configuration, then names the configuration according to the name that you created when installing the application server. For example, IDMPROV.

IMPORTANT: NetIQ recommends that you make a note of the specified **Application Context**. You will use this application name in the URL when you start the User Application from a browser.

- 23 Click **Next**.

- 24 (Optional) To send log events to an auditing server, complete the following steps in the Select Audit Logging Type window:

24a Click **Yes** and then click **Next**.

24b In the Audit Logging window, specify the type(s) of logging that you want to enable:

Novell Identity Audit or NetIQ Sentinel

Enables logging through a Novell or NetIQ client for the User Application.

OpenXDAS

Enables the User Application to send events to your OpenXDAS logging server.

24c Click **Next**.

24d (Conditional) If you chose in [Step 29](#) to send log events through a Novell client, in the Novell Identity Audit or Novel Sentinel window, specify the hostname or IP address for the client server and the path to the log cache.

For more information about setting up loggin, see the *User Application Administration Guide*.

- 25 Click **Next**.

- 26 (Optional) To import an existing master key, complete the following steps in the Security - Master Key window:

NOTE:

- ◆ The User Application uses the master key to access encrypted data.
- ◆ You must complete these steps after installing the first instance of the User Application in a cluster. Every instance of the User Application in a cluster must use the same master key. For more information, see [Section 27.2.4, “Using the Same Master Key for Each User Application in the Cluster,”](#) on page 223.
- ◆ Complete these steps if you are moving your installation from a staging system to a production system and want to keep access to the database you used with the staging system.

- ◆ Complete these steps also if you are restoring your User Application and you want to access the encrypted data stored by your previous version of the User Application.
 - ◆ By default, the installation procedure writes the encrypted master key to the `master-key.txt` file in the installation directory.
-

- 26a** Click **Yes** and then click **Next**.
- 26b** In the Import Master Key window, copy and paste the master key from the `master-key.txt` file.
- 27** Click **Next**.
- 28** (Conditional) If, at this time, you do not want specify the settings for the User Application to interact with RBPM, click **No** in the Configure IDM window.
-

NOTE: After installing the User Application, you can modify most of the settings in the `configureupdate.sh` or `configureupdate.bat` files. For more information about specifying the values for the settings, see the tables in [Section 30.2, “Configuring the User Application,” on page 277](#). The tables also explain which settings are required, and whether you can edit them with the configuration update files.

- 29** (Conditional) To immediately configure the User Application to interact with RBPM, complete the following steps in the Configure IDM window:
- 29a** Click **Yes** and then click **Next**.
- 29b** In the Roles Based Provisioning Module Configuration window, click **Show Advanced Options**.
- 29c** Modify the settings as needed.
-

NOTE

- ◆ For more information about specifying the values, see the tables in [Section 30.2, “Configuring the User Application,” on page 277](#). The tables also explain which settings are required, and whether you can edit them with the configuration update files.
 - ◆ In production environments, all administrator assignments are restricted by licensing. NetIQ collects monitoring data in the audit database to ensure that production environments comply. Also, NetIQ recommends that only one user be given the permissions of the Security Administrator.
-

- 29d** Click **OK**.
- 30** Click **Next**.
- 31** In the Pre-Installation Summary window, click **Install**.
- 32** (Optional) Review the installation log files. For results of the basic installation, see the `Identity_Manager_User_Application_InstallLog.log` file. For information about the User Application configuration performed in [Step 29](#), see the `Novell-Custom-Install.log` file.

28.2.4 Configuring the WebLogic Environment for the User Application

To ensure that the User Application runs properly, you must prepare your WebLogic environment. This process includes the following activities:

- ◆ “Specifying RBPM Configuration File Locations” on page 244
- ◆ “Removing OpenSAML JAR Files” on page 246
- ◆ “Modifying the Workflow Administration Plug-in” on page 246

Specifying RBPM Configuration File Locations

1 To ensure that the WebLogic application server can find the appropriate .xml files for the User Application, complete the following steps:

1a Open the `setDomainEnv.cmd` or `setDomainEnv.sh` file.

1b Locate the `JAVA_PROPERTIES` entry. For example, set `JAVA_PROPERTIES` or export `JAVA_PROPERTIES`.

1c Below the `JAVA_PROPERTIES` entry, add the following entries:

- ◆ `-Dextend.local.config.dir==directory-path` where *directory-path* specifies the folder (not the file itself) that contains the `sys-configuration.xml` file.
- ◆ `-Didmuserapp.logging.config.dir==directory-path` where *directory-path* specifies the folder (not the file itself) that contains the `idmuserapp_logging.xml` file.
- ◆ `-Dlog.init.file==file-name` where *file-name* specifies the `wl_idmuserapp_logging.xml` file, which is used for log4j configuration.

The `wl_idmuserapp_logging.xml` file handles the appender and logger configurations required for the User Application in situations where multiple applications are installed on the same application server.

For example on Windows, you might add the following entries:

```
set JAVA_OPTIONS=-Dextend.local.config.dir=c:\novell\idm
set JAVA_OPTIONS=%JAVA_OPTIONS% -
Didmuserapp.logging.config.dir=c:\novell\idm
set JAVA_OPTIONS=%JAVA_OPTIONS%
-Dlog.init.file=wl_idmuserapp_logging.xml
```

1d Ensure that the environment variable `EXT_PRE_CLASSPATH` points to the following JAR files:

- ◆ `antlr-2.7.6.jar`
- ◆ `log4j.jar`
- ◆ `commons-logging.jar`

NOTE: You must download this JAR file from the Apache site.

- ◆ `xalan.jar`
- ◆ `xercesImpl.jar`
- ◆ `xsltc.jar`
- ◆ `serializer.jar`

NOTE: Alternatively, you can copy these files into WEB-INF/lib directory within the IDMProv.war file.

1d1 Below the ADD EXTENSIONS TO CLASSPATH line, add EXT_PRE_CLASSPATH.

For example, on Windows:

```
set
EXT_PRE_CLASSPATH=C:\bea\user_projects\domains\base_domain\lib\antlr-
2.7.6.jar;C:\bea\user_projects\domain\base_domain\lib\log4j.jar;C:\bea
\user_projects\domains\base_domain\lib\commons-
logging.jar;C:\bea\user_projects\domains\base_domain\lib\xalan.jar;C:\
bea\user_projects\domains\base_domain\lib\xercesImpl.jar;C:\bea\user_p
rojects\domains\base_domain\lib\xsltc.jar;C:\bea\user_projects\domains
\base_domain\lib\serializer.jar
```

For example, on Linux:

```
export EXT_PRE_CLASSPATH=/opt/bea/user_projects/domains/base_domain/
lib/antlr-2.7.6.jar:/opt/bea/user_projects/domain/base_domain/lib/
log4j.jar:/opt/bea/user_projects/domains/base_domain/lib/commons-
logging.jar:/opt/bea/user_projects/domains/base_domain/lib/xalan.jar:/
opt/bea/user_projects/domains/base_domain/lib/xercesImpl.jar:/opt/bea/
user_projects/domains/base_domain/lib/xsltc.jar:/opt/bea/
user_projects/domains/base_domain/lib/serializer.jar
```

1e Save and exit the file.

2 To ensure that configuration update utility uses the appropriate .xml files, complete the following steps:

2a Open the configuration update file. For example, configupdate.bat or configupdate.sh.

2b In the -Duser.language=en -Duser.region=" line, add the path to the sys-configuration.xml file.

For example, on Windows:

```
-Dextend.local.config.dir=c:\novell\idm
```

For example, on Linux:

```
-Dextend.local.config.dir=/opt/novell/idm
```

2c Save and close the file.

2d Run the configuration update utility to install the certificate into the keystore of the JDK under BEA_HOME.

When you run configupdate, you are prompted for the cacerts file under the JDK you are using. If you are not using that same JDK that was specified during the installation you must run configupdate on the WAR. Pay attention to the JDK specified because this entry must point to the JDK used by WebLogic. This is done to import a certificate file for the connection to the Identity Vault. The purpose for this is to import a certificate for the connection to eDirectory.

The Identity Vault Certificates value in the configupdate utility must point to the following location:

```
c:\jrockit\jre\lib\security\cacerts
```

Removing OpenSAML JAR Files

WebLogic uses OpenSAML JAR files that conflict with the files that the User Application needs to run on WebLogic. This requirement applies to any User Application that does not have SSO enabled.

Remove the following JAR files from the `WebLogic /WL103/modules` directory:

- ♦ `com.bea.core.bea.opensaml_1.0.0.0_5-0-2-0.jar`
- ♦ `com.bea.core.bea.opensaml2_1.0.0.0_5-0-2-0.jar`

Modifying the Workflow Administration Plug-in

The Workflow Administration plug-in to iManager cannot connect to the User Application Driver running on WebLogic if the `enforce-valid-basic-auth-credentials` flag is set to true. You must disable this flag.

- 1 Open the `config.xml` file, by default in the `WLHome\user_projects\domains\idm\config\` folder.
- 2 At the end of the `<security-configuration>` section, add the following line:

```
<enforce-valid-basic-auth-credentials>>false</enforce-valid-basic-auth-credentials>
</security-configuration>
```
- 3 Close and save the file.
- 4 Restart the server.
- 5 (Optional) To verify the change, log on to the Workflow Administration plug-in.

28.2.5 Start the User Application on the WebLogic Server

Your User Application should be installed and ready for deployment. For more information about post-installation tasks, see [Chapter 30, "Completing the Roles Based Provisioning Module / User Application Installation,"](#) on page 277.

- 1 Log on to the WebLogic application server that hosts the User Application.
- 2 Using the standard WebLogic deployment procedure, deploy the User Application WAR.
- 3 To access the User Application portal, enter the following URL in a supported Web browser:

```
http://application-server-host:port/application-context
```

For example:

```
http://localhost:8180/IDMProv
```

28.3 Installing on a WebSphere Application Server

This section describes how to install the User Application for RBPM on a WebSphere Application Server by using the graphical user interface version of the installation program.

For more information about ...	See ...
Prerequisites for installing on a WebSphere Application Server	Section 6.7, “Prerequisites and Requirements for Installing the User Application and Roles Based Provisioning Module,” on page 69
Hardware and software requirements for installing on a WebSphere Application Server	Section 6.7.6, “System Requirements for Installing the User Application and Roles Based Provisioning Module,” on page 75
Using the console to install the User Application	Section 29.1, “Performing a Guided Installation from the Command Line,” on page 260
Using a single command to install the User Application	Section 29.2, “Installing the User Application with a Single Command,” on page 263

28.3.1 Checklist for Installing the User Application on WebSphere

Use the following checklist to guide you through the process of installing the User Application on a WebSphere application server.

	Checklist Items
<input type="checkbox"/>	1. Prepare the DB2 database to support the User Application. For more information, see “Configuring a DB2 Database” on page 215 .
<input type="checkbox"/>	2. Configure a data source file and JDBC provider for the database. For more information, see Section 28.3.2, “Configuring a Data Source for the User Application Database on WebSphere,” on page 248 .
<input type="checkbox"/>	3. Install a supported version of WebSphere application server and Java development kit or runtime environment. For more information, see Section 6.7.6, “System Requirements for Installing the User Application and Roles Based Provisioning Module,” on page 75 .
<input type="checkbox"/>	4. Create a WebSphere-enabled WAR for the User Application. For more information, see Section 28.2.3, “Installing the User Application with the Installation Wizard,” on page 240 .
<input type="checkbox"/>	5. Prepare the WebSphere application server environment for running the User Application. For more information, see the following sections: <ul style="list-style-type: none"> ◆ Section 28.3.4, “Adding User Application Configuration Files and JVM System Properties,” on page 253 ◆ Section 28.3.5, “Creating and Applying a Shared Library,” on page 254 ◆ Section 28.3.6, “Importing the eDirectory Trusted Root to the WebSphere Keystore,” on page 255 ◆ Section 28.3.7, “Applying the Unrestricted Policy Files for the IBM JDK,” on page 256 ◆ Section 28.3.8, “Passing the preferIPv4Stack Property to JVM,” on page 256
<input type="checkbox"/>	6. Deploy and log on to the User Application. For more information, see Section 28.3.9, “Starting the User Application on the WebSphere Server,” on page 257 .

28.3.2 Configuring a Data Source for the User Application Database on WebSphere

Before installing the User Application, you must have an existing data source file that points to the database. For WebSphere environments, you must manually create a JDBC Provider and a data source file.

- 1 Open the Integrated Solutions Console, which allows you to configure and administer WebSphere Application Server (WAS). By default, `http://host_name:9060/ibm/console`.
- 2 In the left pane of the console, expand **Resources > JDBC**.
- 3 To create the JDBC provider, complete the following steps:
 - 3a Click **JDBC providers**.
 - 3b In the content pane, expand **Scope**.
 - 3c Select **Node=yourservername, Server=server1**.
 - 3d Click **New**.
 - 3e For **Database Type**, specify the type of database you plan to use. For example, DB2.
 - 3f Click **Next**.
 - 3g Specify the classpath for the JDBC provider.
 - 3h Click **Next**.
 - 3i Click **Finish**.
 - 3j Click **Save** to save the changes directly to the master configuration.
- 4 To create the data source file, complete the following steps:
 - 4a Click **Data sources** (in the left pane under **JDBC**).
 - 4b In the content pane, expand **Scope**.
 - 4c Select **Node=yourservername, Server=server1**.
 - 4d Click **New**.
 - 4e Specify the name of the data source file and the JNDI. For example, `IDMUADatasource` for both fields.
 - 4f Click **Next**.
 - 4g Click **Select an existing JDBC provider**.
 - 4h Select the JDBC Provider that you created in [Step 3](#).
 - 4i Click **Next**.
 - 4j Specify the name, server name, port, username, and password for the database.
 - 4k Click **Next**.
 - 4l (Optional) Specify information for the Security Alias.
 - 4m Click **Next**.
 - 4n Click **Finish**.
 - 4o Click **Save**.
 - 4p In the Data Sources pane, click the box to the left of your new data source file.
 - 4q To verify the settings, click **Test Connection**.

28.3.3 Installing the User Application on a WebSphere Server

This section explains how to use the User Application installation wizard. The following considerations apply to this process:

- ◆ You must install a supported version of WebSphere Application Server before installing the User Application.
- ◆ The installation program does not save the values that you enter as you progress through the windows in the wizard. If you click **Previous** to return to an earlier window, you must re-enter the configuration values.
- ◆ The installation program creates the **novlua** user account and sets the permissions in the JBoss files to this user. The `jboss_init` script uses this user account to run JBoss.

To install the User Application with the installation wizard:

- 1 Log on as a root user to the computer where you want to install the User Application.
- 2 Apply the unrestricted policy files to the supported IBM JDK. Refer to your documentation for a link to these files from IBM and instructions for applying them. The JAR file for unrestricted policy files must be located in `JAVA_HOME\jre\lib\security`.

Without these unrestricted policy files, an error will occur that says “Illegal key size”. The root cause of this problem is the lack of unrestricted policy files, so be sure to use the correct IBM JDK.

- 3 In the IBM Java environment, enter one of the following commands to start the `.jar` file, by default in the `products/RBPM/user_app/install` folder within the `.iso` image file for Identity Manager. For example:

Linux

```
$ /opt/WS/IBM/WebSphere/AppServer/java/bin/java -jar IdmUserApp.jar
```

Windows

```
C:\WS\IBM\WebSphere\AppServer\java\bin\java -jar IdmUserApp.jar
```

- 4 In the Welcome page of the User Application installation program, specify the language that you want to use for installation, and then click **OK**.
- 5 In the License Agreement window, click **I accept the terms of the License Agreement** and then click **Next**.
- 6 In the Application Server Platform window, click **WebSphere** and then click **Next**.
- 7 In the Install Folder window, specify the folder where you want to place the installation files and then click **Next**.
- 8 In the Database Platform window, specify the platform of the User Application database. For example, Oracle. Click **Next**.
- 9 In the Database Host and Port window, specify the hostname or IP address of the server hosting the User Application database.
For a cluster, you must specify the same name or IP addresses for each member of the cluster.
- 10 For **Port**, specify the number of the listener port for the database.
For a cluster, you must specify the same port for each member of the cluster.
- 11 Click **Next**.
- 12 In the Database Username and Password window, specify the name of the database according to the database platform. By default, the database name is `idmuserappdb`.
 - ◆ For a PostgreSQL, DB2, or SQL Server database, specify the name or Security Identifier (SID).

- ♦ For an Oracle database, specify the SID that you created with the database instance.
 - ♦ For a cluster, you must specify the same database name or SID for each member in the cluster.
- 13** Specify the name for the database user account to use with the User Application and the password associated with the user account.
- In a cluster environment, you must use the same user account and password for each member in the cluster.
- 14** (Conditional) For a DB2 database, specify the two JAR files for the database server: `db2jcc.jar` and `db2jcc_license_cu.jar`.
- To separate the names, use the correct file separator for the operating system on which you want to install the database.
- For example, on Windows computers, enter:
- ```
c:\db2jars\db2jcc.jar;c:\db2jars\db2jcc_license_cu.jar
```
- On Linux computers, enter:
- ```
/home/lab/db2jars/db2jcc.jar:/home/lab/db2jcc_license_cu.jar
```
- 15** (Conditional) For SQL Server, PostgreSQL, and Oracle databases, specify the JAR file for the database server.
- The database vendor provides the driver JAR file, which represents the Thin Client JAR for the database server. For example, for PostgreSQL, specify `postgresql-8.4-701.jdbc4.jar`, by default in the `novell\idm\Postgres` folder. NetIQ does not support driver JAR files from third-party vendors.
- 16** Click **Next**.
- 17** (Optional) In the Database Administrator window, specify the name and password for the database administrator.
- This field automatically lists the same user account and password that you specified in [Step 14](#). To use that account, do not make any changes.
- 18** Click **Next**.
- 19** In the Create Database Tables window, select one of the following options:
- Create Tables Now**
- The installation program creates the database tables as part of the installation process.
- Create Tables at Application Startup**
- The installation program leaves instructions to create the tables when the User Application starts for the first time.
- Write SQL to File**
- Create a schema file at installation time for the database administrator to use later to create the tables. When selecting this option, you must also specify a name for the file in the Schema Output File window.
- 20** Click **Next**.
- 21** (Conditional) If you chose **Create Tables Now** or **Write SQL to File** in [Step 19](#), specify whether the database is a new or empty database or it already exists from a previous installation. Click **Next**.

- 22 To verify that the User Application can connect to the specified database, click **Test Database Connection** and then click **Next**.

This step enables the installer to connect to the database for creating tables directly or for creating the .sql file.

NOTE: You can continue with installation if the database connection fails. However, after installation, you must manually create the tables and connect to the database. For more information, see “[Recreating the Database after Installation](http://www.netiq.com/documentation/idm402/agpro/?page=/documentation/idm402/agpro/data/bncf7rj.html)” (<http://www.netiq.com/documentation/idm402/agpro/?page=/documentation/idm402/agpro/data/bncf7rj.html>) in the *User Application Administration Guide*.

- 23 In the Java Install window, specify the path to the Java root installation folder and then click **Next**.

- 24 For **Application Context** in the IDM Configuration window, specify a name that represents the application server configuration, the application WAR file, and the name in the URL context.

The installation script creates a server configuration, then names the configuration according to the name that you created when installing the application server. For example, `IDMProv`.

IMPORTANT: NetIQ recommends that you make a note of the specified **Application Context**. You will use this application name in the URL when you start the User Application from a browser.

- 25 Click **Next**.

- 26 (Optional) To send log events to an auditing server, complete the following steps in the Select Audit Logging Type window:

26a Click **Yes** and then click **Next**.

26b In the Audit Logging window, specify the type(s) of logging that you want to enable:

Novell Identity Audit or NetIQ Sentinel

Enables logging through a Novell client for the User Application.

OpenXDAS

Enables the User Application to send events to your OpenXDAS logging server.

26c Click **Next**.

26d (Conditional) If you chose in [Step 26b](#) to send log events through a Novell or NetIQ client, in the Novell Identity Audit or NetIQ Sentinel window, specify the hostname or IP address for the client server and the path to the log cache.

For more information about setting up logging, see the *User Application Administration Guide*.

- 27 Click **Next**.

- 28 (Optional) To import an existing master key, complete the following steps in the Security - Master Key window:

NOTE:

- ◆ The User Application uses the master key to access encrypted data.
- ◆ You must complete these steps after installing the first instance of the User Application in a cluster. Every instance of the User Application in a cluster must use the same master key. For more information, see [Section 27.2.4, “Using the Same Master Key for Each User Application in the Cluster,”](#) on page 223.
- ◆ Complete these steps if you are moving your installation from a staging system to a production system and want to keep access to the database you used with the staging system.

- ◆ Complete these steps also if you are restoring your User Application and you want to access the encrypted data stored by your previous version of the User Application.
 - ◆ By default, the installation procedure writes the encrypted master key to the `master-key.txt` file in the installation directory.
-

28a Click **Yes** and then click **Next**.

28b In the Import Master Key window, copy and paste the master key from the `master-key.txt` file.

29 Click **Next**.

30 (Conditional) If, at this time, you do not want to specify the settings for the User Application to interact with RBPM, click **No** in the Configure IDM window.

NOTE: After installing the User Application, you can modify most of the settings in the `configureupdate.sh` or `configureupdate.bat` files. For more information about specifying the values for the settings, see the tables in [Section 30.2, “Configuring the User Application,” on page 277](#). The tables also explain which settings are required, and whether you can edit them with the configuration update files.

31 (Conditional) To immediately configure the User Application to interact with RBPM, complete the following steps in the Configure IDM window:

31a Click **Yes** and then click **Next**.

31b In the Roles Based Provisioning Module Configuration window, click **Show Advanced Options**.

31c Modify the settings as needed.

NOTE

- ◆ For more information about specifying the values, see the tables in [Section 30.2, “Configuring the User Application,” on page 277](#). The tables also explain which settings are required, and whether you can edit them with the configuration update files.
 - ◆ In production environments, all administrator assignments are restricted by licensing. NetIQ collects monitoring data in the audit database to ensure that production environments comply. Also, NetIQ recommends that only one user be given the permissions of the Security Administrator.
-

31d Click **OK**.

32 Click **Next**.

33 In the Pre-Installation Summary window, click **Install**.

34 (Optional) Review the installation log files. For results of the basic installation, see the `Identity_Manager_User_Application_InstallLog.log` file. For information about the User Application configuration performed in [Step 31](#), see the `Novell-Custom-Install.log` file.

28.3.4 Adding User Application Configuration Files and JVM System Properties

This section helps you create new JVM system properties that the User Application requires to function on a WebSphere application server.

- 1 Copy the `sys-configuration-xmldata.xml` file from the User Application installation directory to a directory on the computer that hosts the WebSphere server. For example /`UserAppConfigFiles`. For more information about the file, see [Section 27.4, “Preparing a WebSphere Cluster for the User Application,” on page 224](#).

IMPORTANT: `Configupdate.sh` will update the local version of this file. In the future, if you run `Configupdate.sh`, you must update WebSphere's version of this file by copying it again. As a precaution, you should also make backup copies of all of the versions of this file.

- 2 Log on to the WebSphere admin console as an admin user.
- 3 Set the path to the `sys-configuration-xmldata.xml` file in the JVM system properties.
- 4 In the left pane, click **Servers > Application Servers**.
- 5 In the list of servers, click the server name. For example, `server1`.
- 6 In the list of settings in the content pane, click **Java and Process Management** under **Server Infrastructure**.
- 7 Expand the link and select **Process Definition**.
- 8 Under the list of **Additional Properties**, select **Java Virtual Machine**.
- 9 Select **Custom Properties** under the **Additional Properties** heading for the JVM page.
- 10 To add the `idmuserapp.logging.config.dir` JVM system property, complete the following steps:
 - 10a Click **New**.
 - 10b For **Name**, specify `extend.local.config.dir`.
 - 10c For **Value**, specify the name of the install folder (directory) that you specified during installation.

The installer wrote the `sys-configuration-xmldata.xml` file to this folder.
 - 10d For **Description**, specify a description for the property, for example `path to sys-configuration-xmldata.xml`.
 - 10e Click **OK** to save the property.
- 11 To add the `idmuserapp.logging.config.dir` JVM system property, complete the following steps:
 - 11a Click **New**.
 - 11b For **Name**, specify `idmuserapp.logging.config.dir`.
 - 11c For **Value**, specify the name of the install folder (directory) that you specified during installation.
 - 11d For **Description**, specify a description for the property, for example `path to idmuserapp_logging.xml`.
 - 11e Click **OK** to save the property.

The `idmuserapp-logging.xml` file does not exist until you persist the changes through **User Application > Administration > Application Configuration > Logging**.

- 12 (Conditional) To specify the workflow engine ID for a clustered environment, complete the following steps:
 - 12a Click **New**.
 - 12b For **Name**, specify `com.novell.afw.wf.engine-id`.
 - 12c For **Value**, specify the ID for the workflow engine.
 - 12d For **Description**, specify a description for the property, for example `workflow engine ID`.
 - 12e Click **OK** to save the property.

28.3.5 Creating and Applying a Shared Library

If you are using WebSphere 7.0 with Version 4.0.2 of the RBPM, you must configure a shared library for RBPM. You must also apply the shared library to a new class loader. This will ensure that WebSphere uses the RBPM versions of these JAR files. Otherwise, you will encounter class loading problems with JAR files that have shipped with WebSphere. WebSphere class loading problems can manifest as the following kinds of exceptions:

- ♦ `ClassCastException`
- ♦ `ClassNotFoundException`
- ♦ `NoClassDefFoundException`
- ♦ `UnsatisfiedLinkError`
- ♦ `LinkageError`

This process includes the following activities:

- ♦ [“Configuring the Shared Library” on page 254](#)
- ♦ [“Applying the Shared Library to a New Class Loader” on page 255](#)

Configuring the Shared Library

- 1 Log on to the WebSphere admin console as an admin user.
- 2 In the left pane, expand **Environment**.
- 3 Click **Shared Libraries**.
- 4 In the content pane, click **New**.
- 5 Specify a name, such as `IDMUA Classpath`.
- 6 In the **Classpath** field, add the following required JAR files:
 - ♦ `antlr.jar`
 - ♦ `log4j.jar`
 - ♦ `commons-logging.jar`

NOTE: You need to download this JAR file from the Apache site.

- ♦ `xalan.jar`
 - ♦ `xercesImpl.jar`
 - ♦ `xslt.jar`
 - ♦ `jaxb-impl.jar`
- 7 Select **Use an isolated class loader for this shared library**.

- 8 Click **OK**.
- 9 Click **Save** to save the changes to the master configuration.

Applying the Shared Library to a New Class Loader

- 1 Log on to the WebSphere admin console as an admin user.
- 2 Expand **Application servers > server-name > Class loader**.

NOTE: By default, this option is collapsed under the **Java and Process Management** section.

- 3 In the content pane, click **New** to create a new class loader.
- 4 Select **Classes loaded with local class loader first (parent last)**.
- 5 Click **Apply**.
- 6 Select **Shared library references**.
- 7 Click **Add** and then select the shared library that you created in [“Configuring the Shared Library” on page 254](#).
- 8 Click **Apply**.
- 9 Click **OK**.
- 10 Click **Save** to save the changes to the master configuration.

28.3.6 Importing the eDirectory Trusted Root to the WebSphere Keystore

This section helps you import the eDirectory trusted root certificates to the keystore on the computer hosting the WebSphere server. You can perform this process in one of the following ways:

- ♦ [“Importing Certificates with the WebSphere Administrator’s Console” on page 255](#)
- ♦ [“Importing Certificates with the Command Line” on page 256](#)

Importing Certificates with the WebSphere Administrator’s Console

- 1 Copy the eDirectory trusted root certificates to the computer hosting the WebSphere server.
The User Application installation procedure exports the certificates to the directory in which you install the User Application.
- 2 Log on to the WebSphere administration console as an admin user.
- 3 In the left pane, expand **Security > SSL Certificate and Key Management**.
- 4 In the content pane, select **Key stores and certificates** under **Related Items**.
- 5 Select **NodeDefaultTrustStore** (or the trust store that you are using).
- 6 Under **Additional Properties**, select **Signer Certificates**.
- 7 Click **Add**.
- 8 Type the Alias name and full path to the certificate file.
- 9 Change the Data type in the drop-down list to **Binary DER data**.
- 10 Click **OK**.
You should now see the certificate in the list of signer certificates.
- 11 Click **Save** to save the changes to the master configuration.

Importing Certificates with the Command Line

You must use the WebSphere keytool to import the certificate into the WebSphere keystore. By default, the WebSphere keytool is located in `/IBM/WebSphere/AppServer/java/bin`. The store type is PKCS12.

- 1 Copy the eDirectory trusted root certificates to the computer hosting the WebSphere server.
The User Application installation procedure exports the certificates to the directory in which you install the User Application.
- 2 From the command line on the machine hosting the WebSphere server, run the WebSphere keytool.

For example:

```
keytool -import -trustcacerts -file servercert.der -alias myserveralias  
-keystore trust.p12 -storetype PKCS12
```

NOTE: If you have more than one `trust.p12` file on your system, you might need to specify the full path to the file.

28.3.7 Applying the Unrestricted Policy Files for the IBM JDK

In [Step 2 on page 249](#) for installing the User Application WAR file, you applied the unrestricted policy files to the supported IBM JDK on the server where you installed the User Application. You must also apply these unrestricted policy files for each WebSphere IBM JDK server that is running RBPM.

Review each WebSphere server IBM JDK to ensure that you have applied the unrestricted policy files. Without these unrestricted policy files, the error “Illegal key size” will occur during startup of RBPM.

28.3.8 Passing the preferIPv4Stack Property to JVM

The User Application uses JGroups for the caching implementation. In some configurations, JGroups requires that the `preferIPv4Stack` property be set to true to ensure that the `mcast_addr` binding is successful.

Without this option, the following error might occur:

```
[10/1/09 16:11:22:147 EDT] 0000000d UDP          W org.jgroups.util.Util  
createMulticastSocket could not bind to /228.8.8.8 (IPv4 address); make sure  
your mcast_addr is of the same type as the IP stack (IPv4 or IPv6).
```

You might also see this error:

```
[3/21/12 10:04:32:470 EDT] 00000024 UDP          E org.jgroups.protocols.TP down  
failed sending message to null (131 bytes)  
    java.lang.Exception: dest=/228.8.8.8:45654 (134 bytes)  
    at org.jgroups.protocols.UDP._send(UDP.java:353)
```

The parameter `java.net.preferIPv4Stack=true` is a system property that can be set in the same manner as other system properties such as `extend.local.config.dir`. For instructions on setting system properties, see [Section 28.3.4, “Adding User Application Configuration Files and JVM System Properties,” on page 253](#).

28.3.9 Starting the User Application on the WebSphere Server

Your User Application should be installed and ready for deployment. For more information about post-installation tasks, see [Chapter 30, “Completing the Roles Based Provisioning Module / User Application Installation,”](#) on page 277.

- 1 Log on to the WebSphere application server that hosts the User Application.
- 2 Using the standard WebSphere deployment procedure, deploy the User Application WAR file.
- 3 Log on to the WebSphere administrator’s console as an admin user.
- 4 In the left navigation pane, expand **Applications > Enterprise Applications**.
- 5 Select the check box beside the User Application context that you want to start, and then click **Start**.
- 6 Log out of the console.
- 7 To access the User Application portal, enter the following URL in a supported Web browser:

`http://application-server-host:port/application-context`

For example:

`http://localhost:9080/IDMProv`

29 Installing RBPM Components from the Command Line

This section describes the methods that you can perform from the command line to install RBPM components, such as the User Application, Resource Information Services (RIS) facility, and JBossPostgreSQL.

Ensure that your environment has a supported version of an application server and Java development kit or runtime environment. Use the following checklist to help you complete the installation.

	Checklist Items
<input type="checkbox"/>	1. Complete items 1 through 9 in the installation checklist. For more information, see Chapter 22, “Main Checklist for Installing RBPM and the User Application,” on page 201.
<input type="checkbox"/>	2. (Conditional) Review considerations for installing the User Application on JBoss in a cluster environment. For more information, see Section 27.1, “Understanding Cluster Groups in JBoss and WebSphere Environments,” on page 221.
<input type="checkbox"/>	3. Ensure that the application server environment has the right settings. For more information, see the section related to your application server in Chapter 28, “Installing the User Application on an Application Server,” on page 227.
<input type="checkbox"/>	4. (Conditional) To install in a WebLogic or WebSphere environment, configure a data source file. For more information, see Section 28.2.2, “Configuring the Data Source for the User Application Database on WebLogic,” on page 240 or Section 28.3.2, “Configuring a Data Source for the User Application Database on WebSphere,” on page 248.
<input type="checkbox"/>	5. (Conditional) To use the guided installation process from the command line (console) for installing the User Application, see Section 29.1, “Performing a Guided Installation from the Command Line,” on page 260.
<input type="checkbox"/>	6. (Conditional) To install the User Application with a single command from the command line (silent installation), see Section 29.2, “Installing the User Application with a Single Command,” on page 263.
<input type="checkbox"/>	7. To run the JBossPostgreSQL utility from the command line, see Section 29.3, “Running the JBossPostgreSQL Utility in Silent or Command Mode,” on page 272.
<input type="checkbox"/>	8. To run the Resource Information Services (RIS) facility from the command line, see Section 29.4, “Running the RIS Installation Program in Silent or Command Mode,” on page 275.
<input type="checkbox"/>	9. Deploy and log on to the User Application. For more information, see the appropriate information for your application server environment in Chapter 28, “Installing the User Application on an Application Server,” on page 227.

29.1 Performing a Guided Installation from the Command Line

This section describes how to perform a guided installation of the User Application from the console (command line). The installation program walks you through each step similar to the installation wizard described in [Section 28.1.3, “Installing the User Application on a JBoss Server,”](#) on page 228.

For more information about ...	See ...
Prerequisites for installing on an application server	Section 6.7, “Prerequisites and Requirements for Installing the User Application and Roles Based Provisioning Module,” on page 69
Hardware and software requirements for installation	Section 6.7.6, “System Requirements for Installing the User Application and Roles Based Provisioning Module,” on page 75
Using the installation wizard to install the User Application	Chapter 28, “Installing the User Application on an Application Server,” on page 227
Using a single command to install the User Application	Section 29.2, “Installing the User Application with a Single Command,” on page 263

To install the User Application with the command line:

- 1 Log on as a root user to the computer where you want to install the User Application.
- 2 (Conditional) If you are installing the User Application on JBoss 5.1.2 Enterprise Application Platform (EAP), copy the `jbossex.jar` file from the `%jboss-root%/lib` directory to the `%jboss-root%/common/lib` directory. Complete the installation steps in this section, and then continue to [“Deploying the User Application on JBoss 5.1.2 EAP”](#) on page 233.
- 3 Open a terminal session.
- 4 To launch the installation program for your platform with Java, enter the following command:

```
java -jar IdmUserApp.jar -i console
```
- 5 Follow the same steps described for the graphical user interface under [Section 28.1.3, “Installing the User Application on a JBoss Server,”](#) on page 228, reading the prompts at the command line and entering responses at the command line, through the steps on importing or creating the master key.
- 6 Specify the language that you want to use for installation.
- 7 Accept the License Agreement.
- 8 Specify the platform for your application server.
- 9 Specify the folder where you want to place the installation files.
- 10 Specify the platform of the User Application database. For example, Oracle.
- 11 Specify the hostname or IP address of the server hosting the User Application database.
For a cluster, you must specify the same name or IP address for each member of the cluster.
- 12 Specify the number of the listener port for the database.
For a cluster, you must specify the same port for each member of the cluster.

- 13 For the Database Username and Password, specify the name of the database according to the database platform. By default, the database name is `idmuserappdb`.
- ◆ For a DB2, PostgreSQL, My SQL, or SQL Server database, specify the name.
 - ◆ For an Oracle or DB2 database, specify the Security Identifier (SID) that you created with the database instance.
 - ◆ For a cluster, you must specify the same database name or SID for each member in the cluster.

- 14 Specify the name for the database user account to use with the User Application and the password associated with the user account.

In a cluster environment, you must use the same user account and password for each member in the cluster.

- 15 Specify the JAR file for the database platform.

The database vendor provides the driver JAR file, which represents the Thin Client JAR for the database server. For example, for PostgreSQL, specify `postgresql-8.4-701.jdbc4.jar`, by default in the `novell\idm\Postgres` folder. NetIQ does not support driver JAR files from third-party vendors.

For a DB2 database, you must specify two JAR files. For more information, see [Section 26.1.1, "Providing the Database Driver JARs," on page 215](#).

- 16 (Optional) For the Database Administrator window, specify the name and password for the database administrator.

This field automatically lists the same user account and password that you specified in [Step 14](#). To use that account, do not make any changes.

- 17 Specify how you want to create the database tables:

Create Tables Now

The installation program creates the database tables as part of the installation process.

Create Tables at Application Startup

The installation program leaves instructions to create the tables when the User Application starts for the first time.

Write SQL to File

Create a schema file at installation time for the database administrator to use later to create the tables. When selecting this option, you must also specify a name for the file in the Schema Output File window.

- 18 (Conditional) If you chose **Create Tables Now** or **Write SQL to File** in [Step 17](#), specify whether the database is a new or empty database or it already exists from a previous installation.

- 19 (Optional) Verify that the User Application can connect to the specified database.

This step enables the installer to connect to the database for creating tables directly or for creating the `.sql` file.

NOTE: You can continue with installation if the database connection fails. However, after installation, you must manually create the tables and connect to the database. For more information, see ["Recreating the Database after Installation"](http://www.netiq.com/documentation/idm402/agpro/?page=/documentation/idm402/agpro/data/bncf7rj.html) (<http://www.netiq.com/documentation/idm402/agpro/?page=/documentation/idm402/agpro/data/bncf7rj.html>) in the *User Application Administration Guide*.

- 20 For Java Install, specify the path to the JRE file used to launch the installation program.

- 21 For the JBoss Configuration, specify the path to the installation files for the JBoss server.

- 22** (Conditional) If you install on a JBoss application server, for the IDM Configuration, specify the server's configuration :
- default**
- Specifies that this installation is on a single node that is not part of a cluster.
- If you select this option and decide later than you need a cluster, you must reinstall the User Application.
- all**
- Specifies that this installation is on a node within a cluster.
- 23** For **Application Context**, specify a name that represents the application server configuration, the application WAR file, and the name in the URL context.
- The installation script creates a server configuration, then names the configuration according to the name that you created when installing the application server. For example, `IDMProv`.
- IMPORTANT:** NetIQ recommends that you make a note of the specified **Application Context**. You will use this application name in the URL when you start the User Application from a browser.
- 24** (Conditional) When installing the provisioning WAR file on a node in a JBoss cluster, you must also specify the **Workflow Engine ID**. The engine ID cannot exceed 32 characters. For more information about workflow engine IDs, see the section on configuring workflows for clustering in the [User Application: Administration Guide](#).
- 25** (Optional) To send log events to an auditing server, complete the following steps in the Select Audit Logging Type window:
- 25a** Specify that you want to send log events to an auditing server.
- 25b** Specify the type(s) of logging that you want to enable:
- Novell Identity Audit or NetIQ Sentinel**
- Enables logging through a Novell or NetIQ client for the User Application.
- OpenXDAS**
- Enables the User Application to send events to your OpenXDAS logging server.
- 25c** (Conditional) If you chose in [Step 25b](#) to send log events through a Novell or NetIQ client, specify the hostname or IP address for the client server and the path to the log cache.
- For more information about setting up logging, see the [User Application Administration Guide](#).
- 26** To set the User Application configuration parameters, complete the following steps:
- 26a** Manually launch the configuration update utility from the command line: `configupdate.sh` (Linux) or `configupdate.bat` (Windows).
- 26b** Specify the values as described in [Section 30.2, "Configuring the User Application," on page 277](#).
- 27** (Optional) If you are using an external password management WAR, manually copy the WAR to the installation directory and to the remote JBoss server deploy directory that runs the external password WAR functionality.
- 28** (Conditional) If you are installing the User Application on JBoss 5.1.2 Enterprise Application Platform (EAP), continue to ["Deploying the User Application on JBoss 5.1.2 EAP" on page 233](#).
- 29** Continue with the post-installation tasks described in [Chapter 30, "Completing the Roles Based Provisioning Module / User Application Installation," on page 277](#).

29.2 Installing the User Application with a Single Command

This section describes how to perform a silent install of the User Application. A silent installation requires no interaction during the installation and can save you time, especially when you install on more than one system. You can perform silent installations supported on Linux computers. This process includes the following activities:

- ♦ [Section 29.2.1, “Setting Passwords in the Environment for a Silent Installation,” on page 263](#)
- ♦ [Section 29.2.2, “Editing the silent.properties File,” on page 264](#)
- ♦ [Section 29.2.3, “Executing a Silent Installation of the User Application,” on page 272](#)

For more information about ...	See ...
Prerequisites for installing on an application server	Section 6.7, “Prerequisites and Requirements for Installing the User Application and Roles Based Provisioning Module,” on page 69
Hardware and software requirements for installation	Section 6.7.6, “System Requirements for Installing the User Application and Roles Based Provisioning Module,” on page 75
Using the installation wizard to install the User Application	Chapter 28, “Installing the User Application on an Application Server,” on page 227
Using the console to install the User Application	Section 29.1, “Performing a Guided Installation from the Command Line,” on page 260

29.2.1 Setting Passwords in the Environment for a Silent Installation

If you do not want to specify the passwords in the `silent.properties` file for the User Application installation, you can set the passwords in the environment instead. In this case, the silent installer will read the passwords from the environment, rather than from the `silent.properties` file. This can provide some additional security.

You must specify the following passwords for the User Application installation:

- ♦ `NOVL_DB_USER_PASSWORD`
- ♦ `NOVL_CONFIG_DBADMIN_PASSWORD`
- ♦ `NOVL_CONFIG_LDAPADMINPASS`
- ♦ `NOVL_CONFIG_KEYSTOREPASSWORD`

Linux

Use the `export` command. For example:

```
export NOVL_DB_USER_PASSWORD=myPassWord
```

Windows

Use the `set` command. For example:

```
set NOVL_DB_USER_PASSWORD=myPassWord
```

29.2.2 Editing the silent.properties File

You must edit the parameter values in the `silent.properties` file before performing the silent installation. The table in this section provides a list of the installation parameters. The parameters correspond to the basic installation parameters as well as for configuring RBPM and the User Application. For more information about specifying the parameter values, see [Section 28.1.3, “Installing the User Application on a JBoss Server,” on page 228](#) and [Section 30.2, “Configuring the User Application,” on page 277](#).

- 1 Log on as a root user to the computer where you want to install the User Application.
- 2 Ensure that the `silent.properties` file is stored on the local computer.

By default, you can find the file in the `products/RBPM/user_app_install` directory within the `.iso` image file for the Identity Manager installation package for each operating system environment directory.

- 3 Open the `silent.properties` file on the local computer.
- 4 Modify the following parameters in the `silent.properties` file:

User Application Parameter Name in <code>silent.properties</code>	Equivalent Parameter Name in the User Application Configuration Parameters File
NOVL_CONFIG_LDAPHOST=	eDirectory Connection Settings: LDAP Host. Specifies the hostname or IP address for your LDAP server.
NOVL_CONFIG_LDAPADMIN=	eDirectory Connection Settings: LDAP Administrator. Specifies the credentials for the LDAP Administrator. This user must already exist. The User Application uses this account to make an administrative connection to the Identity Vault. This value is encrypted, based on the master key.
NOVL_CONFIG_LDAPADMINPASS=	eDirectory Connection Settings: LDAP Administrator Password. Specifies the LDAP Administrator password. This password is encrypted, based on the master key.
NOVL_CONFIG_ROOTCONTAINERNAME=	eDirectory DNs: Root Container DN. Specifies the LDAP distinguished name of the root container. This is used as the default entity definition search root when no search root is specified in the directory abstraction layer.
NOVL_CONFIG_PROVISIONROOT=	eDirectory DNs: Provisioning Driver DN. Specifies the distinguished name of the User Application driver. For example, if your driver is <code>UserApplicationDriver</code> and your driver set is called <code>myDriverSet</code> , and the driver set is in a context of <code>o=myCompany</code> , you type a value of: <code>cn=UserApplicationDriver,cn=myDriverSet,o=myCompany</code>

User Application Parameter Name in silent.properties	Equivalent Parameter Name in the User Application Configuration Parameters File
NOVL_CONFIG_LOCKSMITH=	<p data-bbox="870 247 1300 268">eDirectory DNs: User Application Admin.</p> <p data-bbox="870 300 1442 436">An existing user in the Identity Vault who has the rights to perform administrative tasks for the User Application user container specified. This user can use the Administration tab of the User Application to administer the portal.</p> <p data-bbox="870 468 1442 688">If the User Application Administrator participates in workflow administration tasks exposed in iManager, Novell Designer for Identity Manager, or the User Application (Requests & Approvals tab), you must grant this administrator appropriate trustee rights to object instances contained in the User Application driver. Refer to the <i>User Application: Administration Guide</i> for details.</p> <p data-bbox="870 720 1442 800">To change this assignment after you deploy the User Application, you must use the Administration > Security pages in the User Application.</p>
NOVL_CONFIG_PROVLOCKSMITH=	<p data-bbox="870 831 1382 852">eDirectory DNs: Provisioning Application Admin.</p> <p data-bbox="870 884 1442 1136">This user is available in the provisioning version of Identity Manager. The Provisioning Application Administrator uses the Provisioning tab (under the Administration tab) to manage the Provisioning Workflow functions. These functions are available to users through the Requests and Approvals tab of the User Application. This user must exist in the Identity Vault prior to being designated the Provisioning Application Administrator.</p> <p data-bbox="870 1167 1442 1247">To change this assignment after you deploy the User Application, you must use the Administration > Security pages in the User Application.</p>
NOVL_CONFIG_ROLECONTAINERDN=	<p data-bbox="870 1272 1442 1440">This role is available in RBPM. This role allows members to create, remove, or modify all roles, and grant or revoke any role assignment to any user, group, or container. It also allows its role members to run any report for any user. By default, the User Application Admin is assigned this role.</p> <p data-bbox="870 1472 1442 1551">To change this assignment after you deploy the User Application, use the Roles > Role Assignment page in the User Application.</p>
NOVL_CONFIG_COMPLIANCECONTAINERDN	<p data-bbox="870 1577 1442 1713">The Compliance Module Administrator is a system role that allows members to perform all functions on the Compliance tab. This user must exist in the Identity Vault prior to being designated as the Compliance Module Administrator.</p>

User Application Parameter Name in <code>silent.properties</code>	Equivalent Parameter Name in the User Application Configuration Parameters File
NOVL_CONFIG_USERCONTAINERDN=	<p>Meta-Directory User Identity: User Container DN.</p> <p>Specify the LDAP distinguished name (DN) or fully qualified LDAP name of the user container. This defines the search scope for users and groups. Users in this container (and below) are allowed to log on to the User Application.</p> <p>IMPORTANT: Be sure the User Application Administrator specified during User Application driver set up exists in this container if you want that user to be able to execute workflows.</p>
NOVL_CONFIG_GROUPCONTAINERDN=	<p>Meta-Directory User Groups: Group Container DN.</p> <p>Specify the LDAP distinguished name (DN) or fully qualified LDAP name of the group container. Used by entity definitions within the directory abstraction layer.</p>
NOVL_CONFIG_KEYSTOREPATH=	<p>eDirectory Certificates: Keystore Path. Required.</p> <p>Specify the full path to your keystore (<code>cacerts</code>) file of the JRE that the application server uses. The User Application installation modifies the keystore file. On Linux, the user must have permission to write to this file.</p>
NOVL_CONFIG_KEYSTOREPASSWORD=	<p>eDirectory Certificates: Keystore Password.</p> <p>Specify the <code>cacerts</code> password. The default is <code>changeit</code>.</p>
NOVL_CONFIG_SECUREADMINCONNECTION=	<p>eDirectory Connection Settings: Secure Admin Connection.</p> <p>Required. Specify True to require that all communication using the admin account be done using a secure socket (this option can have adverse performance implications). This setting allows other operations that don't require SSL to operate without SSL.</p> <p>Specify False if the admin account does not use secure socket communication.</p>
NOVL_CONFIG_SECUREUSERCONNECTION=	<p>eDirectory Connection Settings: Secure User Connection.</p> <p>Required. Specify True to require that all communication done on the logged-in user's account be done using a secure socket (this option can have severe adverse performance implications). This setting allows other operations that don't require SSL to operate without SSL.</p> <p>Specify False if the user's account does not use secure socket communication.</p>

User Application Parameter Name in <code>silent.properties</code>	Equivalent Parameter Name in the User Application Configuration Parameters File
NOVL_CONFIG_SESSIONTIMEOUT=	Miscellaneous: Session Timeout. Required. Specify an application session timeout interval.
NOVL_CONFIG_LDAPPLAINPORT=	eDirectory Connection Settings: LDAP Non-Secure Port. Required. Specify the non-secure port for your LDAP server, for example 389.
NOVL_CONFIG_LDAPSECUREPORT=	eDirectory Connection Settings: LDAP Secure Port. Required. Specify the secure port for your LDAP server, for example 636.
NOVL_CONFIG_ANONYMOUS=	eDirectory Connection Settings: Use Public Anonymous Account. Required. Specify True to allow users who are not logged in to access the LDAP Public Anonymous Account. Specify False to enable NOVL_CONFIG_GUEST instead.
NOVL_CONFIG_GUEST=	eDirectory Connection Settings: LDAP Guest. Allows users who are not logged in to access permitted portlets. You must also deselect Use Public Anonymous Account . The Guest user account must already exist in the Identity Vault. To disable the Guest user, select Use Public Anonymous Account .
NOVL_CONFIG_GUESTPASS=	eDirectory Connection Settings: LDAP Guest Password.
NOVL_CONFIG_EMAILNOTIFYHOST=	Email: Notify Template HOST token. Specify the application server hosting the Identity Manager User Application. For example: <code>myapplication serverServer</code> This value replaces the \$HOST\$ token in e-mail templates. The URL that is constructed is the link to provisioning request tasks and approval notifications.
NOVL_CONFIG_EMAILNOTIFYPORT=	Email: Notify Template Port token. Used to replace the \$PORT\$ token in e-mail templates used in provisioning request tasks and approval notifications.
NOVL_CONFIG_EMAILNOTIFYSECUREPORT=	Email: Notify Template Secure Port token. Used to replace the \$SECURE_PORT\$ token in e-mail templates used in provisioning request tasks and approval notifications.

User Application Parameter Name in <code>silent.properties</code>	Equivalent Parameter Name in the User Application Configuration Parameters File
NOVL_CONFIG_NOTFSMTPEMAILFROM=	<p>Email: Notification SMTP Email From.</p> <p>Required. Specify e-mail From a user in provisioning e-mail.</p>
NOVL_CONFIG_NOTFSMTPEMAILHOST=	<p>Email: Notification SMTP Email Host.</p> <p>Required. Specify the SMTP e-mail host that provisioning e-mail is using. This can be an IP address or a DNS name.</p>
NOVL_CONFIG_USEEXTPWDWAR=	<p>Password Management: Use External Password WAR.</p> <p>Specify True if you are using an external password management WAR. If you specify True, you must also supply values for NOVL_CONFIG_EXTPWDWARPTH and NOVL_CONFIG_EXTPWDWARRTPATH.</p> <p>Specify False to use the default internal Password Management functionality, <code>./jsps/pwdmgt/ForgotPassword.jsp</code> (without the http(s) protocol at the beginning). This redirects the user to the Forgot Password functionality built into the User Application, rather than to an external WAR.</p>
NOVL_CONFIG_EXTPWDWARPATH=	<p>Password Management: Forgot Password Link.</p> <p>Specify the URL for the Forgot Password functionality page, <code>ForgotPassword.jsp</code>, in an external or internal password management WAR. Or, accept the default internal password management WAR. For details, see Section 30.5, "Configuring External Forgot Password Management," on page 290.</p>
NOVL_CONFIG_EXTPWDWARRTPATH=	<p>Password Management: Forgot Password Return Link.</p> <p>Specify the Forgot Password Return Link so that the user can click after performing a forgot password operation.</p>
NOVL_CONFIG_FORGOTWEBSERVICEURL=	<p>Password Management: Forgot Password Web Service URL.</p> <p>This is the URL that the External Forgot Password WAR will use to call back to the User Application to perform core forgot password functionalities. The format of the URL is:</p>
NOVL_CONFIG_USEROBJECTATTRIBUTE=	<p><code>https://idmhost:sslport/idm/pwdmgt/service</code></p> <p>Meta-Directory User Identity: User Object Class.</p> <p>Required. The LDAP user object class (typically <code>inetOrgPerson</code>).</p>

User Application Parameter Name in <code>silent.properties</code>	Equivalent Parameter Name in the User Application Configuration Parameters File
NOVL_CONFIG_LOGINATTRIBUTE=	<p>Meta-Directory User Identity: Login Attribute.</p> <p>Required. The LDAP attribute (for example, CN) that represents the user's login name.</p>
NOVL_CONFIG_NAMINGATTRIBUTE=	<p>Meta-Directory User Identity: Naming Attribute.</p> <p>Required. The LDAP attribute used as the identifier when looking up users or groups. This is not the same as the login attribute, which is used only during login, and not during user/group searches.</p>
NOVL_CONFIG_USERMEMBERSHIPATTRIBUTE=	<p>Meta-Directory User Identity: User Membership Attribute. Optional.</p> <p>Required. The LDAP attribute that represents the user's group membership. Do not use spaces in this name.</p>
NOVL_CONFIG_GROUPOBJECTATTRIBUTE=	<p>Meta-Directory User Groups: Group Object Class.</p> <p>Required. The LDAP group object class (typically <code>groupofNames</code>).</p>
NOVL_CONFIG_GROUPMEMBERSHIPATTRIBUTE=	<p>Meta-Directory User Groups: Group Membership Attribute.</p> <p>Required. Specify the attribute representing the user's group membership. Do not use spaces in this name.</p>
NOVL_CONFIG_USEDYNAMICGROUPS=	<p>Meta-Directory User Groups: Use Dynamic Groups.</p> <p>Required. Specify True to use dynamic groups. Otherwise, specify False.</p>
NOVL_CONFIG_DYNAMICGROUPOBJECTCLASS=	<p>Meta-Directory User Groups: Dynamic Group Object Class.</p> <p>Required. Specify the LDAP dynamic group object class (typically <code>dynamicGroup</code>).</p>
NOVL_CONFIG_TRUSTEDSTOREPATH=	<p>Trusted Key Store: Trusted Store Path.</p> <p>The Trusted Key Store contains all trusted signers' certificates. If this path is empty, the User Application gets the path from System property <code>javax.net.ssl.trustStore</code>. If the path isn't there, it is assumed to be <code>jre/lib/security/cacerts</code>.</p>
NOVL_CONFIG_TRUSTEDSTOREPASSWORD=	<p>Trusted Key Store: Trusted Store Password.</p>

User Application Parameter Name in <code>silent.properties</code>	Equivalent Parameter Name in the User Application Configuration Parameters File
NOVL_CONFIG_ICSSLOGOUTENABLED=	<p>Access Manager and iChain Settings: Simultaneous Logout Enabled.</p> <p>Specify True to enable simultaneous logout of the User Application and either Novell Access Manager or iChain. The User Application checks for a Novell Access Manager or iChain cookie on logout and, if the cookie is present, reroutes the user to the ICS logout page.</p> <p>Specify False to disable simultaneous logout.</p>
NOVL_CONFIG_ICSSLOGOUTPAGE=	<p>Access Manager and iChain Settings: Simultaneous Logout Page.</p> <p>Specify the URL to the Novell Access Manager or iChain logout page, where the URL is a hostname that Novell Access Manager or iChain expects. If ICS logging is enabled and a user logs out of the User Application, the user is rerouted to this page.</p>
NOVL_CONFIG_EMAILNOTIFYPROTOCOL=	<p>Email: Notify Template PROTOCOL token.</p> <p>Refers to a non-secure protocol, HTTP. Used to replace the \$PROTOCOL\$ token in e-mail templates used in provisioning request tasks and approval notifications.</p>
NOVL_CONFIG_EMAILNOTIFYSECUREPROTOCOL=	<p>Email: Notify Template Secure Port token.</p>
NOVL_CONFIG_OCSPURI=	<p>Miscellaneous: OCSP URI.</p> <p>If the client installation uses the On-Line Certificate Status Protocol (OCSP), supply a Uniform Resource Identifier (URI). For example, the format is <code>http://hostport/ocspLocal</code>. The OCSP URI updates the status of trusted certificates online.</p>
NOVL_CONFIG_AUTHCONFIGPATH=	<p>Miscellaneous: Authorization Config Path.</p> <p>The fully qualified name of the authorization configuration file.</p>
NOVL_CONFIG_CREATEDIRECTORYINDEX	<p>Miscellaneous: Create eDirectory Index</p> <p>Specify true if you want the silent installer to create indexes on the manager, ismanager, and srvrprivUID attributes on the eDirectory server specified in the NOVL_CONFIG_SERVERDN. If this parameter is set to true, NOVL_CONFIG_REMOVEEDIRECTORYINDEX cannot be set to true.</p> <p>For best performance results, the index creation should be complete. The indexes should be in Online mode before you make the User Application available.</p>

User Application Parameter Name in silent.properties	Equivalent Parameter Name in the User Application Configuration Parameters File
NOVL_CONFIG_REMOVEDIRECTORYINDEX	<p>Miscellaneous: Remove eDirectory Index</p> <p>Specify true if you want the silent installer to remove indexes on the server specified in the NOVL_CONFIG_SERVERDN. If this parameter is set to true NOVL_CONFIG_CREATEEDIRECTORYINDEX cannot be true.</p>
NOVL_CONFIG_SERVERDN	<p>Miscellaneous: Server DN</p> <p>Specify the eDirectory server where indexes should be created or removed.</p>
NOVL_CREATE_DB	<p>Indicates how the database will be created. Choices are:</p> <ul style="list-style-type: none"> ◆ now - Creates the database right away. ◆ file - Writes SQL output to a file ◆ startup - Creates the database at application startup
NOVL_DATABASE_NEW	<p>Indicates whether the database is new or existing. Specify True if it's a new database. Specify False if it's an existing database.</p>
NOVL_RBPM_SEC_ADMINDN	<p>Security Administrator</p> <p>This role gives members the full range of capabilities within the Security domain.</p> <p>The Security Administrator can perform all possible actions for all objects within the Security domain. The Security domain allows the Security Administrator to configure access permissions for all objects in all domains within RBPM. The Security Administrator can configure teams, and also assign domain administrators, delegated administrators, and other Security Administrators.</p>
NOVL_RBPM_RESOURCE_ADMINDN	<p>Resources Administrator</p> <p>This role gives members the full range of capabilities within the Resource domain. The Resources Administrator can perform all possible actions for all objects within the Resource domain.</p>
NOVL_RBPM_CONFIG_ADMINDN	<p>This role gives members the full range of capabilities within the Configuration domain. The RBPM Configuration Administrator can perform all possible actions on all objects within the Configuration domain. The RBPM Configuration Administrator controls access to navigation items within RBPM. In addition, the RBPM Configuration Administrator configures the delegation and proxy service, the provisioning user interface, and the workflow engine.</p>

User Application Parameter Name in <code>silent.properties</code>	Equivalent Parameter Name in the User Application Configuration Parameters File
<code>RUN_LDAPCONFIG=</code>	<p>Specifies when you want to configure LDAP settings now or later. Values are:</p> <ul style="list-style-type: none"> ◆ Now - Executes the LDAP configure right away by populating the WAR with the LDAP configuration settings provided. ◆ Later - Just installs the User Application files without configuring LDAP settings.

29.2.3 Executing a Silent Installation of the User Application

- 1 Log on as a root user to the computer where you want to install the User Application.
- 2 (Conditional) If you are installing the User Application on JBoss 5.1.2 Enterprise Application Platform (EAP), copy the `jbossx.jar` file from the `%jboss-root%/lib` directory to the `%jboss-root%/common/lib` directory. Complete the installation steps in this section, and then continue to [“Deploying the User Application on JBoss 5.1.2 EAP” on page 233](#).
- 3 Open a terminal session.
- 4 Specify the values for the installation. For more information, see [Section 29.2.2, “Editing the `silent.properties` File,” on page 264](#) and [Section 29.3.1, “Setting Passwords in the Environment for a Silent Installation,” on page 273](#).
- 5 To launch the installation program for your platform with Java, enter the following command:

```
java -jar IdmUserApp.jar -i silent -f /yourdirectorypath/silent.properties
```

NOTE: If the `silent.properties` file is in a different directory from the installer script, you must specify the full path to the file. The script unpacks the necessary files to a temporary directory and then launches the silent installation.

29.3 Running the JBossPostgreSQL Utility in Silent or Command Mode

This section describes how to run the JBossPostgreSQL utility in console or silent mode. A silent installation requires no interaction during the installation and can save you time, especially when you install on more than one system. This process includes the following activities:

- ◆ [Section 29.3.1, “Setting Passwords in the Environment for a Silent Installation,” on page 273](#)
- ◆ [Section 29.3.2, “Editing the `silent.properties` File,” on page 273](#)
- ◆ [Section 29.3.3, “Performing a Silent or Command Installation for the JBossPostgreSQL Utility,” on page 274](#)

29.3.1 Setting Passwords in the Environment for a Silent Installation

If you do not want to specify the passwords in the `silent.properties` file for the JBossPostgreSQL installation, you can set the passwords in the environment instead. In this case, the silent installer will read the passwords from the environment, rather than from the `silent.properties` file. This can provide some additional security.

You must specify the following passwords for the User Application installation:

- ◆ `NOVL_DB_PASSWORD`
- ◆ `NOVL_DB_USER_PASSWORD`

Linux

Use the `export` command. For example:

```
export NOVL_DB_USER_PASSWORD=myPassWord
```

Windows

Use the `set` command. For example:

```
set NOVL_DB_USER_PASSWORD=myPassWord
```

29.3.2 Editing the `silent.properties` File

You can run the JBossPostgreSQL utility in console or silent mode. Before running the utility in silent mode, you need to edit the properties file for the JBossPostgreSQL utility.

NOTE: PostgreSQL requires several Microsoft VC++ libraries when running on Windows. If these libraries are not installed on the Windows server, the PostgreSQL installer automatically installs them. When you run the JBossPostgreSQL installer in silent mode on Windows, a pop-up window appears for about three seconds while these libraries are being installed if those libraries are not already installed on the machine.

- 1 Log on as a root user to the computer where you want to run the JBossPostgreSQL silent installation.
- 2 Open the `silent.properties` file on the local computer.
- 3 Modify the following parameters in the `silent.properties` file:

Property	Description
<code>USER_INSTALL_DIR</code>	Path to where you want JBoss and the JRE installed. Required if installing JBoss; otherwise, leave blank.
<code>NOVL_DB_NAME</code>	Name of the database to use. The default database name is <code>idmuserapdb</code> . Required if installing PostgreSQL. If you are not installing PostgreSQL, this value will be ignored.

Property	Description
NOVL_DB_PASSWORD	Database root password. Required if installing PostgreSQL. If you are not installing PostgreSQL, this value will be ignored.
NOVL_DB_PASSWORD_CONFIRM	Confirms the database root password. Required if installing PostgreSQL. If you are not installing PostgreSQL, this value will be ignored.
CHOSEN_INSTALL_FEATURE_LIST	Install sets to install. Required. You can choose both JBoss and PostgreSQL, or install just one of these products. Examples: <pre>CHOSEN_INSTALL_FEATURE_LIST=JBoss, PostgreSQL</pre> <pre>CHOSEN_INSTALL_FEATURE_LIST=JBoss, ""</pre>
USER_MAGIC_FOLDER_1	Name of the installation directory for PostgreSQL. Required if installing PostgreSQL. This property will be ignored if CHOSEN_INSTALL_FEATURE_LIST does not include PostgreSQL.
START_DB	Indicates whether the installer will start the database at installation time. Assign the value Start if you want the installer to start the database; otherwise, leave this property blank. Optional.

29.3.3 Performing a Silent or Command Installation for the JBossPostgreSQL Utility

- 1 Log on as a root user to the computer where you want to install the User Application.
- 2 Open a terminal session.
- 3 Specify the values for the installation. For more information, see [Section 29.3.1, “Setting Passwords in the Environment for a Silent Installation,”](#) on page 273 and [Section 29.3.2, “Editing the silent.properties File,”](#) on page 273.
- 4 Launch the installation with the following command:

```
JBossPostgreSQL -i silent -f path_to_properties_file
```

For example:

```
JBossPostgreSQL -i silent -f /home/jdoe/idm-install-files/silent.properties
```

29.4 Running the RIS Installation Program in Silent or Command Mode

This release ships with an installation program that you can use to configure the Resource Information Services (RIS) facility, which is a standalone component that interacts with the Identity Manager User Application. The RIS facility configures the `RIS.war` file, which supports REST resources. The REST resources exposed through RIS make SOAP calls to gather information from various RBPM systems. By default, you can find the `RIS.war` file in the `products/RBPM/RIS` directory within the `.iso` image file for the Identity Manager installation package for each operating system environment directory.

You can run the RIS installation in console or silent mode. Before running the installer, you must edit the properties file for the RIS installation program.

29.4.1 Editing the `silent.properties` File

You can run the RIS installer in console or silent mode. Before running the installer, specify the following parameters in the `silent.properties` file for the RIS installer:

Property	Description
<code>NOVL_INSTALL_HOST</code>	Name of the host computer where <code>RIS.war</code> will be executed. Do not specify <code>localhost</code> . Required.
<code>NOVL_USERAPP_PORT</code>	Port on which the RBPM User Application is configured to run. Required.
<code>NOVL_CONTEXT_NAME</code>	Context name for the User Application. Required.
<code>RIS_INSTALL_DIRECTORY</code>	Directory that contains the <code>RIS.war</code> file. Required.
<code>RIS_WAR_FILE</code>	Name of the <code>RIS.war</code> file. Do not change this value.
<code>RIS_INSTALL_LOG</code>	Name of the log file for the installation program. You can name the file whatever you like. The installer writes the file to the location specified in the <code>RIS_INSTALL_DIR</code> property. If you leave this property blank, the default log file is <code>RIS-Install.log</code> . Optional.

29.4.2 Performing a Silent or Command Installation for the RIS Facility

Launch the RIS installation program with the following command:

```
RisUpdateWar -i silent -f path_to_properties_file
```

For example:

```
RisUpdateWar -i silent -f /home/jdoe/idm-install-files/silent.properties
```

30 Completing the Roles Based Provisioning Module / User Application Installation

This section provides instructions for activities that you might want to perform after installing RBPM and the User Application:

- ♦ [Recording the Master Key](#)
- ♦ [Configuring the User Application](#)
- ♦ [Configuring Identity Vault for the User Application](#)
- ♦ [Reconfiguring the User Application WAR File](#)
- ♦ [Configuring External Forgot Password Management](#)
- ♦ [Updating Forgot Password Settings](#)
- ♦ [Defining the Java Heap Size for the Role and Resource Service Driver](#)

30.1 Recording the Master Key

NetIQ recommends that you copy the encrypted master key and record it in a safe place immediately after installation. If this installation is on the first member of a cluster, use this encrypted master key when installing the User Application on other members of the cluster.

If you installed the User Application from the console, the installation program did not automatically create the `master-key.txt` file. Instead, you must manually copy the master key from the `/opt/novell/idm/jboss/server/IDMProv/conf/sys-configuration-xmldata.xml` file.

- 1 Open the `master-key.txt` file in the installation directory.
- 2 Copy the encrypted master key to a safe place that is accessible in event of system failure.

WARNING: Always keep a copy of the encrypted master key. You need the encrypted master key to regain access to encrypted data if the master key is lost. For example, you might need the key after an equipment failure.

30.2 Configuring the User Application

The installation wizard for the User Application gives you the option to modify the settings for RBPM during the installation process or wait until after the installation finishes. If you choose to modify the settings during installation, the wizard displays the Roles Based Provisioning Module Configuration window.

To configure the settings for installation...	See ...
On a JBoss application server	Step 34 on page 233

To configure the settings for installation...	See ...
On a WebLogic application server	Step 29 on page 243
On a WebSphere application server	Step 31 on page 252
From a console (command line)	Step 26 on page 262
As a single command (silent installation)	Section 29.2.2, “Editing the silent.properties File,” on page 264

Otherwise, you can edit most of the settings by running the `configupdate.sh` script or the Windows `configupdate.bat` file located by default in the installation subdirectory. In a cluster, the configuration settings in the configuration update file must be identical for all members of the cluster.

This section provides information for specifying each configuration setting. It also indicates whether or when you can modify the values in the `configupdate.sh` script and `configupdate.bat` file.

30.2.1 Identity Vault Settings

This section defines the values that the User Application users when communicating with the Identity Vault. Some settings are required for completing the installation process.

By default, the window displays the basic options. To see all settings, you must click **Show Advanced Options**.

Identity Vault Server

Required

Specifies the hostname or IP address for your LDAP server. For example: `myLDAPhost`.

LDAP Port

Specifies the non-secure port for your LDAP server. For example: `389`.

Secure LDAP Port

Specifies the secure port for your LDAP server. For example: `636`.

Identity Vault Administrator

Required

Specifies the credentials for the LDAP Administrator. For example, `cn=admin`. This user must already exist in the Identity Vault.

The User Application uses this account to make an administrative connection to the Identity Vault. This value is encrypted, based on the master key.

Identity Vault Administrator Password

Required

Specifies the password associated the LDAP Administrator. This password is encrypted, based on the master key.

Use Public Anonymous Account

Specifies whether users who are not logged in can access the LDAP Public Anonymous Account.

If you select this setting, you cannot enable LDAP guest access.

LDAP Guest

Specifies the guest account for users who are not logged in to access permitted portlets. This user account must already exist in the Identity Vault.

To use this setting, you cannot select **Use Public Anonymous Account**.

LDAP Guest Password

Specifies the password for the LDAP Guest account.

Secure Administrator Connection

Specifies whether RBPM uses SSL protocol for all communication related to the admin account. This setting allows other operations that do not require SSL to operate without SSL.

NOTE: This option might have adverse performance implications.

Secure User Connection

Specifies whether RPBM uses SSL protocol for all communication related to the logged-in user's account. This setting allows other operations that do not require SSL to operate without SSL.

NOTE: This option might have adverse performance implications.

30.2.2 Identity Vault DNs

This section defines the distinguished names for containers and user accounts that enable communication between the User Application and other Identity Manager components. Some settings are required for completing the installation process.

By default, the window displays the basic options. To see all settings, you must click **Show Advanced Options**.

Root Container DN

Required

Specifies the LDAP distinguished name of the root container. This is used as the default entity definition search root when no search root is specified in the directory abstraction layer. For example, `o=mycompany`.

User Application Driver

Required

Specifies the distinguished name of the User Application driver.

For example, if your driver is `UserApplicationDriver` and your driver set is called `myDriverSet`, and the driver set is in a context of `o=myCompany`, specify `cn=UserApplicationDriver,cn=myDriverSet,o=myCompany`.

User Application Administrator

Required

Specifies an existing user account in the Identity Vault that has the rights to perform administrative tasks for the specified user container for User Application. The following considerations apply to this setting:

- ◆ If you have started the application server hosting the User Application, you cannot change this setting with the `configupdate.sh` or `configupdate.bat` files.

- ◆ To change this assignment after you deploy the User Application, you must use the **Administration > Security** pages in the User Application.
- ◆ This user account has the right to use the **Administration** tab of the User Application to administer the portal.
- ◆ If the User Application Administrator participates in workflow administration tasks exposed in iManager, Designer for Identity Manager, or the User Application (**Requests & Approvals** tab), you must grant this administrator appropriate trustee rights to object instances contained in the User Application driver. For more information, see the *User Application Administration Guide* for details.

Provisioning Administrator

Specifies an existing user account in the Identity Vault that will manage Provisioning Workflow functions available throughout the User Application.

To change this assignment after you deploy the User Application, you must use the **Administration > Administrator Assignments** page in the User Application.

Compliance Administrator

Specifies an existing account in the Identity Vault that performs a system role to allow members to perform all functions on the **Compliance** tab. The following considerations apply to this setting:

- ◆ To change this assignment after you deploy the User Application, use the **Administration > Administrator Assignments** page in the User Application.
- ◆ During a configupdate, changes to this value take effect only if you do not have a valid Compliance Administrator assigned. If a valid Compliance Administrator exists, then your changes are not saved.

Roles Administrator

Specifies the role that allows members to create, remove, or modify all roles, and grant or revoke any role assignment to any user, group, or container. It also allows its role members to run any report for any user. The following considerations apply to this setting:

- ◆ By default, the User Application Admin is assigned this role.
- ◆ To change this assignment after you deploy the User Application, use the **Administration > Administrator Assignments** page in the User Application.
- ◆ During a configupdate, changes to this value take effect only if you do not have a valid Roles Administrator assigned. If a valid Roles Administrator exists, then your changes are not saved.

Security Administrator

Specifies the role that gives members the full range of capabilities within the Security domain. The following considerations apply to this setting:

- ◆ The Security Administrator can perform all possible actions for all objects within the Security domain. The Security domain allows the Security Administrator to configure access permissions for all objects in all domains within RBPM. The Security Administrator can configure teams, and also assign domain administrators, delegated administrators, and other Security Administrators.
- ◆ To change this assignment after you deploy the User Application, use the **Administration > Administrator Assignments** page in the User Application.

Resources Administrator

Specifies the role that gives members the full range of capabilities within the Resource domain. The following considerations apply to this setting:

- ◆ The Resources Administrator can perform all possible actions for all objects within the Resource domain.
- ◆ To change this assignment after you deploy the User Application, use the [Administration > Administrator Assignments](#) page in the User Application.

RBPM Configuration Administrator

Specifies the role that gives members the full range of capabilities within the Configuration domain. The following considerations apply to this setting:

- ◆ The RBPM Configuration Administrator can perform all possible actions on all objects within the Configuration domain. The RBPM Configuration Administrator controls access to navigation items within RBPM. In addition, the RBPM Configuration Administrator configures the delegation and proxy service, the provisioning user interface, and the workflow engine.
- ◆ To change this assignment after you deploy the User Application, use the [Administration > Administrator Assignments](#) page in the User Application.

RBPM Reporting Administrator

Specifies the Reporting Administrator. By default, the installation program lists this value as the same user as the other security fields.

Reinitialize RBPM Security

Specifies whether you want to reset security.

IDMReport URL

Specifies the URL for the user interface of the Identity Reporting Module.

30.2.3 Identity Vault User Identity

This section defines the values that enable the User Application to communicate with a user container in the Identity Vault. Some settings are required for completing the installation process.

The installation program does not display these settings by default. You must click [Show Advanced Options](#).

User Container DN

Required

Specifies the LDAP distinguished name (DN) or fully qualified LDAP name of the user container. The following considerations apply to this setting:

- ◆ Users in this container (and below) are allowed to log on to the User Application.
- ◆ If you have started the application server hosting the User Application, you cannot change this setting with the `configupdate.sh` or `configupdate.bat` files.
- ◆ This container must include the User Application Administrator that you specified as you set up the User Application driver. Otherwise, the specified account cannot execute workflows.

User Container Scope

Specifies the depth of scope that Identity Vault users can search the container.

User Object Class

Specifies the object class of the LDAP user. Usually the class is `inetOrgPerson`.

Login Attribute

Specifies the LDAP attribute that represents the user's login name. For example, `cn`.

Naming Attribute

Specifies the LDAP attribute used as the identifier when looking up users or groups. This is not the same as the login attribute, which is used only during login. For example, `cn`.

User Membership Attribute

(Optional) Specifies the LDAP attribute that represents the user's group membership. Do not use spaces when specifying the name.

30.2.4 Identity Vault User Groups

This section defines the values that enable the User Application to communicate with a group container in the Identity Vault. Some settings are required for completing the installation process.

The installation program does not display these settings by default. You must click **Show Advanced Options**.

Group Container DN

Required

Specifies the LDAP distinguished name (DN) or fully qualified LDAP name of the group container. The following considerations apply to this setting:

- ◆ Entity definitions within the directory abstraction layer use this DN.
- ◆ If you have started the application server hosting the User Application, you cannot change this setting with the `configupdate.sh` or `configupdate.bat` files.

Group Container Scope

Specifies the depth of scope that Identity Vault users can search for the group container.

Group Object Class

Specifies the object class of the LDAP group. Usually the class is `groupofNames`.

Group Membership Attribute

(Optional) Specifies the user's group membership. Do not use spaces in this name.

Use Dynamic Groups

Specifies whether you want to use dynamic groups.

Dynamic Group Object Class

Specifies the object class of the LDAP dynamic group. Usually the class is `dynamicGroup`.

30.2.5 Identity Vault Certificates

This section defines the path and password for the JRE keystore. Some settings are required for completing the installation process.

The installation program does not display these settings by default. You must click **Show Advanced Options**.

Keystore Path

Required

Specifies the full path to your keystore (`cacerts`) file of the JRE that the application server uses to run. You can manually enter the path or browse to the `cacerts` file. The following considerations apply to this setting:

- ◆ In environments, you must specify the installation directory of RBPM. The default value is set to the correct location.
- ◆ The User Application installation program modifies the keystore file. On Linux, the user must have permission to write to this file.

Keystore Password

Required

Specifies the password for the keystore file. The default is `changeit`.

Confirm Keystore Password

Specifies the password for the keystore file to verify that you entered the correct value.

30.2.6 Email Server Configuration

This section defines the values that enable email notifications. The installation program does not display these settings by default. You must click **Show Advanced Options**.

Notification Template Host

Specifies the name or IP address of the application server that hosts the User Application. For example, `myapplication serverServer`.

This value replaces the `$HOST$` token in e-mail templates. The installation program uses this information to create a URL to provisioning request tasks and approval notifications.

Notification Template Port

Specifies the port number of the application server that hosts the User Application.

This value replaces the `$PORT$` token in e-mail templates that are used in provisioning request tasks and approval notifications.

Notification Template Secure Port

Specifies the secure port number of the application server that hosts the User Application.

This value replaces the `$SECURE_PORT$` token in e-mail templates used in provisioning request tasks and approval notifications.

Notification Template Protocol

Specifies a non-secure protocol included in the URL when sending user email. For example, `HTTP`.

This value replaces the `$PROTOCOL$` token in e-mail templates used in provisioning request tasks and approval notifications.

Notification Template Secure Protocol

Specifies the secure protocol included in the URL when sending user email. For example, `HTTPS`. This value replaces the `$SECURE_PROTOCOL$` token in e-mail templates used in provisioning request tasks and approval notifications.

Notification SMTP Email From

Specifies the email account that the User Application uses to send email notifications.

SMTP Server Name

Specifies the IP address or DNS name of the SMTP email host that the User Application users for provisioning emails.

Email Notification Image Location

Specifies the path to the image that you want to include in email notifications. For example, `http://localhost:8080/IDMProv/images`.

30.2.7 Trusted Key Store

This section defines the values for the trusted keystore for the User Application. The installation program does not display these settings by default. You must click **Show Advanced Options**.

Trusted Store Path

Specifies the path to the Trusted Key Store that contains all trusted signers' certificates. If this path is empty, the User Application gets the path from System property `javax.net.ssl.trustStore`. If the System property cannot provide the path, the installation program defaults to `jre/lib/security/cacerts`.

Trusted Store Password

Specifies the password for the Trusted Key Store. If you leave this field is empty, the User Application gets the password from System property `javax.net.ssl.trustStorePassword`. If the System property cannot provide the path, the installation program defaults to `changeit`.

This password is encrypted, based on the master key.

Confirm Trusted Store Password

Specifies the password for the Trusted Key Store to verify that you entered the correct value

Keystore Type JKS

Specifies whether the trusted store path uses JKS for digital signing.

Keystore Type PKCS12

Specifies whether the trusted store path uses PKCS12 for digital signing.

30.2.8 Novell Audit Digital Signature Certificate & Key

This section configures your JBoss environment to take advantage of the digital signature support provided with the User Application. The User Application does not support digital signatures in WebLogic or WebSphere environments. For more information about digital signatures, see “[Digital Signature Configuration](https://www.netiq.com/documentation/idm402/agpro/data/b762gfb.html)” (<https://www.netiq.com/documentation/idm402/agpro/data/b762gfb.html>) in the *User Application Administration Guide*.

NOTE: You must use Novell Identity Audit to preserve documents that you digitally sign. Digital signature documents are not stored with workflow data in the User Application database, but are stored in the logging database. You must also enable logging to preserve these documents.

The installation program does not display these settings by default. You must click **Show Advanced Options**.

Novell Audit Digital Signature Certificate

Specifies the digital signature certificate for the audit service.

Novell Audit Digital Signature Private Key

Specifies the private key of the digital signature. This key is encrypted, based on the master key.

30.2.9 Access Manager Settings

This section defines the values that allow you to access the User Application with Novell Access Manager or iChain. The installation program does not display these settings by default. You must click **Show Advanced Options**.

Simultaneous Logout Enabled

Specifies whether the User Application supports simultaneous log out of the User Application and either Novell Access Manager or iChain. The User Application checks for a Novell Access Manager or iChain cookie on logout. When the cookie is present, the User Application reroutes the user to the ICS logout page.

Simultaneous Logout Page

Specifies the URL to the Novell Access Manager or iChain logout page, where the URL is a hostname that Novell Access Manager or iChain expects. If ICS logging is enabled and a user logs out of the User Application, the user is rerouted to this page.

30.2.10 Password Management

This feature enables you to specify a self-service Web page where users who have forgotten their password can remedy their problem. The URL to the forgotten password page resides in an external Forgot Password WAR. The WAR uses the URL to call back the User Application through a Web service. For more information about configuring the User Application for managing password self-

service and user authentication features, see “Password Management Configuration” (<https://www.netiq.com/documentation/idm402/agpro/data/b6mixux.html>) in the *User Application Administration Guide*.

The installation program does not display these settings by default. You must click **Show Advanced Options**.

Use External Password WAR

Specifies whether you want to use a self-service Web page where users who have forgotten their password can remedy their problem. The following considerations apply to this setting:

- ◆ If you do not select **Use External Password WAR**, Identity Manager uses the default internal Password Management functionality, `./jssps/pwdmgt/ForgotPassword.jsp` (without the http(s) protocol at the beginning). This redirects the user to the Forgot Password functionality built into the User Application, rather than to an external WAR.
- ◆ If you select this setting, you must also specify values for **Forgot Password Link**, **Forgot Password Return Link**, and **Forgot Password Web Service URL**.

Forgot Password Link

Specifies the URL that points to a `ForgotPassword.jsp` file in an external or internal password management WAR. For example, `http://pwdmgthost:port/pwdmgtwar/jssps/pwdmgt/ForgotPassword.jsp`.

Forgot Password Return Link

Specifies the URL that the user can click after performing a forgotten password operation.

Forgot Password Web Service URL

Specifies the URL that the External Forgot Password WAR uses to call back to the User Application to perform core forgot password functionalities. Use the following syntax:

```
https://idmhost:sslport/idm/  
pwdmgt/service
```

30.2.11 Miscellaneous

The installation program does not display these settings by default. You must click **Show Advanced Options**.

Session Timeout

Specifies the time, in minutes, allowed before the User Application times out a user session. The default value is 20.

OCSP URI

Specifies the Uniform Resource Identifier (URI) to use when the client installation uses the On-Line Certificate Status Protocol (OCSP). For example, `http://host:port/ocspLocal`.

The OCSP URI updates the status of trusted certificates online.

Authorization Config Path

Specifies the fully qualified name of the authorization configuration file.

Create Identity Vault Index

Specifies whether you want the installation program to create indexes on the manager, ismanager, and srprvUUID attributes. The following considerations apply to this setting:

- ◆ Without indexes on these attributes, User Application users can experience impeded performance of the User Application, particularly in a cluster environment.
- ◆ You can create these indexes manually by using iManager after you install the User Application. For more information, see [Section 30.3.1, “Creating Indexes in eDirectory,” on page 288](#).
- ◆ For best performance, you should create the index during installation. The indexes must be in Online mode before you make the User Application available to users.

Remove Identity Vault Index

Specifies whether to remove indexes on the manager, ismanager, and srprvUUID attributes.

Server DN

Specifies the eDirectory server where you want the indexes to be created or removed. To configure indexes on multiple eDirectory servers, you must run the configupdate utility multiple times. You can specify only one server at a time.

Reinitialize RBPM Security

Specifies whether you want to reset RBPM security when the installation process completes. You must also redeploy the User Application.

IDMReport URL

Specifies the URL of the Identity Manager Reporting Module. For example, `http://hostname:port/IDMRPT`.

Log Message Identifier Prefix

Specifies the value that you want to use in the layout pattern for the CONSOLE and FILE appenders in the `idmuserapp_logging.xml` file. The default value is RBPM.

30.2.12 Container Object

This section helps you to define the values for container objects or create new container objects. The installation program does not display these settings by default. You must click **Show Advanced Options**.

Selected

Specifies the Container Object Types that you want to use.

Container Object Type

Specifies the container: locality, country, organizationalUnit, organization, or domain.

You can also define your own containers in iManager and add them under **Add a new Container Object**.

Container Attribute Name

Specifies the name of the Attribute Type associated with the specified Container Object Type.

Add a New Container Object: Container Object Type

Specifies the LDAP name of an object class from the Identity Vault that can serve as a new container.

Add a New Container Object: Container Attribute Name

Specifies the name of the Attribute Type associated with the new Container Object Type.

30.3 Configuring Identity Vault for the User Application

The User Application must be able to interact with the objects in your Identity Vault. In some cases, you might need to configure the authentication methods and indexes in eDirectory to enable the Identity Vault and User Application to communicate effectively.

30.3.1 Creating Indexes in eDirectory

To improve User Application performance, the eDirectory Administrator should create indexes for the manager, ismanager and srvprvUUID attributes. Without indexes on these attributes, User Application users can experience impeded performance, particularly in a clustered environment.

You can create these indexes automatically during installation by selecting **Create eDirectory Indexes** on the **Advanced** tab of the User Application Configuration Panel. For more information about using Index Manager to create indexes, see the *Novell eDirectory Administration Guide* (<https://www.netiq.com/documentation/edir88/>).

30.3.2 Installing and Configuring SAML Authentication Method

This configuration is only required if you want to use the SAML authentication method and are not also using Access Manager. If you are using Access Manager, your eDirectory tree will already include the method. The procedure includes the following activities:

- ♦ “Installing the SAML method in your eDirectory tree” on page 288
- ♦ “Editing eDirectory Attributes” on page 288

Installing the SAML method in your eDirectory tree

- 1 Locate and then unzip the `nmassaml.zip` file.
- 2 To install the SAML method in your eDirectory tree, complete the following steps:

2a Extend the schema stored in the `authsaml.sch`

For example, on Linux, enter the following command:

```
ndssch -h edir_ip edir_admin authsaml.sch
```

2b Install the SAML method.

For example, on Linux, enter the following command:

```
nmasinst -addmethod edir_admin tree ./config.txt
```

Editing eDirectory Attributes

- 1 Open iManager.
- 2 Expand **Roles and Tasks > Directory Administration > Create Object**.
- 3 Select **Show all object classes**.
- 4 Create a new object of class `authsamlAffiliate`.

- 5 Select `authsamlAffiliate`, then click **OK**.
You can give this object any valid name.
- 6 To specify the Context, select the **SAML Assertion.Authorized Login Methods.Security** container object in the tree, then click **OK**.
- 7 To add attributes to the class object `authsamlAffiliate`, complete the following steps:
 - 7a Click the iManager **View Objects > Browse** tab.
 - 7b Locate your new affiliate object in the SAML Assertion.Authorized Login Methods.Security container.
 - 7c Select the new affiliate object, then select **Modify Object**.
 - 7d Add an `authsamlProviderID` attribute to the new affiliate object.
This attribute is used to match an assertion with its affiliate. The contents of this attribute must be an exact match with the Issuer attribute sent by the SAML assertion.
 - 7e Click **OK**.
 - 7f Add `authsamlValidBefore` and `authsamlValidAfter` attributes to the affiliate object.
These attributes define the amount of time, in seconds, around the `IssueInstant` in an assertion when the assertion is considered valid. A typical default is 180 seconds.
 - 7g Click **OK**.
- 8 Select the Security container.
- 9 Select **Create Object** to create a **Trusted Root Container** in your Security Container.
- 10 To create a **Trusted Root** objects in the Trusted Root Container, complete the following steps:
 - 10a Go to **Roles and Tasks > Directory Administration**, then select **Create Object**.
 - 10b Select **Show all object classes**.
 - 10c To create a **Trusted Root** object for the certificate that your affiliate will use to sign assertions. You must have a der encoded copy of the certificate to do this.
 - 10d Create new trusted root objects for each certificate in the signing certificate's chain up to the root CA certificate.
 - 10e Set the Context to the Trusted Root Container created earlier, then click **OK**.
- 11 Return to the Object Viewer.
- 12 Add an `authsamlTrustedCertDN` attribute to your affiliate object, then click **OK**.
This attribute should point to the "Trusted Root Object" for the signing certificate that you created in the previous step. (All assertions for the affiliate must be signed by certificates pointed to by this attribute, or they will be rejected.)
- 13 Add an `authsamlCertContainerDN` attribute to your affiliate object, then click **OK**.
This attribute should point to the "Trusted Root Container" that you created before. (This attribute is used to verify the certificate chain of the signing certificate.)

30.4 Reconfiguring the User Application WAR File

To update your User Application WAR file, run the `configupdate` utility.

- 1 Run the `ConfigUpdate` utility in the User Application install directory by executing `configupdate.sh` or `configupdate.bat`.

For more information about `ConfigUpdate` utility parameters, see [Section 30.2, "Configuring the User Application,"](#) on page 277.

- 2 Deploy the new WAR file to your application server, with the following considerations:
 - ♦ For WebLogic and WebSphere, redeploy the WAR file to the application server.
 - ♦ For JBoss single server, the changes are applied to the deployed WAR.
 - ♦ For a JBoss cluster, update the WAR file on each JBoss server in the cluster.

30.5 Configuring External Forgot Password Management

Use the **Forgot Password Link** configuration parameter to specify the location of a WAR file containing Forgot Password functionality. You can specify a WAR file that is external or internal to the User Application. This process includes the following activities:

- ♦ [Section 30.5.1, “Specifying an External Forgot Password Management WAR File,” on page 290](#)
- ♦ [Section 30.5.2, “Specifying an Internal Password WAR File,” on page 291](#)
- ♦ [Section 30.5.3, “Testing the External Forgot Password WAR Configuration,” on page 291](#)
- ♦ [Section 30.5.4, “Configuring SSL Communication between JBoss Servers,” on page 291](#)

30.5.1 Specifying an External Forgot Password Management WAR File

- 1 Use either the install procedure or the configupdate utility.
- 2 In the User Application configuration parameters, select the **Use External Password WAR** configuration parameter check box.
- 3 For the **Forgot Password Link** configuration parameter, specify the location for the external password WAR.
Include the host and port, for example `http://localhost:8180/ExternalPwd/jsp/pwdmgt/ForgotPassword.jsp`. An external password WAR can be outside the firewall protecting the User Application.
- 4 For the **Forgot Password Return Link**, specify the link shown after the user finishes performing the forgot password procedure. When the user clicks this link, the user is redirected to the link specified.
- 5 For the **Forgot Password Web Service URL**, supply the URL for the Web Service that the external forward password WAR uses to call back to the User Application. The format for the URL must be as follows:

```
https://idmhost:sslport/idm/pwdmgt/service
```

The return link must use SSL to ensure secure Web Service communication to the User Application. For more information, see [Section 30.5.4, “Configuring SSL Communication between JBoss Servers,” on page 291](#).

- 6 Manually copy `ExternalPwd.war` to the remote JBoss server deploy directory that runs the external password WAR functionality.

30.5.2 Specifying an Internal Password WAR File

- 1 In the User Application configuration parameters, do not select **Use External Password WAR**.
- 2 Accept the default location for the **Forgot Password Link**, or supply a URL for another password WAR.
- 3 Accept the default value for **Forgot Password Return Link**.

30.5.3 Testing the External Forgot Password WAR Configuration

If you have an external password WAR file and want to test the Forgot Password functionality by accessing it, you can access it in the following locations:

- ♦ Directly, in a browser. Go to the Forgot Password page in the external password WAR file. For example, `http://localhost:8180/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsp`.
- ♦ At the User Application login page, click the **Forgot Password** link.

30.5.4 Configuring SSL Communication between JBoss Servers

If you select **Use External Password WAR** in the User Application configuration file during installation, you must configure SSL communication between the JBoss servers on which you are deploying the User Application WAR and the External Forgot Password Management WAR file. Refer to your JBoss documentation for directions.

30.6 Updating Forgot Password Settings

You can change the values of **Forgot Password Link**, **Forgot Password Return Link**, and **Forgot Password Web Service URL** after installation. Use either the `configupdate` utility or the User Application.

Using the `configupdate` utility. At a command line, change directories to the install directory and enter `configupdate.sh` (Linux) or `configupdate.bat` (Windows). If you are creating or editing an external password management WAR, you must then manually rename that WAR before you copy it to the remote JBoss server.

Using the User Application. Log on as the User Application Administrator and go to **Administration > Application Configuration > Password Module Setup > Login**. Modify these fields:

- ♦ **Forgot Password Link** (for example: `http://localhost:8180/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsp`)
- ♦ **Forgot Password Return Link** (for example: `http://localhost/IDMProv`)
- ♦ **Forgot Password Web Service URL** (for example: `https://idmhost:sslport/idm/pwdmgt/service`)

30.7 Defining the Java Heap Size for the Role and Resource Service Driver

In an enterprise environment, the Role and Resource Service driver will require more maximum Java heap than the default amount defined in Identity Manager. A maximum Java heap size of 256mb is suggested in order to avoid OutOfMemoryError conditions.

The Java heap size can be specified via iManager under the Misc section of the Driver Set properties or by setting the DHOST_JVM_INITIAL_HEAP and DHOST_JVM_MAX_HEAP environment variables. See the [Identity Manager Common Driver Administration Guide \(http://www.netiq.com/documentation/idm402/idm_common_driver/index.html?page=/documentation/idm402/idm_common_driver/data/front.html\)](http://www.netiq.com/documentation/idm402/idm_common_driver/index.html?page=/documentation/idm402/idm_common_driver/data/front.html) for more information on configuring Java VM options.

VIII Installing the Identity Information Warehouse

This section guides you through the process of installing the required components for the Identity Information Warehouse (the Warehouse). The installation process includes all components required for the application:

- ◆ NetIQ Identity Reporting Module (Reporting Module)
- ◆ NetIQ Event Auditing System (EAS)
- ◆ Identity Manager Managed System Gateway Driver (MSGW)
- ◆ Identity Manager Driver for Data Collection Service (DCS)

NOTE: This section provides instructions for installing EAS, which sends audit information to the Warehouse. As an alternative for the EAS component, you can use a product such as NetIQ Sentinel.

The installation files are located in the `products/EAS` and `products/Reporting` directories within the `.iso` image file for the Identity Manager installation package. By default, the installation program installs the components in the following locations:

- ◆ **Linux:** `/opt/novell/idm`
- ◆ **Windows:** `C:\Program Files\IdentityReporting`

NetIQ recommends that you review the installation process before beginning. For more information, see [Chapter 31, “Preparing to Install the Information Warehouse,”](#) on page 295.

31 Preparing to Install the Information Warehouse

This section provides guidance for preparing to install the Identity Information Warehouse.

31.1 Checklist for Installing the Identity Information Warehouse

NetIQ recommends that you complete the steps in the following checklist.

	Checklist Items
<input type="checkbox"/>	1. Learn about the interaction among Identity Manager components. For more information, see Section 3.3.4, "Identity Information Warehouse," on page 29.
<input type="checkbox"/>	2. Review the considerations for installing the Identity Information Warehouse. For more information, see Section 6.8, "Prerequisites for Installing the Identity Information Warehouse," on page 77.
<input type="checkbox"/>	3. Review the hardware and software requirements for the computers that will host the Identity Information Warehouse. For more information, see Section 6.8.3, "System Requirements for the Reporting Module," on page 78 and Section 6.8.4, "System Requirements for the Event Auditing Service," on page 80.
<input type="checkbox"/>	4. Ensure that you have installed RBPM. For more information, see Chapter 22, "Main Checklist for Installing RBPM and the User Application," on page 201.
<input type="checkbox"/>	5. Install EAS: <ul style="list-style-type: none">◆ For a guided installation, see Section 32.2, "Using the Wizard to Install Event Auditing Service," on page 298.◆ For a silent installation, see Section 32.3, "Installing Event Auditing Service Silently," on page 299. <p>NOTE: You can install an alternative event auditing service, such as NetIQ Sentinel. However, this guide does not provide instructions for that type of installation.</p>
<input type="checkbox"/>	6. Install the Reporting Module: <ul style="list-style-type: none">◆ For a guided installation, see Section 33.1, "Using the Wizard to Install the Reporting Module," on page 301.◆ To install EAS silently, see Section 33.2, "Installing the Reporting Module Silently," on page 304.
<input type="checkbox"/>	7. To complete the Reporting Module set up, see Section 33.3, "Configuring the Reporting Module," on page 305.
<input type="checkbox"/>	8. (Conditional) To configure the Reporting Module in a WebLogic or WebSphere environment, see Section 33.4, "Configuring the Reporting Module for WebLogic and WebSphere," on page 307.

	Checklist Items
<input type="checkbox"/>	9. Configure the Managed System Gateway and Data Collection Service drivers. For more information, see Section 34.1, "Configuring Drivers for the Reporting Module," on page 311.
<input type="checkbox"/>	10. Deploy and start the drivers. For more information, see Section 34.2, "Deploying and Starting Drivers for the Reporting Module," on page 315.
<input type="checkbox"/>	11. Back up the driver schema in the database. For more information, see Section 34.3, "Backing up the Schema for the Drivers," on page 320.
<input type="checkbox"/>	12. Configure the environment for the drivers. For more information, see Section 34.4, "Configuring the Runtime Environment," on page 321.
<input type="checkbox"/>	13. Configure Identity Manager and eDirectory to send data to the drivers. For more information, see Section 34.5, "Setting Auditing Flags for the Drivers," on page 328.

31.2 Understanding the Users Created during the Installation Process

When you install EAS, the installation process creates a *novell* group and a *novell* user account. The *novell* user account does not have a password until you log on as the user. For example, you might log on to EAS to install patches. When you log on, you can create a password for this user.

The installation processes for an event auditing service and the Reporting Module create the following database users:

User name	Description
dbauser	Administrator of the PostgreSQL server and owner of the EAS schema and views.
admin	User identity for use with EAS administrative utilities.
idmrptsrv and idmrptuser	Owner of the Identity Reporting schema and views, as well as credentials used for Identity Reporting database connectivity.
rptuser and appuser	Available when you use NetIQ Sentinel as the event auditing service.

32 Installing the Event Auditing System

The installation program for EAS performs the following functions:

- ♦ Installs and optionally configures the service
- ♦ Configures the user account that can perform administration tasks for the service
- ♦ Configures the DBA used by the service to interact with the database
- ♦ Allows you to define the port on which the PostgreSQL database runs

NOTE

- ♦ NetIQ recommends that you synchronize the time on the computer where you install EAS with the computers hosting components that interact with the service, such as the Reporting Module and other Identity Manager components. Otherwise, you might experience configuration problems.
 - ♦ You can install an alternative event auditing service, such as NetIQ Sentinel. However, this guide provide instructions only for installing NetIQ Event Auditing Service.
-

32.1 Preparing the Environment for Event Auditing Service

You must prepare your Linux environment before installing EAS. For example, you must update the kernel SHMMAX parameter to enable PostgreSQL and enable your firewall if you want to forward the syslog file.

- 1 To ensure that the Linux system properly returns the hostname, complete the following steps:
 - 1a In a text editor, open the `/etc/hosts` file.
 - 1b In the line containing the IP address, such as 127.0.0.1, enter `hostname -f`.
- 2 To enable the PostgreSQL database to run on the server, complete the following steps:
 - 2a In a text editor, open the `/etc/sysctl.conf` file.
 - 2b Change the minimum value for the kernel SHMMAX parameter to enable the database.
For example, on a RHEL 6.x system, enter the following text at the end of the file:

```
# for Sentinel Postgresql
kernel.shmmax=1073741824
```

NOTE: Your system might require more memory that this minimum value. For more information, see “Managing Kernel Resources” in the PostgreSQL documentation (<http://www.postgresql.org/docs/8.2/static/kernel-resources.html>).

- 2c To set the parameter, execute the following commands:

```
cd /proc/sys/kernel
echo new_val_to_set > shmmax
```

- 3 To forward the syslog file for auditing, complete one of the following steps:
 - ◆ When installing EAS, enable the option to configure the firewall for syslog port forwarding.
 - ◆ Execute the following command:

```
iptables -t nat -A PREROUTING -p udp --destination-port 514 -j REDIRECT -  
toports 1514
```

32.2 Using the Wizard to Install Event Auditing Service

The following procedure describes how to install EAS using an installation wizard, either in GUI format or from the console. To perform a silent, unattended installation, see [Section 32.3, “Installing Event Auditing Service Silently,” on page 299](#).

To prepare for the installation, review the prerequisites and system requirements listed in [Section 6.8.4, “System Requirements for the Event Auditing Service,” on page 80](#). Also see the Release Notes accompanying the release.

- 1 Log on to a supported computer where you want to install EAS.
- 2 (Conditional) If you have the `.iso` image file for the Identity Manager installation package, navigate to the directory containing the EAS installation files, located by default in the `products/EAS/` directory.
- 3 (Conditional) If you downloaded the EAS installation files from the [Novell Downloads Web site \(http://download.novell.com\)](http://download.novell.com), complete the following steps:
 - 3a Navigate to the `.tgz` file for the downloaded image.
 - 3b Extract the contents of the file to a folder on the local computer.
- 4 From the directory that contains the installation files, launch the installation program:

```
./EASInstall.bin
```
- 5 In the installation program, specify the language that you want to use for installation, and then click **OK**.
- 6 Accept the License Agreement, and then click **Next**.
- 7 Review the Introduction text, and then click **Next**.
- 8 In the Installation Directory window, click **Next**.
- 9 In the Utilities Administrator Password window, specify the password for the admin user of the EAS utilities, and then click **Next**.
- 10 In the EAS Administrator Password window, specify the password for the dbauser, and then click **Next**.
- 11 Specify the port on which the PostgreSQL database runs, and then click **Next**.
- 12 Read the **Pre-Installation Summary**, and then click **Install**.
- 13 (Conditional) To use the Syslog UDP connector, select **Enable Port Forwarding**, and then click **Next**.
- 14 When the installation process completes, click **Done**.

32.3 Installing Event Auditing Service Silently

A silent (non-interactive) installation does not display a user interface or ask the user any questions. Instead, the system uses information from a `.properties` file. You can run the silent installation with the default file or edit the file to customize the installation process. To perform a guided installation, see [“Using the Wizard to Install Event Auditing Service” on page 298](#).

To prepare for the installation, review the prerequisites and system requirements listed in [Section 6.8.4, “System Requirements for the Event Auditing Service,” on page 80](#). Also see the Release Notes accompanying the release.

- 1 (Conditional) To avoid specifying the administrator passwords for the EAS utilities and PostgreSQL database in the `.properties` file for a silent installation, use the `export` command:

```
export ADMIN_PWD=EAS_utilities_admin_password
export DBA_PWD=PostgreSQL_dbouser_password
```

For example:

```
export ADMIN_PWD=myPassWord
```

The silent installation process reads the passwords from the environment, rather than from the `.properties` file.

- 2 In a text editor, modify one of the following properties files, located by default in the `products/EAS` directory of the `.iso` image:
 - ♦ `eas_install.properties` to use the default installation settings
 - ♦ `eas_configure.properties` to customize the installation settings, such as specifying passwords for the EAS utilities and PostgreSQL database
- 3 Launch the installation with the following command:

```
./EASInstall.bin -i silent -f path_to_properties_file
```

For example:

```
./EASInstall.bin -i silent -f /root/Software/eas_configure.properties
```

33 Installing the Reporting Module

This section describes the process for installing the Reporting Module. The installation program performs the following functions:

- ♦ Allows you to choose an application server platform
- ♦ Deploys the client WAR file, which contains the user interface components for reporting, to the application server
- ♦ Deploys the core WAR file, which contains the core REST services needed for reporting
- ♦ Deploys the authentication services WAR file, which contains the authentication services that control authentication to the reporting module
- ♦ Defines the location of the server for the Event Auditing Service (installed separately)
- ♦ Creates the reporting schema in the Security Information and Event Management (SIEM) database
- ♦ Configures the PostgreSQL JDBC driver that connects to the SIEM database
- ♦ Configures the authentication services for the reporting module
- ♦ Configures the e-mail delivery system for the reporting module
- ♦ Configures the core reporting services for the reporting module

33.1 Using the Wizard to Install the Reporting Module

The following procedure describes how to install the Reporting Module using an installation wizard, either in GUI format or from the console. To perform a silent, unattended installation, see [Section 33.2, “Installing the Reporting Module Silently,” on page 304](#).

To prepare for the installation, review the prerequisites and system requirements listed in [Section 6.8.3, “System Requirements for the Reporting Module,” on page 78](#). Also see the Release Notes accompanying the release.

- 1 Ensure that the database for your event auditing service is running.
The installation program creates users for the database and verifies connectivity. The program also installs a JAR file for the PostgreSQL JDBC driver, and automatically uses this file for database connectivity.
- 2 Log on to the computer where you want to install the Reporting Module.
- 3 (Conditional) To use a JBoss application server to host the Reporting Module, stop JBoss.
- 4 (Conditional) If you have the `.iso` image file for the Identity Manager installation package, navigate to the directory containing the Reporting Module installation files, located by default in the `products/Reporting/` directory.
- 5 (Conditional) If you downloaded the Reporting Module installation files from the [Novell Downloads Web site \(http://download.novell.com\)](http://download.novell.com), complete the following steps:
 - 5a Navigate to the `.tgz` file for the downloaded image.
 - 5b Extract the contents of the file to a folder on the local computer.

- 6 From the directory that contains the installation files, launch the installation program:
 - ♦ **Linux:** `./IDMReport.bin`
 - ♦ **Windows:** `IDMReport.exe`
- 7 In the installation program, specify the language that you want to use for installation, and then click **OK**.
- 8 Review the Introduction text, and then click **Next**.
- 9 Accept the License Agreement, and then click **Next**.
- 10 Specify the location for the installation files, and then click **Next**.
- 11 Specify the application server that will run the core (`IDMRPT-Core.war`) and authentication (`IDMRPT-Auth.war`) files.

NOTE: Do not change the names of these WAR files. If you change the file names, the deployment process fails.

- 12 Click **Next**.
- 13 (Conditional) If you chose JBoss in [Step 11](#), specify a path to the deployment directory for your JBoss server, and then click **Next**.
- 14 For **EAS Server Host Name**, specify the name or IP address of the server that hosts the event auditing service that you want to use, and then click **Next**.
- 15 (Conditional) If you installed the event auditing service on a separate server, specify a password for the EAS server.

For example, copy the system password from the `system` property in the `activemqusers.properties` file on the computer where EAS is installed, and then paste it in the **EAS System password** field.

- 16 Click **Next**.
- 17 In the Database Values window, complete the following steps:
 - 17a Specify the port number for the database server that hosts the Security Information and Event Management (SIEM) database.
 - 17b Specify passwords for the following users:
 - ♦ `dbauser`, which is the database administrator
 - ♦ `idmrptsrv`, which is the owner of the database schemas and objects for reporting
 - ♦ `idmrptuser`, which is a user with read-only access to the reporting data
 - 17c Click **Next**.
- 18 To verify the settings that you specified for the database, select **Test Database Connection**, and then click **Next**.
- 19 In the Authentication Configuration window, complete the following steps:
 - 19a Specify the name and port number for the server that hosts the Identity Vault. For example `localhost:389`.
 - 19b For **Authenticated User Container**, specify the LDAP distinguished name (DN) of the container that lists the users that can log on to the reporting module.

NOTE: If the DN contains special characters, you might need to escape those characters. For more information, see RFC 2253/4514 Section 2.4.

- 19c For **Expiration Value for Authentication Token**, specify the number of minutes that you want to retain the token for authentication.

19d For **Target Locale**, specify a language that you want to use for the configuration.

19e Click **Next**.

19f Specify whether you want to use Secure Sockets Layer protocols for connections with your LDAP server.

NOTE: (Selecting **Secure (SSL)** can cause adverse performance. This setting allows other operations that do not require SSL to operate without SSL.

19g Click **Next**.

20 In the User Application Driver Information window, specify the settings for your User Application driver.

NOTE: If the DN for the driver set container uses special characters, you might need to escape those characters. For more information, see RFC 2253/4514 Section 2.4.

21 Click **Next**.

22 In the Email Delivery Configuration window, complete the following steps:

22a Specify the host address for the email server that you want the reporting module to use when sending notifications.

22b Specify the port number for the email server.

22c Specify whether you want to use SSL for communication with the email server. For example, select **True** to use SSL.

22d Specify whether you want to use authentication for communications with the email server. For example, select **True** to enable SSL.

If you select **True**, you must specify in [Step 23 on page 303](#) the email address and password to be used for authentication.

22e Click **Next**.

23 (Conditional) If you chose to use authentication for email communications in [Step 22d on page 303](#), complete the following steps:

23a For **SMTP User Name**, specify the email address that you want to use for authentication.

23b For **SMTP User Password**, specify the password associated with the email address that you want to use for authentication.

24 For **Default Email Address**, specify the email address that you want the reporting module to use as the origination for email notifications.

25 Click **Next**.

26 In the Report Retention Values window, complete the following steps:

26a For **Select the Reporting Unit**, specify the unit of measurement that the reporting module uses to retain completed reports before deleting them. For example, to retain reports for six months, select **Month**.

26b For **Report Lifetime**, specify the number associated with the specified **Reporting Unit**. For example, to retain reports for six months, enter **6**.

26c Specify a path where you want to store the report definitions. For example, `/opt/novell/IdentityReporting`.

26d Click **Next**.

27 (Optional) To enable subcontainer searches at login time, complete the following steps:

NOTE

- ◆ If you specify a DN that includes special characters, you might need to escape those characters. For more information, see RFC 2253/4514 Section 2.4.
- ◆ If you disable subcontainer searches, no searches are performed within the subtree of the user container. When the user logs in, the reporting module treats the simple name that the user types as a CN.

27a In the Subcontainer Search window, select **Enable Subcontainer Search**.

27b Specify the user DN and password of an LDAP administrator.

27c Specify the login attribute that you want to use for searching the subtree of the user container.

28 Click **Next**.

29 (Optional) To enable auditing to EAS, complete the following steps:

29a In the Novel Identity Audit window, select **Yes**.

29b Specify the location of the cache folder that you want to use for auditing. For example, /opt/novell/Identity Reporting.

30 Click **Next**.

31 Review the information in the Pre-Installation Summary window, and then click **Install**.

32 (Conditional) To use WebLogic or WebSphere to host the Reporting Module, continue to [Section 33.4, “Configuring the Reporting Module for WebLogic and WebSphere,” on page 307](#).

33.2 Installing the Reporting Module Silently

A silent (non-interactive) installation does not display a user interface or ask the user any questions. Instead, the system uses information from a `.properties` file. You can run the silent installation with the default file or edit the file to customize the installation process. To perform a guided installation, see [“Using the Wizard to Install the Reporting Module” on page 301](#).

To prepare for the installation, review the prerequisites and system requirements listed in [Section 6.8.3, “System Requirements for the Reporting Module,” on page 78](#). Also see the Release Notes accompanying the release.

1 (Conditional) To avoid specifying the administrator passwords for the installation in the `.properties` file for a silent installation, use the `export` or `set` command. For example:

- ◆ **Linux:** `export NOVL_ADMIN_PWD=myPassWord`
- ◆ **Windows:** `set NOVL_ADMIN_PWD=myPassWord`

The silent installation process reads the passwords from the environment, rather than from the `.properties` file.

Specify the following passwords:

NOVL_DB_RPT_USER_PASSWORD

Specifies the password for the administrator for the SIEM database.

NOVL_IDM_SRV_PWD

Specifies the password for the owner of the database schemas and objects for reporting.

NOVL_IDM_USER_PWD

Specifies the password for the `idmrptuser` that has read-only access to reporting data.

NOVL_EAS_SYSTEM_PASSWORD

Specifies the password for the EAS server.

You can copy the system password from the system property in the `activemqusers.properties` file on the computer where EAS is installed.

NOVL_ADMIN_PWD

(Conditional) To enable subcontainer searches at login time, specifies the password of an LDAP administrator.

NOVL_SMTP_PASSWORD

(Conditional) To use authentication for email communications, specifies the password for the default SMTP email user.

- 2 In a text editor, modify one of the following properties files, located by default in the `products/Reporting` directory of the `.iso` image:

- ♦ `rpt_installonly.properties` to use the default installation settings
- ♦ `rpt_configonly.properties` to customize the installation settings

For more information about settings for the installation, see [Section 33.1, “Using the Wizard to Install the Reporting Module,”](#) on page 301.

- 3 Launch the installation with the following command:

```
./IDMReport.bin -i silent -f path_to_properties_file
```

For example:

```
./IDMReport.bin -i silent -f /root/Software/silent.properties
```

33.3 Configuring the Reporting Module

After installing the Reporting Module, you can still modify many of the installation properties. To make changes, run the post-installation configuration tool:

```
./ReportConfig.bin
```

If you change any setting for the reporting module with the configuration tool, you must restart the application server for the changes to take effect. However, you do not need to restart the server after making changes in the Web user interface for the Identity Reporting Module.

33.3.1 Defining User Preferences

The preferences defined with the post-install configuration tool (`ReportConfig.bin`) apply to the user that started the tool. Suppose the “root” user installed the reporting module and configured the settings for reporting during the installation. In this case, the configuration applies to the system preferences, which define the default settings for the application. When another user, such as John Smith, later launches the reporting module, the module runtime uses the system preferences by default. However, John can run the post-installation configuration tool to modify the configuration. In this case, the new configuration does not overwrite the system preferences, but instead saves these preferences separately for John. This behavior applies to all users. In addition, the REST API can be used to configure user preferences for reporting module users. Whenever a particular user launches the reporting module, the application uses the preferences for the logged in user.

For example, the “root” user decides to uninstall the reporting module. This user runs the uninstallation program, which removes the binaries as well as the system preferences and user preferences for the “root” user. However it does not remove the user preferences for any other users.

Later, if the “root” user installs the reporting module again, and John tries to launch the reporting module, John will still be using the user preferences configured for her during the previous installation. Therefore, in some situations, you might to suggest that the individual users of the reporting module clean up their user preferences before an uninstall and reinstall of the product.

33.3.2 Setting System Properties

If you installed the reporting module using 32-bit Java on a 64-bit Windows operating system, you must export and import the configuration settings (stored in Java Preferences) between the 32-bit and 64-bit Java environments. The reporting module provides the `PreferencesUtil.jar` utility to help you do this.

To set the System Properties on a 64-bit Windows operating system:

- 1 Export the system-level configuration into a file by executing the following command:

```
path_to_32bit_java/java -jar PreferencesUtil.jar export_system  
path_to_dump_file
```

For example:

```
c:\Program Files (x86)\Java\jdk1.6.0_31\bin\java.exe" -jar  
PreferencesUtil.jar export_system c:\reporting32bitprops.xml
```

- 2 Import the configuration from the file to the 64-bit Java environment by executing the following command:

```
path_to_64bit_java/java -jar PreferencesUtil.jar import path_to_dump_file
```

For example:

```
c:\Program Files\Java\jdk1.6.0_31\bin\java.exe" -jar PreferencesUtil.jar  
import c:\reporting32bitprops.xml
```

After importing the configuration, you should see the configuration properties under:

```
HKEY_LOCAL_MACHINE  
SOFTWARE  
  JavaSoft  
    Prefs
```

At this point, you should be able to start the reporting module using 64-bit Java and use all components of the application.

33.4 Configuring the Reporting Module for WebLogic and WebSphere

This section helps you configure your WebLogic and WebSphere application servers to work with the Reporting Module.

33.4.1 Preparing WebSphere and WebLogic Environments

The installation program for the reporting module creates the users `idmrptsrv` and `idmrptuser` in the PostgreSQL database. You need these users to test the data sources required by the reporting module. Also, the data sources need to exist before you deploy the application. For more information, see [Section 31.2, “Understanding the Users Created during the Installation Process,” on page 296](#).

To ensure that your environment is set up correctly, you must perform the followings steps in the listed order. Use the following table to identify the appropriate data sources to bind to the PostgreSQL users.

PostgreSQL user	WebLogic data source	WebSphere data source
<code>idmrptsrv</code>	<code>jdbc/IDMRPTDataSource</code>	<code>IDMRPTDataSource</code>
<code>idmrptuser</code>	<code>jdbc/IDMRPTCfgDataSource</code>	<code>IDMRPTCfgDataSource</code>

- 1 Install the Reporting Module as directed in one of the following sections:
 - ♦ [Section 33.1, “Using the Wizard to Install the Reporting Module,” on page 301](#)
 - ♦ [Section 33.2, “Installing the Reporting Module Silently,” on page 304](#)

This step creates the `idmrptsrv` and `idmrptuser` users in the PostgreSQL database, as well as writes the WARs to `/opt/novell/IdentityReporting`.

- 2 Create the two data sources for PostgreSQL that connect to the SIEM database and are bound to the following PostgreSQL users.
- 3 Deploy the Reporting Module using the deployment tools for your application server.

33.4.2 Configuring the WebLogic Environment

This section describes the following activities for configuring the WebLogic application server for the reporting module:

- ♦ [“Ensuring that the Reporting Module Finds Your Identity Vaults” on page 307](#)
- ♦ [“Adding JAR Files to the PRE_CLASSPATH” on page 308](#)

Ensuring that the Reporting Module Finds Your Identity Vaults

On WebLogic, the reporting module does not find your Identity Vaults unless you disable the `enforce-valid-basic-auth-credentials` flag.

- 1 In a text editor, open the `config.xml` file, located by default in the `WebLogicHome\user_projects\domains\idm\config` directory.
- 2 Add the following line to the end of the `<security-configuration>` section:

```
<enforce-valid-basic-auth-credentials>>false</enforce-valid-basic-auth-credentials>
</security-configuration>
```

- 3 Save the file and restart the server.

Adding JAR Files to the PRE_CLASSPATH

If you have installed RBPM and the reporting module on separate servers, add the `antlr-2.7.6.jar` to the `EXT_PRE_CLASSPATH` environment variable for the reporting module configuration on WebLogic.

33.4.3 Configuring the WebSphere Environment

This section describes the following activities for configuring the WebSphere application server for the reporting module:

- ♦ [“Configuring the Spring Framework” on page 308](#)
- ♦ [“Running as a Windows Service” on page 308](#)

Configuring the Spring Framework

WebSphere 7 has the Spring framework 2.5.5 in its system classpath. However, the EAS REST API war contains and uses the Spring framework 3.0.1. Therefore, you need to remove the Spring framework 2.5.5 jars from the WebSphere system classpath.

The WebSphere server should be dedicated to Identity Manager applications. Other applications deployed on the same server that rely on WebSphere's bundled Spring framework do not work.

Remove the following files from the classpath, located by default in `websphere/AppServer/lib`:

```
spring-beans-2.5.5.jar
spring-core-2.5.5.jar
```

NOTE: On Windows, the path to the files should use backslashes instead of forward slashes.

Running as a Windows Service

When you deploy the Reporting Module to a Web container that runs as a Windows Service, you need to set the **Log on as** property of that service so that it can read or write the same configuration data that is set by the installation and configuration tools.

If you do not make this change, you might see problems when WebSphere 7.0 is installed as a Windows service. In this case, the **Log on as** property is set by default to “local system,” which does not map to any user defined in the users and groups for the system. The reporting module uses Java Preferences to store application configuration data, which are associated with the OS user who executes the process (in other words, the application server).

Set the **Log on as** property to the user account that you expect the application server to run as. For example, to run as “administrator,” set **Log on as** to administrator. The post-installation configuration tool must run as the same user. For more information, see [Section 33.3.1, “Defining User Preferences,” on page 305](#).

33.4.4 Configuring WebLogic and WebSphere for SSL Connections

If you are using SSL connections, you need to persist the eDirectory certificate:

- ♦ **WebLogic:** Enter `keytool -importcert -trustcacerts -file MyCACert.der -keystore cacerts`.
- ♦ **WebSphere:** Use the console utility to upload the CA to the Trusted Store.

34 Managing the Drivers for Reporting

The Reporting Module requires the following drivers:

- ◆ Identity Manager Managed System Gateway Driver
- ◆ Identity Manager Driver for Data Collection Service

You can use the package management tools provided with Designer to install and configure the drivers.

34.1 Configuring Drivers for the Reporting Module

This section helps you install and configure the Managed System Gateway and Data Collection Service drivers for the Reporting Module.

NOTE: This section assumes that you have already installed and configured the User Application and Roles and Resources drivers for RBPM. For more information, see [Chapter 25, “Creating the Drivers for the Roles Based Provisioning Module,”](#) on page 213.

34.1.1 Installing the Driver Packages for the Reporting Module

Before you attempt to configure the drivers, you must have all of the necessary packages for the drivers in the Package Catalog. When you create a new Identity Manager project in Designer, the user interface automatically prompts you to import several packages into the new project. You do not need to import the packages during installation but you must install them at some point for the Reporting Module to function appropriately.

- 1 Open your project in Designer.
- 2 Select **Package Catalog > Import Package**.
- 3 In the Select Package dialog box, click **Select All**, and then click **OK**.

Designer adds several new package folders under the **Package Catalog**. These package folders correspond to the objects in the palette on the right side of the Modeler view in Designer.

- 4 Click **Save**.

34.1.2 Configuring the Managed System Gateway Driver

- 1 Open your project in Designer.
- 2 In the palette of the **Modeler** view, select **Service > Managed System Gateway**.
- 3 Drag the icon for **Managed System Gateway** onto the **Modeler** view.
- 4 In the Driver Configuration Wizard, select **Managed System Gateway Base**, and then click **Next**.

NOTE: For the 4.0.2 release, you need to have version 2.0.0.20120509205929 of the Managed System Gateway Base package.

- 5 In the Select Mandatory Features window, select the mandatory features, and then click **Next**.

- 6 (Conditional) If the application prompts you for an additional package called **Advanced Java Class**, select the package and then click **OK**.
- 7 (Optional) Specify the name that you want to use for the driver.
- 8 Click **Next**.
- 9 For Connection Parameters, specify the values that the reporting module uses to request data from the driver.

When you specify more than one IP address, you continue to use the same port number to listen on all the interfaces. For example, if you specify `164.99.88.30,127.0.0.1` for the address and `9000` for the port, then the driver uses the following settings:

```
164.99.88.30:9000
127.0.0.1:9000
```

- 10 (Optional) To enable end-point tracing, select **true** and then specify a location for the trace file.
- 11 Click **Next**.
- 12 (Optional) To connect the driver to a remote loader, complete the following steps:
 - 12a In the Remote Loader window, select **yes**.
 - 12b Specify the settings for the remote loader that you want to use.
- 13 Click **Next**.
- 14 Review the information in the Confirm Installation Tasks window, and then click **Finish**.
- 15 (Optional) To configure additional settings for the driver, complete the following steps in the Modeler view:
 - 15a Right-click the line connecting the Managed System Gateway Driver to the driver set, and then click **Properties**.
 - 15b In the Properties dialog box, select **Driver Configuration > Startup Option**.
 - 15c Select **Manual** for the startup option, and then click **Apply**.
 - 15d Select the **Driver Parameters** tab.
 - 15e (Optional) In the **Driver Options** tab, modify the settings for the driver, connections, and end-point tracing.

You might need to select **show** under **Connection Parameters** and **Driver Parameters** to display the settings.
 - 15f (Optional) To have the driver send periodic status messages on the Publisher channel, click the **Publisher Options** tab, and then specify a value in minutes for **Publisher heartbeat interval**.

If no traffic occurs on the Publisher channel within the specified interval, the driver sends a new heartbeat.
 - 15g Click **Apply**.
- 16 (Optional) To specify global configuration values for the server, complete the following steps:
 - 16a In the navigation pane, select **GCVs**.
 - 16b Specify global configuration values, such as the following:

Query Managed Systems across driversets

Defines the scope of operation for the Managed System Gateway Driver. If set to **true**, the driver returns information about managed systems across driversets. Otherwise, the scope is restricted to the local driverset.

Add end-point request data to queries

Specifies whether end-point request data be added to the queries sent by the driver. This will be added as an `operation-data` node.

End-point request data node name

Specifies a node-name that will be added to the `operation-data` of the queries. The node attributes will contain the details about the request.

16c Click **Apply**.

17 (Optional) To review the packages that have been installed, click **Packages** in the navigation pane.

You do not need to change the **Operation** settings unless you want to uninstall a particular package.

18 Click **OK**.

19 Enable the Subscriber channel for the Reporting Module to function correctly.

34.1.3 Configuring the Driver for Data Collection Service

1 Open your project in Designer.

2 In the palette of the **Modeler** view, select **Service > Data Collection Service**.

3 Drag the icon for **Data Collection Service** onto the **Modeler** view.

4 In the Driver Configuration Wizard, select **Data Collection Service Base**, and then click **Next**.

NOTE: For the 4.0.2 release, you need to have version 2.0.0.20120509205929 of the Data Collection Service Base package.

5 In the Select Mandatory Features window, select the mandatory features, and then click **Next**.

6 Select the optional features that you want to apply, and then click **Next**.

7 (Conditional) If the application prompts you for an additional package called **LDAP Library**, complete the following steps:

7a Select the package, and then click **OK**.

7b (Optional) To configure a global connection profile for all drivers, on the Install LDAP Library page, select **Yes**.

8 Click **Next**.

9 (Optional) Specify the name that you want to use for the driver.

10 Click **Next**.

11 For Connection Parameters, specify the values that the reporting module uses to request data from the driver.

For example, specify the user and password of the Reporting Administrator for authentication.

When you specify more than one IP address, you continue to use the same port number to listen on all the interfaces. For example, if you specify `164.99.88.30,127.0.0.1` for the address and `9000` for the port, then the driver uses the following settings:

```
164.99.88.30:9000
127.0.0.1:9000
```

12 Click **Next**.

13 For **Identity Vault Registration**, specify the settings for the Identity Vault.

- 14 (Optional) To register the Managed System Gateway driver, complete the following steps:
 - 14a For **Managed System Gateway Registration**, click **yes**.
 - 14b Specify the DN for the driver, as well as the user and password for the LDAP administrator.

NOTE: Because the driver has not yet been deployed, the browse function does not show the Managed System Gateway driver you just configured, so you might need to type the DN for the driver.

- 15 Click **Next**.
- 16 (Optional) To connect the driver to a remote loader, complete the following steps:
 - 16a In the Remote Loader window, select **yes**.
 - 16b Specify the settings for the remote loader that you want to use.
- 17 Click **Next**.
- 18 For **Scoping Configuration**, specify the role for the Data Service Collection driver.
- 19 Review the information in the Confirm Installation Tasks window, and then click **Finish**.
- 20 (Optional) To configure additional settings for the driver, complete the following steps in the Modeler view:
 - 20a Right-click the line connecting the Data Collection Service driver to the driver set, and then click **Properties**.
 - 20b In the Properties dialog box, select **Driver Configuration > Startup Option**.
 - 20c Select **Manual** for the startup option, and then click **Apply**.
 - 20d Select the **Driver Parameters** tab.
 - 20e (Optional) In the **Driver Options** tab, modify the settings for the driver, connections, and registration.

In a test environment, you might want to use low numbers to be sure your events are processed correctly. However, in a production environment, you probably want to use higher numbers so that the system does not process events unnecessarily.

IP Address

Specifies the IP address of the server that hosts the reporting module.

Port

Specifies the port number that the reporting module uses for REST connections.

Protocol

Specifies the protocol for accessing the reporting module. If you select HTTPS, you must also indicate whether you want to trust the server's certificate.

Name

Specifies the name that you want to use to refer to your Identity Vault within the reporting module.

Description

Specifies a short description of the Identity Vault.

Address

Specifies the IP address of the Identity Vault.

164.99.130.127

NOTE: You must specify an IP address. Do not specify an address of "localhost" for the Identity Vault Registration.

Register Managed System Gateway

Specifies whether you want to register the Managed System Gateway Driver.

Managed System Gateway Driver DN (LDAP)

Specifies the DN of the Managed System Gateway Driver in slash format.

Managed System Gateway Driver Configuration Mode

Specifies whether the driver is configured locally or is remote.

User DN (LDAP)

Specifies the LDAP DN of the user that the driver should use to authenticate to the Managed System Gateway Driver. This DN must exist in the Identity Vault.

Password

Specifies the password for the user.

Time interval between submitting events

The maximum amount of time, in minutes, that an event can remain in the persistence layer before being submitted to the DCS (and to the database for the reporting module).

- 20f Click **Apply**.
- 21 To configure DN's, complete the following steps:
 - 21a In the navigation menu, select **Engine Control Values**.
 - 21b For the **Qualified form for DN-syntax attribute values** setting, select **True**.
 - 21c Click **Apply**.
- 22 (Optional) To specify global configuration values for the server, complete the following steps:
 - 22a In the navigation pane, select **GCVs**.
 - 22b For **Show override options**, select **Show**.
 - 22c Modify the settings to override the global configuration values.
 - 22d Click **Apply**.
- 23 Click **OK**.

34.2 Deploying and Starting Drivers for the Reporting Module

The Reporting Module requires the following drivers:

- ♦ Identity Manager Managed System Gateway Driver
- ♦ Identity Manager Driver for Data Collection Service

For more information about installing and configuring these drivers, see [Section 34.1, "Configuring Drivers for the Reporting Module,"](#) on page 311.

34.2.1 Deploying the Drivers

You must deploy the two drivers for the Reporting Module.

- 1 Open your project in Designer.
- 2 In the **Modeler** or **Outline** view, right-click the driver set that you want to deploy.

- 3 Select **Live > Deploy**.
- 4 Specify the Identity Vault credentials for the selected driver.

34.2.2 Verifying that the Managed Systems are Working

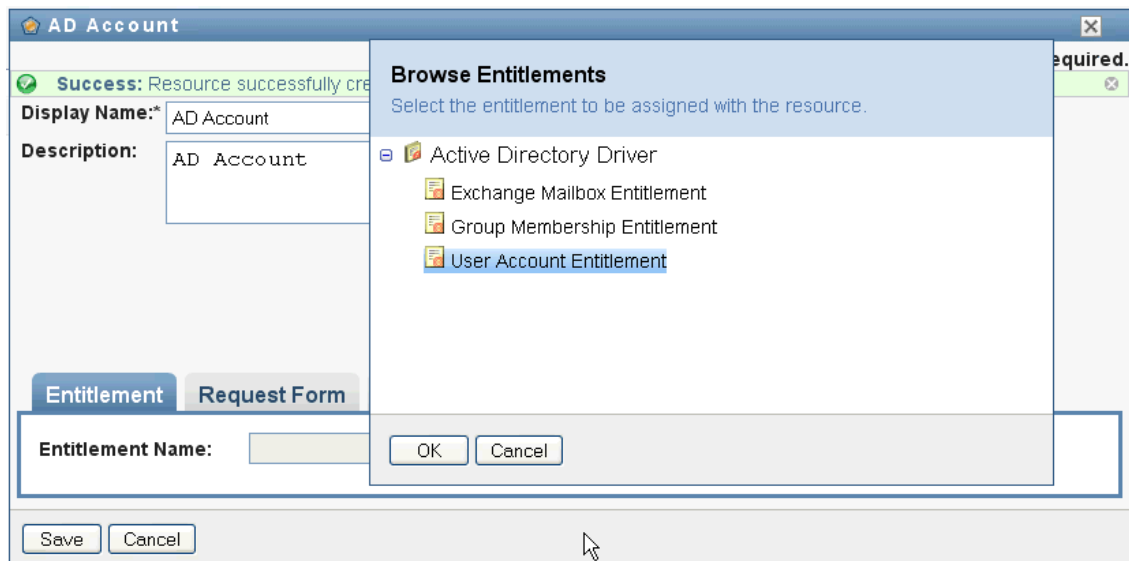
Before you start the Managed System Gateway Driver and the Data Collection Service Driver, you should confirm that the underlying managed systems are properly configured. This process helps you isolate problems with your environment that do not relate to the configuration of the reporting drivers.

To troubleshoot your Active Directory environment, for example, you might want to test an Active Directory entitlement by assigning a resource in the User Application.

NOTE: For more information about the Active Directory driver, see the [Driver for Active Directory Implementation Guide](http://www.netiq.com/documentation/idm40drivers/index.html) (<http://www.netiq.com/documentation/idm40drivers/index.html>).

The following steps demonstrate one way to confirm that Active Directory is properly configured:

- 1 Ensure that the User Application and the Reporting Module are both running on the same server.
- 2 In iManager, verify that the User Application Driver and the Role and Resource Service Driver are running, then ensure that the driver for the managed system is running.
- 3 To verify that the User Application can retrieve information from Active Directory, log on to the User Application as a User Application Administrator.
- 4 In the Resource Catalog, create a new resource for Active Directory accounts:
- 5 Bind the resource to an entitlement within the Active Directory Driver, such as **User Account Entitlement**.



The User Application can retrieve the entitlement from the driver.

- 6 Because this particular resource pertains to accounts, configure the resource to assign an account value.

Entitlement Request Form Approval Assignments Request Status

Entitlement Name: User Account Entitlement

Entitlement Description: The User Account entitlement grants or denies an account in Active Directory for the user. When granted, the user is given an enabled logon account. When revoked, the logon account is either disabled or deleted depending on how the drive is configured.

Entitlement Value Information

The **User Account Entitlement** entitlement provides a list of defined values for selection. A user can only be assigned one value.

Assign entitlement value(s) now.
 Allow user to assign entitlement value(s) at resource request time:

Static Value

Selected Value(s)*

- 7 Select the account value, and then click **Add**.
- 8 Create another resource that assigns groups.

New Resource

* - indicates required.

Display Name: AD Group

Description: AD Group

Categories: Default, System Resources

Owners: User

Save Cancel

- 9 Bind the resource to an entitlement that is suitable for groups. For this particular resource, map to the **Group Membership Entitlement**.

- Configure this resource so that the user assigns the entitlement value at request time, and allow the user to select multiple values for a single assignment request.

Entitlement Name: Group Membership Entitlement

Entitlement Description: The Group Entitlement grants or denies membership in a group in Active Directory. The group must be associated with a group in the Identity Vault. When revoked, the user is removed from the group. The group membership entitlement is not enforced on the publisher channel: If a user is added to a controlled group in Active Directory by some external tool, the user is not removed by the driver. Further, if the entitlement is removed from the user object instead of being simply revoked, the driver takes no action.

Entitlement Value Information

The **Group Membership Entitlement** entitlement provides a list of defined values for selection. A user can be assigned more than one value.

Assign entitlement value(s) now.

Allow user to assign entitlement value(s) at resource request time:

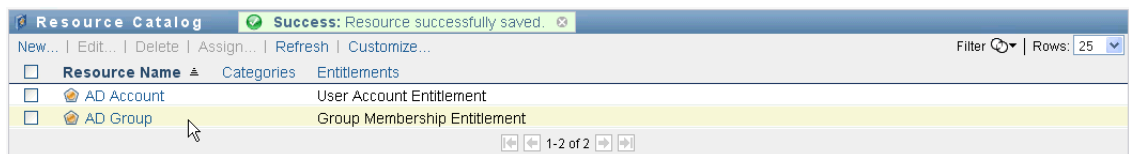
Dynamic Value

Label for value field:* Select Group(s)

Display values from Entitlement List:* Group

Allow user to request multiple assignments by selecting more than one value.

- Verify that the entitlements were created successfully.



At this point, you can see that the underlying architecture for the managed system (in this case, Active Directory) is functioning properly. This can help you to troubleshoot any problems that might arise later on.

34.2.3 Starting the Drivers for the Reporting Module

This section provides instructions for starting the Managed System Gateway Driver and the Data Collection Service Driver.

- Open iManager.
- Right-click the Managed System Gateway Driver, and then click **Start driver**.
- Right-click the Data Collection Service Driver, and then click **Start driver**.
- After the drivers have started, verify that the console displays additional information in the server console. For example:

```
21:22:56,399 INFO [LogEvent] [DCS_Driver_Registration_Add] DCS Driver DN
TREE\novell\TestDrivers\Data Collection Service Driver; DCS-Report Driver
d44571a5708446bad65832481bb401d
```

- 5 Log on to the reporting module as a Reporting Administrator.
- 6 In the navigation pane on the left, click **Overview**.
- 7 Verify that the **Configuration** section reports that an Identity Vault has been configured.
- 8 In the navigation pane, click **Identity Vaults**.
- 9 Verify that the Identity Vault page provides details about the Data Collection Service Driver and the Managed System Gateway Driver. The Managed System Gateway Driver status should indicate that the driver has been initialized.

At this point, you can look at the contents of the Identity Information Warehouse to learn more about the rich data that is stored about the Identity Vault, as well as the managed systems in your enterprise.

- 10 To see the data in the Identity Information Warehouse, use a database administration tool such as PGAdmin for PostgreSQL to look at the contents of the SIEM database. When you look at the SIEM database, you should see the following schemas:

idm_rpt_cfg

Contains reporting configuration data, such as report definitions and schedules. The installation program for the Reporting Module adds this schema to the database.

idm_rpt_data

Contains information collected by the Managed System Gateway Driver and the Data Collection Service Driver. The installation program for the Reporting Module adds this schema to the database.

public

Provides information about events captured by EAS. The EAS installation program installs the SIEM database.

- 11 To view data collected by the drivers, expand **idm_rpt_data > Tables > idmrpt_idv**.
- 12 Verify that a single row was added to this table for the new Data Collection Service Driver:

Property	Value
Name	idmrpt_idv
OID	24407
Owner	idmrptsrv
Tablespace	sendata1
ACL	
Primary key	idv_id
Rows (estimated)	0
Fill factor	
Rows (counted)	1
Inherits tables	No
Inherited tables count	0
Has OIDs?	No
System table?	No
Comment	

- 13 Verify that the data for this table shows the name of the Identity Vault:

	idv_id [PK] character varying(256)	idv_guid character varying(256)	idv_name character varying(256)	data_locale character varying(256)	idv_desc character varying(256)	idv_host character varying(256)
1	Ba35b842b1a04	BFB7F089-C1C2	My Identity Vault			
*						

If you see the new row in this table, the driver registration process was successful.

34.3 Backing up the Schema for the Drivers

If necessary, you can back up the EAS PostgreSQL database the Identity Reporting Module uses to store audit data, event data, and configuration information. The database contains three separate schemas:

- ♦ **public**: Stores audit data, event source configuration information, and other administrative information.
- ♦ **idm_rpt_data**: Stores data collected by the Managed System Gateway Driver and the Data Collection Service Driver, as well as data collection configuration information.
- ♦ **idm_rpt_cfg**: Stores reporting configuration information, reports, and report scheduling information.

This process includes the following activities:

- ♦ Section 34.3.1, “Backing Up and Restoring the idm_rpt_data and idm_rpt_cfg Schemas,” on page 320
- ♦ Section 34.3.2, “Backing Up and Restoring the public Schema,” on page 320

34.3.1 Backing Up and Restoring the idm_rpt_data and idm_rpt_cfg Schemas

NetIQ recommends that you use the standard PostgreSQL backup and restore procedures to back up or restore the `idm_rpt_data` and `idm_rpt_cfg` schemas. For detailed information on backing up and restoring PostgreSQL databases, see “Backup and Restore” in the PostgreSQL documentation (<http://www.postgresql.org/docs/8.4/static/backup.html>)

34.3.2 Backing Up and Restoring the public Schema

To back up the `public` schema, use the `backup_util.sh` utility provided with Identity Manager. The utility is located in the `/opt/novell/sentinel/bin` directory on the Identity Manager server.

For detailed information on using the `backup_util.sh` script, see “Backing Up and Restoring Data” (https://www.netiq.com/documentation/sentinel70/s701_admin/data/bn1fcap.html), in the *NetIQ Sentinel Administration Guide* (https://www.netiq.com/documentation/sentinel70/s701_admin/data/bookinfo.html).

34.4 Configuring the Runtime Environment

This section provides some additional configuration steps you should take to ensure that the runtime environment is operating correctly. It also provides troubleshooting techniques, as well as some information about database tables that are of particular interest.

If you have problems with one or more of the drivers that are difficult to understand, see “Troubleshooting the Drivers” (<https://www.netiq.com/documentation/idm402/reporting/data/bs5bqb3.html>) in the *Identity Reporting Module Guide*.

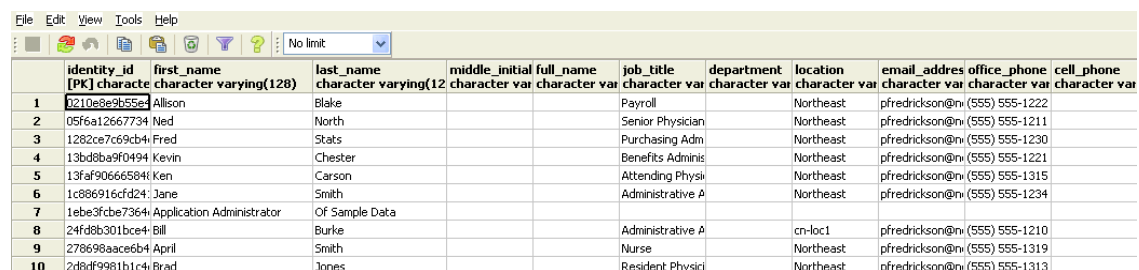
34.4.1 Migrating the Data Collection Service Driver

For the objects to synchronize into the Identity Information Warehouse, you must migrate the Data Collection Service driver.

- 1 Log on to the iManager.
- 2 In the **Overview** panel for the Data Collection Service Driver, select **Migrate From Identity Vault**.
- 3 Select the organizations that contain relevant data, and click **Start**.

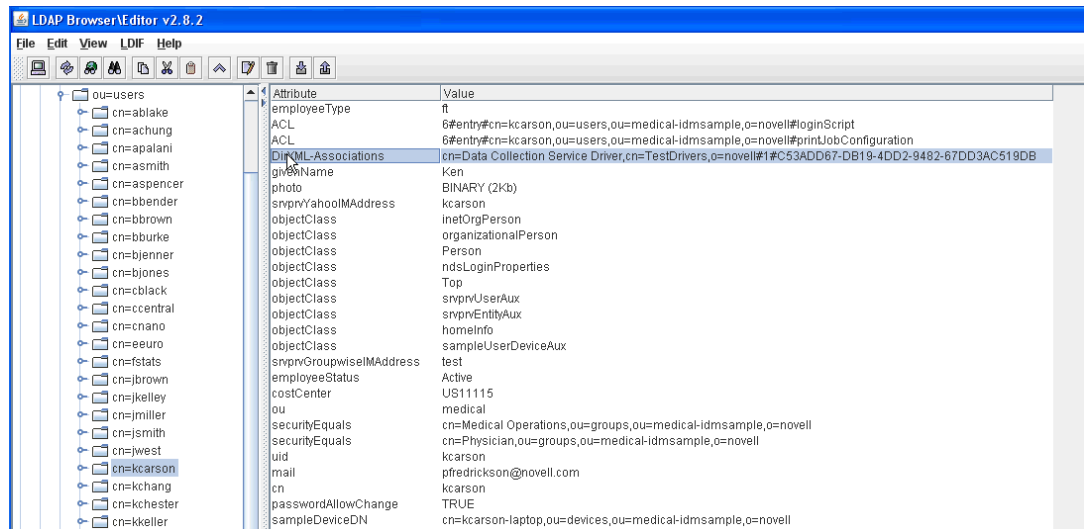
NOTE: Depending on the amount of data that you have, the migration process could take several minutes. Be sure to wait until the migration process is complete before you proceed.

- 4 Wait for the migration process to complete.
- 5 In the **idmrpt_identity** and **idmrpt_acct** tables, which provide information about the identities and accounts in the Identity Vault, ensure they contain the following type of information:

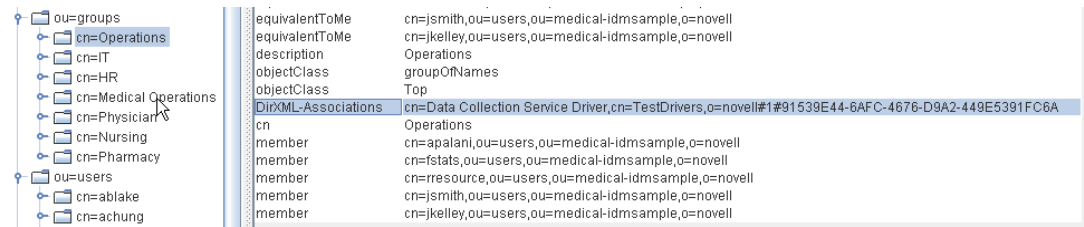


	identity_id [PK] character character varying(128)	first_name character varying(128)	last_name character varying(128)	middle_initial character varying(12)	full_name character varying(255)	job_title character varying(255)	department character varying(255)	location character varying(255)	email_address character varying(255)	office_phone character varying(255)	cell_phone character varying(255)
1	0210e8e9b55e4	Allison	Blake			Payroll		Northeast	pfredrickson@ni.(555) 555-1222		
2	05f6a12667734	Ned	North			Senior Physician		Northeast	pfredrickson@ni.(555) 555-1211		
3	1282ce7c69cb4	Fred	Stats			Purchasing Adm		Northeast	pfredrickson@ni.(555) 555-1230		
4	13bd8b9f0494	Kevin	Chester			Benefits Adminis		Northeast	pfredrickson@ni.(555) 555-1221		
5	13faf90666584	Ken	Carson			Attending Physi		Northeast	pfredrickson@ni.(555) 555-1315		
6	1c886916efd24	Jane	Smith			Administrative A		Northeast	pfredrickson@ni.(555) 555-1234		
7	1ebe3fcb7364	Application Administrator	Of Sample Data								
8	24fd8b301bce4	Bill	Burke			Administrative A		cn-loc1	pfredrickson@ni.(555) 555-1210		
9	278698aace6b4	April	Smith			Nurse		Northeast	pfredrickson@ni.(555) 555-1319		
10	2d8df9981b1c4	Brad	Jones			Resident Physi		Northeast	pfredrickson@ni.(555) 555-1313		

- 6 In the LDAP browser, verify that the migration process adds the following references for DirXML-Associations:
 - ♦ For each user, verify the following type of information:



- ◆ For each group, verify the following type of information:



7 Ensure that the data in the `idmrpt_group` table appears similar to the following information:

group_name character var	group_desc character var	dynamic_group boolean	dynamic_rule character var	nested_group boolean	idmrpt_valid_from timestamp without time zone	idmrpt_deleted boolean	idmrpt_syn_state smallint
Pharmacy	Pharmacy	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1
IT	Information Tec	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1
HR	Human Resources	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1
Physician	Physician	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1
Operations	Operations	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1
Medical Operations	Medical Operations	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1
Nursing	Nursing	FALSE		FALSE	2010-07-07 21:28:11	FALSE	1

This table shows the name for each group, as well as flags indicating whether the group is dynamic or nested. It also shows whether the group has been migrated. The synchronization status (`idmrpt_syn_state`) could possibly be set to 0 if an object had been modified in the User Application but not yet migrated. For example, if a user were added to a group, and the driver had not been migrated yet, this value might be set to 0.

8 (Optional) Verify the data in the following tables:

- ◆ `idmrpt_approver`
- ◆ `idmrpt_association`
- ◆ `idmrpt_category`
- ◆ `idmrpt_container`
- ◆ `idmrpt_idv_drivers`
- ◆ `idmrpt_idv_prd`
- ◆ `idmrpt_role`

- ◆ idmrpt_resource
 - ◆ idmrpt_sod
- 9 (Optional) Verify that the **idmrpt_ms_collect_state** table, which shows information about the data collection state for the Managed System Gateway Driver, contains now rows.

This table includes data about which REST endpoints for managed systems have been executed. At this point, the table has no rows because you have not started the collection process for this driver.

34.4.2 Adding Support for Custom Attributes and Objects

You can configure the Data Collection Service driver to gather and persist data for custom attributes and objects that are not part of the default data collection scheme. To do this, you need to modify the Data Collection Service driver filter. Modifying the filter does not trigger object synchronization immediately. Instead, the newly added attributes and objects are sent to the data collection services when add, modify, or delete events occur in the Identity Vault.

When you add support for custom attributes and objects, you need to modify the reports in order to include the extended attribute and object information. The following views provide current and historic data on the extended objects and attributes:

- ◆ idm_rpt_cfg.idmrpt_ext_idv_item_v
- ◆ idm_rpt_cfg.idmrpt_ext_item_attr_v

This process includes the following activities:

- ◆ [“Configuring the Driver to Use Extended Objects” on page 323](#)
- ◆ [“Including a Name and Description in the Database” on page 324](#)
- ◆ [“Adding Extended Attributes to Known Object Types” on page 325](#)

Configuring the Driver to Use Extended Objects

You can add any object or attribute to the Data Collection Service filter policy. When you add a new object or attribute, you need to make sure you map the GUID (with subscriber sync) and the Object Class (with subscriber notify), as shown in the following example:

```

<filter-class class-name="Device" publisher="ignore" publisher-create-
homedir="true" publisher-track-template-member="false" subscriber="sync">
<filter-attr attr-name="CN" merge-authority="default" publisher="ignore"
publisher-optimize-modify="true" subscriber="sync"/>
<filter-attr attr-name="Description" merge-authority="default" publisher="ignore"
publisher-optimize-modify="true" subscriber="sync"/>
<filter-attr attr-name="GUID" merge-authority="default" publisher="ignore"
publisher-optimize-modify="true" subscriber="sync"/>
<filter-attr attr-name="Object Class" merge-authority="default" publisher="ignore"
publisher-optimize-modify="true" subscriber="notify"/>
<filter-attr attr-name="Owner" merge-authority="default" publisher="ignore"
publisher-optimize-modify="true" subscriber="sync"/>
<filter-attr attr-name="Serial Number" merge-authority="default"
publisher="ignore" publisher-optimize-modify="true" subscriber="sync"/>
<filter-attr attr-name="sampleDeviceModel" from-all-classes="true" merge-
authority="default" publisher="ignore" publisher-optimize-modify="true"
subscriber="sync"/>
<filter-attr attr-name="sampleDeviceType" from-all-classes="true" merge-
authority="default" publisher="ignore" publisher-optimize-modify="true"
subscriber="sync"/>
</filter-class>

```

Including a Name and Description in the Database

If you want the object to have a name and description in the database, you need to add a schema mapping policy for `_dcsName` and `_dcsDescription`. The schema mapping policy maps the attribute values on the object instance to the columns `idmrpt_ext_idv_item.item_name` and `idmrpt_ext_idv_item.item_desc`, respectively. If you do not add a schema mapping policy, the attributes will be populated in the child table `idmrpt_ext_item_attr`.

For example:

```

<attr-name class-name="Device">
<nds-name>CN</nds-name>
<app-name>_dcsName</app-name>
</attr-name>
<attr-name class-name="Device">
<nds-name>Description</nds-name>
<app-name>_dcsDescription</app-name>
</attr-name>

```

The following example of SQL allows you to show these object and attribute values in the database:

```

SELECT
    item.item_dn,
    item.item_name,
    item.item_desc,
    attr.attribute_name,
    itemAttr.attribute_value,
    item.idmrpt_deleted as item_deleted,
    itemAttr.idmrpt_deleted as attr_deleted,
    item.item_desc,
    obj.object_class
FROM
    idm_rpt_data.idmrpt_ext_idv_item as item, idm_rpt_data.idmrpt_ext_item_attr
itemAttr, idm_rpt_data.idmrpt_ext_attr as attr, idm_rpt_data.idmrpt_ext_obj as obj
WHERE
    item.object_id = obj.object_id and itemAttr.attribute_id = attr.attribute_id
and itemAttr.cat_item_id = item.item_id
ORDER BY
    item.item_dn, item.item_name

```

Adding Extended Attributes to Known Object Types

If an attribute is added to the filter policy on the Data Collection Service driver and not explicitly mapped to the reporting database in the XML reference file (`IdmrptIdentity.xml`), the value is populated and maintained in the `idmrpt_ext_item_attr` table, with an attribute reference in the `idmrpt_ext_attr` table.

The following example of SQL shows these extended attributes:

```

SELECT
    acct.idv_acct_dn,
    attrDef.attribute_name,
    attribute_value,
    attrVal.idmrpt_valid_from,
    cat_item_attr_id,
    attrVal.idmrpt_deleted,
    attrVal.idmrpt_syn_state
FROM
    idm_rpt_data.idmrpt_ext_item_attr as attrVal, idm_rpt_data.idmrpt_ext_attr as
attrDef, idm_rpt_data.idmrpt_identity as idd, idm_rpt_data.idmrpt_idv_acct as acct
WHERE attrVal.attribute_id = attrDef.attribute_id and idd.identity_id =
acct.identity_id and attrVal.cat_item_id = acct.identity_id and cat_item_type_id =
'IDENTITY'

```

In addition to the User object, you can add extended attributes to the filter policy on the following objects and populate the database with these attributes:

- ◆ nrfRole
- ◆ nrfResource
- ◆ Containers

NOTE: The installed product provides support for organizationUnit, Organization, and Domain. The container types are maintained in the `idmrpt_container_types` table.

- ◆ Group
- ◆ nrfSod

You can see the association of the extended attributes to the parent table or object by looking at the `idmrpt_cat_item_types.idmrpt_table_name` column. This column describes how to join the `idm_rpt_data.idmrpt_ext_item_attr.cat_item_id` column to the primary key of the parent table.

34.4.3 Adding Support for Multiple Driver Sets

The new Data Collection Service Scoping package (NOVLDCSSCPNG) provides static and dynamic scoping capabilities for enterprise environments with multiple driversets and multiple pairs of Data Collection Service Drivers and Managed System Gateway Drivers.

During or after installation, you need to determine the role for the Data Collection Service Driver that the package is being installed on. You need to select one of the following roles:

- ♦ **Primary** The driver synchronizes everything except subtrees of other driver sets. A primary Data Collection Service Driver may well service a whole Identity Vault or it may work in conjunction with one or multiple secondary drivers.
- ♦ **Secondary** The driver synchronizes only its own driver set, but nothing else. A secondary Data Collection Service Driver usually requires a primary driver to run in a different driverset or no data outside the local driver set is sent to the Data Collection Service.
- ♦ **Custom** Allows the administrator to define custom scoping rules. The only implicit scope is the local driver set, everything else is considered out-of-scope, unless it is explicitly added to the list of custom scopes. A custom scope is the distinguished name in slash format of a container in the Identity Vault whose subordinates or subtree should be synchronized.

The scoping package is only required in some configuration scenarios, as described below:

- ♦ **Single server with a single driver set Identity Vault** For this scenario, you do not need scoping, and, therefore, you do not need to install the scoping package.
- ♦ **Multiple servers with a single driver set Identity Vault** For this scenario, you need to follow these guidelines:
 - ♦ Make sure the Identity Manager server holds replicas of all partitions from which data should be collected.
 - ♦ For this scenario, no scoping is required, so do not install the scoping package
- ♦ **Multiple servers with a multiple driver set Identity Vault** In this scenario, there are two basic configurations:
 - ♦ All servers hold a replica of all partitions from which data should be collected.
For this configuration, you need to follow these guidelines:
 - ♦ Scoping is required to avoid the same change being processed by multiple DCS drivers.
 - ♦ You need to install the scoping package on all DCS drivers.
 - ♦ You need to select one DCS driver to be the Primary driver.
 - ♦ You need to configure all other DCS drivers to be Secondary drivers.
 - ♦ All servers *do not* hold a replica of all partitions from which data should be collected.

Within this configuration, there are two possible situations:

- ♦ All partitions from which data should be collected are being held by *only one* Identity Manager server

In this case, you need to follow these guidelines:

- ♦ Scoping is required to avoid the same change being processed by multiple DCS drivers.

- ◆ You need to install the scoping package on all DCS drivers.
- ◆ You need to configure all DCS drivers to be Primary drivers.
- ◆ All partitions from which data should be collected are *not being held by only one* Identity Manager server (some partitions are held by more than one Identity Manager server).

In this case, you need to follow these guidelines:

- ◆ Scoping is required to avoid the same change being processed by multiple DCS drivers.
 - ◆ You need to install the scoping package on all DCS drivers.
 - ◆ You need to configure all DCS drivers to be Custom drivers.
- You need to define custom scoping rules for each driver and be sure not to create any overlapping scopes.

34.4.4 Configuring the Drivers to Run in Remote Mode with SSL

When running in remote mode, you can configure the Data Collection Service and Managed System Gateway drivers to use SSL. This section provides steps for configuring the drivers to run in remote mode with SSL.

To configure SSL using a Keystore for the Managed System Gateway Driver:

- 1 Create a server certificate in iManager.
 - 1a In the **Roles and Tasks** view, click **Novell Certificate Server > Create Server Certificate**.
 - 1b Browse to and select the server object where the Managed System Gateway Driver is installed.
 - 1c Specify a certificate nickname.
 - 1d Select **Standard** as the creation method, then click **Next**.
 - 1e Click **Finish**, then click **Close**.
- 2 Export the server certificate using iManager.
 - 2a In the **Roles and Tasks** view, click **Novell Certificate Access > Server Certificates**.
 - 2b Select the certificate created in [Step 1 on page 327](#) and click **Export**.
 - 2c Select your certificate name from the **Certificates** drop-down.
 - 2d Ensure that the option **Export private key** is checked.
 - 2e Enter a password and click **Next**.
 - 2f Click **Save the exported certificate**, and save the exported pfx certificate.
- 3 Import the pfx certificate exported in [Step 2 on page 327](#) into the java key-store.
 - 3a Use the keytool available with Java. You must use JDK 6 or later.
 - 3b Enter the following command at a command prompt:

```
keytool -importkeystore -srckeystore pfx certificate -srcstoretype
PKCS12 -destkeystore Keystore Name
```

For example:

```
keytool -importkeystore -srckeystore cert.pfx -srcstoretype PKCS12
-destkeystore msgw.jks
```

- 3c Enter the password when prompted to do so.

- 4 Modify the Managed System Gateway Driver configuration to use the keystore using iManager.
 - 4a From **Identity Manager Overview**, click the driverset containing the Managed System Gateway Driver.
 - 4b Click on the driver state icon and select **Edit properties > Driver configuration**.
 - 4c Set **Show Connection Parameters** to true and set the **Driver configuration mode** to remote.
 - 4d Enter the complete path of the keystore file and the password.
 - 4e Save and restart the driver.
- 5 Modify the Data Collection Service Driver configuration to use the keystore using iManager.
 - 5a From **Identity Manager Overview**, click the driverset containing the Managed System Gateway Driver.
 - 5b Click on the driver state icon and select **Edit properties > Driver configuration**.
 - 5c Under the **Managed System Gateway Registration** header, set **Managed System Gateway Driver Configuration Mode** to remote.
 - 5d Enter the complete path of the keystore, password and the alias enter in [Step 1c on page 327](#).
 - 5e Save and restart the driver.

34.5 Setting Auditing Flags for the Drivers

This section outlines the recommended auditing settings for the Managed System Gateway Driver and the Data Collection Service Driver.

34.5.1 Setting Audit Flags in Identity Manager

NetIQ recommends that you set auditing flags in Identity Manager for the drivers. These flags are for Novell Auditing (not XDAS).

To set the flags in iManager, go to **Driver Set Properties > Log Level > Log specific events**.

Category	Recommended Flags
Metadirectory Engine Events	<ul style="list-style-type: none"> ◆ Metadirectory Engine Warnings
Status Events	<ul style="list-style-type: none"> ◆ Success <p>NOTE: The Correlated Resource Assignment Events per User report requires the Success flag. If you want to be able to run this report or customized versions of it, then you need to enable the Success flag.</p> <ul style="list-style-type: none"> ◆ Error ◆ Fatal

Category	Recommended Flags
Operation Events	<ul style="list-style-type: none"> ◆ Modify ◆ Add Association ◆ Check Password ◆ Add Value ◆ Add ◆ Rename ◆ Remove Association ◆ Check Object Password ◆ Clear Attribute ◆ Remove Value ◆ Get Named Password ◆ Remove ◆ Move ◆ Change Password ◆ Add Value (on modify) ◆ Reset Attributes
Transformation Events	<ul style="list-style-type: none"> ◆ Password Reset ◆ User Agent Request ◆ Password Sync
Credential Provisioning Events	<ul style="list-style-type: none"> ◆ Set SSO Credentials ◆ Clear SSO Credentials ◆ Set SSO Passphrase

34.5.2 Setting Audit Flags in eDirectory

NetIQ recommends that you set auditing flags in eDirectory for the drivers. These flags are for Novell Auditing (not XDAS).

To set the flags in iManager, go to **eDirectory Auditing > Audit Configuration > Novell Auditing**.

Category	Recommended Flags
Global	<ul style="list-style-type: none"> ◆ Do Not Send Replicated Events
Meta	<ul style="list-style-type: none"> ◆ <i>(Select all flags)</i>

Category	Recommended Flags
Objects	<ul style="list-style-type: none"> ◆ Add Property ◆ Allow Login ◆ Change Password ◆ Change Security Equals ◆ Create ◆ Delete ◆ Delete Property ◆ Login ◆ Logout ◆ Modify RDN ◆ Move (Source) ◆ Move (Destination) ◆ Remove ◆ Rename ◆ Restore ◆ Search ◆ Verify Password
Attributes	<ul style="list-style-type: none"> ◆ <i>(Select all flags)</i>
Agent	<ul style="list-style-type: none"> ◆ DS Reloaded ◆ Local Agent Opened ◆ Local Agent Closed ◆ NLM Loaded
Miscellaneous	<ul style="list-style-type: none"> ◆ Generate CA Keys ◆ Recertified Public Key

Category	Recommended Flags
LDAP	<ul style="list-style-type: none">◆ LDAP Bind◆ LDAP Bind Response◆ LDAP Modify◆ LDAP Modify Response◆ LDAP Password Modify◆ LDAP Unbind◆ LDAP Delete◆ LDAP Delete Response◆ LDAP Modify DN◆ LDAP Modify DN Response◆ LDAP Search◆ LDAP Search Response◆ LDAP Add◆ LDAP Add Response

IX Installing a Role Administrator Component

To allow your business and security analysts to manage user roles and resources, install one of the following Web-based components:

- ◆ Identity Manager **Catalog Administrator**
- ◆ Identity Manager **Role Mapping Administrator**

NetIQ recommends Catalog Administrator, which provides more functionality. For more information, see [Section 2.3, “Role Administration,” on page 24](#).

NetIQ recommends that you review the installation process before beginning. For more information, see one of the following sections:

- ◆ [Section 35.1, “Checklist for Installing Catalog Administrator,” on page 335](#)
- ◆ [Chapter 36, “Preparing to Install Role Mapping Administrator,” on page 337](#)

35 Preparing and Installing Catalog Administrator

Catalog Administrator leverages the Identity Manager resource model and provides an up-to-date and easy-to-manage view of an organization's roles and resources. Catalog Administrator gets role and resource information from the User Application driver.

The download package for Catalog Administrator contains the following files:

- ♦ `rra.war`: Provides the user interface for Catalog Administrator
- ♦ `IDMProv.war`: Provisioning Dashboard functionality with Catalog Administrator functionality included
- ♦ `CatalogAdminTiles.zip`: Script that adds two Catalog Administrator tiles to Identity Manager Home and the Provisioning Dashboard.

35.1 Checklist for Installing Catalog Administrator

NetIQ recommends that you perform the steps in the following checklist:

	Checklist Items
<input type="checkbox"/>	1. Learn about the interaction among Identity Manager components. For more information, see Section 2.3, "Role Administration," on page 24.
<input type="checkbox"/>	2. Review the considerations for installing Catalog Administrator to ensure that the computers meet the prerequisites. For more information, see Section 6.9.1, "Prerequisites and System Requirements for Catalog Administrator," on page 80.
<input type="checkbox"/>	3. Review the hardware and software requirements for the computers that will host Catalog Administrator. For more information, see Section 6.10.2, "System Requirements for Installing Identity Manager Home," on page 84.
<input type="checkbox"/>	4. Ensure that you have installed Identity Manager Home. For more information, see Part X, "Installing Identity Manager Home and the Provisioning Dashboard," on page 381.
<input type="checkbox"/>	5. Install Catalog Administrator. For more information, see Section 35.2, "Installing Catalog Administrator," on page 336.
<input type="checkbox"/>	6. Begin using Catalog Administrator. For more information, see the NetIQ Identity Manager Catalog Administrator User Guide .

35.2 Installing Catalog Administrator

These instructions assume that you used the default context, `IDMProv`, for the User Application URL. If you used a different context, such as `IDMStartHere`, the file and directory names in these steps might match your specified context. For example, `IDMStartHere.war`.

This sections assumes that you already have Identity Manager Home with the Provisioning Dashboard installed.

1. Log on to the server where you deployed the User Application.
2. Stop JBoss.
3. At a command prompt, navigate to the `IDMProv/tmp` directory, then enter the following command:

```
rm -rf *
```

4. At a command prompt, navigate to the `IDMProv/work/jboss.web` directory, then enter the following command:

```
rm -rf *
```

5. Copy the `rra.war` and `IDMProv.war` files to the `deploy` folder. For example, `/opt/novell/idm/rbpm/jboss/server/IDMProv/deploy`.
6. At a command prompt, navigate to the `perminde` directory. For example, `/tmp/perminde`.
7. Enter the following command:

```
rm -rf *
```

8. Start the User Application Configuration utility by running `./configupdate.sh` from the command prompt.
9. In the *SSO Clients* tab, ensure that the information in the Catalog Administration section at the bottom is correct.
10. (Conditional) To specify the actual server DNS name or IP address, change all instances of `localhost`.
The specified address must be resolvable from all clients. Use `localhost` only if all access to Identity Manager Home and the Provisioning Dashboard will be local, including access through a browser.
11. (Conditional) If you configured non-default ports in your environment for use with Catalog Administrator, modify the port numbers as necessary.
12. (Conditional) If you use a database other than PostgreSQL, follow the instructions in [“Configuring Non-PostgreSQL Databases” on page 398](#).
13. Start JBoss.
14. Click **OK**.
15. To create Catalog Admin Roles and Catalog Admin Resources links on the Identity Manager Home page, run the `CatalogAdminTile/createCatalogAdminTiles.sh` script in the `CatalogAdminTiles.zip` package.

36 Preparing to Install Role Mapping Administrator

This section provides guidance for preparing to install Role Mapping Administrator.

36.1 Checklist for Installing Role Mapping Administrator

NetIQ recommends that you perform the steps in the following checklist:

	Checklist Items
<input type="checkbox"/>	1. Learn about the interaction among Identity Manager components. For more information, see Section 2.3, "Role Administration," on page 24.
<input type="checkbox"/>	2. Review the considerations for installing Role Mapping Administrator to ensure that the computers meet the prerequisites. For more information, see Section 6.9, "Prerequisites and Requirements for Installing Role Administration," on page 80.
<input type="checkbox"/>	3. Review the hardware and software requirements for the computers that will host Role Mapping Administrator. For more information, see Section 6.9.5, "System Requirements for Installing Role Mapping Administrator," on page 83.
<input type="checkbox"/>	4. Ensure that you have one or more user accounts with appropriate rights to manage Role Mapping Administrator. For more information, see Section 36.2, "Setting Permissions for Role Mapping Administrator," on page 338.
<input type="checkbox"/>	5. Ensure that you have installed the Identity Manager engine, the Identity Vault, Designer, iManager plug-ins, and RBPM.
<input type="checkbox"/>	6. (Conditional) To use a guided process to install Role Mapping Administrator, see Section 37.1, "Using the Wizard to Install Role Mapping Administrator," on page 341.
<input type="checkbox"/>	7. (Conditional) To perform a silent, unattended installation, see Section 37.2, "Installing Role Mapping Administrator Silently," on page 342.
<input type="checkbox"/>	8. (Optional) To modify any of the settings that you specified during the installation, see Section 38.7, "Changing Role Mapping Administrator Settings," on page 350.
<input type="checkbox"/>	9. To run Role Mapping Administrator, see Section 38.1, "Starting and Stopping Role Mapping Administrator," on page 345.
<input type="checkbox"/>	10. To ensure appropriate functionality, you must configure Role Mapping Administrator to connect to the Identity Vault. For more information, see Section 38.3, "Connecting Role Mapping Administrator to the Identity Vault," on page 346.
<input type="checkbox"/>	11. Use Identity Manager drivers to add authorizations to Role Mapping Administrator. For more information, see Section 38.4, "Configuring the Drivers for Role Mapping Administrator," on page 347.
<input type="checkbox"/>	12. (Optional) Use TLS/SSL protocols for communications between Role Mapping Administrator, the Identity Vault, RBPM, and users' browsers. For more information, see Section 38.6, "Enabling TLS/SSL Communications for Role Mapping Administrator," on page 348.

	Checklist Items
<input type="checkbox"/>	13. (Optional) Create a single sign-on process for individuals using Role Mapping Administrator, RBPM, and Access Manager. You might also need to install Access Manager. For more information, see Chapter 39, “Configuring Authentication to Role Mapping Administrator,” on page 353 .
<input type="checkbox"/>	14. (Optional) Create an audit log of events in Role Mapping Administrator. For more information, see Chapter 40, “Auditing Role Mapping Administrator,” on page 367 . To support the audit functionality, you also must install the Identity Information Warehouse. For more information, see Chapter 31, “Preparing to Install the Information Warehouse,” on page 295 .

36.2 Setting Permissions for Role Mapping Administrator

Users authorized in Role Mapping Administrator to manage and configure other users must be members of the Role Manager role or the Role Module Administrator role in RBPM. You can make these role assignments to specific users or you can make the assignments to a group or a container, then assign users to the group or add users to the container.

You can grant rights to the authorized user in two ways: assigning the user to specific roles in RBPM or modifying the individual rights in iManager.

36.2.1 Assigning Administrator Rights to Specific Roles

You can create an authorized user that is a member of the Role Manager role or the Role Module Administrator role in RBPM.

- 1 Log on to RBPM as an administration user.
- 2 Click **Roles > Roles Assignments**.
- 3 Select **User**, **Group**, or **Container** to make the role assignment.
- 4 Search for the user, group, or container, then select the desired object.
- 5 Click **New Assignment**.
- 6 For **Initial Request Description**, complete the following steps:
 - 6a Search for the following roles:
 - ◆ Role Manager
 - ◆ Role Administrator
 - ◆ Resource Manager
 - ◆ Resource Administrator
 - 6b Select the roles.
 - 6c Click **Select**.
- 7 (Optional) For **Select Roles: Effective Date:**, specify the date when the assignment for these roles goes into effect.
- 8 (Optional) For **Expiration Date**, specify whether the role assignment expires.
- 9 Click **Submit** to enable the role assignments.

36.2.2 Assigning Administrator Rights to Specific Users or Groups

You can assign rights to the authorized user account (as a specific user) or you can make the assignments to a group or a container, then assign the account to the group or to the container.

- 1 Log on to iManager as an administrative user for your Identity Vault.
- 2 Select **View Objects**.
- 3 Browse to and select the user, group, or container to which you want to assign rights.
- 4 Select the object.
- 5 Click **Actions > Modify Trustees**.
- 6 Add the rights to the authorized user account.

For more information about the required rights, see [Section 6.9, "Prerequisites and Requirements for Installing Role Administration,"](#) on page 80.

- 7 Click **OK** to save the changes.

37 Installing Role Mapping Administrator

This chapter guides you through the process of installing the required components for Role Mapping Administrator. The installation process includes all components required for the application:

- ♦ Role Mapping Administrator
- ♦ HSQL database
- ♦ Tomcat

The installation file is located in the `products/RMA/installs/` directory within the `.iso` image file for the Identity Manager installation package. By default, the installation program installs the components in the following locations:

- ♦ **Linux:** `/opt/novell/idm`
- ♦ **Windows:** `C:\Novell\IDM`

To prepare for the installation, review the prerequisites and system requirements provided in the following sections:

- ♦ [Section 6.9, “Prerequisites and Requirements for Installing Role Administration,”](#) on page 80
- ♦ [Section 6.9.5, “System Requirements for Installing Role Mapping Administrator,”](#) on page 83
- ♦ Release Notes accompanying the release

37.1 Using the Wizard to Install Role Mapping Administrator

The following procedure describes how to install Role Mapping Administrator on a Linux or Windows platform using an installation wizard, either in GUI format or from the console. To perform a silent, unattended installation, see [Section 37.2, “Installing Role Mapping Administrator Silently,”](#) on page 342.

To prepare for the installation, review the prerequisites and system requirements listed in [Section 36.1, “Checklist for Installing Role Mapping Administrator,”](#) on page 337.

NOTE: To reduce security risks, NetIQ recommends that you install Role Mapping Administrator as a non-root user on Linux platforms.

- 1 Log on to the computer where you want to install Role Mapping Administrator, using one of the following account types:
 - ♦ **Linux:** `non-root` user
 - ♦ **Windows:** Administrator
- 2 (Conditional) If you have the `.iso` image file for the Identity Manager installation package, navigate to the directory containing Role Mapping Administrator installation files, located by default in the `products/RMA/` directory.

- 3 Conditional) If you downloaded Role Mapping Administrator installation files from the [Novell Downloads Web site \(http://download.novell.com\)](http://download.novell.com), complete the following steps:
 - 3a Navigate to the `.tgz` or `win.zip` file for the downloaded image.
 - 3b Extract the contents of the file to a folder on the local computer.
- 4 In the command line, navigate to the `products/Analyzer/` directory, which contains the `IDMRMAP.jar` installation file.
- 5 Enter the following command:

```
java -jar IDMRMAP.jar.
```
- 6 Accept the license agreement.
- 7 (Optional) To install Role Mapping Administrator files in a non-default directory, specify the path. The default directory is `products/Analyzer/`.
- 8 (Optional) To use a non-default value to represent Role Mapping Administrator name, specify the URL. The default value is `IDMRMAP`. The URL links to Web portal for the application.
- 9 (Optional) To specify a non-default HTTP port, enter the port number. The default port is 8081.
- 10 Specify a password for the account responsible for configuring Role Mapping Administrator.
- 11 To start Role Mapping Administrator, run one of the following scripts located by default in the installation directory:
 - ♦ **Linux:** `start.sh`
 - ♦ **Windows:** `start.bat`
- 12 To ensure appropriate functionality, continue to the following sections to configure Role Mapping Administrator:
 - [Section 38.3, "Connecting Role Mapping Administrator to the Identity Vault," on page 346](#)
 - [Section 38.4, "Configuring the Drivers for Role Mapping Administrator," on page 347](#)
 - [Section 38.5, "Loading Authorizations into the Database," on page 348](#)
 - [Section 38.6, "Enabling TLS/SSL Communications for Role Mapping Administrator," on page 348](#)
 - [Section 38.3, "Connecting Role Mapping Administrator to the Identity Vault," on page 346](#)
- 13 (Optional) To modify any of the settings that you specified during the installation, see [Section 38.7, "Changing Role Mapping Administrator Settings," on page 350.](#)

37.2 Installing Role Mapping Administrator Silently

A silent (non-interactive) installation does not display a user interface or ask the user any questions. Instead, `InstallAnywhere` uses information from a default `install.properties` file. You can run the silent installation with the default file or edit the file to customize the installation process.

NOTE: If you do not specify any parameters other than `-s` for the silent installation, the program uses the default values.

- 1 Log on to the computer using one of the following account types:
 - ♦ **Linux:** `non-root` user
 - ♦ **Windows:** Administrator

2 (Conditional) If you have the `.iso` image file for the Identity Manager installation package, navigate to the directory containing Role Mapping Administrator installation files, located by default in the `products/RMA/` directory.

3 Conditional) If you downloaded Role Mapping Administrator installation files from the [Novell Downloads Web site \(http://download.novell.com\)](http://download.novell.com), complete the following steps:

3a Navigate to the `.tgz` or `win.zip` file for the downloaded image.

3b Extract the contents of the file to a folder on the local computer.

4 Run the following command from the directory containing the `IDMRMAP.jar` file:

```
java -jar IDMRMAP.jar -s
```

For example, enter the following command:

```
java -jar IDMRMAP.jar -s -p c:\NetIQ\Catalog_Administrator -p 8083 -w env:RMA_PASSWD -n IDMCATMAP -l c:\NetIQ\Catalog_Administrator
```

Use the following parameters in the command line.

-s

Specifies that you want to run a silent, unattended installation.

-h

Specifies that you want to view help messages during the installation.

-i

Specifies a path for the installation files. The default value is `\programs\RMA`.

-l log directory

Specifies a path for the installation log file, `rma-install.log`. The default path is `\programs\RMA`.

-n name

Specifies the value to represent Role Mapping Administrator name in the URL that links to Web portal for the application. The default value is `IDMRMAP`.

-p port

Specifies the HTTP port. The default port is 8081.

-w password|env:var

Specifies the password for the account responsible for configuring Role Mapping Administrator. The password can be passed in clear text or through a user-defined environment variable.

For example, specify `-w mypassword` to use clear text or `-w env:RMA_PASSWD` to use an environment variable.

5 (Optional) To use the environment variable for the specified password, run one of the following commands:

- ◆ **Linux:** `export RMA_PASSWD=novell`
- ◆ **Windows:** `set RMA_PASSWD=novell`

The installation program reads the password from the environment variable.

6 To ensure appropriate functionality, continue to the following sections to configure Role Mapping Administrator:

[Section 38.3, "Connecting Role Mapping Administrator to the Identity Vault," on page 346](#)

[Section 38.4, "Configuring the Drivers for Role Mapping Administrator," on page 347](#)

[Section 38.5, "Loading Authorizations into the Database," on page 348](#)

[Section 38.6, “Enabling TLS/SSL Communications for Role Mapping Administrator,”](#) on page 348

[Section 38.3, “Connecting Role Mapping Administrator to the Identity Vault,”](#) on page 346

- 7** (Optional) To modify any of the settings that you specified during the installation, see [Section 38.7, “Changing Role Mapping Administrator Settings,”](#) on page 350.

38 Configuring Role Mapping Administrator

Role Mapping Administrator is a Web application. It does not require direct access to the managed systems. Instead, when Role Mapping Administrator connects to the Identity Vault, it automatically detects the Identity Manager drivers configured in the vault. Role Mapping Administrator displays each system that is connected through a driver and allows you to retrieve authentications from any of those systems.

38.1 Starting and Stopping Role Mapping Administrator

Role Mapping Administrator does not automatically start after you install the application. To stop and start the application, use the scripts in the installation directory, by default `\install_path\RMA`.

- ♦ **Linux:** `start.sh` and `stop.sh`
- ♦ **Windows:** `start.bat` and `stop.bat`

You can also configure Role Mapping Administrator service to automatically start.

38.1.1 Automatically Starting Role Mapping Administrator on Linux

In a Linux environment, Role Mapping Administrator service automatically stops and starts during reboot. It uses the `/etc/init.d/rma_init` script, which is installed for the `root` user only and is executed during the runlevels 3 and 5.

```
# /etc/init.d/rma_init start
# /etc/init.d/rma_init stop
```

This script is also present in the `rma_install_location/rma_init` install location for both `root` and non `root` user installations.

38.1.2 Automatically Starting Role Mapping Administrator on Windows

In a Windows environment, you must configure Role Mapping Administrator to run as an automated service. For more information, see the following Microsoft documentation:

- ♦ Follow the steps mentioned under [How To Create a User-Defined Service \(http://support.microsoft.com/kb/137890\)](http://support.microsoft.com/kb/137890).
- ♦ The resource kit necessary for creating a user defined service is available at [Windows Server 2003 Resource Kit Tools \(http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=9d467a69-57ff-4ae7-96ee-b18c4790cffd\)](http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=9d467a69-57ff-4ae7-96ee-b18c4790cffd).

38.2 Logging in to the Administrator Configuration Page for Role Mapping Administrator

From the Administrator Configuration page of Role Mapping Administrator Web portal, you can configure the application with the information required for it to connect to the Identity Vault. You can also configure the Identity Manager drivers and load the managed system authorizations into Role Mapping Administrator database.

- 1 In a supported Web browser, enter the URL for Role Mapping Administrator Web portal in the following format: `http://server_name:HTTP_port`. You can specify the DNS or IP address for the server name. For example, `http://localhost:8081`.
- 2 On the login page, specify the Administrator password, and then click **Login**.

For more information about the password, see [Section 38.7.2, “Changing the Password for Role Mapping Administrator,” on page 351](#).

38.3 Connecting Role Mapping Administrator to the Identity Vault

In Role Mapping Administrator, you must create a configuration profile for the Identity Vault. You can create multiple profiles.

- 1 Log on to the Administrator Configuration page for Role Mapping Administrator.

For more information, see [Section 38.2, “Logging in to the Administrator Configuration Page for Role Mapping Administrator,” on page 346](#).

- 2 Under **System Configuration**, complete the following steps:

- 2a For **Vault Display Name**, specify a display name to represent the Identity Vault in Role Mapping Administrator.

- 2b For **Role Vault Address**, specify the DNS address of the Identity Vault.

NOTE: NetIQ does not recommend specifying an IP address.

- 2c For **Role Vault Port**, specify the port for the Identity Vault. To use the SSL protocol, the default port is 389 or 636.

- 2d (Optional) For **Use SSL**, specify whether you want to connect to the Identity Vault using the SSL protocol.

- 2e For **Admin DN**, specify the LDAP distinguished name (LDAP DN) of an Identity Vault administrator user. For example, `cn=admin,ou=sa`.

The administrator user provides a proxy through which Role Mapping Administrator can perform LDAP operations in the Identity Vault.

- 2f For **Admin Password**, specify the password associated with the **Admin DN**.

- 2g For **Root User Container**, specify the root container for the user objects in the Identity Vault. Use the fully qualified LDAP DN. For example, `ou=users,ou=data,o=novell`.

- 2h For **User App. Driver DN**, specify the User Application driver located in the Identity Vault. Use the fully qualified LDAP DN. For example, `cn=UserApp1,cn=IDMDrivers,o=novell`.

- 2i (Optional) For **Driver Discovery DN**, specify the root location to search for drivers. For example, if you only have one driver set, specify the driver set. If you have multiple driver sets, specify the container that holds the driver sets.

NOTE

- ♦ If you do not specify a value, the application performs an LDAP search of the entire Identity Vault.
- ♦ If you change this value after you have loaded the authorizations, the authorizations can change.

-
- 2j (Optional) To allow simultaneous logout from Role Mapping Administrator and Access Manager, for **Access Manager Logout URL** specify the URL for the Access Manager Identity Server.

NOTE: Although you can specify the URL for connecting with Access Manager, this setting does not enable the ability to simultaneous logout. For more information, see [Chapter 39, “Configuring Authentication to Role Mapping Administrator,”](#) on page 353

-
- 2k (Optional) For **User Application REST API URL**, specify the URL for the REST API of the User Application.

Role Mapping Administrator uses the REST API to trigger synchronization of authorizations between RBPM and the managed system.

- 3 Click **Save**.

- 4 (Optional) To launch Role Mapping Administrator, click **Login To Role Mapping Administrator**.

38.4 Configuring the Drivers for Role Mapping Administrator

You can use Identity Manager drivers to add authorizations to Role Mapping Administrator. However, when you first log on to Role Mapping Administrator, the drivers might not be configured to allow you to populate the authorizations. If the drivers are not configured, the **Authorizations** panel displays the message: **No drivers or logical systems were detected in the Identity Vault**. You must configure the global configuration values (GCVs) for the drivers.

NOTE: To use drivers for adding authorizations to the Catlog Administrator, the following conditions apply:

- ♦ Role Mapping Administrator must support the Identity Manager drivers. For more information, see [Section 6.9, “Prerequisites and Requirements for Installing Role Administration,”](#) on page 80 and the documentation accompanying the driver.
- ♦ The drivers must be running. For more information, see “[Starting, Stopping, or Restarting the Driver](#)” in the *NetIQ Identity Manager 4.0.2 Common Driver Administration Guide*.

To configure Identity Manager drivers for adding authorizations to Role Mapping Administrator:

- 1 In Designer or iManager, access the properties of the driver.
- 2 Click **GCVs**.
- 3 Select **show** for the **Catalog > Show role mapping configuration**.
- 4 Select **Yes** to enable role mapping.

The options for each driver vary. For more information about driver-specific parameters, see the guide for each driver.


- 5 Click **OK** to save the changes.

38.5 Loading Authorizations into the Database

Role Mapping Administrator uses a local HSQLDB database to store authorizations that it retrieves from the managed systems. This local database allows you to quickly display authorizations for mapping. You must load the authorizations into the database before users can map authorizations to roles. Any user who is authorized to log on to Role Mapping Administrator can load and reload the database. Load the database the first time you log on so that it is ready for immediate use. Role Mapping Administrator retrieves the authorizations from the selected managed systems.

NOTE

- ◆ The time required to retrieve and load the authorizations depends on the number of managed systems that you select and the number of authorizations contained in each system. You can modify the timeout setting for the load authorization by editing the `web.xml` file, stored by default in the following directories:
 - ◆ **Linux:** `/opt/novell/idm/rma/tomcat/webapps/IDMRMAP/WEB-INF`
 - ◆ **Windows:** `rma_install_path\rma\tomcat\webapps\IDMRMAP\WEB-INF`
- ◆ After you load authorizations into the database, you must manually refresh the authorizations to reflect any new authorizations in the managed systems.

-
- 1 In the **Authorizations** panel, click the **Load Authorizations**  icon to display the load authorizations dialog box.
 - 2 Select the types of authorizations (Groups, Roles, and Profiles) that you want to load for each system displayed.
If you select **Roles**, Role Mapping Administrator loads both single roles and composite roles.
 - 3 Click **OK**.

38.6 Enabling TLS/SSL Communications for Role Mapping Administrator

To ensure a secure environment, NetIQ recommends that you use a Transport Layer Security / Secure Sockets Layer (TLS/SSL) protocol for connections among Role Mapping Administrator, the Identity Vault, and users' browsers. You must configure TLS/SSL for Role Mapping Administrator and for Tomcat.

38.6.1 Enabling Role Mapping Administrator to Use SSL for Connecting to the Identity Vault

- 1 Log on to the Administrator Configuration page for Role Mapping Administrator.
For more information, see [Section 38.2, "Logging in to the Administrator Configuration Page for Role Mapping Administrator,"](#) on page 346.
- 2 Under **System Configuration**, complete the following steps:
 - 2a Select **Use SSL**.
 - 2b For **Role Vault Port**, specify the port for the Identity Vault. When using SSL, the default port is 389 or 636.
 - 2c Click **Save**.

- 3 (Conditional) If you do not have a self-signed certificate, complete the following steps to export a certificate from the certificate authority in the Identity Vault:
 - 3a Log on to iManager.
 - 3b In the **Roles and Tasks** view, click **Directory Administration > Modify Object**.
 - 3c Select the certificate authority object for the Identity Vault, located by default in the Security container and with the naming convention: *TREENAME CA.Security*.
 - 3d Click **OK**.
 - 3e Click **Certificate > Self Signed Certificate**.
 - 3f Click **Export**.
 - 3g At the prompt to export the private key with the certificate, click **No**, and then click **Next**.
 - 3h Select the format for the certificate, and then click **Next**.
Role Mapping Administrator uses a Java-based keystore or trust store, so you can choose either **File in binary DER format** or **File in Base64 format**.
 - 3i Click **Save the exported certificate**.
 - 3j Specify the path where you want to save the file, and then click **Save**.
 - 3k Click **Close**.
- 4 To import the self-signed certificate into Role Mapping Administrator's trust store, complete one of the following actions:

- ♦ Use the keytool executable, which is included with any Java JDK, to import the certificate. For more information on keytool, see “[Keytool - Key and Certificate Management Tool](http://java.sun.com/j2se/1.5.0/docs/tooldocs/windows/keytool.html)” (<http://java.sun.com/j2se/1.5.0/docs/tooldocs/windows/keytool.html>).
- ♦ Enter the following command at a command prompt:

```
keytool -import -file name_of_cert_file -trustcacerts -noprompt
-keystore filename -storepass password
```

For example:

```
keytool -import -file tree_ca_root.b64 -trustcacerts -noprompt -keystore
cacerts -storepass changeit
```

NOTE

- ♦ You must import the new certificate into the trust store of the JRE that launches Role Mapping Administrator.
 - ♦ Ensure that you set the JAVA_HOME environmental variable to the Java install directory and include \$JAVA_HOME/bin/ in the PATH environmental variable.
-

38.6.2 Enabling SSL for a Browser to Access Role Mapping Administrator

To ensure that users have a secure connection in a browser to Role Mapping Administrator, you must configure Tomcat to use TLS/SSL. For more information, see the [Apache Tomcat Documentation Web site](http://tomcat.apache.org/tomcat-6.0-doc/ssl-howto.html) (<http://tomcat.apache.org/tomcat-6.0-doc/ssl-howto.html>).

You must create a new certificate in the keystore file.

- 1 To create a certificate, enter the following command:

```
JDK_HOME/bin/keytool -genkey -alias tomcat -keyalg RSA
```

The default file name is `$HOME/.keystore`, which is the default keystore for Tomcat.

- 2 In a text editor, open the `server.xml` file, located by default in the following directory: `/installation_directory/tomcat/conf`.
- 3 In the file, unremark the section to enable TLS/SSL for Tomcat:

```
<Connector port="8444" protocol="HTTP/1.1" SSLEnabled="true" maxThreads="150"
scheme="https" secure="true" clientAuth="false" sslProtocol="TLS"
keystoreFile="/path_to_keystore" keystorePass="password" />
```

- 4 Add the correct path to the keystore file and the correct password for your environment.
- 5 Restart Tomcat.

38.7 Changing Role Mapping Administrator Settings

This section provides instructions for updating the port number, Administrator password, and Java heap size for Role Mapping Administrator.

NOTE: If you change the following information within Role Mapping Administrator, you must uninstall and reinstall the application:

- ♦ Installation location
- ♦ Application context

For more information about uninstalling, see [Section 49.6, “Uninstalling Role Mapping Administrator,” on page 454](#).

38.7.1 Changing Port Numbers for Role Mapping Administrator

To change the ports that Role Mapping Administrator uses, you must edit the `server.xml` file, located by default in the `rma_install_path/rma/tomcat/conf` directory. You can make these changes even when the ports are in use.

The default HTTP ports are 8081 and 8443. The default port that the operating system uses to shut down the Tomcat service is 8006.

- 1 In a text editor, open the `server.xml` file.
- 2 (Conditional) To change the ports used for the HTTP service, modify the numbers in the following lines:

```
Connector port="8081" protocol="HTTP/1.1"
redirectPort="8443" /
```

- 3 (Conditional) To change the port used for stopping the Tomcat service, modify the following line:

```
Server port="8006" shutdown="SHUTDOWN"
```

38.7.2 Changing the Password for Role Mapping Administrator

During installation, you should specify the administration password that you need to configure Role Mapping Administrator. However, if you did not specify the password, the Web portal for Role Mapping Administrator will prompt you to set the password.

- 1 Start Role Mapping Administrator by executing the start script, located by default in the `\install_path\RMA` directory:

- ♦ **Linux:** `start.sh`
- ♦ **Windows:** `start.bat`

- 2 To launch the Web portal for Role Mapping Administrator, enter the following URL in a Web browser.

```
http://localhost:HTTP_port
```

The default HTTP port is 8081.

- 3 At the **Set the Administration password** prompt in the Web portal, enter and confirm the new password.
- 4 Click **OK**.
- 5 (Optional) To log on to the Web portal, enter the new Administrator Password.

38.7.3 Changing the Java Heap Size for the Role Mapping Administrator

By default, the minimum Java heap size for Role Mapping Administrator is 64 MB and the maximum is 256 MB. If you have a large set of roles or authorizations, increasing the Java heap size helps the performance of the application.

- 1 In a text editor, open the `/installation_directory/idmrmmap/tomcat/bin/catalina.sh` file.
- 2 Search for the following lines:

```
# Setup var for IDMRMAP configuration file
JAVA_OPTS="$Java_OPTS -Xms64m -Xmx256m -
Didmuserapp.logging.config.dir=$CATALINA_HOME/config -
Dlog.init.file=idmrmmap_logging.xml"
```

- 3 To increase the amount of memory allocated to the application, change the `-Xms` values. For example, replace `-Xms64m` with `-Xms128m`.

The amount of memory to add depends upon your environment.

- 4 Save your changes and exit the file.
- 5 To restart Role Mapping Administrator, use stop and start scripts.

38.8 Tuning Session Timeouts for Role Mapping Administrator

Web applications identify every user by a session. The session holds information about the user. For example, when you shop online, the Web application stores the content of your shopping cart in a session. To prevent the number of sessions from increasing infinitely, the application destroys sessions after a certain time of inactivity from the user. This is a **session timeout**. When a session times out, all of the data stored in the session is gone.

If you set the session timeout to a long interval, a user who forgets to log out leaves the session open for the next user who comes to the same computer. This action leaves the previous user, and possibly the server and user data vulnerable to security risks. Reducing the session timeout reduces the chance of having two users use the same session.

As a best practice, NetIQ recommends that you use a short session timeout for Role Mapping Administrator page.

To reduce a session timeout:

- 1 In a text editor, open the `web.xml` file, located by default in the `tomcat_home/conf/web.xml` directory.
- 2 In the following section of the file, specify the desired value for `session-timeout` in minutes:

```
<session-config>
  <session-timeout>30</session-timeout>
</session-config>
```

- 3 Save the file.
- 4 For the change to take effect, restart Tomcat.

39 Configuring Authentication to Role Mapping Administrator

You can configure authentication to Role Mapping Administrator in three ways:

- ♦ **Direct login:** The user provides credentials (username and password) on Role Mapping Administrator login page.
- ♦ **Single sign-on through RBPM:** RBPM provides a link to Role Mapping Administrator. When a user clicks the link, RBPM passes the user's credentials to Role Mapping Administrator.
- ♦ **Single sign-on through Access Manager:** NetIQ Access Manager provides the user's credentials (username and password or SAML token) to Role Mapping Administrator through Access Manager Identity Injection. The user is not prompted for any credential information.

Users can log on directly to Role Mapping Administrator once you have installed the application. You must configure RBPM and Access Manager to provide single sign-on authentication.

39.1 Configuring Single Sign-on through the Roles Based Provisioning Module

RBPM provides a link to Role Mapping Administrator to provide single sign-on. When a user clicks the link, RBPM passes the user's credentials to Role Mapping Administrator.

This solution uses the iFrame portlet of RBPM. The iFrame portlet invokes a URL inside an iFrame control that allows the portlet to pass the authentication parameters from RBPM to Role Mapping Administrator.

39.1.1 Enabling the Roles Based Provisioning Module for Single Sign-on

Complete the following steps to allow user to log on to Role Mapping Administrator from RBPM.

- 1 Log on to RBPM as the administrator user.
- 2 Select the.
- 3 On the **Administration** tab, under **Application Configuration**, select **Password Module Setup > Login**.
- 4 For **Enable SSO**, select **true**.
- 5 Click **Save**, and then log out to enable single sign-on.

39.1.2 Creating a Shared Page for Role Mapping Administrator

The Identity Manager user interface includes many shared pages, which provide the major content within its container pages. To provide users with a link from RBPM to Role Mapping Administrator, you must modify an existing shared page or create a new one.

This section describes how to create a new page that invokes a URL inside an iFrame control that allows the iFrame portlet to pass user authentication parameters from RBPM to Role Mapping Administrator.

- 1 Log on to RBPM as the administrator user.
- 2 Select **Administration > Page Admin**.
- 3 Select **Maintain Shared Pages**.
- 4 Under **Page Actions** at the bottom of this page, select **New**.
- 5 For **Page Link Name**, specify the URL of the shared page that contains the iFrame in RBPM.
- 6 (Optional) For **Page Name**, modify the name of the shared page.

The application automatically applies the same value that you specified for **Page Link Name**.

- 7 For **Assign Categories**, select the categories where the shared page link will be displayed in RBPM. You can select one or more of the following options:
 - ◆ Administration
 - ◆ General
 - ◆ Information Management
 - ◆ Directory Management
 - ◆ Guest Pages
 - ◆ Password Management
- 8 (Optional) For **Description**, specify a brief description of the shared page.
- 9 Click **Save Page**.
- 10 To grant users access to the new shared page, continue to [Section 39.1.3, “Assigning Permissions for Single Sign-on to Role Mapping Administrator,”](#) on page 354.

39.1.3 Assigning Permissions for Single Sign-on to Role Mapping Administrator

By default, only users with administrator rights can see new shared pages that you create in RBPM. You must assign permissions to the users before they can see the page. For more information about creating a new shared page that contains the link to Role Mapping Administrator, see [Section 39.1.2, “Creating a Shared Page for Role Mapping Administrator,”](#) on page 354.

- 1 Log on to RBPM as the administrator user.
- 2 Select **Administration > Page Admin**.
- 3 At the bottom of the **Page Admin** tab, click **Assign Permissions**.
- 4 Search for users, groups, or containers that you want to assign rights to view this page.
- 5 Select the users, groups, or containers.
- 6 Click the right-arrow to add the selected users to the **Current Assignments** list.
- 7 Click **Save**, and then close the window.

39.1.4 Specifying the Content for the Page that Links to Role Mapping Administrator

After you create a shared page, the next step is to add content by selecting portlets to place on the page. You can use prebuilt portlets supplied with the Identity Manager User Application or other portlets that you have registered.

- 1 Log on to RBPM as the administrator user.
- 2 Select **Administration > Page Admin**.
- 3 At the bottom of the **Page Admin** tab, click **Select Content**.
- 4 In the **Available Content** pane, select **iFrame**.
- 5 Click **Add**.
- 6 In the **Selected Content** pane, click **Content Preferences**.
- 7 In the message stating something has changed on the page, click **OK**.
- 8 For **URL**, specify the URL to the login page for Role Mapping Administrator. For example, `http://dns_name:8081/IDMRMAP/login`.
- 9 For **URL / Form Parameters**, specify the following three parameters in the same order as listed below:
 - ◆ `login_panel_user=$PORTLET_AUTH_ID$`
 - ◆ `login_panel_pwd=$PORTLET_AUTH_PWD$`
 - ◆ `url=./com.novell.rolemap.client.ui.UI/UI.html`
- 10 For **Encode URL parameters**, specify **True**.
- 11 For **Form Post?**, specify **True**.
- 12 For **Authentication Required?** specify **True**.
- 13 For **Username**, specify the format that users must enter when logging on to RBPM. Use one of the following values:
 - ◆ **`${Application/login-user}`** passes the exact ID that is entered in RBPM.
 - ◆ **`${User/simpleid}`** provides the CN of the user.
 - ◆ **`${User/canonical}`** provides the dot notation of the logged in user.
- 14 For **Password**, complete the following steps:
 - 14a Click **Use scope path**.
 - 14b In the **Password** field, specify `${Application/login-pass}`.
- 15 For **Height and Width**, specify the size of the page as required.
- 16 Click **Save Preferences**.
- 17 Click **Save Contents** to save the iFrame configuration.

39.2 Configuring Single Sign-on through Access Manager

NetIQ Access Manager allows users to log on to Active Directory and then launch a Web browser to automatically access Role Mapping Administrator. The user does not need to enter a username or password. Access Manager provides the user's credentials (username and password or SAML token) to Role Mapping Administrator through Access Manager Identity Injection.

To use single sign-on through Access Manager, you must configure Active Directory, Access Manager, and the user's Web browser. Also, your environment must meet the conditions defined in [Section 6.9, "Prerequisites and Requirements for Installing Role Administration," on page 80](#).

39.2.1 Understanding Single Sign-on through Access Manager

The single sign-on process functions as follows:

1. A user logs in to an Active Directory workstation and is issued a Kerberos ticket.
2. Access Manager accepts the Kerberos ticket issued by Active Directory and extracts the **userPrincipalName** of the Active Directory user from the ticket.
3. Access Manager maps the **userPrincipalName** (from the Kerberos ticket) to a user object attribute in the Identity Vault as defined by the Access Manager Kerberos class. For example, the mail attribute.

This attribute can be any attribute in the Identity Vault, including a custom attribute, as long as the value in the attribute matches the **userPrincipalName** attribute value in Active Directory.
4. When the user launches a Web browser and navigates to Role Mapping Administrator URL, the configured Access Manager Proxy Service forwards the username and password, via a SAML assertion, to Role Mapping Administrator. If the username and password match a user in the Identity Vault, the user is automatically authenticated without needing any additional credentials.

39.2.2 Configuring Active Directory to Assign Kerberos Tickets

When users log on to Active Directory they are automatically issued a Kerberos ticket. You must enable Active Directory to assign Kerberos tickets. This process requires the following activities:

- ♦ ["Installing the spn and ktpass Utilities" on page 356](#)
- ♦ ["Creating a User Account for the Identity Server" on page 357](#)
- ♦ ["Creating a Keytab File" on page 357](#)

Installing the spn and ktpass Utilities

You must install the spn and ktpass utilities on the Active Directory domain controller. These utilities are not installed by default. You need both of these utilities to configure the Access Manager Identity Server for Kerberos authentication.

- 1 Insert the Windows 2003 disk into the CD drive.
- 2 To install the utilities, run `\SUPPORT\TOOLS\SUPTOOLS.MSI` on the CD.

The utilities are installed in `C:\Program Files\Support Tools`.

Creating a User Account for the Identity Server

You must create an account in Active Directory that allows the Access Manager Identity Server to run as a service.

- 1 In the tool that you use for managing users, complete the following steps:
 - 1a Create a new account.
 - 1b For **firstname**, specify a name for the Identity Server.
 - 1c For **lastname**, specify a name for the Identity Server.
 - 1d For **userPrincipalName**, specify a name with an attribute in Active Directory that matches an attribute in the Identity Vault. Use the following format:

```
HTTP/your.idp.fqdn@YOUR.DOMAIN
```

For example, `HTTP/amser.provo.novell.com@AD.NOVELL.COM`
 - 1e For **samAccountName**, specify the name for the user. Use the format required by the `setspn` utility: `firstname-lastname`.
 - 1f For **password**, specify the password for this user account.
 - 1g Deselect the option **User must change password at next logon**.
 - 1h Select the option **Password never expires**.

The user account needs a password, but it must never expire or be changed.
 - 1i Accept the changes for the new user.
- 2 To set the **servicePrincipalNames** on the user object, complete the following steps:

NOTE: This process sends the Kerberos token to the Identity Server instead of directly to the managed system Portal, so the single sign-on can occur.

- 2a At a command line, enter:

```
setspn -a HTTP/amserv.provo.novell.com@AD.NOVELL.COM samAccountName
```

- 2b At a command line, enter:

```
setspn -a HTTP/amserv.provo.novell.com samAccountName
```

Creating a Keytab File

The keytab file contains the secret encryption key that is used to decrypt the Kerberos ticket. You need to generate the keytab file and copy it to the Access Manager Identity Server. You can use the `ktpass` utility to export the keytab file.

- 1 On the Active Directory server, enter the following `ktpass` command:

```
ktpass /out value /princ value /mapuser value /pass value
```

For example, to create a keytab file named `nidkey`, enter:

```
ktpass /out nidkey.keytab /princ HTTP/amser.provo.novell.com@AD.NOVELL.COM /  
mapuser/ amser@AD.NOVELL /pass novell
```

Use the following parameters in the command line:

/out outputFilename

Specifies a name for the file, with `.keytab` as the extension. For example: `nidpkey.keytab`

/princ servicePrincipalName@KERBEROS_REALM

Specifies the service principal name for the Identity Server, then @, followed by the Kerberos realm. The default value for the Kerberos realm is the Active Directory domain name in all capitals. The Kerberos realm value is case sensitive.

/mapuser identityServerUser@AD_DOMAIN

Specifies the username of the Identity Server user and the Active Directory domain to which the user belongs.

/pass userPassword

Specifies the password for this user.

- 2 Copy the keytab file to the `security` directory on the Identity Server, located by default in the following paths:

- ♦ **Linux:** `/opt/novell/java/jre/lib/security`
- ♦ **Windows:** `C:\Program Files\Novell\jre\lib\security`

39.2.3 Configuring Access Manager Identity Server to Consume the Kerberos Tickets

Access Manager can use the authentication information in the Kerberos tickets to enable single sign-on for Role Mapping Administrator. You must configure Access Manager to consume the Kerberos tickets from Active Directory. This process requires the following activities:

- ♦ [“Enabling Logging for Kerberos Transactions” on page 358](#)
- ♦ [“Creating the bcsLogin.conf File” on page 359](#)
- ♦ [“Creating a User Store for the Active Directory Domain” on page 360](#)
- ♦ [“Creating a Kerberos Authentication Class, Method, and Contract for the Identity Server” on page 360](#)
- ♦ [“Verifying the Kerberos Configuration” on page 361](#)
- ♦ [“Creating a SAML Identity Injection Policy” on page 362](#)
- ♦ [“Saving the Configuration Changes” on page 363](#)
- ♦ [“Creating a Protected Resource for Role Mapping Administrator” on page 363](#)

Enabling Logging for Kerberos Transactions

When you log Kerberos transactions, you can troubleshoot issues related to user authentication.

- 1 In the Access Manager Administration Console, click **Devices > Identity Server > Edit > Logging**.
- 2 (Optional) To enable logging, select **File Logging**.
- 3 (Optional) To enable echo to console, select **Echo to Console**.
- 4 Under **Component File Loggers Levels**, set the **Application** option to **debug**.
- 5 Enable **Trace Logging**.
- 6 For **Component Content Filters**, select **Application**, **Configuration**, and **User Store**.
- 7 Click **OK**, and then update the Identity Server.

Creating the bcsLogin.conf File

The `bcsLogin.conf` file serves as an authentication file for the Java Authentication and Authorization Service (JAAS).

NOTE: When you create or change the `bcsLogin.conf` file, you must restart Tomcat.

1 In a text editor, complete the following steps:

1a Create a file name `bcsLogin.conf`.

1b Add the following lines to the file:

```
com.sun.security.jgss.accept {
com.sun.security.auth.module.Krb5LoginModule required
debug="true"
useTicketCache="true"
ticketCache="SPECIFY_VALUE"
doNotPrompt="true"
principal="SPECIFY_VALUE"
useKeyTab="true"
keyTab="SPECIFY_VALUE"
storeKey="true";
};
```

NOTE: The file cannot contain any white space, only end-of-line characters.

1c For **ticketCache**, specify the location of the cache file where the Kerberos ticket is stored. For example, for SLES 10, use `/opt/novell/java/jre/lib/security/spnegoTicket.cache`.

For Windows computers, the path must contain double slashes. The default location is `C:\Program Files\Novell\jre\lib\security\nidpkey.keytab`.

1d For **principal**, specify the service principal name for the Access Manager Identity Server. For example, `HTTP/amser.provo.novell.com@AD.NOVELL.COM`. This value is unique to your configuration.

1e For **keyTab**, specify the location of the keytab that you created in “[Creating a Keytab File](#)” on [page 357](#). For example, for SLES 10, use `/opt/novell/java/jre/lib/security/nidpkey.keytab`. This value is unique to your configuration.

For Windows computers, the path must contain double slashes. The default location is `C:\Program Files\Novell\jre\lib\security\spnegoTicket.cache`.

2 Copy the `bcsLogin.conf` file to the directory where the keytab file is stored, located by default in the following paths:

- ♦ **Linux:** `/opt/novell/java/jre/lib/security`
- ♦ **Windows:** `C:\Program Files\Novell\jre\lib\security`

3 Ensure that the permissions for the `bcsLogin.conf` file are set to 644.

4 (Conditional) On Linux computers, enter the following command to restart Tomcat on the Identity Server:

```
/etc/init.d/novell-tomcat5 restart
```

5 (Conditional) On Windows computers, use the control panel to stop and restart the Tomcat service on the Identity Server.

Creating a User Store for the Active Directory Domain

You need to either configure your Access Manager Identity Server to use Active Directory as a user store or verify the existing configuration for your Active Directory user store.

- 1 Log on to Access Manager.
- 2 In the Administration Console, select **Devices > Identity Servers > Edit**.
- 3 To view your user stores, click **Local**.
If you haven't configured a user store for the Active Directory server, click **New**.
- 4 (Conditional) If you have already configured your Identity Server to use the Active Directory server, click the name of the AD server.
- 5 (Conditional) If you have not configured a user store for the Active Directory server, click **New**.
- 6 For a new user store, fill in the following fields. For an existing Active Directory user store, verify the values.

Name: Specifies a name for the user store for reference.

Admin name: Specifies the name of the administrator of the Active Directory server. Administrator-level rights are required for setting up a user store. This ensures read/write access to all objects used by Access Manager.

Directory Type: Select **Active Directory**.

Server replica: (Conditional) For a new Active Directory user store, click **New** to add a replica, and then specify the following values:

- ♦ **Name:** Specifies a name of the replica for reference. This can be the name of the Active Directory server.
- ♦ **IP Address:** Specifies the IP address of the Active Directory server and the port you want the Identity Server to use when communicating with the Active Directory server.
- ♦ **Port:** Specifies the port that the Active Directory server uses to communicate to the Identity Server. This communication occurs over LDAP. The default non-secure port is 389. The default secure port is 636.

Search Context: For a new user store, click **New** and specify the context of the administrator of the Active Directory server. For an existing user store, verify that you have an entry for the context of the administrator. Add a context if it is missing.

- 7 Click **OK** to save the changes.

Creating a Kerberos Authentication Class, Method, and Contract for the Identity Server

To ensure that Access Manager can consume Kerberos tickets for single sign-on to Role Mapping Administrator, you must create a Kerberos authentication class for the Access Manager Identity Server. You must also create a method and contract in Identity Server for Kerberos.

- 1 Log on to Access Manager.
- 2 To create an authentication class for Kerberos, complete the following steps:
 - 2a In the **Local** tab of the Identity Server, select **Classes > New**.
 - 2b For **Display name**, specify a name to identify the new class.
 - 2c For **Java Class**, select **KerberosClass**.
 - 2d Click **Next**.

- 2e For **Service Principal Name**, specify the value of the `servicePrincipalName` attribute of the Identity Server user.
This is the user account that you created in [“Creating a User Store for the Active Directory Domain” on page 360](#).
 - 2f For **Kerberos Realm**, specify the name of the Kerberos realm. The default value for this realm is the domain name of the Active Directory server, entered in all uppercase. The value is case sensitive.
 - 2g For **JAAS config file for Kerberos**, specify the path to the `bcsLogin.conf` file.
This is the file that you created in [“Creating the bcsLogin.conf File” on page 359](#).
 - 2h For **Kerberos KDC**, specify the IP address of the Active Directory server.
 - 2i For **User Attribute**, specify the attribute in the Identity Vault that contains the `userPrincipalName` from Active Directory. For example, the mail attribute in the Identity Vault can store the `userPrincipalName` from Active Directory.
If this attribute does not contain the `userPrincipalName` from Active Directory, the authentication to Role Mapping Administrator fails.
 - 2j Click **Finish**.
- 3 To create a Kerberos method for the Identity Server, complete the following steps:
- 3a In the **Local** tab of the Identity Server, click **Method > New**.
 - 3b For **Display name**, specify a name to identify this method.
 - 3c For **Class**, select the Kerberos class that you created in [Step 2](#).
 - 3d For **User stores**, move the user store for the Identity Vault to the list of **User stores**.
Ensure that you move the user store for the Identity Vault, not the user store for Active Directory.
 - 3e Click **Finish**.
- 4 To create a Kerberos contract for the Identity Server, complete the following steps:
- 4a In the **Local** tab of the Identity Server, click **Contract > New**.
 - 4b For **Display name**, specify a name to identify this contract.
 - 4c For **URI**, specify a value that uniquely identifies the contract from all other contracts. For example, `kerberos/contract`.
The URI cannot begin with a slash.
 - 4d For **Methods**, move the method that you created in [Step 3](#) to the *Methods* list.
 - 4e Click **Finish**.

Verifying the Kerberos Configuration

To verify the configuration that you created for Kerberos, view one of the following files for the Identity Server:

- ♦ **Linux:** `catalina.out`
- ♦ **Windows:** `stdout.log`

To verify the Kerberos configuration:

- 1 Log on to Access Manager.
- 2 In the Administration Console, select **Auditing > General Logging**.
- 3 In the Identity Servers section, select the `catalina.out` or `stdout.log` file.

- 4 Download the file.
- 5 Open the downloaded file in a text editor.
- 6 In the file, search for Kerberos and verify that a subsequent line contains a `Commit Succeeded` phrase. For the configuration example, the lines look similar to the following:

```
principal's key obtained from the keytab
principal is HTTP/amser.provo.novell.com@AD.NOVELL.COM
Added server's keyKerberos Principal HTTP/
amser.provo.novell.com@AD.NOVELL.COMKey Version 3key EncryptionKey: keyType=3
keyBytes (hex dump)=0000: CB 0E 91 FB 7A 4C 64 FE

[Krb5LoginModule] added Krb5Principal HTTP/
amser.provo.novell.com@AD.NOVELL.COM to Subject
Commit Succeeded
```

- 7 If the file does not contain any lines similar to these, verify that you have enabled logging. See [“Enabling Auditing of Role Mapping Administrator” on page 367](#).
- 8 If the commit did not succeed, search backward in the file and verify the following values:
 - ◆ Service Principal Name
 - ◆ Name of the keytab file

For the example configuration, the file contains lines with text similar to the following:

```
Principal is HTTP/amser.provo.novell.com

KeyTab is /usr/lib/java/jre/lib/security/nidpkey.keytab
```

- 9 (Conditional) If you modify the configuration, either in the Administration Console or the `bcsLogin` file, restart Tomcat on the Identity Server.

Creating a SAML Identity Injection Policy

You must create a SAML identity injection policy for Access Manager to use. This allows the authentication information in the Kerberos tickets to be passed to the Catalog Application.

- 1 Log on to Access Manager.
- 2 In the Administration Console, select **Policies > Policies > Master_Container**.
The policy must reside in the master container.
- 3 To create a new policy, click **New**.
- 4 Specify a name to identify the policy.
- 5 For the policy type, select **Access Gateway: Identity Injection**.
- 6 Click **OK**.
- 7 To define the policy, complete the following steps:
 - 7a For **Description**, describe the policy.
 - 7b For **Priority**, use the default value, which is 1.
 - 7c For **Actions**, click **New > Inject into Authentication Header**.
 - 7d For **User Name**, select **Credential Profile > LDAP Credentials:LDAP User Name**.
 - 7e For **Password**, select **Credential Profile > SAML Credentials:SAML Assertion**.

- 7f For **Multi-Value Separator**, use the default value, which is a comma.
- 7g For **DN Format**, use the default value, which is LDAP.
- 8 Click **OK** twice to save the policy.

Saving the Configuration Changes

To ensure that the changes to the Identity Server take effect, you must refresh the Identity Server.

- 1 Log on to Access Manager.
- 2 In the Administration Console, select **Devices > Identity Servers**.
- 3 Select your Identity Server, and then click **Refresh**.
- 4 Click **Close**.

Creating a Protected Resource for Role Mapping Administrator

You must configure Role Mapping Administrator as a protected resource in the Access Gateway. You must also refresh the Access Gate to ensure that your changes for the protected resource take effect.

- 1 Log on to Access Manager.
- 2 In the Administration Console, select **Devices > Access Gateways**.
- 3 Select the name of your Access Gateway.
- 4 (Conditional) If you have a Proxy Service defined for Role Mapping Administrator, skip to [Step 5](#). Otherwise, complete the following steps to create the Proxy Service for Role Mapping Administrator:
 - 4a In the Proxy Service List, click **New**.
 - 4b For **Proxy Service Name**, specify a name to identify Role Mapping Administrator as a Proxy Service.
 - 4c For **Multi-Homing Type**, select **Domain-Based**.
 - 4d For **Published DNS Name**, specify the DNS name for Role Mapping Administrator server.
 - 4e For **Path**, specify the application context for Role Mapping Administrator. The default context is IDMRMAP. There should be two entries. For example:

/*

/IDMRMAP/*
 - 4f For **Web Server IP Address**, specify the IP address of the Web server.
 - 4g For **Host Header**, select **Web Server Host Name**, which publishes the DNS name that the user sent in the request to be replaced by the DNS name of the Web server.
 - 4h For **Web Server Host Name**, specify the DNS name of the Web server.
 - 4i Click **OK**.
- 5 Click the display name of the Proxy Service for Role Mapping Administrator.
- 6 To create a new protected resources, complete the following steps:
 - 6a Click the **Protected Resources** tab, and then click **New**.
 - 6b Specify the name of the protected resource, and then click **OK**.
 - 6c Click the **Overview** tab.
 - 6d For **Description**, describe the protected resource.

- 6e For **Contract**, select the Kerberos contract that you created in “[Creating a Kerberos Authentication Class, Method, and Contract for the Identity Server](#)” on page 360.
- 6f For **URL Path**, click the /* path, and then define the application context for Role Mapping Administrator. For example, /* /IDMRMAP/*.
- 7 Click the **Identity Injection** tab, and then click **Manage Policies**.
- 8 Select the policy that you created in “[Creating a SAML Identity Injection Policy](#)” on page 362.
- 9 Click **Apply Changes**.
- 10 Click **Close**.
- 11 Click **OK**.
- 12 In the Administration Console, select **Devices > Access Gateways**.
- 13 Select your Access Gateway, and then click **Refresh**.
- 14 Click **Close**.

39.2.4 Configuring the User’s Web Browser

To ensure that users can log on to the Catalog Administrator using Access Manager, you must configure each user’s Web browser to trust the Access Manager Identity Server.

- 1 Add the computers of the users to the Active Directory domain.
For instructions, see your Active Directory documentation.
- 2 Log on to the Active Directory domain, rather than the computer.
- 3 (Conditional) To configure Internet Explorer 7 or later to trust the Identity Server, complete the following steps:
 - 3a Open Internet Explorer.
 - 3b Click **Tools > Internet Options > Security > Local intranet > Sites > Advanced**.
 - 3c In **Add this website to the zone**, specify the Base URL for the Identity Server. For example, `http://amser.provo.novell.com`.
 - 3d Click **Add**.
 - 3e Click **Close**.
 - 3f Restart the browser.
- 4 (Conditional) To configure Firefox to trust the Identity Server, complete the following steps:
 - 4a Open Firefox.
 - 4b In the **URL** field, specify `about:config`.
 - 4c To filter the preferences, search for **network.n**.
 - 4d Double-click `network.negotiate-auth.trusted-uris`.
This preference lists the sites that are permitted to engage in SPNEGO Authentication with the browser.
 - 4e Specify a comma-delimited list of trusted domains or URLs. For example, add `http://amser.provo.novell.com`.
 - 4f (Conditional) If the deployed SPNEGO solution uses the advanced Kerberos feature of Credential Delegation, double-click `network.negotiate-auth.delegation-uris`.
This preference lists the sites for which the browser can delegate user authorization to the server. Specify a comma-delimited list of trusted domains or URLs. For example, add `http://amser.provo.novell.com`.

4g Click **OK**.

4h Restart the browser .

- 5** In either Web browser, enter the base URL of the Identity Server with port and application. For example configuration, `http://amser.provo.novell.com:8080/nidp`.

The Identity Server authenticates the user without prompting the user for authentication information.

40 Auditing Role Mapping Administrator

You can record what changes were made to Role Mapping Administrator, who made the changes, and when the changes occurred. To audit Role Mapping Administrator, you must configure the application for auditing. You must also have the Identity Information Warehouse installed in your environment and configured to capture the events. For more information about the Identity Information Warehouse, see [Part VIII, “Installing the Identity Information Warehouse,” on page 293](#) and the *Identity Manager Reporting Guide* (<http://www.novell.com/documentation/idm40/pdfdoc/reporting.pdf>).

This section explains the process for enabling Role Mapping Administrator to audit events, and provides an explanation of the individual events.

40.1 Enabling Auditing of Role Mapping Administrator

The auditing functionality in Role Mapping Administrator is disabled by default. However, you can use the `rmaConfig.jar` file to enable auditing. The file is located by default in the `RMA_Install_Location/rma/` directory. To invoke the `rmaConfig.jar` file, run the following command:

```
java -jar rmaConfig.jar parameters
```

Use the following parameters when you invoke the `rmaConfig.jar` file:

- ◆ **-h** Displays help.
- ◆ **-N** Disables nAudit.
- ◆ **+N** Enables nAudit. For example, enter `java -jar rmaConfig.jar +N`.
- ◆ **-S** Disables Syslog auditing.
- ◆ **+S, @host:port,protocol** Enables Syslog auditing.
 - ◆ For *host*, specify the name or IP address of the server. The default value is localhost.
 - ◆ For *port*, the default value is 1514.
 - ◆ For *protocol* specify UCP, TCP, or SSL. The default value is UDP.

To specify SSL, you must add the Keystore file and the corresponding password in the following format: `ssl: [keyStoreFile]: [keyStorePasswd]`.

For example, to enable sysLog auditing through 192.168.1.1 host address at 1520 port over SSL with the corresponding key file and password, run the following command:

```
java -jar rmaConfig.jar +S,@192.168.1.1:1520,/etc/ssl/mykey.cer,keypass
```

40.2 Understanding the Audit Events Generated by Role Mapping Administrator

This section lists the audit events logged for Role Mapping Administrator, when you have auditing enabled for Identity Manager.

40.2.1 Event ID 00031550

Tracks when someone logs in to the application successfully.

Fields	Values
Event ID	00031550
Description	Login_Success
Originator (B) Title	Login ID
Target (U) Title	Target DN
Subtarget (V) Title	
Text1 (S) Title	Message
Text2 (T) Title	Client IP
Text3 (F) Title	
Value1 (1) Title	
Value1 Type	
Value2 (2) Title	
Value2 Type	
Value3 (3) Title	
Value3 Type	
Group (G) Title	
Group Type	
Data (D) Title	
Data Type	
Display Schema	[[\${rC}] [\${SO}]: \${SB} successfully logged in from \${ST}. \n

40.2.2 Event ID 00031551

Tracks all login failures.

Fields	Values
Event ID	00031551
Description	Login_Failure

Fields	Values
Originator (B) Title	Login ID
Target (U) Title	Target DN
Subtarget (V) Title	
Text1 (S) Title	Message
Text2 (T) Title	Client IP
Text3 (F) Title	
Value1 (1) Title	
Value1 Type	
Value2 (2) Title	
Value2 Type	
Value3 (3) Title	
Value3 Type	
Group (G) Title	
Group Type	
Data (D) Title	
Data Type	
Display Schema	[\$rC] [\$SO]: \$SB failed to log on from \$ST. \n

40.2.3 Event ID 00031630

Tracks when a role is successfully created.

Fields	Values
Event ID	00031630
Description	Create_Role
Originator (B) Title	Initiator ID
Target (U) Title	Role DN
Subtarget (V) Title	
Text1 (S) Title	
Text2 (T) Title	
Text3 (F) Title	
Value1 (1) Title	
Value1 Type	
Value2 (2) Title	

Fields	Values
Value2 Type	
Value3 (3) Title	
Value3 Type	
Group (G) Title	
Group Type	
Data (D) Title	Role Object
Data Type	S
Display Schema	[\$rC] [\$SO]: Initiated by \$SB; Role DN: \$SU\n

40.2.4 Event ID 00031631

Tracks when the creation of a role fails.

Fields	Values
Event ID	00031631
Description	Create_Role_Failure
Originator (B) Title	Initiator ID
Target (U) Title	Role DN
Subtarget (V) Title	
Text1 (S) Title	
Text2 (T) Title	
Text3 (F) Title	Error Message
Value1 (1) Title	
Value1 Type	
Value2 (2) Title	
Value2 Type	
Value3 (3) Title	
Value3 Type	
Group (G) Title	
Group Type	
Data (D) Title	Role Object
Data Type	S
Display Schema	[\$rC] [\$SO]: Initiated by \$SB; Role DN: \$SU; Error Message: \$SF\n

40.2.5 Event ID 00031632

Tracks when a role is successfully deleted.

Fields	Values
Event ID	00031632
Description	Delete_Role
Originator (B) Title	Initiator ID
Target (U) Title	Role DN
Subtarget (V) Title	
Text1 (S) Title	
Text2 (T) Title	
Text3 (F) Title	
Value1 (1) Title	
Value1 Type	
Value2 (2) Title	
Value2 Type	
Value3 (3) Title	
Value3 Type	
Group (G) Title	
Group Type	
Data (D) Title	Role Object
Data Type	S
Display Schema	[\$rC] [\$SO]: Initiated by \$SB; Role DN: \$SU\n

40.2.6 Event ID 00031633

Tracks when a role deletion fails.

Fields	Values
Event ID	00031633
Description	Delete_Role_Failure
Originator (B) Title	Initiator ID
Target (U) Title	Role DN
Subtarget (V) Title	
Text1 (S) Title	
Text2 (T) Title	

Fields	Values
Text3 (F) Title	Error Message
Value1 (1) Title	
Value1 Type	
Value2 (2) Title	
Value2 Type	
Value3 (3) Title	
Value3 Type	
Group (G) Title	
Group Type	
Data (D) Title	Role Object
Data Type	S
Display Schema	[\$rC] [\$SO]: Initiated by \$SB; Role DN: \$SU; Error Message: \$SF\n

40.2.7 Event ID 00031634

Tracks when a role is successfully modified.

Fields	Values
Event ID	00031634
Description	Modify_Role
Originator (B) Title	Initiator ID
Target (U) Title	Role DN
Subtarget (V) Title	
Text1 (S) Title	
Text2 (T) Title	
Text3 (F) Title	
Value1 (1) Title	
Value1 Type	
Value2 (2) Title	
Value2 Type	
Value3 (3) Title	
Value3 Type	
Group (G) Title	
Group Type	

Fields	Values
Data (D) Title	Role Object
Data Type	S
Display Schema	[\$rC] [\$SO]: Initiated by \$SB; Role DN: \$SU\n

40.2.8 Event ID 000361635

Tracks each modify event that fails.

Fields	Values
Event ID	00031635
Description	Modify_Role_Failure
Originator (B) Title	Initiator ID
Target (U) Title	Role DN
Subtarget (V) Title	
Text1 (S) Title	
Text2 (T) Title	
Text3 (F) Title	Error Message
Value1 (1) Title	
Value1 Type	
Value2 (2) Title	
Value2 Type	
Value3 (3) Title	
Value3 Type	
Group (G) Title	
Group Type	
Data (D) Title	Role Object
Data Type	S
Display Schema	[\$rC] [\$SO]: Initiated by \$SB; Role DN: \$SU; Error Message: \$SF\n

40.2.9 Event ID 00031670

Tracks each resource that is created.

Fields	Values
Event ID	00031670
Description	Create_Resource

Fields	Values
Originator (B) Title	Initiator ID
Target (U) Title	Resource DN
Subtarget (V) Title	
Text1 (S) Title	
Text2 (T) Title	
Text3 (F) Title	
Value1 (1) Title	
Value1 Type	
Value2 (2) Title	
Value2 Type	
Value3 (3) Title	
Value3 Type	
Group (G) Title	
Group Type	
Data (D) Title	Resource Object
Data Type	S
Display Schema	\$SB; Resource DN: \$SU

40.2.10 Event ID 00031671

Tracks each failure event during the creation of a resource.

Fields	Values
Event ID	00031671
Description	Create_Resource_Failure
Originator (B) Title	Initiator ID
Target (U) Title	Resource DN
Subtarget (V) Title	
Text1 (S) Title	
Text2 (T) Title	
Text3 (F) Title	Error Message
Value1 (1) Title	
Value1 Type	
Value2 (2) Title	

Fields	Values
Value2 Type	
Value3 (3) Title	
Value3 Type	
Group (G) Title	
Group Type	
Data (D) Title	Resource Object
Data Type	S
Display Schema	\$SB; Resource DN: \$SU; Error Message: \$SF

40.2.11 Event ID 00031674

Tracks the event when a resource is modified.

Fields	Values
Event ID	00031674
Description	Modify_Resource
Originator (B) Title	Initiator ID
Target (U) Title	Resource DN
Subtarget (V) Title	
Text1 (S) Title	
Text2 (T) Title	
Text3 (F) Title	
Value1 (1) Title	
Value1 Type	
Value2 (2) Title	
Value2 Type	
Value3 (3) Title	
Value3 Type	
Group (G) Title	
Group Type	
Data (D) Title	Resource Object
Data Type	S
Display Schema	\$SB; Resource DN: \$SU

40.2.12 Event ID 00031675

Tracks the failure detected during the modification of a resource.

Fields	Values
Event ID	00031675
Description	Modify_Resource_Failure
Originator (B) Title	Initiator ID
Target (U) Title	Resource DN
Subtarget (V) Title	
Text1 (S) Title	
Text2 (T) Title	
Text3 (F) Title	Error Message
Value1 (1) Title	
Value1 Type	
Value2 (2) Title	
Value2 Type	
Value3 (3) Title	
Value3 Type	
Group (G) Title	
Group Type	
Data (D) Title	Resource Object
Data Type	S
Display Schema	\$SB; Resource DN: \$SU; Error Message: \$SF

40.2.13 Event ID 00031676

Tracks when a resource association is created.

Fields	Values
Event ID	00031676
Description	Create_Resource_Association
Originator (B) Title	Initiator ID
Target (U) Title	Resource Association DN
Subtarget (V) Title	
Text1 (S) Title	
Text2 (T) Title	

Fields	Values
Text3 (F) Title	
Value1 (1) Title	
Value1 Type	
Value2 (2) Title	
Value2 Type	
Value3 (3) Title	
Value3 Type	
Group (G) Title	
Group Type	
Data (D) Title	Resource Association Object
Data Type	S
Display Schema	\$SB; Resource Association DN: \$SU

40.2.14 Event ID 00031677

Tracks when a resource association fails.

Fields	Values
Event ID	00031677
Description	Create_Resource_Association_Failure
Originator (B) Title	Initiator ID
Target (U) Title	Resource Association DN
Subtarget (V) Title	
Text1 (S) Title	
Text2 (T) Title	
Text3 (F) Title	Error Message
Value1 (1) Title	
Value1 Type	
Value2 (2) Title	
Value2 Type	
Value3 (3) Title	
Value3 Type	
Group (G) Title	
Group Type	

Fields	Values
Data (D) Title	Resource Association Object
Data Type	S
Display Schema	\$SB; Resource Association DN: \$SU; Error Message: \$SF

40.2.15 **Event ID 0003167A**

Tracks when a resource association is modified.

Fields	Values
Event ID	0003167A
Description	Modify_Resource_Association
Originator (B) Title	Initiator ID
Target (U) Title	Resource Association DN
Subtarget (V) Title	
Text1 (S) Title	
Text2 (T) Title	
Text3 (F) Title	
Value1 (1) Title	
Value1 Type	
Value2 (2) Title	
Value2 Type	
Value3 (3) Title	
Value3 Type	
Group (G) Title	
Group Type	
Data (D) Title	Resource Association Object
Data Type	S
Display Schema	\$SB; Resource Association DN: \$SU

40.2.16 **Event ID 0003167B**

Tracks failure detected during the modification of a resource association.

Fields	Values
Event ID	0003167B
Description	Modify_Resource_Association_Failure

Fields	Values
Originator (B) Title	Initiator ID
Target (U) Title	Resource Association DN
Subtarget (V) Title	
Text1 (S) Title	
Text2 (T) Title	
Text3 (F) Title	Error Message
Value1 (1) Title	
Value1 Type	
Value2 (2) Title	
Value2 Type	
Value3 (3) Title	
Value3 Type	
Group (G) Title	
Group Type	
Data (D) Title	Resource Association Object
Data Type	S
Display Schema	\$\$B; Resource Association DN: \$\$U; Error Message: \$\$F

X Installing Identity Manager Home and the Provisioning Dashboard

This section guides you through the process of installing required components for Identity Manager Home and Provisioning Dashboard (Identity Manager Home).

Identity Manager Home require access to other Identity Manager components during and after installation. NetIQ recommends that you review the installation process before beginning. For more information, see [Section 41.1, “Checklist for Installing Identity Manager Home,” on page 383](#).

41 Installing Identity Manager Home

This section provides information that helps you prepare for installing Identity Manager Home. The installation package contains the following items:

- ♦ IdmHPD.bin
- ♦ IdmHPD-all-no-prop.properties
- ♦ IdmHPD-all-props.properties
- ♦ IdmHPD-Reporting.properties
- ♦ IdmHPD-UserApp-no-prop.properties
- ♦ hpd-conf-designer-version.zip
- ♦ hpd-conf-eas-version.zip
- ♦ hpd-conf-runtime-version.zip
- ♦ hpd-conf-vault-version.zip

41.1 Checklist for Installing Identity Manager Home

NetIQ recommends that you perform the steps in the following checklist:

	Checklist Items
<input type="checkbox"/>	1. Learn about the interaction among Identity Manager components. For more information, see Chapter 1, “Understanding the Architecture of Identity Manager,” on page 21.
<input type="checkbox"/>	2. Ensure that your environment meets the considerations and requirements for hosting Analyzer. For more information, see Section 6.10, “Prerequisites and Requirements for Installing Identity Manager Home and the Provisioning Dashboard,” on page 83.
<input type="checkbox"/>	3. Create backups of your Designer project, Identity Manager databases, and virtual machines. For more information, see Section 41.2, “Preparing Your Environment,” on page 384.
<input type="checkbox"/>	4. Install Identity Manager Home on your User Application and Reporting Module servers. For more information, see Section 41.3, “Installing Identity Manager Home,” on page 384.
<input type="checkbox"/>	5. (Conditional) If you did not use the default IDMPROV context for the User Application URL, replace the IDMPROV references in the .war file. For more information, see Section 41.3.2, “Updating User Application Files in an Environment that Uses a Non-Default Context,” on page 386.
<input type="checkbox"/>	6. Before using Identity Manager Home, configure the Identity Manager components to work with Identity Manager Home. For more information, see Chapter 42, “Configuring Your Identity Manager Environment for Identity Manager Home,” on page 389.
<input type="checkbox"/>	7. Verify that you can log on to the User Application and then access Identity Manager Home. For more information, see Chapter 43, “Verifying Installation of Identity Manager Home,” on page 401.

	Checklist Items
<input type="checkbox"/>	8. Customize the default Identity Manager Home items that your users need to perform their necessary tasks. For more information, see “ Configuring Identity Manager Home ” (https://www.netiq.com/documentation/idm402/idmhomepage/data/b15pyf43.html) in the <i>NetIQ Identity Manager Home and Provisioning Dashboard User Guide</i> .

41.2 Preparing Your Environment

Before you begin the installation process, ensure that you have installed all system requirements specified in “[Prerequisites and Requirements for Installing Identity Manager Home and the Provisioning Dashboard](#)” on page 83.

After installing all system requirements, complete the following steps to prepare your environment:

- 1 Back up your User Application database. For more information, see the documentation specific to your database.
- 2 Back up your eDirectory Identity Vault. For more information about backing up eDirectory, see “[Backing Up and Restoring eDirectory](#)” in the *eDirectory Administration Guide*.
- 3 In Designer, back up and export your Designer project. For more information about exporting Designer projects, see “[Exporting a Project](#)” in the *Designer 4.0.2 for Identity Manager 4.0.2 Administration Guide*.
- 4 (Conditional) If you use virtual machines to host Identity Manager components, create snapshots of all the virtual machines that you use. Refer to the documentation specific to your virtualization software for instructions.
- 5 (Conditional) To install Identity Manager Home in a JBoss cluster environment, the cluster must already be prepared. For more information, see [Section 27.2, “Preparing a JBoss Cluster for the User Application,”](#) on page 222.
- 6 Download the installation package: `IDM-HPD-version.zip`

41.3 Installing Identity Manager Home

The Identity Manager Home installation program assumes that you used the default path for the Roles Based Provisioning Module (RBPM) and the default context for JBoss:

```
/opt/novell/idm/jboss/server/IDMProv/
```

If you used non-default information, review the following considerations:

- ♦ **If you installed RBPM in a non-default path**, ensure that you specify the custom path during the installation.
- ♦ **If you specified a context other than `IDMPROV` for the User Application URL**, after performing the installation process, complete the steps in [Section 41.3.2, “Updating User Application Files in an Environment that Uses a Non-Default Context,”](#) on page 386.

41.3.1 Installing Identity Manager Home

NetIQ provides a wizard to guide you through the process for installing Home and the Provisioning Dashboard in your Identity Manager environment. You install must Home on the same servers where you installed RBPM, the User Application, and the Reporting Module.

NOTE: If you are installing Identity Manager Home in a JBoss cluster environment, this section assumes that the cluster has already been configured for the User Application. For more information, see [Section 27.2, “Preparing a JBoss Cluster for the User Application,” on page 222.](#)

To install Identity Manager Home:

- 1 Download the Updater files to your User Application server.
- 2 Stop the JBoss application server.
- 3 At a command prompt, navigate to the directory where you downloaded the installation files and enter the following command:

```
./IdmHPD.bin
```

NOTE: You might need to modify the `IdmHPD.bin` file to allow you to execute the file as a program.

- 4 Click **Next**.
- 5 Review and accept the license agreement, then click **Next**.
- 6 Specify the location of the `hpd-conf-runtime-Version.zip` file, then click **Next**.
- 7 Specify whether the User Application, Identity Reporting Module, or both are installed in your environment and click **Next**.
- 8 (Conditional) If you have the `install.properties` file on your User Application server, specify the location, then click **Next**.
- 9 (Conditional) If you do not have your User Application `install.properties` file, complete the following steps:
 - 9a Clear **Load Properties**, then click **Next**.
 - 9b Specify the configuration information for your installation in the subsequent windows.
- 10 Specify the default backup directory to use, then click **Next**.
- 11 Click **Install**, then click **Done** when finished.
- 12 At a command prompt, navigate to the `IDMProv/tmp` directory and enter the following command:

```
rm -rf *
```
- 13 Navigate to the `IDMProv/work/jboss.web` directory and enter the following command:

```
rm -rf *
```
- 14 (Conditional) To enable clustering, complete the following steps:

NOTE: These steps assume that you used the default RBPM path and driver context for the User Application driver: `cn=User Application Driver,cn=driverset1,o=system`.

- 14a Log on to iManager.
- 14b Browse to the location for `configuration.AppDefs.AppConfig.User Application.Driver.driverset1.system`.
- 14c Edit the `XMLData` attribute to find and set the `com.netiq.idm.cis.clustered` property to `true`. For example:

```
<key>com.netiq.idm.cis.clustered</key>
<value>true</value>
</property>
<property>
```

- 14d Optional) Change the value for `com.netiq.idm.cis.groupId`, which represents the JGroups group ID used for permission index distribution. The default value is `com.netiq.idm.cis.groupId`.
- 14e Save your changes, then close the editor.
- 14f Ensure that you use the same OSP settings for each User Application in the cluster. For more information, see the following sections:
 - ♦ [Section 42.5.3, “Modifying SSO Clients and Authentication Settings with the RBPM Configuration Utility,” on page 399](#)
 - ♦ [Section 42.4.1, “Creating a Keystore for One SSO Provider,” on page 394](#)
- 15 (Conditional) If you do not use the default `IDMProv` context for the User Application, complete the steps for updating the content of the `.war` file. For more information, see [Section 41.3.2, “Updating User Application Files in an Environment that Uses a Non-Default Context,” on page 386](#).
- 16 Configure your Identity Manager environment to work with Identity Manager Home. For more information, see [Chapter 42, “Configuring Your Identity Manager Environment for Identity Manager Home,” on page 389](#).

41.3.2 Updating User Application Files in an Environment that Uses a Non-Default Context

The name of the `.war` file for the User Application matches the context that you specified when you installed RBPM. By default, the name is `IDMProv.war`. If you specified a non-default context for RBPM, such as `IDMStartHere`, the name of the file would be `IDMStartHere.war`. The contents of the file also reference the context name. When you install Identity Manager Home, the process places an `IDMProv.war` file in the User Application folder. If you used a non-default context for your User Application URL, you must modify the content of the `.war` file to work with your customized environment.

- 1 At a command prompt, navigate to the JBoss deploy directory. For example, `/opt/novell/idm/jboss/server/IDMProv/deploy`.
- 2 Rename the `IDMProv.war` file in the directory to match the context name for your environment. For example, change the file name to `IDMStartHere.war` from `IDMProv.war`.
- 3 To update the `WEB-INF/web.xml` file, complete the following steps:

- 3a Enter the following command:

```
unzip IDMContext.war WEB-INF/web.xml
```

where `IDMContext` is your customized name of the `IDMProv.war` file.

- 3b In a text editor, open the `WEB-INF/web.xml` file.
- 3c In the `web.xml` file, find the following entry:

```
<display-name>IDMProv</display-name>
```

- 3d Change the `IDMProv` value to match your context name.
- 3e Save and close the file.
- 3f Enter the following command to archive the file:

```
zip -u0 IDMContext.war WEB-INF/web.xml
```

- 4 To update the `config.xml` file, complete the following steps:
 - 4a Enter the following command:

```
unzip IDMContext.war WEB-INF/lib/IDMfw.jar
```

4b Navigate to the `WEB-INF/lib` directory, then enter the following command:

```
unzip IDMfw.jar PortalService-conf/config.xml
```

4c In a text editor, open the `WEB-INF/lib/PortalService-conf/config.xml` file.

4d In the `config.xml` file, find the following entry:

```
<key>portal.context</key>  
<value>${portal.context:IDMProv}</value>
```

4e Change the `IDMProv` value to match your context name.

4f Save and close the file.

4g In the command prompt window, navigate to the `WEB-INF/lib` directory, then enter the following command:

```
zip -u0 IDMfw.jar PortalService-conf/config.xml
```

4h In the command prompt window, navigate to the `deploy` directory, then enter the following command:

```
zip -u0 IDMContext.war WEB-INF/lib/IDMfw.jar
```

5 Delete the `WEB-INF` directory.

6 Close the command prompt.

42 Configuring Your Identity Manager Environment for Identity Manager Home

Before using Identity Manager Home, you must configure other Identity Manager components to ensure that they can interact with Identity Manager Home.

42.1 Checklist for Configuring Your Environment for Identity Manager Home

NetIQ recommends that you perform the steps in the following checklist:

	Checklist Items
<input type="checkbox"/>	1. Update the Identity Vault. For more information, see Section 42.2, “Configuring the Identity Vault for Identity Manager Home,” on page 389.
<input type="checkbox"/>	2. Update the auditing and reporting components. For more information, see Section 42.3, “Configuring the Information Warehouse for Identity Manager Home,” on page 391.
<input type="checkbox"/>	3. Update your SSO settings. For more information, see Section 42.4, “Configuring Single Sign-on Access for Identity Manager Home,” on page 394.
<input type="checkbox"/>	4. Update the drivers, database, and authentication settings for RBPM and the User Application. For more information, see Section 42.5, “Configuring RBPM and the User Application for Identity Manager Home,” on page 396.
<input type="checkbox"/>	5. Update the settings for self-service password. For more information, see Section 42.6, “Reconfiguring Forgotten Password Self-Service,” on page 400.

42.2 Configuring the Identity Vault for Identity Manager Home

You must update your Identity Vault to recognize Identity Manager Home. For proper functionality, you must be using the SAML authentication method for eDirectory and have NetIQ Modular Authentication Service (NMAS) client installed. If not, you can install these features as part of the process for configuring the Identity Vault.

For more information about SAML schema, see [Section 30.3.2, “Installing and Configuring SAML Authentication Method,”](#) on page 288. For more information about NMAS, see [Section 9.6, “Installing NMAS Client Software,”](#) on page 104.

- 1 Download the `hpd-conf-vault-4.0.2A.zip` file to your Identity Vault server.
- 2 Extract the contents of the file to a directory on the server.

3 (Conditional) If you have not previously installed the SAML schema and NMAS methods, complete the following steps:

3a In a terminal, navigate to the *ExtractedDirectory/saml* directory, where *ExtractedDirectory* is the location of the extracted *hpd-conf-vault-4.0.2A.zip* files.

3b Enter the following command:

```
unzip nmassaml.zip
```

3c Navigate to the extracted SAML directory.

3d Enter the following command to install the SAML schema:

```
ndssch -h eDirectoryHostIP eDirectoryAdmin authsaml.sch
```

For example:

```
ndssch -h 164.99.99.99 admin.sa.system authsaml.sch
```

Use the following parameters:

eDirectoryHostIP

Represents the IP address of your eDirectory installation.

eDirectoryAdmin

Represents the administrative user account for eDirectory.

3e Enter the password for your administrative user account.

3f To install the NMAS methods, enter the following command:

```
nmasinst -addmethod eDirectoryAdmin TreeName ./config.txt
```

3g Enter the password for your administrative user account.

4 In a terminal, navigate to the *ExtractedDirectory/schema* directory.

5 Enter the following commands:

```
unzip osp-sch.zip
```

```
ndssch -h eDirectoryHostIP eDirectoryAdmin osp.sch
```

6 Enter the password for your administrative user account.

7 To stop eDirectory, enter the following command on the server command line:

```
/etc/init.d/ndsd stop
```

8 Move the following files from the eDirectory *classes* directory to the */tmp* directory:

- ◆ *nrfdriver.jar*

- ◆ *srvprvUAD.jar*

NOTE: The location of the *classes* directory depends on your installation. The default location is */opt/novell/eDirectory/lib/dirxml/classes*.

9 Copy the following files from the *classes* subdirectory of the extracted *hpd-conf-vault-4.0.2A.zip* directory to the eDirectory *classes* directory:

- ◆ *nrfdriver.jar*

- ◆ *srvprvUAD.jar*

10 To restart eDirectory, enter the following command:

```
/etc/init.d/ndsd start
```

42.3 Configuring the Information Warehouse for Identity Manager Home

If you want to log events for or run reports from the Identity Manager Home page, you must update EAS and the Reporting Module to recognize Identity Manager Home.

42.3.1 Configuring the Event Auditing System for Identity Manager Home

If you have Reporting configured in your Identity Manager environment, you must configure the Event Auditing Service (EAS) to function properly with Identity Manager Home and the Provisioning Dashboard.

- 1 Download the `hpd-conf-eas-version.zip` file to the server where you installed EAS.
- 2 Extract the contents of the file to a directory on the server.
- 3 To stop the EAS service, enter the following command in a terminal:

```
/etc/init.d/sentinel_eas stop
```

- 4 In the terminal, navigate to the `ExtractedDirectory/eas` directory.
- 5 Enter the following command:

```
./update_selfextract.sh
```

- 6 Restart the EAS service.

42.3.2 Updating the WAR File for Event Auditing Service

If you have Reporting configured in your Identity Manager environment, you must update the IP address for the EAS server in the `easwebstart.war` file.

- 1 Log on to the server where you deployed the User Application.
- 2 In a command prompt, navigate to the User Application deploy directory within the JBoss installation. For example, `/opt/novell/idm/jboss/server/IDMProv/deploy`.
- 3 Enter the following command:

```
unzip easwebstart.war WEB-INF/web.xml
```

- 4 In a text editor, open the `web.xml` file.
- 5 Set the `EAS_SERVER_IP` parameter to one of the following values:

- ♦ `localhost`
- ♦ IP address of the server where you installed EAS

- 6 Save and close the `web.xml` file.
- 7 In the command prompt, enter the following commands:

```
zip -u0 easwebstart.war WEB-INF/web.xml  
rm -rf WEB-INF/
```

42.3.3 Configuring the Data Collection Services Driver for OAuth Protocol with Identity Manager Home

For Identity Manager Home and the Provisioning Dashboard to function properly with the Identity Reporting Module, you must configure the Data Collection Service (DCS) driver to support the OAuth protocol.

NOTE

- You only need to install and configure the Data Collection Service Driver if you use the Identity Reporting Module in your environment.
- If you have multiple Data Collection Service Drivers configured in your environment, you must complete the following steps for each driver.

-
- 1 Log on to Designer.
 - 2 (Conditional) If you have not yet updated Designer to the appropriate patch supporting Identity Manager Home, such as AU4a, complete the following steps:

NOTE: For more information about software requirements, see the [Release Notes for Identity Manager Home \(https://www.netiq.com/documentation/idm402/idmhome-releasenotes/data/idmhome-releasenotes.html\)](https://www.netiq.com/documentation/idm402/idmhome-releasenotes/data/idmhome-releasenotes.html).

-
- 2a Select **Help > Check for Designer Updates**.
 - 2b Select **Yes** to update Designer.
 - 2c Select **OK**.
- 3 Open your project in Designer.
 - 4 (Conditional) If your project does not already include a Data Collection Service driver, import the driver into your project. For more information, see [Chapter 25, "Creating the Drivers for the Roles Based Provisioning Module," on page 213](#).
 - 5 (Conditional) If you have not already upgraded your DCS driver to the supported patch version, complete the following steps:
 - 5a Download the latest DCS driver patch file.
 - 5b Extract the patch file to a location on your server.
 - 5c In a terminal, navigate to the location of the extracted patch RPM for your environment and run the following command:

```
rpm -Uvh novell-DXMLdcs.rpm
```
 - 5d Restart eDirectory.
 - 5e In Designer, ensure that you have installed a supported version of the Data Collection Service Base package. If necessary, install the latest version before continuing. For more information about software requirements, see the [Release Notes for Identity Manager Home \(https://www.netiq.com/documentation/idm402/idmhome-releasenotes/data/idmhome-releasenotes.html\)](https://www.netiq.com/documentation/idm402/idmhome-releasenotes/data/idmhome-releasenotes.html).
 - 5f Redeploy and restart the DCS driver in Designer.
 - 6 In the *Outline* view, right-click the DCS driver, then select **Properties**.
 - 7 Click **Driver Configuration**.
 - 8 Click the **Driver Parameters** tab.
 - 9 Click **Show connection parameters**, then select **show**.

- 10 Click **SSO Service Support**, then select **Yes**.
- 11 Specify the IP address and port for the Reporting Module.
- 12 Specify a password for the SSO Service Client. The default password is `driver`.
- 13 Click **Apply**, then click **OK**.
- 14 In the *Modeler* view, right-click the DCS driver, then select **Driver > Deploy**.
- 15 Click **Deploy**.
- 16 If prompted to restart the DCS driver, click **Yes**.
- 17 Click **OK**.

42.3.4 Reconfiguring Auditing and Logging

This section assumes that you previously enabled Auditing or logging (Reporting Module) in your environment. Before starting the application server, you must reconfigure Auditing and logging.

When install Identity Manager Home, the process replaces your logging configuration files for the User Application and Reporting Module (if installed). The utility sets all logging settings back to the default configuration when the User Application or Reporting Module were first installed. In addition, the utility disables Auditing by default.

NOTE: Do not enable Auditing unless you have configured your environment as outlined in “[Setting Up Logging](#)” in the *User Application: Administration Guide*.

- 1 (Conditional) If you have the Reporting Module installed and Auditing enabled, complete the following steps:
 - 1a Navigate to the location of the logging configuration files within the JBoss installation, located by default at `/opt/novell/idm/jboss/server/IDMProv/conf/`.
 - 1b Using a text editor, open the first `idmrptNAME_logging.xml` file.
 - 1c Under `<appender-ref ref="NAUDIT"/>`, uncomment the following entries:


```
<logger additivity="true" name="com.novell" level="INFO">
<logger additivity="true" name="com.netiq" level="INFO">
```
 - 1d Save and close the file.
 - 1e Repeat these steps for each `idmrptNAME_logging.xml` file.
- 2 In a command prompt, enter the following command:


```
/etc/init.d/jboss_init start
```
- 3 In the JBoss log, verify that the server started completely and address any issues or errors.
- 4 To verify that you have configured the SSL Controller correctly, look for the following entry in the `server.log` file:


```
INFO [com.novell.common.auth.saml.AuthTokenGenerator] (main) [RBPM] SSO
Framework is enabled
```
- 5 Using a Web browser, log on to your User Application server as the User Application administrator.
- 6 Click **Administration**, then **Application Configuration**.
- 7 Click **Logging**.

8 Select **Enable audit service**, then click **Submit**.

9 Log out of the User Application.

42.4 Configuring Single Sign-on Access for Identity Manager Home

To use Identity Manager Home and the Provisioning Dashboard, you must configure a single sign-on process (SSO). To create an SSO process, you must use One SSO Provider (OSP). You must create a keystore and then configure eDirectory for single sign-on access.

NOTE: After you configure and enable SSO in your Identity Manager environment, users can no longer access the User Application as a guest or anonymous user. Users are instead prompted to log on to the user interface.

42.4.1 Creating a Keystore for One SSO Provider

To enable single sign-on access, you must create a Java KeyStore (JKS) file for OSP, with the following considerations:

- ♦ For *PublicServerName*, specify a “public” URL or IP address for clients to access your environment. Do not specify an internal host name or IP address.
- ♦ In a distributed or clustered environment, specify a URL that drives client access through your L4 switch or load balancer. The *osp.war* and configuration files must be on each deployment in the environment. Use the same Keystore file for all deployments.

Enter the following command at a command prompt:

```
/JDK_Path/jre/bin/keytool -genkey -keyalg RSA -keysize 2048 -keystore  
JBoss_Installation_Path/server/IDMProv/conf/osp.jks -storepass Keystore_Password -  
keypass Key_Password -alias osp -dname 'cn=PublicServerName'
```

For example:

```
/opt/novell/idm/jdk1.7.0_21/jre/bin/keytool -genkey -keyalg RSA -keysize 2048 -  
keystore /opt/novell/idm/jboss/server/IDMProv/conf/osp.jks -storepass n0v3ll -  
keypass n0v3ll -alias osp -dname 'cn=test.yourcompany.com'
```

42.4.2 Configuring Single Sign-on Settings

Identity Manager uses a single sign-on process to provide authentication between the User Application, Identity Manager Home, and the Identity Manager Provisioning Dashboard.

NOTE: This procedure assumes that your environment will use one certificate for eDirectory, the SSO controller, and the OAuth Provider. If your organization requires additional layers of separation, create a separate certificate for the OAuth Provider.

1 Start your JBoss server.

2 Create the certificates and keys necessary for single sign-on.

For information about creating certificates and keys for single sign-on, see the following sections:

- ♦ [Section 42.4.1, “Creating a Keystore for One SSO Provider,” on page 394](#)
- ♦ [“Creating the Certificates” in the *User Application: Administration Guide*.](#)

3 Configure your eDirectory installation for single sign-on.

For information about configuring eDirectory for single sign-on, see [“Configuring eDirectory”](#) in the *User Application Administration Guide*.

NOTE: If you previously extended the eDirectory schema to include the SAML schema and installed the required NMAS methods, as described in [“Configuring the Identity Vault for Identity Manager Home” on page 389](#), you do not need to perform those steps a second time. Instead, skip to the subsection about creating the Trusted Root Container.

4 Using a Web browser, log on to your User Application server as the User Application administrator.

5 Configure the SSO controller.

For information, see [“Configuring the SSO Controller”](#) in the *User Application: Administration Guide*.

IMPORTANT: Do not restart the application server as instructed in the *User Application: Administration Guide*.

6 To verify that you have configured the SSL Controller correctly, look for the following entry in the `server.log` file:

```
INFO [AuthTokenGenerator] [RBPM] SSO Framework is enabled
```

7 On the User Application Single Sign On (SSO) page, verify that the SSO Providers list includes the OAuth provider.

8 Confirm that **Enable Single Sign On (SSO) To User Application** is selected, then select **OAuth**.

9 For **Expiration Interval**, specify the number of seconds that Identity Manager keeps the OAuth SSO header alive. For example, specify 300 seconds.

10 Select **Distinguished Name**.

11 (Conditional) If not already configured, specify the signing certificate and signing key, and then provide the signing key password.

NOTE: The signing key should be a PKCS8 format key.

12 Select **Save**.

13 Select the OAuth provider and select **Enable**, then click **Enable** to confirm.

14 Verify that the SSO Providers list displays a green check in the Status column for the OAuth provider.

- 15 Close your browser without logging out of the User Application.
- 16 Stop your JBoss server.

42.5 Configuring RBPM and the User Application for Identity Manager Home

Before using Identity Manager Home, you must update the driver and the database schema for the User Application. You must also run the RBPM Configuration Utility to modify settings for Authentication and SSO Clients.

42.5.1 Updating the User Application Driver Package for Identity Manager Home

After you install the Identity Manager Home files on your User Application server, you must update the existing User Application package in your environment. The `hpd-conf-designer-version.zip` file in the installation package allows you to update the User Application driver from your Designer project.

For more information about managing packages in Designer, see “[Managing Packages](#)” in the *Designer 4.0.2 for Identity Manager 4.0.2 Administration Guide*.

- 1 Download the `hpd-conf-designer-version.zip` file to the server where Designer is installed.
- 2 Extract the contents of the ZIP file to a directory on the server.
- 3 Log on to Designer.
- 4 (Conditional) If you have not yet updated Designer to the appropriate patch supporting Identity Manager Home, such as AU4a, complete [Step 2 on page 392](#).

NOTE: For more information about software requirements, see the [Release Notes for Identity Manager Home \(https://www.netiq.com/documentation/idm402/idmhome-releasenotes/data/idmhome-releasenotes.html\)](https://www.netiq.com/documentation/idm402/idmhome-releasenotes/data/idmhome-releasenotes.html).

- 5 Open your project in Designer.
- 6 (Conditional) If your project does not already include a User Application driver, import the driver into your project. For more information, see [Chapter 25, “Creating the Drivers for the Roles Based Provisioning Module,” on page 213](#).
- 7 In the *Outline* view, right-click **Package Catalog**, then select **Import Package**.
- 8 Click **Browse**.
- 9 Navigate to the directory where you extracted the `hpd-conf-designer-version.zip` file.
- 10 Open the `designer` directory and select `NOVLUABASE_3.0.0.20131213110230.jar`, then click **OK**.
- 11 In the Select Package window, select version 3.0.0.20131213110230 of the User Application Base package (`NOVLUABASE`) and click **OK**.
- 12 After Designer imports the package, click **OK**.
- 13 Right-click **Package Catalog** and select **Import Package**.
- 14 Clear **Show Base Packages Only**.
- 15 In the Select Package window, find and select version 2.0.0.20130322140144 of the **Provisioning Notification Templates** package.

NOTE: If the window does not display version 2.0.0.20130322140144 of the **Provisioning Notification Templates** package, click **Cancel** and skip to [Step 17](#).

- 16 Click **OK**, then click **OK** again.
- 17 In the *Outline* view, right-click the User Application driver and select **Properties**.
- 18 Click **Packages**.
- 19 Click **Select Operation** for the User Application Base package and select **Upgrade**.
- 20 Select version **3.0.0.20131213110230** and click **OK**.
- 21 (Conditional) If prompted to upgrade Provisioning Notification Templates, click **OK**.
- 22 Click **Apply**.
- 23 Verify the information in the Package Installation Wizard window and click **Next**.
- 24 Click **Finish**, then click **OK**.
- 25 In the Modeler, right-click the User Application driver and select **Driver > Deploy**.
- 26 Click **Deploy**.
- 27 If prompted to restart the User Application driver, click **Yes**.
- 28 Click **OK**.

42.5.2 Configuring the User Application Database for Identity Manager Home

To install Identity Manager Home, you must modify the existing User Application database schema.

NOTE

- ◆ You can also update the PostgreSQL schema manually using a SQL script. However, you should only use the SQL script to update the schema in the following situations:
 - ◆ Your organization requires that users make all database updates using scripts.
 - ◆ When you installed RBPM, you used the SQL script option to create or update the User Application tables.

For information about updating the PostgreSQL schema using a SQL script, see [“Configuring a PostgreSQL Database” on page 397](#).

- ◆ If you use a database other than PostgreSQL, see [“Configuring Non-PostgreSQL Databases” on page 398](#).
-

Configuring a PostgreSQL Database

NetIQ recommends starting JBoss to automatically update the PostgreSQL database schema. This section walks you through the process for starting your JBoss application server.

- 1 On the computer where you installed JBoss, navigate to the User Application deploy directory. For example: `/opt/novell/idm/jboss/server/IDMProv/deploy`.
- 2 In the `deploy` directory, use a text editor to open the `IDMProv-ds.xml` file.

NOTE: If you specified a different context than `IDMProv` for the User Application URL, the file might be named to match your context. For example, `IDMStartHere-ds.xml`.

- 3 In the `<connection-url>` element, append `?compatible=true` to the existing text. For example:

```
<connection-url>jdbc:postgresql://localhost:5432/
idmuserappdb?compatible=true</connection-url>
```

- 4 Save and close the file.
- 5 In a command prompt, enter the following command:

```
/etc/init.d/jboss_init start
```

- 6 To verify that the server started completely and address any issues or errors, check the JBoss log.

NOTE: JBoss might log an error regarding the OSP keystore. This error occurs when you have not yet configured SSO in your Identity Manager Home environment. You can ignore the error.

Configuring Non-PostgreSQL Databases

This section provides instructions for updating the schema for the User Application database running on the following platforms:

- ♦ Microsoft SQL Server 2008
- ♦ MySQL 5.1
- ♦ Oracle 11g

To update the schema for the User Application database:

- 1 In a command prompt, navigate to the Identity Manager deploy directory and enter the following command:

```
unzip IDMProv.war WEB-INF/classes/hibernate.cfg.xml
```

NOTE: If you specified a different context than `IDMProv` for the User Application URL, the name of the `.war` file matches your specified context. For example, `IDMStartHere.war`.

- 2 In a text editor, open the `WEB-INF/classes/hibernate.cfg.xml` file.
- 3 In the `hibernate.cfg.xml` file, find the `dialect` property.
- 4 Update the value of the `dialect` property for your database, as follows:
 - ♦ **Microsoft SQL Server 2008** `com.netiq.persist.SQLServerDialect`
 - ♦ **MySQL 5.1** `com.netiq.persist.MySQL5InnoDBDialect`
 - ♦ **Oracle 11g** `com.netiq.persist.Oracle10gDialect`

- 5 Save and close the file.
- 6 In the command prompt, enter the following command:

```
zip -u0 IDMProv.war WEB-INF/classes/hibernate.cfg.xml
```

- 7 Delete the `WEB-INF` directory and all its contents, if you have not previously deleted the file.

42.5.3 Modifying SSO Clients and Authentication Settings with the RBPM Configuration Utility

Before using Identity Manager Home, you must configure the Authentication and SSO Clients settings in the RBPM Configuration Utility, `configupdate.sh`.

- 1 Using a text editor, open the `configupdate.sh` file, located by default in the User Application installation directory: `/opt/novell/idm`.

- 2 In `configupdate.sh`, ensure that the following options are configured correctly:

```
-edit_admin true  
  
-use_console false
```

NOTE: You should configure the value of `-use_console` to be `true` only if you want to run the utility in console mode.

- 3 Save and close `configupdate.sh`.
- 4 At the command prompt, enter the following command to run the configuration utility:

```
./configupdate.sh
```

NOTE: You might need to wait a few minutes for the utility to start up.

- 5 Click **Authentication**.
- 6 (Conditional) To specify the actual server DNS name or IP address, change all instances of `localhost`.
 - ◆ The specified address must be resolvable from all clients. Use `localhost` only if all access to Identity Manager Home and the Provisioning Dashboard will be local, including access through a browser.
 - ◆ This “public” host name or IP address should be the same as the value of `PublicServerName` that you specified in [“Creating a Keystore for One SSO Provider” on page 394](#).
 - ◆ In a distributed or clustered environment, all of the OAuth URLs should be the same value. The URL should drive client access through your L4 switch or load balancer. Also, the `osp.war` and configuration files must be installed on each deployment in the environment.
- 7 For **LDAP DN of Admins Container**, click the **Browse** button, then select the container within the Identity Vault that contains your User Application administrator.
- 8 Specify the OAuth keystore file that you created in [“Creating a Keystore for One SSO Provider” on page 394](#). Include the keystore file path, keystore file password, key alias, and key password.

The default keystore file is `osp.jks`, and the default key alias is `osp`.

- 9 Click **SSO Clients**.
- 10 (Conditional) To specify the actual server DNS name or IP address, change all instances of `localhost`.
 - ◆ The specified address must be resolvable from all clients. Use `localhost` only if all access to Identity Manager Home and the Provisioning Dashboard will be local, including access through a browser.

- ◆ This “public” host name or IP address should be the same as the value of *PublicServerName* that you specified in [“Creating a Keystore for One SSO Provider”](#) on page 394.
 - ◆ In a distributed or clustered environment, all of the OAuth redirect URLs should be the same value. The URL should drive client access through your L4 switch or load balancer.
- 11 (Conditional) If you use non-default ports, update the port numbers for the following Identity Manager components:
- ◆ Catalog Administrator
 - ◆ Identity Manager Home
 - ◆ Provisioning Dashboard
 - ◆ Reporting Module
 - ◆ User Application
- 12 Click **OK** to save your changes.

42.6 Reconfiguring Forgotten Password Self-Service

This section assumes that you previously deployed and configured the WAR file for forgotten-password management in your environment.

When you install Identity Manager Home, the process replaces the WAR file, *IDMPwdMgt.war*, with a newer version. You must update the new version of the file for your environment. For more information about configuring the WAR file, see [“Configuring Forgotten Password Self-Service”](#) in the *User Application Administration Guide*.

NOTE: If you deployed the *IDMPwdMgt.war* file on a separate server, copy the new file to that server, then update as described in the *User Application Administration Guide*.

43 Verifying Installation of Identity Manager Home

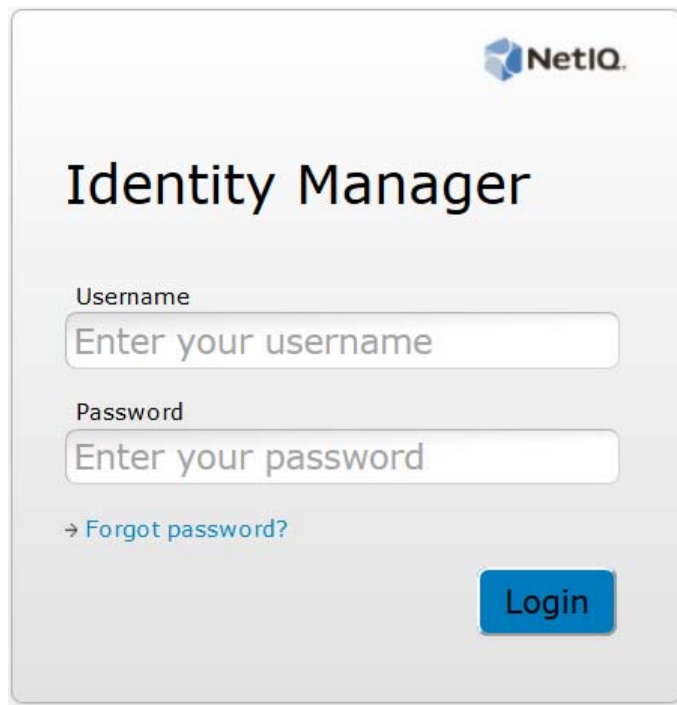
After you install Identity Manager Home and configure Identity Manager, you should verify that you can log on to both Identity Manager Home and the User Application.

To log on separately for the User Application and Identity Manager Home, you must enable single sign-on (SSO) authentication in your Identity Manager environment. Also, after you configure the SSO settings, users cannot access the User Application as a guest or anonymous user. For more information, see [Section 42.4, “Configuring Single Sign-on Access for Identity Manager Home,”](#) on page 394.

- 1 In a new browser window on your User Application server, enter the URL for Identity Manager Home:

`http://server:8180/landing`

Do not log on to Identity Manager Home. However, ensure that the login page looks like the image below.



- 2 In your browser, navigate to the User Application:

`http://server:8180/IDM-context`

- 3 Verify that the User Application displays the same login page as shown in [Step 1](#).

- 4 Log on to the User Application.
- 5 In the top right corner, click the **Home** icon and verify that you can access Identity Manager Home without logging in again.

44 Installing Analyzer

This section guides you through the process of installing the required components for Analyzer. The installation files are located in the `products/Analyzer/` directory within the `.iso` image file for the Identity Manager installation package. By default, the installation program installs the components in the following locations:

- ♦ **Linux:** `home/admin/analyzer`
- ♦ **Windows:** `C:\Novell\Analyzer`

NetIQ recommends that you review the installation process before beginning. For more information, see [Chapter 15, “Checklist for Installing iManager,” on page 147](#).

44.1 Checklist for Installing Analyzer

Before beginning the installation process, NetIQ recommends that you review the following steps.

	Checklist Items
<input type="checkbox"/>	1. Learn about the interaction among Identity Manager components. For more information, see Chapter 1, “Understanding the Architecture of Identity Manager,” on page 21 .
<input type="checkbox"/>	2. Ensure that your environment meets the considerations and requirements for hosting Analyzer. For more information, see Section 6.11, “Prerequisites and Requirements for Installing Analyzer,” on page 86 .
<input type="checkbox"/>	3. To install Analyzer, see the following sections: <ul style="list-style-type: none">♦ To use the installation wizard, see Section 44.2, “Using the Wizard to Install Analyzer,” on page 404.♦ For a silent installation, see Section 44.3, “Installing Analyzer Silently,” on page 404
<input type="checkbox"/>	4. (Optional) To automatically receive and display audit events from Analyzer, install the XDAS client. For more information, see Section 44.5, “Installing an Audit Client for Analyzer,” on page 406 .
<input type="checkbox"/>	5. To activate Analyzer, see Section 45.4.2, “Activating Analyzer,” on page 409 .
<input type="checkbox"/>	6. (Optional) To upgrade Analyzer, see Section 47.5.5, “Upgrading Analyzer,” on page 432 .

44.2 Using the Wizard to Install Analyzer

The following procedure describes how to install Analyzer on a Linux or Windows platform using an installation wizard, either in the GUI format or from the console. To perform a silent, unattended installation, see [Section 44.3, “Installing Analyzer Silently,” on page 404](#).

To prepare for the installation, review the prerequisites and system requirements listed in [Section 44.1, “Checklist for Installing Analyzer,” on page 403](#).

- 1 Log on as `root` or an administrator to the computer where you want to install Analyzer.
- 2 (Conditional) If you have the `.iso` image file for the Identity Manager installation package, navigate to the directory containing the Analyzer installation files, located by default in the `products/Analyzer/` directory.
- 3 (Conditional) If you downloaded the Analyzer installation files, complete the following steps:
 - 3a Navigate to the `.tgz` or `win.zip` file for the downloaded image.
 - 3b Extract the contents of the file to a folder on the local computer.
- 4 From the `products/Analyzer/` directory, execute the installation program:
 - 4a **Linux:** `./install.bin`
 - 4b **Windows:** `install.exe`
- 5 Follow the instructions in the wizard until you finish installing Analyzer.
- 6 When the installation process completes, review the post-installation summary to verify the installation status and the location of the log file for Analyzer.
- 7 Click **Done**.
- 8 (Conditional) On Linux computers, complete the steps in [Section 44.4, “Adding XULrunner to Analyzer.ini on Linux Platforms,” on page 405](#).
- 9 (Optional) To configure role-based services for Analyzer on the Windows computer, open the link to the `gettingstarted.html` Web page, located by default in the `C:\Program Files (x86)\Novell\Tomcat\webapp\nps\help\en\install` directory.
You use iManager to configure the role-based services.
- 10 To activate Analyzer, see [Section 45.4.2, “Activating Analyzer,” on page 409](#).

44.3 Installing Analyzer Silently

A silent (non-interactive) installation does not display a user interface or ask the user any questions. Instead, `InstallAnywhere` uses information from a default `analzerInstaller.properties` file. You can run the silent installation with the default file or edit the file to customize the installation process.

By default, the installation program installs Analyzer in the `Program Files (x86)\Novell\Analyzer` directory.

- 1 Log on as `root` or an administrator to the computer where you want to install Analyzer.
- 2 (Conditional) If you have the `.iso` image file for the Identity Manager installation package, navigate to the directory containing the Analyzer installation files, located by default in the `products/Analyzer/` directory.
- 3 (Conditional) If you downloaded the Analyzer installation files from the [Novell Downloads Web site \(http://download.novell.com\)](http://download.novell.com), complete the following steps:
 - 3a Navigate to the `.tgz` or `win.zip` file for the downloaded image.
 - 3b Extract the contents of the file to a folder on the local computer.

- 4 (Optional) To specify a non-default installation path, complete the following steps:
 - 4a Open the `analyzerInstaller.properties` file, located by default in the `products/Analyzer/` directory.
 - 4b Add the following text to the properties file:


```
USER_INSTALL_DIR=installation_path
```
- 5 To run the silent installation, issue one of the following commands:
 - ♦ **Linux:** `install -i silent -f analyzerInstaller.properties`
 - ♦ **Windows:** `install.exe -i silent -f analyzerInstaller.properties`
- 6 (Conditional) On Linux computers, complete the steps in [Section 44.4, “Adding XULrunner to Analyzer.ini on Linux Platforms,”](#) on page 405.
- 7 To activate Analyzer, see [Section 45.4.2, “Activating Analyzer,”](#) on page 409.

44.4 Adding XULrunner to Analyzer.ini on Linux Platforms

Before running Analyzer on a Linux platform, you must change the XULRunner mapping.

NOTE: The recommended version of XULrunner on SLED 11 is 1.9.0.19. On openSUSE 11.4, it is 1.9.0.2. These versions are shipped with the operating systems.

- 1 Navigate to the `Analyzer` installation directory, by default in the following locations:
 - ♦ **Linux:** `home/admin/analyzer`
 - ♦ **Windows:** `C:\Novell\Analyzer`
- 2 Open the `Analyzer.ini` file in the gedit editor.
- 3 Add the following line to the end of the list of the parameters:

```
-Dorg.eclipse.swt.browser.XULRunnerPath=/usr/lib/xulrunner-1.9/
```

For example, the `Analyzer.ini` file should read as follows:

```
-vmargs
-Xms256m
-Xmx1024m
-XX:MaxPermSize=128m
-XX:+UseParallelGC
-XX:ParallelGCThreads=20
-XX:+UseParallelOldGC
-Dorg.eclipse.swt.browser.XULRunnerPath=/usr/lib/xulrunner-1.9/
```

- 4 Save the `Analyzer.ini` file.
- 5 Launch Analyzer.

44.5 Installing an Audit Client for Analyzer

Analyzer includes an XDAS library that automatically generates audit events from the Data Browser editor when you send data updates back to the application. For more information about using the Data Browser editor to update data in the source application, see “[Modifying Data](#)” in the *Analyzer 4.0.2 for Identity Manager Administration Guide*.

To view these audit events, install an XDAS client that can receive the audit events from Analyzer. More information about XDAS is available at the [OpenXDAS Project \(http://openxdas.sourceforge.net\)](http://openxdas.sourceforge.net).

Analyzer includes both a Linux and a Windows XDAS client as part of its download package. However, the installation program for Analyzer does not install the XDAS client.

- 1 Install Analyzer.
- 2 Navigate to the OpenXDAS installation files, located by default in the `products/Analyzer/openxdas/Operating_system` directory of the `.iso` image file.
- 3 Launch the installation program for the XDAS client:
 - ♦ **Linux:** Use the `rpm` command to install the appropriate XDAS client, 32-bit or 64-bit.
 - ♦ **Windows:** Launch the `.msi` file. The Windows client is 32-bit only.
- 4 Follow the prompts to install the XDAS client.
- 5 After the installation process completes, launch the XDAS client to automatically receive and display audit events from Analyzer.


45 Activating Identity Manager

Some Identity Manager components activate automatically the first time that you log on. Other components require a procedure for activation.

45.1 Installing a Product Activation Credential

NetIQ recommends that you use iManager to install the Product Activation Credential.

NOTE: For each driver that you want to use, activate the driver set that has a driver. You can activate any tree with the credential.

- 1 After you purchase a license, NetIQ sends you an e-mail with your Customer ID. The e-mail also contains a link under the Order Detail section to the site where you can obtain your credential. Click the link to go to the site.
- 2 Click the license download link, and then complete one of the following actions:
 - ♦ Open the Product Activation Credential file, then copy the contents of the Product Activation Credential to your clipboard.
 - ♦ Save the Product Activation Credential file.
 - ♦ If you chose to copy the contents, do not include any extra lines or spaces. You should begin copying from the first dash (-) of the credential (----BEGIN PRODUCT ACTIVATION CREDENTIAL) through the last dash (-) of the credential (END PRODUCT ACTIVATION CREDENTIAL-----).
- 3 Log on to iManager.
- 4 Select **Identity Manager > Identity Manager Overview**.
- 5 To select a driver set in the tree structure, click the browse icon (.
- 6 On the **Identity Manager Overview** page, click the driver set that contains the driver that you want to activate.
- 7 On the **Driver Set Overview** page, click **Activation > Installation**.
- 8 Select the driver set where you want to activate an Identity Manager component, and then click **Next**.
- 9 (Conditional) If you saved the Product Activation Credential file in [Step 2](#), specify the saved location.
- 10 (Conditional) If you copied the contents of the Product Activation Credential file in [Step 2](#), paste the contents into the text area.
- 11 Click **Next**.
- 12 Click **Finish**.

45.2 Reviewing Product Activations for Identity Manager and Drivers

For each of your driver sets, you can view the Product Activation Credentials you have installed for the Identity Manager engine server and Identity Manager drivers. You can also remove an activation credential.

NOTE: After installing a valid Product Activation Credential for a driver set, you might still see “Activation Required” next to the driver name. If this is the case, restart the driver. The message should disappear.

- 1 Log on to iManager.
- 2 Click **Identity Manager > Identity Manager Overview**.
- 3 To select a driver set in the tree structure, use the browse icon (🔍) and the search icon (🔎).
- 4 On the **Identity Manager Overview** page, click the driver set for which you want to review activation information.
- 5 On the **Driver Set Overview** page, click **Activation > Information**.

You can view the text of the activation credential or, if an error is reported, you can remove an activation credential.

45.3 Activating Identity Manager Drivers

When you activate the Identity Manager engine, you also activate the following drivers:

Service Drivers	Common Drivers
Data Collection Service	Active Directory
Entitlements Services	ADAM
ID Provider	eDirectory
Loopback Service	GroupWise
Managed System Gateway	LDAP
Manual Task Service	Lotus Notes
Null Service	
Role and Resource Service	
User Application	
WorkOrder	

To activate other Identity Manager drivers, you must purchase additional Identity Manager Integration modules, which might contain one or more drivers. You receive a Product Activation Credential for each Identity Manager Integration module that you purchase. After receiving the credential, perform the procedure listed in [Section 45.1, “Installing a Product Activation Credential,” on page 407](#). For more information about the drivers, see the [Identity Manager Drivers documentation Web site \(http://www.novell.com/documentation/idm36drivers/index.html\)](http://www.novell.com/documentation/idm36drivers/index.html).

45.4 Activating Specific Identity Manager Components

intro

45.4.1 Activating Designer and Role Mapping Administrator

When you activate the Identity Manager engine or the Identity Manager drivers, you also activate Designer and Role Mapping Administrator.

45.4.2 Activating Analyzer

When you launch the Analyzer perspective without a license, Analyzer opens the activation page, from which you can manage Analyzer licenses.

NOTE: If you close the Activation dialog box, Analyzer remains locked until you provide a license to activate it. When you are ready to add a license, click **Activate Analyzer** in the `Project View` to open the Activation dialog bo.

- 1 Launch Analyzer.
- 2 (Conditional) To acquire an Analyzer license, complete the following steps:
 - 2a In the **Analyzer Activation** window, click **Need a license - Novell Customer Care**.
 - 2b Browse to and select the Analyzer license that you received from the NetIQ Customer Care Portal.
 - 2c Copy the activation code, and then close the Customer Care Portal.
- 3 In the **Analyzer Activation** window, click `Add a new license`.
- 4 In the **License** window, type the activation code that you downloaded from the Novell Customer Care Portal, and then click **OK**.
- 5 In the **Analyzer Activation** window, review the details of the license that you just installed.
- 6 Click **OK** to begin using Analyzer.

XI Upgrading or Migrating Identity Manager Manager

This section provides information for upgrading Identity Manager components or migrating existing data to a new server.

46 Preparing to Upgrade or Migrate Identity Manager

This section provides information to help you prepare for upgrading your Identity Manager solution to the latest version. You can upgrade most components of Identity Manager using an executable file, binary file, or in text mode, depending on the target computer. To perform the upgrade, you must download and unzip or unpack the Identity Manager installation kit.

Before beginning, review the differences between an upgrade and a migration.

46.1 Understanding Upgrade and Migration

When you want to install a newer version of an existing Identity Manager installation, you usually perform an **upgrade**. However, when the new version of Identity Manager does not provide an upgrade path for your existing data, you must perform a migration. NetIQ defines **migration** as the process for installing Identity Manager on a new server, then migrating the existing data to this new server.

In general, you can upgrade Identity Manager 3.5 and later to Identity Manager 4.0.2 Standard and Advanced Editions. However, in some cases you cannot perform an upgrade. For example:

- ♦ **Unsupported OS:** If you previously installed Identity Manager on a server running an operating system that is not supported by Identity Manager 4.0.2, you must perform a migration instead of an upgrade.
- ♦ **Identity Manager 3.0.x:** If you currently have Identity Manager 3.0.x, you cannot perform a direct upgrade. You can perform one of the following options:
 - ♦ Upgrade to Identity Manager 3.5.x. Upgrade to eDirectory 8.8 SP7. Then upgrade to Identity Manager 4.0.2.
 - ♦ Perform a migration to a new server.
- ♦ **Roles Based Provisioning Module (RBPM):** If the current version of Identity Manager is 3.5.x or 3.6.x with RBPM installed, you cannot upgrade. You must perform a migration. For more information see the [Identity Manager RBPM and Repeating Migration Guide](#).

If you have multiple servers associated with a driver set, you can perform an upgrade or a migration on one server at a time. If you do not have time to upgrade the servers at the same time, the drivers continue to work with the different versions of Identity Manager until the upgrades for each server can be completed.

The Identity Manager engine is backward compatible, so the Identity Manager 4.0.2 engine can run Identity Manager 3.6.x drivers without problems.

IMPORTANT: If you enable features for drivers that are supported only on Identity Manager 4.0 or later, the drivers stop working on the servers with mixed versions. The older engines cannot handle the new functionality. This breaks the drivers until all servers are upgraded to Identity Manager 4.0 or later.

46.2 Backing Up the Current Configuration

Before upgrading, NetIQ recommends that you back up the current configuration of your Identity Manager solution. There are no additional steps required if you are using the User Application. All User Application configuration is stored in the User Application driver. You can create the backup in the following ways:

- ♦ [Section 46.2.1, “Exporting the Designer Project,” on page 414](#)
- ♦ [Section 46.2.2, “Exporting the Configuration of the Drivers,” on page 415](#)

46.2.1 Exporting the Designer Project

A Designer project contains the schema and all driver configuration information. Creating a project of your Identity Manager solution allows you to export all of the drivers in one step instead of creating a separate export file for each driver.

- ♦ [“Exporting the Current Project” on page 414](#)
- ♦ [“Creating a New Project from the Identity Vault” on page 414](#)

Exporting the Current Project

If you already have a Designer project, verify that the information in the project is synchronized with what is in the Identity Vault:

- 1 In Designer, open your project.
- 2 In the Modeler, right-click the Identity Vault, then select **Live > Compare**.
- 3 Evaluate the project and reconcile any differences, then click **OK**.

For more information, see [“Using the Compare Feature When Deploying”](#) in the *Designer 4.0.2 for Identity Manager 4.0.2 Administration Guide*.

- 4 On the toolbar, select **Project > Export**.
- 5 Click **Select All** to select all resources to export.
- 6 Select where to save the project and in what format, then click **Finish**.

Save the project in any location, other than the current workspace. When you upgrade to Designer, you must create a new workspace location. For more information, see [“Exporting a Project”](#) in the *Designer 4.0.2 for Identity Manager 4.0.2 Administration Guide*.

Creating a New Project from the Identity Vault

If you do not have a Designer project of your current Identity Manager solution, you must create a project to back up your current solution.

- 1 Install Designer 4.0.2.
You can create an Identity Manager 3.6.x project with Designer 4.0.2. For more information, see [“Installing Designer”](#) in the *Identity Manager 4.0.2 Framework Installation Guide*.
- 2 Launch Designer, then specify a location for your workspace.
- 3 Select whether you want to check for online updates, then click **OK**.
- 4 On the Welcome page, click **Run Designer**.
- 5 On the toolbar, select **Project > Import Project > Identity Vault**.

- 6 Specify a name for the project, then either use the default location for your project or select a different location.
- 7 Click **Next**.
- 8 Specify the Identity Vault connection information:
 - ♦ **Host Name:** Specify the IP address or DNS name of the Identity Vault server.
 - ♦ **User name:** Specify the DN of the user used to authenticate to the Identity Vault.
 - ♦ **Password:** Specify the password of the authentication user.
- 9 Click **Next**.
- 10 Leave the Identity Vault Schema and the Default Notification Collection selected.
- 11 Expand the Default Notification Collection, then deselect the languages you do not need.

The Default Notification Collections are translated into many different languages. You can import all languages or select only the languages that you use.
- 12 Click **Browse**, then browse to and select a driver set to import.
- 13 Repeat [Step 12](#) for each driver set in this Identity Vault, then click **Finish**.
- 14 Click **OK** after the project is imported.
- 15 If you only have one Identity Vault, you are finished. If you have multiple Identity Vaults, proceed with [Step 16](#).
- 16 Click **Live > Import** on the toolbar.
- 17 Repeat [Step 8](#) through [Step 14](#) for each additional Identity Vault.

46.2.2 Exporting the Configuration of the Drivers


Creating an export of the drivers makes a backup of your current configuration. However, Designer currently does not create a backup of the Roles Based Entitlements driver and policies. Use iManager to verify that you have an export of the Roles Based Entitlement driver.

- ♦ [“Using Designer to Export the Driver Configurations” on page 415](#)
- ♦ [“Using iManager to Create an Export of the Driver” on page 415](#)

Using Designer to Export the Driver Configurations

- 1 Verify that your project in Designer has the most current version of your driver. For more information, see [“Importing a Library, a Driver Set, or a Driver from the Identity Vault”](#) in the *Designer 4.0.2 for Identity Manager 4.0.2 Administration Guide*.
- 2 In the Modeler, right-click the driver line of the driver you are upgrading.
- 3 Select **Export to a Configuration File**.
- 4 Browse to a location to save the configuration file, then click **Save**.
- 5 Click **OK** on the results page.
- 6 Repeat [Step 1](#) through [Step 5](#) for each driver.

Using iManager to Create an Export of the Driver

- 1 In iManager, select **Identity Manager > Identity Manager Overview**.
- 2 Browse to and select the location in the tree to search for Driver Set objects, then click the search icon .

- 3 Click the Driver Set object that holds the driver you want to upgrade.
- 4 Click the driver you want to upgrade, then click **Export**.
- 5 Click **Next**, then select **Export all contained policies, linked to the configuration or not**.
- 6 Click **Next**, then click **Save As**.
- 7 Select **Save to Disk**, then click **OK**.
- 8 Click **Finish**.
- 9 Repeat [Step 1](#) through [Step 8](#) for each driver.

46.3 Stopping and Starting Identity Manager Drivers during Upgrade and Migration

When you upgrade or migrate Identity Manager, you need to start and stop the drivers to ensure that the process can modify or replace the correct files. This section includes the following activities:




- ♦ [Section 46.3.1, “Stopping the Drivers,” on page 416](#)
- ♦ [Section 46.3.2, “Starting the Drivers,” on page 417](#)

46.3.1 Stopping the Drivers


Before you upgrade any files, it is important to stop the drivers.


- ♦ [“Using Designer to Stop the Drivers” on page 416](#)
- ♦ [“Using iManager to Stop the Drivers” on page 416](#)

Using Designer to Stop the Drivers

- 1 In Designer, select the Identity Vault  object in the **Outline** tab.
- 2 In the Modeler toolbar, click the **Stop All Drivers** icon .
This stops all drivers that are part of the project.
- 3 Set the drivers to manual start to ensure that the drivers do not start until the upgrade process is complete:
 - 3a Double-click the driver icon  in the **Outline** tab.
 - 3b Select **Driver Configuration > Startup Options**.
 - 3c Select **Manual**, then click **OK**.
 - 3d Repeat [Step 3a](#) through [Step 3c](#) for each driver.

Using iManager to Stop the Drivers

- 1 In iManager, select **Identity Manager > Identity Manager Overview**.
- 2 Browse to and select the location in the tree to search for Driver Set objects, then click the search icon .
- 3 Click the Driver Set object.
- 4 Click **Drivers > Stop all drivers**.
- 5 Repeat [Step 2](#) through [Step 4](#) for each Driver Set object.




- 6 Set the drivers to manual start to ensure that the drivers do not start until the upgrade process is complete:
 - 6a In iManager, select **Identity Manager > Identity Manager Overview**.
 - 6b Browse to and select the location in the tree to search for Driver Set objects, then click the search icon .
 - 6c Click the Driver Set object.
 - 6d In the upper right corner of the driver icon, click **Edit properties**.
 - 6e On the Driver Configuration page under **Startup Options**, select **Manual**, then click **OK**.
 - 6f Repeat [Step 6a](#) through [Step 6e](#) for each driver in your tree.

46.3.2 Starting the Drivers



After all of the Identity Manager components are upgraded, the drivers must be restarted. It is also important to test the drivers after they are running to verify that all of the policies still work.

- ♦ [“Using Designer to Start the Drivers” on page 417](#)
- ♦ [“Using iManager to Start the Drivers” on page 417](#)

Using Designer to Start the Drivers

- 1 In Designer, select the Identity Vault  object in the **Outline** tab.
- 2 Click the **Start All Drivers** icon  in the Modeler toolbar. This starts all of the drivers in the project.
- 3 Set the driver startup options:
 - 3a Double-click the driver icon  in the **Outline** tab.
 - 3b Select **Driver Configuration > Startup Option**.
 - 3c Select **Auto start** or select your preferred method of starting the driver, then click **OK**.
 - 3d Repeat [Step 3a](#) through [Step 3c](#) for each driver.
- 4 Test the drivers to verify the policies are working as designed. For information on how to test your policies, see [“Testing Policies with the Policy Simulator”](#) in *Policies in Designer 4.0.2*.

Using iManager to Start the Drivers

- 1 In iManager, select **Identity Manager > Identity Manager Overview**.
- 2 Browse to and select the location in the tree to search for Driver Set objects, then click the search icon .
- 3 Click the Driver Set object.
- 4 Click **Drivers > Start all drivers** to start all of the drivers at the same time.
or
In the upper right corner of the driver icon, click **Start driver** to start each driver individually.
- 5 If you have multiple drivers, repeat [Step 2](#) through [Step 4](#).
- 6 Set the driver startup options:
 - 6a In iManager, select **Identity Manager > Identity Manager Overview**.
 - 6b Browse to and select the location in the tree to search for Driver Set objects, then click the search icon .

- 6c** Click the Driver Set object.
 - 6d** In the upper right corner of the driver icon, click **Edit properties**.
 - 6e** On the Driver Configuration page, under **Startup Options**, select **Auto start** or select your preferred method of starting the driver, then click **OK**.
 - 6f** Repeat [Step 6b](#) through [Step 6e](#) for each driver.
- 7** Test the drivers to verify the policies are working as designed.
- There is no policy simulator in iManager. To test the policies, cause events to happen that make the policies execute. For example, create a user, modify a user, or delete a user.

47 Upgrading Identity Manager

This section provides information for upgrading Identity Manager components, where the process is not the same as or adds steps to the installation procedure. This section includes the following activities:

- ◆ [Section 47.1, “Checklist for Upgrading Identity Manager,” on page 419](#)
- ◆ [Section 47.2, “Upgrading to a New Version of Advanced Edition,” on page 420](#)
- ◆ [Section 47.3, “Upgrading to Advanced Edition from Standard Edition,” on page 422](#)
- ◆ [Section 47.4, “Upgrading to a New Version of Standard Edition,” on page 424](#)
- ◆ [Section 47.5, “Upgrading Individual Components of Identity Manager,” on page 425](#)
- ◆ [Section 47.6, “Upgrading the Identity Manager Drivers,” on page 433](#)
- ◆ [Section 47.7, “Restoring Custom Policies and Rules to the Driver,” on page 434](#)

47.1 Checklist for Upgrading Identity Manager

To perform the upgrade, NetIQ recommends that you complete the steps in the following checklist.

	Checklist Items
<input type="checkbox"/>	1. Ensure that you have the latest installation kit to upgrade Identity Manager.
<input type="checkbox"/>	2. Learn about the interaction among Identity Manager components. For more information, see Part I, “Introduction,” on page 19 .
<input type="checkbox"/>	3. Ensure that your computers meet the hardware and software prerequisites. For more information, see Chapter 6, “Considerations and Prerequisites for Installation,” on page 45 and the Release Notes for the version to which you want to upgrade.
<input type="checkbox"/>	4. Determine whether you can perform an upgrade versus a migration. For more information, see Section 46.1, “Understanding Upgrade and Migration,” on page 413 .
<input type="checkbox"/>	5. Back up the current project and driver configuration. For more information, see Section 46.2, “Backing Up the Current Configuration,” on page 414 .
<input type="checkbox"/>	6. Perform one of the following procedures: <ul style="list-style-type: none">◆ “Upgrading to a New Version of Advanced Edition” on page 420◆ “Upgrading to Advanced Edition from Standard Edition” on page 422◆ “Upgrading to a New Version of Standard Edition” on page 424◆ “Upgrading Individual Components of Identity Manager” on page 425
<input type="checkbox"/>	7. Update your drivers to the package format. For more information, see Section 47.6, “Upgrading the Identity Manager Drivers,” on page 433 .
<input type="checkbox"/>	8. (Conditional) If you have custom policies and rules, restore your customize settings. For more information, see Section 47.7, “Restoring Custom Policies and Rules to the Driver,” on page 434 .

	Checklist Items
<input type="checkbox"/>	9. Activate your upgraded Identity Manager solution. For more information, see Chapter 45, "Activating Identity Manager," on page 407.
<input type="checkbox"/>	10. (Conditional) If you are using NetIQ Sentinel, ensure that you are running the latest service pack. For more information about upgrading Sentinel, see the NetIQ Sentinel Installation and Configuration Guide .

47.2 Upgrading to a New Version of Advanced Edition

This section helps you upgrade to an Advanced Edition of Identity Manager from the following versions:

- ◆ 4.0.1 Advanced Edition
- ◆ 4.0.1 Standard Edition
- ◆ 3.6.1
- ◆ 3.5.1

To upgrade other versions of Identity Manager, see the following table.

From	To	See
4.0.2 Standard Edition	A new Advanced Edition	Section 47.3, "Upgrading to Advanced Edition from Standard Edition," on page 422
4.01 Standard Edition	A new Standard Edition	Section 47.4, "Upgrading to a New Version of Standard Edition," on page 424

To upgrade to a new version of Advanced Edition:

- 1 Upgrade Designer to the latest version. For more information, see [Section 47.5.1, "Upgrading Designer,"](#) on page 425.
- 2 Create a backup of the current configuration of your Identity Manager solution. For more information, see [Section 46.2, "Backing Up the Current Configuration,"](#) on page 414.
- 3 Install or upgrade iManager to the latest version for Identity Manager. For more information, see one of the following sections:
 - ◆ **Installation:** ["Installing iManager" on page 145](#)
 - ◆ **Upgrade:** ["Upgrading iManager" on page 426](#)
- 4 On the server running Identity Manager, upgrade eDirectory to the latest version for Identity Manager.
Upgrading eDirectory stops ndsd, which in turn stops all drivers. For more information, see the [Novell eDirectory 8.8 Installation Guide](#) and the Release Notes for Identity Manager and eDirectory.
- 5 (Conditional) If you are upgrading from a 32-bit Identity Manager to another 32-bit version, start the drivers and verify that the drivers start.
This step also verifies that the upgrade to eDirectory 8.8 SP7 was successful. For more information, see [Section 46.3.2, "Starting the Drivers,"](#) on page 417.

- 6 (Conditional) To upgrade a version older than 4.0.1, convert the Designer project. For more information, see [“Converting Earlier Projects”](#) in the *Designer 4.0.2 for Identity Manager 4.0.2 Administration Guide*.
- 7 Stop the drivers that are associated with the server where you installed the Identity Manager Engine (Metadirectory). For more information, see [Section 46.3.1, “Stopping the Drivers,”](#) on page 416.
- 8 Upgrade the Identity Manager Engine. For more information, see [Section 47.3.1, “Upgrading the Identity Manager Engine Server,”](#) on page 422.
- 9 (Conditional) If any of the drivers in the driver set for the Identity Manager Engine are Remote Loader drivers, upgrade the Remote Loader servers for each driver. For more information, see [Section 47.5.3, “Upgrading the Remote Loader,”](#) on page 430.
- 10 (Conditional) If you are upgrading Identity Manager 4.0.1 and have the User Application server, perform the following steps:
 - 10a Upgrade the User Application packages.
 - 10b Deploy the upgraded User Application driver into the Identity Vault. For more information, see the [Migrating to the Roles Based Provisioning Module](#) guide.
 - 10c Upgrade the User Application. For more information, see the [Migrating to the Roles Based Provisioning Module](#) guide.
- 11 (Conditional) If you are upgrading a version of Identity Manager older than 4.0.1 and have the User Application server, perform the following steps:
 - 11a Run the NrfCaseUpdate utility for providing support for mixed-case searching on roles and resources.

This procedure updates the schema by modifying the nrfLocalizedDescrs and nrfLocalizedNames attributes, which are used by User Application drivers. For more information, see [Section 24.2, “Extending the eDirectory Schema Using the Wizard,”](#) on page 206.
 - 11b Migrate the User Application driver using Designer 4.0.2. For more information, see the [Migrating to the Roles Based Provisioning Module](#) guide.
 - 11c Create a new Role and Resource Service driver. The Role and Resource Service driver is not migrated. If you have an existing Role and Resource Service driver, delete it and create a new driver for Identity Manager 4.0.2. For more information, see the [Migrating to the Roles Based Provisioning Module](#) guide.
 - 11d Deploy the migrated User Application driver and the Role and Resource Service driver into the Identity Vault. For more information, see the [Migrating to the Roles Based Provisioning Module](#) guide.
 - 11e Upgrade the User Application. For more information, see the [Migrating to the Roles Based Provisioning Module](#) guide.
- 12 (Optional) To upgrade the drivers that you use with Identity Manager, complete one of the following steps:
 - 12a If you are using packages instead of driver configuration files, upgrade the packages on the existing drivers to get new policies. This is only required if a newer version of a package is available and there is a new functionality included in the policies for a driver that you want to add to your existing driver. For more information, see [“Upgrading Installed Packages”](#) in the *Designer 4.0.2 for Identity Manager 4.0.2 Administration Guide*.
- 13 (Optional) Restore custom policies and rules to the drivers.

When you overlay the new driver configuration files, the policies are overwritten, so restoring policies is required only if you did an overlay of the new driver configuration file. For more information, see [Section 47.7, “Restoring Custom Policies and Rules to the Driver,”](#) on page 434.

- 14 (Conditional) If you are upgrading a version of Identity Manager older than 4.0.1, deploy the changes performed in these steps to the Identity Vault. For more information, see [“Deploying and Exporting”](#) in *Designer 4.0.2 for Identity Manager 4.0.2 Administration Guide*.
- 15 Start the drivers associated with the User Application and the Identity Manager Engine. For more information, see [Section 46.3.2, “Starting the Drivers,”](#) on page 417.
- 16 (Optional) For reporting functionality, install or upgrade the Identity Information Warehouse. For more information, see one of the following sections:
 - ♦ **Installation:** [“Installing the Identity Information Warehouse”](#) on page 293
 - ♦ **Upgrade:** [Section 47.5.4, “Upgrading the Identity Information Warehouse,”](#) on page 431
- 17 (Optional) For role administration, install or upgrade a role mapping component. For more information, see [“Installing a Role Administrator Component”](#) on page 333.
- 18 (Optional) Install or upgrade iManager to the latest version for Identity Manager. For more information, see one of the following sections:
 - ♦ **Installation:** [“Installing Analyzer”](#) on page 403
 - ♦ **Upgrade:** [Section 47.5.5, “Upgrading Analyzer,”](#) on page 432

47.3 Upgrading to Advanced Edition from Standard Edition

This section helps you upgrade an existing installation of Identity Manager 4.0.2 Standard Edition to the Advanced Edition. In general, this upgrade involves changes to the configuration of Identity Manager components, rather than running the installation programs. However, the Advanced Edition also supports role administration. For more information, see [“Installing a Role Administrator Component”](#) on page 333.

Perform the following steps to upgrade Identity Manager Standard Edition to the Advanced Edition.

- ♦ [Section 47.3.1, “Upgrading the Identity Manager Engine Server,”](#) on page 422
- ♦ [Section 47.3.2, “Upgrading the User Application,”](#) on page 422
- ♦ [Section 47.3.3, “Upgrading the Identity Reporting Module,”](#) on page 423

47.3.1 Upgrading the Identity Manager Engine Server

In iManager, apply the activation for Identity Manager 4.0.2 Advanced Edition. Otherwise, the upgrade does not proceed.

47.3.2 Upgrading the User Application

- 1 Log on as an administrator to the server where the User Application is installed.
- 2 Stop the JBoss server by entering one of the following commands:
 - ♦ **Linux:** `/etc/init.d/jboss_init stop`
 - ♦ **Windows:** `RBPM_Installation_Location/UserApplication/stop-jboss.bat`
- 3 In the Identity Manager Standard Edition installation subdirectory, run `<RBPM installation directory>/configupdate.sh`.

For example, on Windows, run the following command:

```
C:\Novell\IdentityManager\rbpm\UserApplication\configupdate.bat.
```

By default, the installer runs in console mode. For GUI mode, replace the `-use_console true` Java command argument with `-use_console false` in the `configupdate.bat` file.

- 4 Edit the admin fields by changing the value of `-edit_admin` setting to `true`.
The admin fields are disabled by default.
- 5 Fill the following fields in the default view of the Roles Based Provisioning Module Configuration panel:
 - ♦ Press the Tab key, which displays a prompt. When you click **Yes**, additional admin fields are displayed in the Identity Vault DNs section of the Roles Based Provisioning Module Configuration page.
 - ♦ Update all the admin fields with the appropriate users if you want the admin to be anything other than the User Application admin.
 - ♦ Verify if the advanced options are displayed. Click **Show Advanced Options** to display the advanced options.
- 6 In the Miscellaneous section, select the **Reinitialize RBPM Security** check box, then click **OK**.
- 7 Start the JBoss server by entering one of the following commands:
 - ♦ **Linux:** `/etc/init.d/jboss_init start`
 - ♦ **Windows:** `RBPM_Installation_Location/UserApplication/start-jboss.bat`

This redeploys the WAR file. If you are running in a JBoss cluster, the WAR file needs to be updated in each JBoss server in the cluster.

47.3.3 Upgrading the Identity Reporting Module

- 1 Log on to Designer.
- 2 In Designer, configure the Managed System Gateway Driver. For more information, see [Section 34.1.2, “Configuring the Managed System Gateway Driver,” on page 311](#).
- 3 To update the driver for Data Collection Service (DCS), complete the following steps:
 - 3a In Designer, navigate to **DCS Driver Configuration > Driver Parameters > Driver Options**.
 - 3b In the Managed System Gateway Registration section, change **Set Register Manage System Gateway** to **Yes**.
 - 3c Specify a value for **MSGW Driver DN**. For example, `CN=Managed System Gateway Driver,cn=driverset1,o=system`.
 - 3d Specify a value for **User DN**. For example, `cn=admin,ou=sa,o=system`.
 - 3e Specify the password for **User DN**.

For more information, see [Section 34.1.3, “Configuring the Driver for Data Collection Service,” on page 313](#).

- 4 Save the settings.
- 5 Deploy the Data Collection Service driver.
- 6 Restart the Data Collection Service driver.
- 7 Download the Identity Manager 4.0.2 Advanced Edition Report Templates from the [Identity Reporting \(http://cdn.novell.com/cached/designer/idmrpt/\)](http://cdn.novell.com/cached/designer/idmrpt/) download page.

Upgrading the Identity Information Warehouse might not immediately show the Advanced Edition. The version change occurs after Identity Manager process the next batch of events.

47.4 Upgrading to a New Version of Standard Edition

This section helps you upgrade to a new version of Standard Edition from 4.0.1 Standard Edition.

- 1 Upgrade Designer. For more information, see [Section 47.5.1, “Upgrading Designer,”](#) on page 425.
- 2 Create a backup of the current configuration of your Identity Manager solution by creating a Designer project of your Identity Manager solution. For more information, see [Section 46.2, “Backing Up the Current Configuration,”](#) on page 414.
- 3 Upgrade your iManager server to iManager 2.7.5 or later. For more information, see [Section 47.5.2, “Upgrading iManager,”](#) on page 426.
- 4 Upgrade eDirectory to 8.8 SP7 or later on the server running Identity Manager. For more information, see the [Novell eDirectory 8.8 Installation Guide](#).
- 5 Stop the drivers that are associated with the Identity Manager Engine. For more information, see [Section 46.3.1, “Stopping the Drivers,”](#) on page 416.
- 6 Upgrade the Identity Manager Engine. For more information, see [Section 47.3.1, “Upgrading the Identity Manager Engine Server,”](#) on page 422.
- 7 (Optional) If any of the drivers in the driver set for the Identity Manager Engine server are Remote Loader drivers, upgrade the Remote Loader servers for each driver. For more information, see [Section 47.5.3, “Upgrading the Remote Loader,”](#) on page 430.
- 8 (Conditional) If you have a User Application server, perform the following additional steps:
 - 8a Upgrade the User Application packages.
 - 8b Deploy the upgraded User Application driver into the Identity Vault. For more information, see the [Migrating to the Roles Based Provisioning Module](#) guide.
 - 8c Upgrade the User Application. For more information, see the [Migrating to the Roles Based Provisioning Module](#) guide.
- 9 (Optional) To upgrade the drivers that you use with Identity Manager, complete one of the following steps:
 - 9a If you are using packages instead of driver configuration files, upgrade the packages on the existing drivers to get new policies. This is only required if a newer version of a package is available and there is a new functionality included in the policies for a driver that you want to add to your existing driver. For more information, see “[Upgrading Installed Packages](#)” in the [Designer 4.0.2 for Identity Manager 4.0.2 Administration Guide](#).
 - 9b If you are using configuration files, overlay the new driver configuration files over the existing drivers to get new policies. This is required only if there is new functionality included in the policies for a driver that you want to add to your existing driver.
- 10 (Optional) Restore custom policies and rules to the drivers.

When you overlay the new driver configuration files, the policies are overwritten, so restoring policies is required only if you did an overlay of the new driver configuration file. For more information, see [Section 47.7, “Restoring Custom Policies and Rules to the Driver,”](#) on page 434.
- 11 Start the drivers associated with your Identity Manager Engine and User Application servers. For more information, see [Section 46.3.2, “Starting the Drivers,”](#) on page 417.
- 12 Upgrade the Identity Information Warehouse. For more information, see [Section 47.5.4, “Upgrading the Identity Information Warehouse,”](#) on page 431.
- 13 Upgrade Analyzer. For more information, see [Section 47.5.5, “Upgrading Analyzer,”](#) on page 432.

47.5 Upgrading Individual Components of Identity Manager

This section provides specific information for upgrading individual components of Identity Manager. For example, you might want to upgrade Designer to the latest version without also upgrading iManager. This section also provides steps that you might need to take after performing an upgrade.

To complete the upgrade, see the following sections:

- ◆ [Section 47.5.1, “Upgrading Designer,” on page 425](#)
- ◆ [Section 47.5.2, “Upgrading iManager,” on page 426](#)
- ◆ [Section 47.5.3, “Upgrading the Remote Loader,” on page 430](#)
- ◆ [Section 47.5.4, “Upgrading the Identity Information Warehouse,” on page 431](#)
- ◆ [Section 47.5.5, “Upgrading Analyzer,” on page 432](#)

47.5.1 Upgrading Designer

- 1 Log on as an administrator to the server where Designer is installed.
- 2 To create a backup copy of your projects, export your projects.
For more information about exporting, see [“Exporting a Project” in the *Designer 4.0.2 for Identity Manager 4.0.2 Administration Guide*](#).
- 3 Launch the Designer installation program from Identity Manager media:
 - ◆ **Linux:** `IDM4.0.2_Lin/products/Designer/install`
To execute the binary file, enter `./install`.
 - ◆ **Windows:** `IDM4.0.2_Win:\products\Designer\install.exe`
- 4 Select the language to install Designer in, then read and accept the license agreement.
- 5 Specify the directory where Designer is installed, then click **Yes** in the message stating you already have Designer installed.
- 6 Select whether the shortcuts should be placed on your desktop and in your desktop menu.
- 7 Review the summary, then click **Install**.
- 8 Review the Readme, then click **Next**.
- 9 Select to launch Designer, then click **Done**.
- 10 Specify a location for your Designer workspace, then click **OK**.
- 11 Click **OK** in the warning message stating that your project needs to be closed and converted.
- 12 In the Project view, expand the project, then double-click **Project needs conversion**.
- 13 Review the steps that the Project Converter Wizard performs, then click **Next**.
- 14 Specify a name for the backup of your project, then click **Next**.
- 15 Review the summary of what happens during the conversion, then click **Convert**.
- 16 Review the summary after the conversion finishes, then click **Open**.

After upgrading to the current version of Designer, you must import all Designer projects from the older version. When you initiate the import process, Designer runs the Project Converter Wizard, which converts the older projects to the current version. In the wizard, select **Copy project into the workspace**. For more information about the Project Converter, see the [Designer 4.0.2 for Identity Manager 4.0.2 Administration Guide](#).

47.5.2 Upgrading iManager

In general, the upgrade process for iManager uses the existing configuration values in the `configiman.properties` file, such as port values and authorized users. Before upgrading, NetIQ recommends that you back up the `server.xml` and `context.xml` configuration files if you modified them.

The upgrade process includes the following activities:

- ◆ [Section 47.5.2.1, “Upgrading iManager on Linux,” on page 426](#)
- ◆ [Section 47.5.2.2, “Upgrading iManager on Windows,” on page 427](#)
- ◆ [Section 47.5.2.3, “Upgrading iManager Silently,” on page 429](#)
- ◆ [Section 47.5.2.4, “Updating Role-Based Services,” on page 429](#)
- ◆ [Section 47.5.2.5, “Re-installing or Migrating Plug-in Studio Plug-ins,” on page 430](#)

NOTE: When updating or re-installing iManager, the installation program does not update existing plug-ins. To update plug-ins manually, launch iManager and navigate to **Configure > Plug-in Installation > Available Novell Plug-in Modules**. For more information, see [Section 16.1, “Understanding Installation for iManager Plug-ins,” on page 149](#).

47.5.2.1 Upgrading iManager on Linux

If the setup program for iManager Server detects a previously installed version of iManager, it might give you the option to stop the installation process or remove the existing iManager, JRE, and Tomcat installations.

Before upgrading iManager, ensure that the computer meets the prerequisites and system requirements. For more information, see the following sources:

- ◆ The Release Notes accompanying the update.
- ◆ **iManager:** [Section 6.5.2, “Considerations for Installing iManager on a Linux Platform,” on page 62](#).
- ◆ **iManager Workstation:** [Section 6.5.4, “Considerations for Installing iManager Workstation on Linux Clients,” on page 63](#).

NOTE: The upgrade process uses the the HTTP port and SSL port values that were configured in the previous version of iManager.

To upgrade iManager Server on Linux:

- 1 Log on as `root` or `root`-equivalent to the computer where you want to run the installation program.
- 2 (Conditional) If you modified the `server.xml` and `context.xml` configuration files, save a backup copy of the files in a different location before performing the upgrade.

The upgrade process replaces the configuration files.

- 3 At the [Novell Downloads Web site \(http://download.novell.com\)](http://download.novell.com), search for iManager products, select the iManager version that you want, then download the .tgz file to a directory on your server. For example, `iMan_277_linux.tgz`.
- 4 To extract the iManager folder, enter the following command:


```
tar -zxvf iMan_version_linux.tgz
```
- 5 In a shell, change to the `/extracted_directory/iManager/installs/linux` directory. This path is relative to the directory where you copied or extracted the iManager files.
- 6 (Conditional) To run a command-line (text) installation, enter the following command:


```
./iManagerInstallLinux.bin
```
- 7 (Conditional) To run the wizard for the installation program, enter the following command:


```
./iManagerInstallLinux.bin -i gui
```
- 8 At the splash screen, specify a language, and then click **OK**.
- 9 At the Upgrade prompt, select **Upgrade**.
- 10 Read the Introduction, and then click **Next**.
- 11 Accept the License Agreement, and then click **Next**.
- 12 (Optional) To use IPv6 addresses with iManager, click **Yes** in the Enable IPv6 window. You can enable IPv6 addresses after you upgrade iManager. For more information, see [Section 17.2, "Configuring iManager for IPv6 Addresses after Installation," on page 164](#).
- 13 Click **Next**.
- 14 Read the Pre-Upgrade Summary page, and then click **Next**.
The upgrade process can take several minutes. The process might add new files for iManager components or change the iManager configuration. For more information, see the Release Notes for the upgrade.
- 15 When the upgrade process completes, click **Done**.
- 16 When the initialization of iManager finishes, click the first link in the Getting Started page, and then log on. For more information, see ["Accessing iManager" \(https://www.netiq.com/documentation/imanager/imanager_admin/data/bsxrjzp.html\)](https://www.netiq.com/documentation/imanager/imanager_admin/data/bsxrjzp.html) in the *NetIQ iManager 2.7.7 Administration Guide*.
- 17 (Conditional) If you made backup copies of the `server.xml` and `context.xml` configuration files before starting the upgrade process, replace the new configuration files with the backup copies.

47.5.2.2 Upgrading iManager on Windows

If the setup program for iManager Server detects a previously installed version of iManager, it might prompt you to upgrade the installed version. If you choose to upgrade, the program replaces the existing JRE and Tomcat versions with the latest versions. This will also upgrade the iManager to the latest version.

Before upgrading iManager, ensure that the computer meets the prerequisites and system requirements. For more information, see the following sources:

- ◆ The Release Notes accompanying the update.
- ◆ **iManager:** [Section 6.5.2, "Considerations for Installing iManager on a Linux Platform," on page 62](#).
- ◆ **iManager Workstation:** [Section 6.5.4, "Considerations for Installing iManager Workstation on Linux Clients," on page 63](#).

NOTE: The upgrade process uses the the HTTP port and SSL port values that were configured in the previous version of iManager.

To install iManager Server on Windows:

- 1 Log on as a user with administrator privileges on the computer where you want to upgrade iManager.
- 2 (Conditional) If you modified the `server.xml` and `context.xml` configuration files, save a backup copy of the files in a different location before performing the upgrade.
The upgrade process replaces the configuration files.
- 3 At the [Novell Downloads Web site \(http://download.novell.com\)](http://download.novell.com), select the iManager version that you want, then download the `win.zip` file to a directory on your server. For example, `iMan_277_win.zip`.
- 4 Extract the `win.zip` file to the iManager folder.
- 5 Run `iManagerInstall.exe`, located by default in the `extracted_directory\iManager\installs\win` folder.
- 6 In the iManager welcome window, select a language, and then click **OK**.
- 7 In the **Introduction** window, and then click **Next**.
- 8 Accept the License Agreement, and then click **Next**.
- 9 (Optional) To use IPv6 addresses with iManager, click **Yes** in the **Enable IPv6** window.
You can enable IPv6 addresses after you upgrade iManager. For more information, see [Section 17.2, "Configuring iManager for IPv6 Addresses after Installation," on page 164](#).
- 10 Click **Next**.
- 11 At the Upgrade prompt, select **Upgrade**.
- 12 (Conditional) Review the **Detection Summary** window.
The **Detection Summary** window lists the latest version of Servlet container and JVM software that iManager will use once it is upgraded.
- 13 Click **Next**.
- 14 Read the Pre-installation summary page, and then click **Install**.
The upgrade process can take several minutes. The process might add new files for iManager components or change the iManager configuration. For more information, see the Release Notes for the upgrade.
- 15 (Conditional) If the **Install Complete** window displays the following error message, complete the following steps:

```
The installation of iManager version is complete, but some errors occurred during the install. Please see the installation log Log file path for details. Press "Done" to quit the installer.
```

 - 15a Note the path to the log file that the error message displays.
 - 15b In the **Install Complete** window, click **Done**.
 - 15c Open the log file.
 - 15d (Conditional) If you find the following error in the log file, you can ignore the error message. The installation was successful, and iManager functions properly.

```
Custom Action: com.novell.application.iManager.install.InstallDLLs
Status: ERROR
Additional Notes: ERROR - class
com.novell.application.iManager.install.InstallDLLs
NonfatalInstallException C:\WINDOWS\system32\msvcr71.dll (The process
cannot access the file because it is being used by another process)
```

- 15e (Conditional) If the log file does not contain the error listed in [Step 20d](#), NetIQ recommends that you retry the installation.
- 16 Click **Done**.
- 17 When the initialization of iManager finishes, click the first link in the Getting Started page, and then log on. For more information, see “[Accessing iManager](https://www.netiq.com/documentation/imanager/imanager_admin/data/bsxrjzp.html)” (https://www.netiq.com/documentation/imanager/imanager_admin/data/bsxrjzp.html) in the *NetIQ iManager 2.7.7 Administration Guide*.
- 18 (Conditional) If you made backup copies of the `server.xml` and `context.xml` configuration files before starting the upgrade process, replace the new configuration files with the backup copies.

47.5.2.3 Upgrading iManager Silently

A silent (non-interactive) upgrade does not display a user interface or ask the user any questions. Instead, InstallAnywhere uses information from a properties file.

To perform a standard silent install on a Linux or Windows server, use the default installation values.

- 1 At the [Novell Downloads Web site](http://download.novell.com) (<http://download.novell.com>), select the iManager version that you want. For example:
 - ♦ **Linux:** `iMan_version_linux.tgz`
 - ♦ **Windows:** `iMan_version_win.zip`
- 2 Download the upgrade file to a directory on your server.
- 3 (Conditional) On Windows computers, extract the `win.zip` file to the iManager folder.
- 4 In a console window, go to the directory containing the upgrade file that you downloaded.
- 5 On the command line, enter one of the following commands:
 - ♦ **Linux:** `./iManagerInstallplatform.bin -i silent`
 - ♦ **Windows:** `iManagerInstall.exe -i silent`

47.5.2.4 Updating Role-Based Services

The first time that you use iManager to log on to an eDirectory tree that already contains a Role-Based Services (RBS) collection, you might not see all of the roles information. This behavior is normal because you must update some of the plug-ins to function with the latest version of iManager. NetIQ recommends that you update your RBS modules to the latest version so that you can see and use all of the available functionality in iManager. The RBS Configuration table lists which RBS modules need to be updated.

Be aware that you might have multiple roles with the same name. Starting with iManager 2.5, some plug-in developers changed task IDs or module names but retained the same display names. This issue causes the roles to appear to be duplicated when, in fact, one instance is from one version and the other is from a newer version.

NOTE

- ◆ When updating or re-installing iManager, the installation program does not update existing plug-ins. To update plug-ins manually, launch iManager and navigate to **Configure > Plug-in Installation > Available Novell Plug-in Modules**. For more information, see [Section 16.1, “Understanding Installation for iManager Plug-ins,”](#) on page 149.
 - ◆ Different installations of iManager might have a different number of plug-ins locally installed. As a result, you might see discrepancies in the module report for any given collection from the **Role Based Services > RBS Configuration** page. For the numbers to match between iManager installations, ensure that you install the same subset of plug-ins on each iManager instance in the tree.
-

To check for and update outdated RBS objects:

- 1 Log on to iManager.
- 2 In the Configure view, select **Role Based Services > RBS Configuration**.
Review the table in the 2.x Collections tabbed page for any out-of-date modules.
- 3 (Optional) To update a module, complete the following steps:
 - 3a For the Collection that you want to update, select the number in the **Out-Of-Date** column. iManager displays the list of outdated modules.
 - 3b Select the module you that want to update.
 - 3c Click **Update** at the top of the table.

47.5.2.5 Re-installing or Migrating Plug-in Studio Plug-ins

You can migrate or replicate Plug-in Studio plug-ins to another iManager instance, as well as to a new or updated version of iManager.

- 1 Log on to iManager.
- 2 In the iManager Configure view, select **Role Based Services > Plug-in Studio**.
The Content frame displays the Installed Custom Plug-ins list, including the location of the RBS collection to which the plug-ins belong.
- 3 Select the plug-in that you want to re-install or migrate, then click **Edit**.

NOTE: You can edit only one plug-in at a time.

- 4 Click **Install**.
- 5 Repeat these steps for every plug-in that you need to re-install or migrate.

47.5.3 Upgrading the Remote Loader

If you are running the Remote Loader, you need to upgrade the Remote Loader files.

- 1 Create a backup of the Remote Loader configuration files. The default location of the files is as follows:
 - ◆ **Windows:** C:\Novell\RemoteLoader\remoteloadername-config.txt
 - ◆ **Linux:** Create your own configuration file in the path of rdxml.
- 2 Verify that the drivers are stopped. For instructions, see [Section 46.3.1, “Stopping the Drivers,”](#) on page 416.

- 3 Stop the Remote Loader service or daemon for each driver.
 - ♦ **Windows:** In the Remote Loader Console, select the Remote Loader instance, then click **Stop**.
 - ♦ **Linux:** `rdxml -config path_to_configfile -u`
 - ♦ **Java Remote Loader:** `dirxml_jremote -config path_to_configfile -u`
- 4 On Linux, stop the lcache process.
 - ♦ If the Metadirectory server and Remote Loader are on the same server, manually stop the lcache process.
 - ♦ If the Metadirectory server and Remote Loader are not on the same server, the lcache process is automatically stopped by the ndsd process during upgrade.

On Windows and Solaris, kill the lcache process before starting the upgrade.
- 5 Run the installation program for the Remote Loader.

The installation process updates the files and binaries to the current version. For more information, see “[Installing the Remote Loader](#)” in the *Identity Manager 4.0.2 Framework Installation Guide*.
- 6 After the installation finishes, verify that your configuration files contain your environment’s information.
- 7 (Conditional) If there is a problem with the configuration file, copy the backup file you created in [Step 1](#). Otherwise, continue with [Step 8](#).
- 8 Start the Remote Loader service or daemon for each driver.
 - ♦ **Java Remote Loader:** `dirxml_jremote -config path_to_config_file`
 - ♦ **Linux:** `rdxml -config path_to_config_file`
 - ♦ **Windows:** In the Remote Loader Console, select the Remote Loader instance, then click **Start**.

NOTE: After upgrading the Remote Loader from 32-bit to 64-bit, the GroupWise driver and the native custom drivers do not work.

47.5.4 Upgrading the Identity Information Warehouse

The Identity Information Warehouse includes the Identity Reporting module, Event Auditing System, and two drivers. Perform the upgrade in the following order:

1. Upgrade the driver package for the Data Collection Services.
2. Upgrade the driver package for the Managed System Gateway Service.
3. Upgrade the Event Auditing Service
4. Upgrade the Identity Reporting Module.

For more information, see the following sections:

- ♦ [Section 47.5.4.1, “Upgrading the Event Auditing Service,” on page 432](#)
- ♦ [Section 47.5.4.2, “Upgrading the Identity Reporting Module,” on page 432](#)

47.5.4.1 Upgrading the Event Auditing Service

Before upgrading EAS, review the following considerations:

- ◆ To upgrade EAS from version 4.0.x on a server running SLES 11 Service Pack 1 64-bit, include the following steps
 1. Before upgrading, login as `novleas` and then copy the following files from the `/etc/opt/novell/sentinel_eas/config/` directory to a non-installation location:
 - ◆ `xdas_out.map`
 - ◆ `xdas_tax.map`
 2. After upgrading, copy the files to the `/etc/opt/novell/sentinel_eas/config/` directory in the new or upgraded location.
- ◆ If you are upgrading EAS from Novell Audit, verify that the `logevent.conf` file points to EAS and uses the correct ports. This ensures that events are routed to EAS rather than to the Novell Auditing server.

To upgrade EAS, simply install the new version on top of the older version. For more information about installing EAS, see [Chapter 32, “Installing the Event Auditing System,”](#) on page 297.

47.5.4.2 Upgrading the Identity Reporting Module

Before upgrading the Identity Reporting module, you must upgrade the User Application and the Event Auditing Service.

To upgrade Identity Reporting Module 4.0.1. to 4.0.2, simply install the new version on top of the older version. For more information about installation, see [“Installing the Reporting Module”](#) on page 301.

47.5.5 Upgrading Analyzer

To upgrade Analyzer, NetIQ provides patch files in `.zip` format. Before upgrading Analyzer, ensure that the computer meets the prerequisites and system requirements. For more information, see the Release Notes accompanying the update.

- 1 Download the patch file, such as `analyzer_402_patch1_20121128.zip`, from the NetIQ download Web site.
- 2 Extract the `.zip` file to the directory that contains the Analyzer installation files, such as the plugins, uninstallation script, and other Analyzer files.
- 3 Restart Analyzer.
- 4 To verify that you successfully applied the new patch, complete the following steps:
 - 4a Launch Analyzer.
 - 4b Click **Help > About Analyzer**.
 - 4c Check whether the program displays the new version, such as **4.0.2 Update 1** and Build ID **20121128**.

47.6 Upgrading the Identity Manager Drivers

Starting with Identity Manager 4.0.2, NetIQ delivers new driver content through **packages** instead of through driver configuration files. You manage, maintain, and create packages in Designer. Although iManager is package-aware, Designer does not maintain any changes to driver content that you make in iManager. For more information about managing packages, see “[Managing Packages](#)” in the *Designer 4.0.2 for Identity Manager 4.0.2 Administration Guide*.

NOTE: If you upgrade the 3.x version of the User Application driver to the User Application version 4.0.2 package, Designer installs both 3.x and 4.0 versions of the same driver policies. Having both 3.x and 4.0 policies within the package catalog may cause Designer to not function properly. Delete the version 3.x policies and retain the version 4.0 policies.

You can upgrade your drivers to packages in the following ways:

- ♦ [Section 47.6.1, “Creating a New Driver,” on page 433](#)
- ♦ [Section 47.6.2, “Replacing Existing Content with Content from Packages,” on page 433](#)
- ♦ [Section 47.6.3, “Keeping the Current Content and Adding New Content with Packages,” on page 434](#)

47.6.1 Creating a New Driver

The simplest and cleanest way to upgrade drivers to packages is to delete your existing driver and create a new driver with packages. Add all the functionality you want in the new driver. The steps are different for each driver. For instructions, see the individual driver guides on the [Identity Manager Drivers documentation Web site](#). The driver now functions as before, but with content from packages instead of from a driver configuration file.

47.6.2 Replacing Existing Content with Content from Packages

If you need to keep the associations created by the driver, you do not need to delete and re-create the driver. You can keep the associations and replace the driver content with packages.

To replace the existing content with content from packages:

- 1 Create a backup of the driver and all of the customized content in the driver.
For instructions, see [Section 46.2.2, “Exporting the Configuration of the Drivers,” on page 415](#).
- 2 In Designer, delete all objects stored inside of the driver. Delete the policies, filters, entitlements, and all other items stored inside of the driver.

NOTE: Designer 4.0.2 provides the auto-import facility for importing the latest packages. You don’t need to manually import the driver packages into the package catalog.

For instructions, see “[Importing Packages into the Package Catalog](#)” in the *Designer 4.0.2 for Identity Manager 4.0.2 Administration Guide*.

- 3 Install the latest packages to the driver.

These steps are specific for each driver. For instructions, see each driver guide at the [Identity Manager Drivers documentation Web site](#).

- 4 Restore any custom policies and rules to the driver. For instructions, see [Section 47.7, “Restoring Custom Policies and Rules to the Driver,” on page 434](#).

47.6.3 Keeping the Current Content and Adding New Content with Packages

You can keep the driver as it currently is and add new functionality to the driver through packages, as long as the functionality in packages does not overlap the current functionality of the driver.

Before you install a package, create a backup of the driver configuration file. When you install a package, it can overwrite existing policies, which might cause the driver to stop working. If a policy is overwritten, you can import the backup driver configuration file and recreate the policy.

Before you begin, make sure that any customized policies have different policy names than the default policies. When a driver configuration is overlaid with a new driver file, the existing policies are overwritten. If your custom policies do not have a unique name, you will lose them.

To add new content to the driver with packages:

- 1 Create a backup of the driver and all of the customized content in the driver.

For instructions, see [Section 46.2.2, “Exporting the Configuration of the Drivers,” on page 415.](#)

NOTE: Designer 4.0.2 provides the auto-import facility for importing the latest packages. You don't need to manually import the driver packages into the package catalog.

For instructions, see “[Importing Packages into the Package Catalog](#)” in the *Designer 4.0.2 for Identity Manager 4.0.2 Administration Guide*.

- 2 Install the packages on the driver.

For instructions, see each driver guide at the [Identity Manager Drivers documentation Web site](#).

- 3 Add the desired packages to the driver. These steps are specific for each driver.

For instructions, see the [Identity Manager Drivers documentation Web site](#).

The driver contains the new functionality added by the packages.


47.7 Restoring Custom Policies and Rules to the Driver

After installing or upgrading to new packages for your drivers, you must restore any custom policies or rules to the driver after you overlay the new driver configuration file. If these policies have different names, they are still stored in the driver, but the links are broken and need to be reestablished.

- ♦ [Section 47.7.1, “Using Designer to Restore Custom Policies and Rules to the Driver,” on page 434](#)
- ♦ [Section 47.7.2, “Using iManager to Restore Custom Policies and Rules to the Driver,” on page 435](#)

47.7.1 Using Designer to Restore Custom Policies and Rules to the Driver

You can add policies into the policy set. You should perform these steps in a test environment before you move the upgraded driver to your production environment.

- 1 In the **Outline** view, select the upgraded driver, then click the **Show Policy Flow** icon .
- 2 Right-click the policy set where you need to restore the customized policy to the driver, then select **Add Policy > Copy Existing**.


- 3 Browse to and select the customized policy, then click **OK**.
- 4 Specify the name of the customized policy, then click **OK**.
- 5 Click **Yes** in the file conflict message to save your project.
- 6 After the Policy Builder opens the policy, verify that the information is correct in the copied policy.
- 7 Repeat [Step 2](#) through [Step 6](#) for each customized policy you need to restore to the driver.
- 8 Start the driver and test the driver.

For more information on starting the driver, see [Section 46.3.2, “Starting the Drivers,” on page 417](#). For more information on testing the driver, see “Testing Policies with the Policy Simulator” in *Policies in Designer 4.0.2*.

- 9 After you verify that the policies work, move the driver to the production environment.

47.7.2 Using iManager to Restore Custom Policies and Rules to the Driver

Perform these steps in a test environment before you move the upgraded driver to your production environment.

- 1 In iManager, select **Identity Manager > Identity Manager Overview**.
- 2 Browse to and select the location in the tree to search for Driver Set objects, then click the search icon .
- 3 Click the Driver Set object that contains the upgraded driver.
- 4 Click the driver icon, then select the policy set where you need to restore the customized policy.
- 5 Click **Insert**.
- 6 Select **Use an existing policy**, then browse to and select the custom policy.
- 7 Click **OK**, then click **Close**.
- 8 Repeat [Step 3](#) through [Step 7](#) for each custom policy you need to restore to the driver.
- 9 Start the driver and test the driver.

For information on starting the driver, see [Section 46.3.2, “Starting the Drivers,” on page 417](#). There is no policy simulator in iManager. To test the policies, cause events to happen that make the policies execute. For example, create a user, modify a user, or delete a user.

- 10 After you verify that the policies work, move the driver to the production environment.

48 Performing a Migration

This section provides information for migrating data for Identity Manager components to a new installation. You might need to perform a migration when you cannot upgrade an existing installation. This section includes the following activities:

- ♦ [Section 48.1, “Checklist for Performing a Migration,” on page 437](#)
- ♦ [Section 48.2, “Preparing For Mixed-case Searches on Roles and Resources,” on page 438](#)
- ♦ [Section 48.3, “Updating the User Application,” on page 443](#)
- ♦ [Section 48.4, “Adding the New Server to the Driver Set,” on page 444](#)
- ♦ [Section 48.5, “Copying Server-Specific Information for the Driver Set,” on page 444](#)
- ♦ [Section 48.6, “Removing the Old Server from the Driver Set,” on page 446](#)

48.1 Checklist for Performing a Migration

To perform a migration, NetIQ recommends that you complete the steps in the following checklist.

	Checklist Items
<input type="checkbox"/>	1. Ensure that you have the latest installation kit to upgrade Identity Manager.
<input type="checkbox"/>	2. Learn about the interaction among Identity Manager components. For more information, see Part I, “Introduction,” on page 19 .
<input type="checkbox"/>	3. Ensure that your computers meet the hardware and software prerequisites. For more information, see Chapter 6, “Considerations and Prerequisites for Installation,” on page 45 and the Release Notes for the version to which you want to upgrade.
<input type="checkbox"/>	4. Determine whether you can perform an upgrade versus a migration. For more information, see Section 46.1, “Understanding Upgrade and Migration,” on page 413 .
<input type="checkbox"/>	5. Back up the current project and driver configuration. For more information, see Section 46.2, “Backing Up the Current Configuration,” on page 414 .
<input type="checkbox"/>	6. Upgrade eDirectory to the latest supported version for the Identity Vault. For more information, see Section 6.3, “Prerequisites and Requirements for Installing the Identity Vault,” on page 47 .
<input type="checkbox"/>	7. Add the eDirectory replicas that are on the current Identity Manager server to the new server. For more information, see “Administering Replicas” (http://www.novell.com/documentation/edir88/edir88/data/fbgciaad.html) in the <i>Novell eDirectory 8.8 Administration Guide</i> .
<input type="checkbox"/>	8. Install Identity Manager on the new server. For more information, see “Planning to Install Identity Manager” on page 37 .
<input type="checkbox"/>	9. (Conditional) To upgrade from RBPM 3.6.1 or earlier, ensure that your environment supports mixed-case searches in the identity applications. For more information, see Section 48.2, “Preparing For Mixed-case Searches on Roles and Resources,” on page 438 .
<input type="checkbox"/>	10. (Conditional) If any of the drivers in the driver set are Remote Loader drivers, upgrade the Remote Loader server for each driver. For more information, see Section 47.5.3, “Upgrading the Remote Loader,” on page 430 .

	Checklist Items
<input type="checkbox"/>	11. (Conditional) If you are running the User Application on your old server, update the component and its drivers. For more information, see Section 48.3, "Updating the User Application," on page 443.
<input type="checkbox"/>	12. Add the new server to the driver set. For more information, see Section 48.4, "Adding the New Server to the Driver Set," on page 444.
<input type="checkbox"/>	13. Change the server-specific information for each driver. For more information, see Section 48.5, "Copying Server-Specific Information for the Driver Set," on page 444.
<input type="checkbox"/>	14. (Conditional) If you have RBPM, update the server-specific information from the old server to the new server for the User Application. For more information, see Section 48.5.3, "Changing the Server-specific Information for the User Application," on page 446.
<input type="checkbox"/>	15. Update your drivers to the package format. For more information, see Section 47.6, "Upgrading the Identity Manager Drivers," on page 433.
<input type="checkbox"/>	16. (Conditional) If you have custom policies and rules, restore your customize settings. For more information, see Section 47.7, "Restoring Custom Policies and Rules to the Driver," on page 434.
<input type="checkbox"/>	17. Remove the old server from the driver set. For more information, see Section 48.6, "Removing the Old Server from the Driver Set," on page 446.
<input type="checkbox"/>	18. Activate your upgraded Identity Manager solution. For more information, see Chapter 45, "Activating Identity Manager," on page 407.
<input type="checkbox"/>	19. (Conditional) If you are using NetIQ Sentinel, ensure that you are running the latest service pack. For more information about upgrading Sentinel, see the NetIQ Sentinel Installation and Configuration Guide .

48.2 Preparing For Mixed-case Searches on Roles and Resources

If your eDirectory tree was created with 3.6.1 or an earlier release of the RBPM, you must ensure that your environment supports mixed-case searches on roles and resources. Perform the `NrfCaseUpdate` procedure before migrating your existing drivers in Designer 4.0.2 or later. This procedure updates the schema by modifying the `nrfLocalizedDescrs` and `nrfLocalizedNames` attributes, which are used by the User Application drivers. This step is not required if you are installing the latest version of the identity applications or are upgrading from 3.7 or later.

48.2.1 How NrfCaseUpdate Affects the Schema

When the `NrfCaseUpdate` utility updates existing attributes in the eDirectory schema, any existing instances of those attributes are effectively deleted. User Application drivers use these attributes and thus will be affected by this schema update, specifically roles and separation of duties names and descriptions, custom attestation requests, and reports.

The `NrfCaseUpdate` procedure updates existing User Application drivers by providing a utility for exporting existing User Application drivers to an LDIF file before running the schema update. Importing the LDIF files after the schema update effectively recreates any objects deleted during the schema update.

As always, it is important that you back up any existing User Application drivers as a precaution. Remember that schema updates will affect all Identity Manager partitions, so it is very important to use NrfCaseUpdate to export any User Application drivers in the tree.

48.2.2 Creating a Backup of the User Application Drivers

Before running the NrfCaseUpdate procedure, you should back up your existing User Application drivers.

- 1 Install Designer.
- 2 Create an Identity Vault and map it to your Identity Manager server containing your User Application drivers.
- 3 Use the **Live->Import** command to import your Driver Set and User Application drivers.
- 4 Save and archive this Designer project.

48.2.3 Running NrfCaseUpdate

NrfCaseUpdate will prompt you to export each driver and then will perform the schema update. If you are unsure about the existence or location of any existing User Application drivers, you should not proceed, as the schema update may invalidate any existing User Application drivers.

The JRE provided under the Identity Manager installation directory, typically `/root/idm/jre`, can be used to run NrfCaseUpdate. If you require SSL connections to eDirectory, you will need to enable your JRE for SSL connections by following the instructions in [Section 48.2.5, “Enabling the JRE for SSL Connections,” on page 441](#).

Alternatively, you may run the NrfCaseUpdate utility remotely from a host with a JRE that contains the eDirectory certificate, such as the User Application server host. In this case, you will need to exit the NrfCaseUpdate utility using CTRL-C after exporting all drivers to LDIF and before the schema update. Then, you can manually update the schema on the eDirectory host using the `ndssch` command, as shown below:

```
ndssch -h hostname adminDN update-nrf-case.sch
```

NOTE: NrfCaseUpdate can accept several arguments to the command line. Pass `-help` or `-?` for more information.

To run NrfCaseUpdate:

- 1 Verify that you have completed a health check of the Identity Vault before running the NrfCaseUpdate utility. Use TID 3564075 to complete the health check.
- 2 Identify all the DNs of any existing User Application drivers before you start the utility. You will need authentication credentials to export these drivers to LDIF.
- 3 Run the NrfCaseUpdate utility. You may optionally pass the `-v` option to obtain more verbose output:

```
/root/idm/jre/bin/java -jar NrfCaseUpdate.jar -v
```

- 4 You will be asked if you have an existing User Application driver. Answer true if you have an existing User Application driver. Otherwise, answer false and skip to [Step 15 on page 440](#).

```
Do you currently have a User Application Driver configured [DEFAULT true] :
```

- 5** Next, the utility asks if you have more than one User Application driver. Answer true if you have more than one User Application driver:

Do you currently have more than one (1) User Application Driver configured [DEFAULT false] :
- 6** Specify the DN of the administrator with proper credentials for exporting the User Application driver:

Specify the DN of the Identity Vault administrator user.
This user must have inherited supervisor rights to the user application driver specified above.
(e.g. cn=admin,o=acme):
- 7** Enter the password for this administrator:

Specify the Identity Vault administrator password:
- 8** Enter the host name or IP address of the Identity Manager server hosting the User Application driver:

Specify the DNS address of the Identity Vault (e.g acme.com):
- 9** Specify the port to be used for the connection:

Specify the Identity Vault port [DEFAULT 389]:
- 10** The next question asks if you will use SSL for the connection. If you want to use SSL, the JRE requires the eDirectory certificate to be in the trusted store. To persist the certificate, follow the instructions in [Section 48.2.5, "Enabling the JRE for SSL Connections," on page 441](#).

Use SSL to connect to Identity Vault: [DEFAULT false] :
- 11** Specify the fully qualified distinguished name of the User Application driver that will be exported:

Specify the fully qualified LDAP DN of the User Application driver located in the Identity Vault
(e.g. cn=UserApplication,cn=driverset,o=acme):

If the DN includes a space, it has to be included in single quotes, as shown below:

'cn=UserApplication driver,cn=driverset,o=acme'
- 12** Specify a name for the LDIF file where the User Application will be exported:

Specify the LDIF file name where the restore data will be written (enter defaults to nrf-case-restore-data.ldif):
- 13** The utility will post information about the objects saved to the LDIF.
- 14** If you indicated you have multiple drivers, you will see the following prompt:

You indicated you have more than one (1) User Application Driver to configure.
Do you have another driver to export? [DEFAULT false] :

If you have another driver to export then specify true. The utility will repeat Steps 5 through 12 for each driver.

If you do not have another driver to export then specify false. Ensure that you have exported all existing drivers before proceeding as the utility will proceed with the schema update.
- 15** You will be prompted for the location of your ndssch utility, along with the typical locations. The ndssch utility is used for updating the schema.

Please enter the path to the schema utility:
For Unix/Linux typically /opt/novell/eDirectory/bin/ndssch
For Windows C:\Novell\NDS\schemaStart.bat:

- 16 The utility will post the status message for the schema update:

```
Schema has successfully been updated for mixed case compliance!
```

NOTE: Be sure to give eDirectory enough time to synchronize the schema changes. If you don't allow enough time, the import of the LDIF file fail.

- 17 Run another health check on the Identity Vault to verify that the schema was extended properly before importing the LDIF file. Use TID 3564075 to complete the health check.
- 18 After all drivers have been exported and the schema update has been applied successfully, you need to import each LDIF file. You should indicate to allow forward references in your `ice` command. A suggested command line is shown below:

```
ice -l [mylogfile.log] -v -SLDIF -f [your_created_ldif] -c -LDAP -s [hostname]
-p [389/636] -d [cn=myadmin,o=mycompany] -w [MYPASSWORD] -F -B
```
- 19 After all drivers have been re-imported, verify that the `NrfCaseUpdate` process was successful. See [Section 48.2.4, "Verifying the NrfCaseUpdate Process," on page 441](#) for more information.
- 20 After you have verified that the `NrfCaseUpdate` process was successful, you may continue with the RBPM 4.0.2 installation.

48.2.4 Verifying the NrfCaseUpdate Process

After all drivers have been re-imported, verify that the restoration was successful by reviewing the following items in the User Application:

- ♦ Role names and descriptions
- ♦ Separation of duties names and descriptions
- ♦ Attestation requests, including custom requests
- ♦ Reporting

After you complete the verification, you can continue with installation and upgrade to RBPM 4.0.2.

48.2.5 Enabling the JRE for SSL Connections

This section explains how to configure the JRE to use an SSL connection.

First, export a self-signed certificate from the certificate authority in the Identity Vault:

- 1 From iManager, in the **Roles and Tasks** view, click **Directory Administration > Modify Object**.
- 2 Select the certificate authority object for the Identity Vault, then click **OK**. It is usually found in the Security container and named as `TREENAME CA.Security`.
- 3 Click **Certificate > Self Signed Certificate**.
- 4 Click **Export**.
- 5 When you are asked if you want to export the private key with the certificate, click **No**, then click **Next**.
- 6 Select binary DER format.
- 7 Click the link **Save the exported certificate**.

- 8 Browse to a location on your computer where you want to save the file, then click **Save**.
- 9 Click **Close**.

Next, import the self-signed certificate into the JRE's trusted store.

- 1 Use the keytool utility that is included in the JRE.
- 2 Import the certificate into the Role Mapping Administrator's trust store by entering the following command at a command prompt:

```
keytool -import -file name_of_cert_file -trustcacerts -noprompt -keystore  
filename -storepass password
```

For example:

```
keytool -import -file tree_ca_root.b64 -trustcacerts -noprompt -keystore  
cacerts -storepass changeit
```

48.2.6 Restoring Invalidated User Application Drivers

If the schema update is applied to an existing User Application driver before that driver has been processed using NrfCaseUpdate, it will be invalidated and you will need to restore that driver using a backup.

IMPORTANT: It is essential that you do *not* delete or rename the invalidated User Application driver, since doing so will also invalidate all the driver's associations. Additionally, if the Role and Resource Service driver is running, and you delete the User Application driver, the Role and Resource Service driver will detect the role deletions and remove the roles from the assigned users.

Additionally, it is not sufficient to redeploy the backed up driver to Identity Manager as the schema change cannot be reconciled in this manner. The following procedure performs the restoration by deploying a renamed copy of the driver in order to generate the data to be restored.

The following procedure outlines the process for restoring the User Application driver backup using Designer 4.0.2:

- 1 Restart the eDirectory server to ensure that the schema modification has taken effect.
- 2 Open a copy of the Designer 4.0.2 project containing the backup of the User Application driver, UserAppDriver. Since this procedure modifies the driver name so it is important to use a copy of the project.
- 3 Select the connector between the User Application driver and the Identity Vault, right-click and choose **Properties**.
- 4 Specify a new name such as UserAppDriver_restore. Select **Apply** and **OK**.
- 5 Click **Save** to save the project.
- 6 Synchronize the ID Vault schema by selecting the ID Vault and choosing **Live->Schema->Compare** and choose to **Update Designer for the Reconcile Action**.
- 7 Save the project.
- 8 Deploy the renamed driver by selecting the driver and choosing **Driver->Deploy**.
- 9 Run NrfCaseUpdate and export the newly named driver to an LDIF file.
- 10 Make a copy of the LDIF file for editing.

- 11 Edit the LDIF file and rename all the driver references to reflect the User Application driver that you are restoring. For example, if your original User Application driver is `cn=UserAppDriver` then you would rename `cn=UserAppDriver_restore` to `cn=UserAppDriver`. This step effectively builds an LDIF file reflecting the real User Application driver.
- 12 Import the modified LDIF file using `ice`:


```
ice -l[mylogfile.log] -v -SLDIF -f[your_created_ldif] -c -DLDAAP -s[hostname] -p[389/636] -d[cn=myadmin,o=mycompany] -w[MYPASSWORD] -F -B
```
- 13 Note the status of the import using `ice` to ensure it was successful.
- 14 Follow the instructions under [Section 48.2.4, “Verifying the NrfCaseUpdate Process,”](#) on [page 441](#) to verify the restoration of the driver.
- 15 Delete the renamed driver from the Driver Set.

48.3 Updating the User Application

If the User Application runs on your old server, you must complete the following steps:

- 1 Run the `NrfCaseUpdate` utility for providing support for mixed-case searching on roles and resources.


This procedure updates the schema by modifying the `nrfLocalizedDescrs` and `nrfLocalizedNames` attributes, which are used by User Application drivers. For more information, see [Section 24.2, “Extending the eDirectory Schema Using the Wizard,”](#) on [page 206](#) and [Section 48.2, “Preparing For Mixed-case Searches on Roles and Resources,”](#) on [page 438](#).

- 2 In Designer, migrate the User Application driver. For more information, see the [Migrating to the Roles Based Provisioning Module](#) guide.
- 3 Create a new Role and Resource Service driver.

The Role and Resource Service driver is not migrated. If you have an existing Role and Resource Service driver, you must create a new driver for Identity Manager 4.0.2. For more information, see [Section 25.2, “Creating the Role and Resource Service Driver,”](#) on [page 214](#).
- 4 Deploy the migrated User Application driver to the Identity Vault. For more information, see [Section 25.3, “Deploying the Drivers for the User Application,”](#) on [page 214](#).
- 5 Install the User Application on the new server. For more information, see the following documentation:
 - ♦ “Migrating the User Application” (<https://www.netiq.com/documentation/idm402/migration/data/bmbw11t.html>) in the [Migrating to the Roles Based Provisioning Module](#) guide
 - ♦ “Installing the User Application and Roles Based Provisioning Module” on [page 199](#)
- 6 Ensure that you perform the post-installation steps described in “Migrating the User Application” (<https://www.netiq.com/documentation/idm402/migration/data/bmbw11t.html>) in the [Migrating to the Roles Based Provisioning Module](#) guide.

48.4 Adding the New Server to the Driver Set

If you are using iManager, you must add the new server to the driver set. Designer contains a Migration Wizard for the server that does this step for you. If you are using Designer, skip to [Section 48.5, “Copying Server-Specific Information for the Driver Set,” on page 444](#). If you are using iManager, complete the following procedure:

- 1 In iManager, click  to display the Identity Manager Administration page.
- 2 Click **Identity Manager Overview**.
- 3 Browse to and select the container that holds the driver set.
- 4 Click the driver set name to access the Driver Set Overview page.
- 5 Click **Servers > Add Server**.
- 6 Browse to and select the new Identity Manager 4.0.2 server, then click **OK**.

48.5 Copying Server-Specific Information for the Driver Set

You must copy all server-specific information that is stored in each driver and driver set to the new server’s information. This also includes GCVs and other data on the driver set that will not be there on the new server and need to be copied. The server-specific information is contained in:

- ♦ Global configuration values
- ♦ Engine control values
- ♦ Named passwords
- ♦ Driver authentication information
- ♦ Driver startup options
- ♦ Driver parameters
- ♦ Driver set data

You can do this in Designer or iManager. If you use Designer, it is an automated process. If you use iManager, it is a manual process. If you are migrating from an Identity Manager server earlier than 3.5 version to an Identity Manager server greater than or equal to 3.5, you should use iManager. For all other supported migration paths, you can use Designer.

- ♦ [Section 48.5.1, “Copying the Server-specific Information in Designer,” on page 444](#)
- ♦ [Section 48.5.2, “Changing the Server-specific Information in iManager,” on page 445](#)
- ♦ [Section 48.5.3, “Changing the Server-specific Information for the User Application,” on page 446](#)

48.5.1 Copying the Server-specific Information in Designer

This procedure affects all drivers stored in the driver set.

- 1 In Designer, open your project.
- 2 In the **Outline** tab, right-click the server, then select **Migrate**.
- 3 Read the overview to see what items are migrated to the new server, then click **Next**.
- 4 Select the target server from the list available servers, then click **Next**.


The only servers listed are servers that are not currently associated with a driver set and are equal to or newer than the source server's Identity Manager version.

- 5 Select one of the following options:
 - ♦ **Make the target server active:** Copies the settings from the source server to the target server and disables the drivers on the source server. NetIQ recommends using this option.
 - ♦ **Keep the source server active:** Does not copy the settings and disables all drivers on the target server.
 - ♦ **Makes both target and source servers active:** Copies settings from the source server to the target server without disabling the drivers on the source or target servers. This option is not recommended. If both drivers are started, the same information is written to two different queues and this can cause corruption.
- 6 Click **Migrate**.
- 7 Deploy the changed drivers to the Identity Vault.

For more information, see “[Deploying a Driver to an Identity Vault](#)” in the *Designer 4.0.2 for Identity Manager 4.0.2 Administration Guide*.
- 8 Start the drivers.

For more information, see [Section 46.3.2, “Starting the Drivers,”](#) on page 417.

48.5.2 Changing the Server-specific Information in iManager

- 1 In iManager, click  to display the Identity Manager Administration page.
- 2 Click **Identity Manager Overview**.
- 3 Browse to and select the container that holds the driver set.
- 4 Click the driver set name to access the Driver Set Overview page.
- 5 Click the upper right corner of the driver, then click **Stop driver**.
- 6 Click the upper right corner of the driver, then click **Edit properties**.
- 7 Copy or migrate all server-specific driver parameters, global configuration values, engine control values, named passwords, driver authentication data, and driver startup options that contain the old server's information to the new server's information. Global configuration values and other parameters of the driver set, such as max heap size, Java settings, and so on, must have identical values to those of the old server.
- 8 Click **OK** to save all changes.
- 9 Click the upper right corner of the driver to start the driver.
- 10 Repeat [Step 5](#) through [Step 9](#) for each driver in the driver set.

48.5.3 Changing the Server-specific Information for the User Application

You must reconfigure the User Application to recognize the new server. Run `configupdate.sh` or `configupdate.bat`.

- 1 Navigate to the configuration update utility located by default in the installation subdirectory of the User Application.
- 2 At a command prompt, launch the configuration update utility):
 - ♦ **Linux:** `configupdate.sh`
 - ♦ **Windows:** `configupdate.bat`
- 3 Specify the values as described in [Section 30.2, "Configuring the User Application,"](#) on page 277.

48.6 Removing the Old Server from the Driver Set

After the new server is running all of the drivers, you can remove the old server from the driver set.


- ♦ [Section 48.6.1, "Using Designer to Remove the Old Server from the Driver Set,"](#) on page 446
- ♦ [Section 48.6.2, "Using iManager to Remove the Old Server from the Driver Set,"](#) on page 446
- ♦ [Section 48.6.3, "Decommissioning the Old Server,"](#) on page 447

48.6.1 Using Designer to Remove the Old Server from the Driver Set

- 1 In Designer, open your project.
- 2 In the Modeler, right-click the driver set, then select **Properties**.
- 3 Select **Server List**.
- 4 Select the old Identity Manager server in the **Selected Servers** list, then click the < to remove the server from the **Selected Servers** list.
- 5 Click **OK** to save the changes.
- 6 Deploy the change to the Identity Vault.

For more information, see ["Deploying a Driver Set to an Identity Vault"](#) in the *Designer 4.0.2 for Identity Manager 4.0.2 Administration Guide*.

48.6.2 Using iManager to Remove the Old Server from the Driver Set

- 1 In iManager, click  to display the Identity Manager Administration page.
- 2 Click **Identity Manager Overview**.
- 3 Browse to and select the container that holds the driver set.
- 4 Click the driver set name to access the Driver Set Overview page.
- 5 Click **Servers > Remove Server**.
- 6 Select the old Identity Manager server, then click **OK**.

48.6.3 Decommissioning the Old Server

At this point, the old server is not hosting any drivers. If you no longer need this server, you must complete additional steps to decommission it:

- 1 Remove the eDirectory replicas from this server.

For more information, see [“Deleting Replicas”](#) in the *Novell eDirectory 8.8 Administration Guide*.

- 2 Remove eDirectory from this server.

For more information, see [TID 10056593](#), [“Removing a Server From an NDS Tree Permanently”](#).

49 Uninstalling Identity Manager Components

This section describes the process for uninstalling the components of Identity Manager. Some components have prerequisites for uninstallation. Ensure that you review full section for each component before beginning the uninstallation process.

49.1 Removing Objects from the Identity Vault

The first step in uninstalling Identity Manager is to delete all Identity Manager objects from the Identity Vault. When the driver set is created, the wizard prompts you to make the driver set a partition. If any driver set objects are also partition root objects in eDirectory, the partition must be merged into the parent partition before you can delete the driver set object.

To remove objects from the Identity Vault:

- 1 Perform a health check on the eDirectory database, then fix any errors that occur before proceeding.

For more information, see ["Keeping eDirectory Healthy"](http://www.novell.com/documentation/edir88/edir88/data/a5ziqam.html) (<http://www.novell.com/documentation/edir88/edir88/data/a5ziqam.html>) in the *Novell eDirectory 8.8 Administration Guide*.

- 2 Log on to iManager as an administrator with full rights to the eDirectory tree.
- 3 Select **Partitions and Replica > Merge Partition**.
- 4 Browse to and select the driver set object that is the partition root object, then click **OK**.
- 5 Wait for the merge process to complete, then click **OK**.
- 6 Delete the driver set object.

When you delete the driver set object, the process deletes all the driver objects associated with that driver set.

- 7 Repeat [Step 3](#) through [Step 6](#) for each driver set object that is in the eDirectory database, until they are all deleted.
- 8 Repeat [Step 1](#) to ensure that all merges completed and all of the objects have been deleted.

49.2 Uninstalling the Identity Manager Engine

When you install the Identity Manager engine, the installation process places an uninstallation script on the Identity Manager server. This script allows you to remove all services, packages, and directories that were created during the installation.

NOTE: Before uninstalling the Identity Manager engine, prepare the Identity Vault. For more information, see [Section 49.1, "Removing Objects from the Identity Vault,"](#) on page 449.

49.2.1 Uninstalling the Identity Manager Engine on Linux/UNIX

On the Linux or UNIX server that hosts the Identity Manager engine, navigate to the `Uninstall_Identity_Manager` script, located by default in the `/root/idm/Uninstall_Identity_Manager` directory.

To execute the script, enter the following command:

```
./Uninstall_Identity_Manager
```

49.2.2 Uninstalling the Identity Manager Engine as a Non-root User

If you installed the Identity Manager engine as a non-root user, the installation process places the `idm` directory in the directory of the user who performed the installation.

To uninstall the Identity Manager engine:

- 1 Log on as the user who installed the Identity Manager engine.
- 2 Navigate to the installation directory for the Identity Manager engine, by default `eDirectory_Base_Directory/opt/novell/eDirectory/bin/idm-uninstall`.
- 3 To execute the uninstallation script, enter the following command:

```
./Uninstall_Identity_Manager
```

49.2.3 Uninstalling the Identity Manager Engine on Windows

To uninstall the Identity Manager engine on a Windows server, use the Control Panel utility for adding and removing programs. For example, on Windows Server 2008, click **Programs and Features**. Right-click **Identity Manager**, then click **Uninstall**.

49.3 Uninstalling the Remote Loader

When you install the Remote Loader, the installation process places an uninstallation script on the server. This script allows you to remove all services, packages, and directories that were created during the installation.

49.3.1 Uninstalling the Remote Loader on Linux/UNIX

To uninstall the Remote Loader on a Linux or UNIX server, navigate to the uninstallation script, located by default in the `/root/idm/Uninstall_Identity_Manager` directory. To execute the script, enter `./Uninstall_Identity_Manager`.

If you installed the Remote Loader as a non-root user, the `idm` directory is by default in the directory of the user who performed the installation.

49.3.2 Uninstalling the Remote Loader as a Non-root User

If you installed the Remote Loader as a non-`root` user, the process places the `idm` directory in the directory of the user who performed the installation.

- 1 Log on as the user who installed the Remote Loader.
- 2 Navigate to the installation directory for the Remote Loader, by default `/user_directory/idm/Uninstall_Identity_Manager`.
- 3 To execute the uninstallation script, enter the following command:

```
./Uninstall_Identity_Manager
```

49.3.3 Uninstalling the Remote Loader on Windows

To uninstall the Remote Loader on a Windows server, use the Control Panel utility for adding and removing programs. For example, on Windows Server 2008, click **Programs and Features**. Right-click **Identity Manager**, then click **Uninstall**.

49.4 Uninstalling the Roles Based Provisioning Module

You must uninstall each component of the Roles Based Provisioning Module (RBPM), such as the drivers and the database.

If you need to uninstall the runtime components associated with RBPM, the uninstallation program automatically reboots your server, unless you are running the uninstall program in silent mode on Windows. You must manually reboot the Windows server. In addition, if you want to uninstall Identity Manager outside of the Integrated Installer, stop the `nds` service before launching the uninstall program.

NOTE: Before uninstalling RBPM, uninstall the Identity Manager engine. For more information, see [Section 49.2, “Uninstalling the Identity Manager Engine,” on page 449](#).

49.4.1 Deleting the Drivers for the Roles Based Provisioning Module

You can use Designer or iManager to delete the User Application driver and the Role and Resource Service driver.

- 1 Stop the User Application driver and the Role and Resource Service driver. Depending on the component that you use, complete one of the following actions:
 - ♦ **Designer:** Right-click the driver line, then click **Live > Stop Driver**.
 - ♦ **iManager:** On the Driver Set Overview page, click the upper right corner of the driver image, then click **Stop Driver**.
- 2 Delete the User Application driver and the Role and Resource Service driver. Depending on the component that you use, complete one of the following actions:
 - ♦ **Designer:** Right-click the driver line, then click **Delete**.
 - ♦ **iManager:** On the Driver Set Overview page, click **Drivers > Delete drivers**, then click the driver that you want to delete.

49.4.2 Uninstalling the User Application on Linux/UNIX

You must uninstall the User Application and its database from the application server. This procedure explains how to remove the User Application and its database from JBoss and PostgreSQL. If you are using another application server and database, refer to that product's documentation for instructions.

IMPORTANT: Be cautious when you remove the User Application because the process removes all the folders and files from the folder where the User Application scripts and supporting files were installed. When you remove the files, you might unintentionally uninstall JBoss or PostgreSQL. For example, the installation folder is typically `/opt/novell/idm/rbpm`. This folder also contains the folders for JBoss and PostgreSQL.

- 1 Log on to the server where you installed the User Application.
- 2 To uninstall the User Application, complete the following steps:

2a Navigate to the `Uninstall_Identity_Manager.bin` script, located by default in the `/root/idm/Uninstall_Identity_Manager` directory.

2b Enter the following command:

```
./Uninstall\ Roles\ Based\ Provisioning\ Module\ for\ Novell\ Identity\
Manager
```

- 3 To uninstall the database, complete the following steps:

3a Navigate to the `Uninstall_JBossPostgreSQL` script, located by default in the `/opt/novell/idm/Postgres/JBossPostgreSQL_Uninstaller/Uninstall_JBossPostgreSQL` directory.

3b Enter the following command:

```
./Uninstall_JBossPostgreSQL
```

49.4.3 Uninstalling the User Application on Windows

You must uninstall the User Application and its database from the application server. This procedure explains how to remove the User Application and its database from JBoss and PostgreSQL. If you are using another application server and database, refer to that product's documentation for instructions.

IMPORTANT: Be cautious when you remove the User Application because the process removes all the folders and files from the folder where the User Application scripts and supporting files were installed. When you remove the files, you might unintentionally uninstall JBoss or PostgreSQL. For example, the installation folder is typically `/opt/novell/idm/rbpm`. This folder also contains the folders for JBoss and PostgreSQL.

- 1 Log on to the server where you installed the User Application.
- 2 Open the Control Panel utility for adding and removing programs. For example, on Windows Server 2008, click **Programs and Features**.
- 3 In the utility, right-click **Roles Based Provisioning Module**, then select **Uninstall**.
- 4 Right-click **JBossPostgreSQL**, then click **Uninstall**.

49.5 Uninstalling the Identity Information Warehouse

You must uninstall the Identity Information Warehouse components in the following order:

1. Delete the drivers. For more information, see [Section 49.5.1, “Deleting the Reporting Drivers,” on page 453](#).
2. Delete the Reporting Module. For more information, see [Section 49.5.2, “Uninstalling the Identity Reporting Module,” on page 453](#).
3. Delete the Event Auditing System. For more information, see [Section 49.5.3, “Uninstalling the Event Auditing Service,” on page 454](#).

NOTE: To conserve disk space, the installation programs for EAS and the Identity Reporting Module do not install a Java virtual machine (JVM). Therefore, to uninstall one or more components, ensure that you have a JVM available and also make sure that the JVM is in the PATH . If you encounter an error during an uninstallation, add the location of a JVM to the local PATH environment variable, then run the uninstallation program again.

49.5.1 Deleting the Reporting Drivers

You can use Designer or iManager to delete the Data Collection and Managed System Gateway drivers.

- 1 Stop the drivers. Depending on the component that you use, complete one of the following actions:
 - ♦ **Designer:** For each driver, right-click the driver line, then click **Live > Stop Driver**.
 - ♦ **iManager:** On the Driver Set Overview page, click the upper right corner of each driver image, then click **Stop Driver**.
- 2 Delete the drivers. Depending on the component that you use, complete one of the following actions:
 - ♦ **Designer:** For each driver, right-click the driver line, then click **Delete**.
 - ♦ **iManager:** On the Driver Set Overview page, click **Drivers > Delete drivers**, then click the driver that you want to delete.

49.5.2 Uninstalling the Identity Reporting Module

Before deleting the Reporting Module, ensure that you have deleted the Data Collection and Managed System Gateway drivers. For more information, see [Section 49.5.1, “Deleting the Reporting Drivers,” on page 453](#).

To uninstall the Reporting Module, complete the following action for your operating system:

Linux and UNIX

Navigate to the `Uninstall_Identity_Reporting` script, located by default in the `/opt/novell/IdentityReporting/` directory.

To execute the script, enter `./Uninstall\ Identity\ Reporting`.

Windows

Use the Control Panel utility for adding and removing programs. For example, on Windows Server 2008, click **Programs and Features**. Right-click **Identity Reporting**, then click **Uninstall**.

49.5.3 Uninstalling the Event Auditing Service

Before uninstalling the Event Auditing Service, ensure that you have uninstalled the Reporting Module. For more information, see [Section 49.5.2, “Uninstalling the Identity Reporting Module,”](#) on page 453.

- 1 Navigate to the directory containing the uninstallation script, by default `/opt/novell/sentinel_eas/Uninstall_Event Auditing Service/Uninstall Event Auditing Service`.
- 2 Enter the following command: `./Uninstall\ Event\ Auditing\ Service`

49.6 Uninstalling Role Mapping Administrator

Role Mapping Administrator stores mappings and authorizations in the Identity Vault. Uninstalling Role Mapping Administrator deletes all the data from Role Mapping Administrator installation location. Uninstalling and reinstalling Role Mapping Administrator does not affect the information stored in the Identity Vault.

- 1 Navigate to the directory containing the installation files for Role Mapping Administrator, by default in the following locations:
 - ♦ **Linux:** `install-path/rma/`
 - ♦ **Windows:** `install-path/rma/`
- 2 To stop Role Mapping Administrator, execute the stop script:
 - ♦ **Linux:** `./stop.sh`
 - ♦ **Windows:** `stop.bat`
- 3 To run the uninstallation script, enter the following command:
 - ♦ **Linux:** `./rma-uninstall.sh -h -s`
 - ♦ **Windows:** `rma-uninstall.bat -h -s`

NOTE: The `-h` specifies help and `-s` specifies silent mode.

- 4 Delete the installation log that contains the parameters specified during the installation. The default location is `install-path/rma-install.log`.
- 5 Delete the installation directory.

49.7 Uninstalling Catalog Administrator

Uninstall Catalog Administrator only if you also want to uninstall all components of Identity Manager Home. Because Catalog Administrator is used along with the Identity Manager Home, you do not normally uninstall the component by itself. However, to stop using Catalog Administration, remove the `rra.war` file. If you remove `IDMProv.war`, Identity Manager Home stops working.

49.8 Uninstalling eDirectory

Before you uninstall eDirectory, you must understand your eDirectory tree structure and replica placements. For example, you should know whether you have more than one server in the tree.

- 1 (Conditional) If you have more than one server in your eDirectory tree, complete the following steps:
 - 1a (Conditional) If the server where you installed eDirectory holds any master replicas, promote another server in the replica ring to be a master before you remove eDirectory.
For more information, see “Managing Partitions and Replicas” (<http://www.novell.com/documentation/edir88/edir88/data/a2iiiiik.html>) in the *Novell eDirectory 8.8 Administration Guide*.
 - 1b (Conditional) If the tree on the server where you installed eDirectory holds the only copy of a partition, either merge this partition into the parent partition or add a replica of this partition to another server and make it the master replica holder.
For more information, see “Managing Partitions and Replicas” (<http://www.novell.com/documentation/edir88/edir88/data/a2iiiiik.html>) in the *Novell eDirectory 8.8 Administration Guide*.
 - 1c Perform a health check on the eDirectory database. Fix any errors that occur before proceeding.
For more information, see “Keeping eDirectory Healthy” (<http://www.novell.com/documentation/edir88/edir88/data/a5ziqam.html>) in the *Novell eDirectory 8.8 Administration Guide*.

- 2 Uninstall eDirectory according to the operating system:

Linux and UNIX

Navigate to the `nds-uninstall` script, located by default in the `/opt/novell/eDirectory/sbin` directory.

To execute the script, enter `./nds-uninstall`.

Windows

Use the Control Panel utility for adding and removing programs. For example, on Windows Server 2008, click **Programs and Features**. Right-click **Novell eDirectory**, then click **Uninstall**.

- 3 (Conditional) If you have more than one server in your eDirectory tree, complete the following steps:
 - 3a Delete any server-specific objects left in the tree.
 - 3b Perform another health check to verify that the server was properly removed from the tree.
For more information, see “Keeping eDirectory Healthy” (<http://www.novell.com/documentation/edir88/edir88/data/a5ziqam.html>) in the *Novell eDirectory 8.8 Administration Guide*.

49.9 Uninstalling Analyzer

- 1 Close Analyzer.
- 2 Uninstall Analyzer according to the operating system:

Linux and UNIX

Navigate to the `Uninstall Analyzer for Identity Manager` script, located by default in the `<installation_directory>/analyzer/UninstallAnalyzer` directory.

To execute the script, enter `./Uninstall\ Analyzer\ for\ Identity\ Manager`.

Windows

Use the Control Panel utility for adding and removing programs. For example, on Windows Server 2008, click **Programs and Features**. Right-click **Analyzer for Identity Manager**, then click **Uninstall**.

49.10 Uninstalling iManager

This section explains how to uninstall iManager and iManager Workstation. You do not need to follow a specific sequence for uninstalling iManager or the associated third-party components. NetIQ recommends reviewing the considerations for uninstalling any of these components:

- ♦ If you uninstall either the Web server or the servlet container, you cannot run iManager.
- ♦ On all platforms, the uninstallation removes only files that the process installed in the first place. The uninstallation process does not remove any files that the application creates as it runs. For example, the log files and auto-generated configuration files that are created while Tomcat runs.
- ♦ The uninstallation process does not remove any files that were created or modified files within the directory structure that were originally added during the installation. This action ensures that the process does not unintentionally delete data.
- ♦ Uninstalling iManager does not affect any of the RBS configurations that you have set in your tree. The uninstallation process does not remove log files or custom content.

After uninstalling iManager, ensure that the following directories are removed:

- ♦ `/var/opt/novell/iManager/`
- ♦ `/etc/opt/novell/iManager/`
- ♦ `/var/opt/novell/tomcat7/`
- ♦ `/etc/opt/novell/tomcat7/`

If you try reinstalling iManager with these directories still existing, the installation is not successful and the installation program generates errors.

IMPORTANT: Before uninstalling iManager, back up any custom content or other special iManager files that you want to retain. For example, customized plug-ins.

49.10.1 Uninstalling iManager on Linux

The process for uninstalling iManager does not uninstall NCI. You can uninstall NCI separately, if required.

IMPORTANT: If eDirectory is installed on the same server as iManager, NCI is required to continue to run eDirectory.

- 1 Log on as `root` to the computer where you want to uninstall iManager.
- 2 In a shell, execute the following command:

```
/var/opt/novell/iManager/nps/UninstallerData/UninstalliManager
```

49.10.2 Uninstalling iManager on Windows

To uninstall iManager components use the Control Panel utility for adding and removing programs. The following conditions apply to the uninstallation process:

- ♦ The Control Panel utility lists Tomcat and NCI separately from iManager. If you are no longer using them, uninstall these programs.
- ♦ If eDirectory is installed on the same server as iManager, do not uninstall NCI. eDirectory requires NCI to run.
- ♦ When uninstalling iManager, the program asks whether you want to remove all iManager files. If you select **Yes**, the program removes the files, including all custom content. However, the program does not remove 2.7 RBS objects from the eDirectory tree, and the schema remains in the same state.

49.10.3 Uninstalling iManager Workstation

To uninstall iManager Workstation, delete the directory where you extracted the files.

49.11 Uninstalling Designer

- 1 Close Designer.
- 2 Uninstall Designer according to the operating system:

Linux and UNIX

Navigate to the directory containing the uninstallation script, by default

```
<installation_directory>/designer/UninstallDesigner/Uninstall Designer for Identity Manager.
```

To execute the script, enter `./Uninstall\ Designer\ for\ Identity\ Manager`.

Windows

Use the Control Panel utility for adding and removing programs. For example, on Windows Server 2008, click **Programs and Features**. Right-click **Designer for Identity Manager**, then click **Uninstall**.

50 Troubleshooting

This section provides useful information for troubleshooting problems with installing Identity Manager. For more information about troubleshooting Identity Manager, see the guide for the specific component.

50.1 Troubleshooting the User Application and RBPM Installation

The following table lists the issues you might encounter and the suggested actions for working on these issues. If the problem persists, contact your NetIQ representative.

Issue	Suggested Actions
<p>You want to modify one or more of the following the User Application configuration settings created during installation:</p> <ul style="list-style-type: none">◆ Identity Vault connections and certificates◆ E-mail settings◆ Identity Manager Engine User Identity and User Groups◆ Access Manager or iChain settings	<p>Run the configuration utility independent of the installer.</p> <p>Linux: Run the following command from the installation directory (by default, <code>/opt/novell/idm</code>):</p> <pre>configupdate.sh</pre> <p>Windows: Run the following command from the installation directory (by default, <code>c:\opt\novell\idm</code>):</p> <pre>configupdate.bat</pre>
<p>Starting the application server causes the following exception:</p> <pre>port 8180 already in use</pre>	<p>Shut down any instances of Tomcat (or other server software) that might already be running. If you reconfigure the application server to use a port other than 8180, edit the <code>config</code> settings for the User Application driver.</p>
<p>When you start the JBoss or WebLogic server, the application reports that the administration credentials cannot be decrypted or used.</p>	<p>Check whether the AUTHPROPS table contains an entry for the LDAP administrator. For example, <code>ldap.admin.pwd</code> or <code>ldap.admin.user</code>. If yes, remove the entry or entries, then restart the application server.</p> <p>This issue might occur after migrating from version 4.0.0 or earlier.</p>
<p>When the application server starts, the application reports it cannot find trusted certificates.</p>	<p>Ensure that you start the application server by using the JDK specified during the installation of the User Application.</p>
<p>Cannot log in to the portal admin page.</p>	<p>Ensure that the User Application Administrator account exists. This account is not the same as your iManager administrator account.</p>
<p>Cannot create new users even with administrator account.</p>	<p>The User Application Administrator must be a trustee of the top container and should have Supervisor rights. You can try setting the User Application Administrator's rights equivalent to the LDAP Administrator's rights (using iManager).</p>

Issue	Suggested Actions
Starting application server throws keystore errors.	<p>Your application server is not using the JDK specified during the installation of the User Application.</p> <p>Use the <code>keytool</code> command to import the certificate file:</p> <pre>keytool -import -trustcacerts -alias aliasName -file certFile -keystore ..\lib\security\cacerts -storepass changeit</pre> <ul style="list-style-type: none"> ◆ Replace <i>aliasName</i> with a unique name of your choice for this certificate. ◆ Replace <i>certFile</i> with the full path and name of your certificate file. ◆ The default keystore password is <code>changeit</code> (if you have a different password, specify it).
Email notification not sent.	<p>Run the <code>configupdate</code> utility to check whether you supplied values for the following User Application configuration parameters: <i>Email From</i> and <i>Email Host</i>.</p> <p>Linux: Run the following command from the installation directory (by default, <code>/opt/novell/idm</code>):</p> <pre>configupdate.sh</pre> <p>Windows: Run the following command from the installation directory (by default, <code>c:\opt\novell\idm</code>):</p> <pre>configupdate.bat</pre>

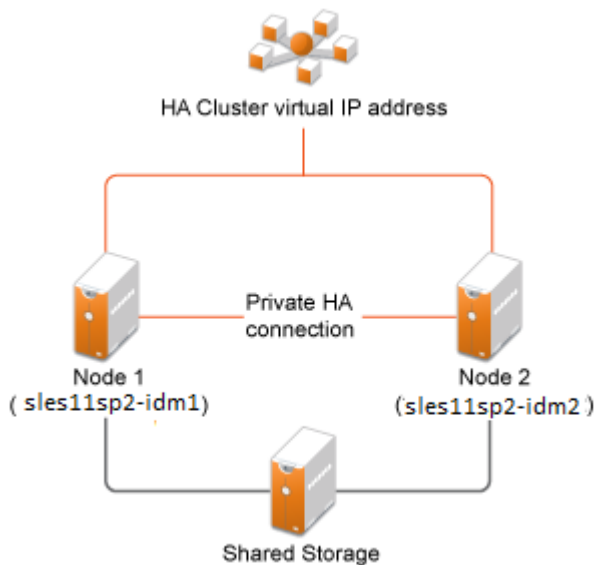
A Sample Identity Manager Cluster Deployment Solution

The appendix provides step-by-step instructions on how to configure eDirectory and Identity Manager into a cluster environment with shared storage and an example of a clustered Identity Manager deployment.

- ♦ [Section A.1, “Prerequisites,” on page 461](#)
- ♦ [Section A.2, “Installation Procedure,” on page 462](#)

For a production-level Linux High Availability (HA) solution with shared storage, implementing a fencing mechanism in the cluster is recommended. Although there are different methods of implementing fencing mechanisms in the cluster, in our example, we use a STONITH resource which uses the Split Brain Detector (SBD). [Figure A-1](#) shows a sample cluster deployment solution.

Figure A-1 Sample cluster deployment solution



A.1 Prerequisites

- ♦ Two servers running SuSE Linux Enterprise Server (SLES) 11 SP2 64-bit for nodes
- ♦ One server running SLES 11 SP2 64-bit for iSCSI Server
- ♦ SLES11 SP2 64-bit HA extension ISO image file
- ♦ Six static IPs:
 - ♦ Two static IP addresses for each node. One IP address is used for public network and the other for Heartbeat.

- ♦ One static IP address for the cluster. This IP address is dynamically assigned to the node currently running eDirectory.
- ♦ One IP address for iSCSI Server.

A.2 Installation Procedure

This section explains the procedure to install and configure the following to set up the cluster environment.

A.2.1 Configuring the iSCSI Server

An iSCSI target is a device that is configured as a common storage for all nodes in a cluster. It is a virtual disk that is created on the Linux server to allow remote access over an Ethernet connection by an iSCSI initiator.

An iSCSI initiator is any node in the cluster that is configured to contact the target (iSCSI) for services. The iSCSI target should be always up and running so that any host acting as an initiator can contact the target. Before installing iSCSI target on the iSCSI server, ensure that the iSCSI target has sufficient space for a common storage.

Install the iSCSI initiator packages on the other two nodes after installing SLES 11 SP2.

During the SLES 11 SP2 installation:

- 1 Create a separate partition and specify the partition path as the iSCSI shared storage partition.
- 2 Install the iSCSI target packages.

To configure the iSCSI server:

- 1 Create a block device on the target server.
- 2 Type the `yast2 disk` command in terminal.
- 3 Create a new Linux partition, and select `Do not format`.
- 4 Select the `Do not mount the partition`.
- 5 Specify the partition size.
- 6 Type the `yast2 iscsi-server` command in terminal.
- 7 Click the **Service** tab, then select `When Booting in Service Start`.
- 8 In the **Targets** tab, click **Add** to enter the partition path (as created during the SLES installation).
- 9 Click **Finish**.
- 10 Run the `cat /proc/net/iet/volume` command in the terminal to verify if the iSCSI target is installed

A.2.2 Configuring the iSCSI initiator on all Nodes

You must configure the iSCSI initiator on all cluster nodes to connect to the iSCSI target.

To configure the iSCSI initiator:

- 1 Install the iSCSI initiator packages.
- 2 Run the `yast2 iscsi-client` in terminal.
- 3 Click the **Service** tab and select **When Booting in Service Start**.

- 4 Click the **Connected Targets** tab, and click **Add** to enter the IP address of the iSCSI target server.
- 5 Select **No Authentication**.
- 6 Click **Next**, then click **Connect**.
- 7 Click **Toggle Start-up** to change the start-up option from manual to automatic, then click **Next**.
- 8 Click **Next**, then click **OK**.
- 9 To check the status of the connected initiator on the target server, run the `cat /proc/net/iet/session` command on the target server. The list of initiators that are connected to iSCSI server are displayed.

A.2.3 Partitioning the Shared Storage

Create two shared storage partitions: one for SBD and the other for Oracle Cluster File System 2 (OCFS2).

To partition the shared storage:

- 1 Run the `yast2 disk` command in terminal.
- 2 In the **Expert Partitioner** dialog box, select the shared volume. In our example, select `sdb` from the **Expert Partitioner** dialog box.
- 3 Click **Add**, select **Primary partition** option, and click **Next**.
- 4 Select **Custom size**, and click **Next**. In our example, the custom size is 10 MB.
- 5 Under **Formatting options**, select **Do not format partition**. In our example, the File system ID is `0x83 Linux`.
- 6 Under **Mounting options**, select **Do not mount partition**, then click **Finish**.
- 7 Click **Add**, then select **Primary partition**.
- 8 Click **Next**, then select **Maximum Size**, and click **Next**.
- 9 In **Formatting options**, select **Do not format partition**. In our example, specify the File system ID as `0x83 Linux`.
- 10 In **Mounting options**, select **Do not mount partition**, then click **Finish**.

A.2.4 Installing the HA Extension

To install the HA extension:

- 1 Go to the [Novell Downloads Web site \(http://download.novell.com\)](http://download.novell.com).
- 2 In the **Product or Technology** menu, select **SUSE Linux Enterprise HAExtension**, then click **Search**.

NOTE: Select and install the appropriate HA extension ISO file based on your system architecture.

- 3 Download the ISO file on each server.
- 4 Open **YaST Control Center** dialog box, click **Add-on products > Add**.
- 5 Click **Browse** and select the local ISO image, then click **Next**.
- 6 In the **Software selection and system tasks** dialog box, select **High Availability**. Repeat this step on the other server.

A.2.5 Configuring the HA Cluster

Configure the unicast IP addresses for Heartbeat:

- 1 Configure the other interface on both the nodes with the static IP addresses, which will be used for node communication (Heartbeat). In our example, the IP addresses are 10.10.10.13 and 10.10.10.14 on Node1 and Node2, respectively.
- 2 Ping the two servers using their host names to test the connectivity between the two servers.

IMPORTANT: If the machines are unable to ping each other, edit the local `/etc/hosts` file and add the host names of the other nodes and their IP addresses. In our example, the `/etc/hosts` file contains the following:

- ◆ 10.10.10.13 sles11sp2-idm1
- ◆ 10.10.10.14 sles11sp2-idm2

-
- 3 On Node1, run the `yast2 cluster` command in the terminal.
 - 4 In the **Cluster - Communication Channels** dialog box, specify the following details:
 - 4a Set the Transport protocol to UDPU.
 - 4b Specify the **Bind Network Address**, which is the network address of the unicast IP addresses. In our example, the bind network address is 10.10.10.0.
 - 4c Specify the **Multicast port**. In our example, the Multicast port is 5405.
 - 4d Click **Add** to enter the IP address for each node at the member address. In our example, the IP addresses are 10.10.10.13 and 10.10.10.14 on Node1 and Node2, respectively.
 - 4e Select **Auto generate Note ID**, then click **Next**.
 - 5 In the **Cluster -Security** dialog box, select the **Enable Security Auth**, set **Threads** to **1**, then click **Generate Auth Key File**.

This creates an authentication key to allow other nodes to join your cluster. The key is stored in the `/etc/corosync/authkey` location. Copy this file to the other node.

- 6 In the **Cluster - Service** dialog box, select **On--Start openais at booting**, then click **Start openais Now**.
- 7 Select **Start Management as well** to allow the cluster to be managed by `crm_gui`. For more information, see [Section A.2.2, "Configuring the iSCSI initiator on all Nodes," on page 462](#).
- 8 In the **Sync Host** panel, perform the following actions:
 - 8a Click **Add** to add hostnames of the cluster nodes.
 - 8b Click **Generate Pre-Shared-Keys** to synchronize the configuration file between nodes, then copy it to the other node. The key file is stored in `/etc/csync2/key_hagroup`.
 - 8c In the **Sync File** pane, click **Add Suggested Files** to automatically generate a list of common files to synchronize between nodes.
 - 8d Click **Turn csync2 ON**, then click **Next**.
 - 8e Click **Next**, then click **Finish**.
- 9 Run the `passwd hacluster` command to set the hacluster user password on all nodes.

NOTE: Set the same password for hacluster user on nodes.

- 10 Run the following commands to copy the configuration files and authentication keys to the other node:
 - ◆ `# scp /etc/csync2/csync2.cfg node2:/etc/csync2/`

- ◆ # scp /etc/csync2/key_hagroup node2:/etc/csync2/
- ◆ # scp /etc/corosync/authkey node2:/etc/corosync/
- ◆ # scp /etc/corosync/corosync.conf node2:/etc/corosync/

11 Reboot all the nodes after the configuration files are copied to Node2.

12 Run the `csync2 -xv` command.

13 Create the `mkdir -p /share` directory to mount the shared storage.

14 On Node2, do the following:

14a Run the `yast2 cluster` command in the terminal.

NOTE: The wizard window does not appear, because the configuration file is already copied over.

14b In the **Service** tab, select **Check On -- Start openais at booting**, then click **Start openais Now**.

14c In the **Configure Csync2** tab, click **Turn csync2 ON**, then click **Finish**.

14d Create the `mkdir -p /share` directory to mount the shared storage.

The cluster should be up and running.

15 Run the `crm_mon` command in the terminal to verify the status. Following is a sample output:

```

=====
Last updated: Fri Aug 5 16:38:36 2011
Stack: openais
Current DC: node1 - partition with quorum
Version: 1.1.2-2e096a41a5f9e184a1c1537c82c6da1093698eb5
2 Nodes configured, 2 expected votes
0 Resources configured.
=====
Online: [node1 node2]
```

A.2.6 Configuring Global Cluster Options

A resource is a service or an application that is managed by the cluster. The cluster software stack monitors the resources to check if they are up and running. If the resources stop running for some reason, the cluster detects the failure and starts or restarts that resource on the other node to provide high availability. In our example, the global cluster options are configured on Node1.

To configure the HA resource on Node1:

1 Run the `crm_gui` command in the terminal.

2 Click **Connection menu >Login**. Log on using the IP address of either of the nodes.

3 Click the **CRM Config** tab, then change **Default Resource Stickiness** to a positive value.

This is to ensure that the resources in the cluster remain in the current location. In our example, the value is 1.

4 Change **No Quorum Policy** to **ignore**.

This ensures that the cluster services are up and running even if one of the nodes is down.

5 Click **Apply**.

A.2.7 Configuring the OCFS Resources

Before you create the OCFS2 volume, you must configure the following resources as services in the cluster:

- ♦ distributed lock manager (DLM)
- ♦ O2CB
- ♦ STONITH resource

OCFS2 requires a DLM resource to run on all nodes in the cluster and is usually configured as a clone. In our example, OCFS resources are configured on Node1.

A.2.7.1 Configuring the DLM and O2CB Resources

To configure the DLM and O2CB resources on Node1:

- 1 Start shell and log on as root or equivalent.
- 2 Run the `crm configure` command in terminal.
- 3 Run the following command to create primitive resources for DLM and O2CB:

```
primitive dlm ocf:pacemaker:controld op monitor interval="60" timeout="60"  
primitive o2cb ocf:ocfs2:o2cb op monitor interval="60" timeout="60"
```

NOTE: The DLM clone resource controls the DLM service to ensure that the service is started on all nodes in the cluster. Due to the base group's internal co-location and ordering, the O2CB service is only started on nodes where a copy of the DLM service is already running.

- 4 Run the following command to create base group and base clone:

```
group base-group dlm o2cb clone base-clone base-group meta interleave="true"  
target-role="Started"
```

- 5 Run the `show` command to view the changes.
- 6 Run the `commit` command, then type **Exit**.

A.2.7.2 Configuring STONITH Resources

It is recommended to create a 10 MB partition at the start of the device. (In our example, the SBD partition is referred as `/dev/sdb1`.)

IMPORTANT: Ensure that you work on device names that do not change. You must work on a device using `/dev/disk/by-id` at the beginning of the device name. For example, to assign the device `/dev/disk/by-id/scsi-149455400000000000000000003000000250600000f000000` as the SBD STONITH device, use `sd -d /dev/disk/by-id/scsi-149455400000000000000000003000000250600000f000000 create`.

Run the `ls -l` command to verify the device name.

- 1 In a terminal, run the following command to initialize the SBD device on Node1:

```
sd -d /dev/sdb1 create
```
- 2 Run the `sd -d /dev/sdb1 dump` command to check that the following details that have been written to the device:
 - ♦ Header version: 2

- ◆ Number of slots: 255
- ◆ Sector size: 512
- ◆ Timeout (watchdog): 5
- ◆ Timeout (allocate): 2
- ◆ Timeout (loop): 1
- ◆ Timeout (msgwait): 10

A.2.7.3 Setting Up the Software Watchdog

In SLES HA Extension, the Watchdog support in the kernel is enabled by default. It is shipped with a number of different kernel modules that provide hardware-specific watchdog drivers. The appropriate watchdog driver for your hardware is automatically loaded during system boot.

Softdog is the most generic driver. As most watchdog driver names contain strings such as wd, wdt, and dog, run the following command to check the driver that is currently loaded:

```
lsmod | grep wd
```

A.2.7.4 Starting the SBD Daemon

To start the SBD daemon on Node1:

- 1 In a terminal, run the `rcopenais stop` command to stop OpenAIS.
- 2 Create the `/etc/sysconfig/sbd` file, then add the following:

```
SBD_DEVICE="/dev/sdb1"

#The next line enables the watchdog support:

SBD_OPTS="-W"
```

NOTE: If the SBD device is not accessible, the daemon fails to start and inhibit OpenAIS startup.

- 3 Run the `yast2 cluster` command in the terminal.
- 4 In the **Configure Csync2** tab, click **Add** under the **Sync File** pane and specify the SBD file path as follows:

```
/etc/sysconfig/sbd
```

- 5 Click **OK**.
- 6 In the **Sync File** pane, click **Add Suggested Files** to automatically generate a list of common files to synchronize between nodes.
- 7 Run the `csync2 -xv` command.
- 8 Run the `sbd -d /dev/sdb1 allocate <nodename>` command to allocate the nodes. Run this command twice to allocate the node names to SDB device. In our example, the following commands are executed as follows.

```
sbd -d/dev/sdb1 allocate sles11sp2-idm1
sbd -d/dev/sdb1 allocate sles11sp2-idm2
```

- 9 Run the `rcopenais start` command to start OpenAIS.

A.2.7.5 Testing the SBD

To test the SBD on Node1:

- 1 Run the `sbd -d /dev/sdb1 list` command to dump the node slots and their current messages from the SBD device.
- 2 Run the `sbd -d /dev/sdb1 message SLES11SP2-idm2 test` command to send a test message to one of the nodes.

The node acknowledges the receipt of the message in the system logs. The following is a sample message:

```
Aug 29 14:10:00 SLES11SP2-idm2 sdb1: [13412]: info: Received command test from
SLES11SP2-idm1 on disk /dev/sdb1
```

IMPORTANT: The acknowledgement confirms that the SBD is up and running on the node and indicates that the SBD is ready to receive messages.

A.2.7.6 Configuring the Fencing Resource

To complete the SBD setup, activate SBD as a STONITH/fencing mechanism in Cluster Information Base (CIB). Run the following commands in the terminal on Node1:

```
node1# crm configure
crm(live)configure# property stonith-enabled="true"
crm(live)configure# property stonith-timeout="60s"
crm(live)configure# primitive stonith_sbd stonith:external/sbd params
sbd_device="/dev/sdb1" meta is-managed="true"
crm(live)configure# commit
crm(live)configure# quit
```

NOTE: The value set for `stonith-timeout` depends on the `msgwait timeout`. For example, if you set the default `msgwait timeout` value to 10 seconds, set the `stonith-timeout` value to 60 seconds.

A.2.7.7 Creating an OCFS2 Volume

Before you begin, prepare the block devices you plan to use for your OCFS2 volume. Leave the devices where you plan to use the OCFS2 volume as unallocated free space, then create and format the OCFS2 volume using the `mkfs.ocfs2` utility.

To create the OCFS2 volume on Node1:

- 1 Open a terminal window and log on as root.
- 2 Run the `crm_mon` command to check if the cluster is online.
- 3 Create a OCFS2 file system on `/dev/sdb2` that supports up two cluster nodes, then run the following command: `mkfs.ocfs2 -N 2 /dev/sdb2`

A.2.7.8 Mounting an OCFS2 Volume

To mount an OCFS2 volume on Node 1:

- 1 Start a shell and log on as root or equivalent.
- 2 Run the `crm configure` command.
- 3 Configure Pacemaker to mount the OCFS2 file system on each node in the cluster:

```
primitive ocfs2-1 ocf:heartbeat:Filesystem params device="/dev/sdb2"
directory="/share" fstype="ocfs2" options="acl" op monitor interval="20"
timeout="40"
```

- 4 With the following steps, add the file system primitive to the base group that you have configured in [“Configuring the DLM and O2CB Resources”](#) on page 466:

4a Specify the **edit base-group**.

4b In the vi editor, modify the group as follows, then save your changes:

```
group base-group dlm o2cb ocfs2-1 meta target-role = "Started"
```

NOTE: Due to the base group’s internal co-location and ordering, Pacemaker only starts the OCFS2-1 resource on nodes that have an O2CB resource already running.

- 5 Run the `show` command to check that you have configured all the required resources.
- 6 Run the `commit` command, then type **Exit**.

A.2.8 Configuring IP Resource

Run the following commands to configure the IP resource on Node1:

```
node1# crm configure
```

```
crm(live)configure# primitive clusterip ocf:heartbeat:IPaddr operations $id="clusterip-
operations" op monitor interval="5s" timeout="60s" params ip="10.52.190.15" meta
resource-stickiness="100" target-role="Started"
```

```
crm(live)configure# group eDir_group clusterip meta is-managed="true" target-
role="Started"
```

```
crm(live)configure# show
```

```
crm(live)configure# commit
```

A.2.9 Installing and Configuring eDirectory and Identity Manager on Cluster Nodes

- 1 To install eDirectory on cluster nodes:

Install eDirectory 8.8 SP7. For step-by-step instructions to configure eDirectory on HA clusters, see [“Deploying eDirectory on High Availability Clusters”](#) in the *eDirectory 8.8 SP7 Installation Guide*.

IMPORTANT: Ensure that the virtual IP is configured on the Node1 before you install eDirectory on Node1.

- 2 Install Identity Manager on Node 1 using the Metadirectory Server option.

3 Install Metadirectory on Node 2 Server using the `DCLUSTER_INSTALL` option.

Run the `./install.bin -DCLUSTER_INSTALL="true"` command in the terminal.

The installer installs the Identity Manager files are installed without any interaction with eDirectory.

A.2.10 Configuring the eDirectory Resource

Run the following commands to configure the eDirectory resource on Node 1:

```
node1# crm configure
```

```
crm(live)configure# primitive eDirectory ocf:heartbeat:edir88 operations
$Id="eDirectory-operations" op monitor interval="15s" enabled="true" timeout="60s" on-
fail="restart" start-delay="30s" params edir_config_file="/etc/opt/novell/eDirectory/
conf/nds.conf" meta resource-stickiness="100" target-role="Started"
```

```
crm(live)configure# edit eDir_group
```

In the In the vi editor, modify the group, then add the text “eDirectory” after clusterip, as follows to save your changes:

```
group eDir_group clusterip eDirectory \
meta is-managed="true" target-role="Started"

crm(live)configure# show

crm(live)configure# commit
```

In the PaceMaker GUI main window, click Management tab, then start **eDir_group** if the resources are not running. The following figure shows the resources that are up and running in the cluster setup.

Pacemaker GUI

Connection View Shadow Tools Help

Live

- Configuration
 - CRM Config
 - Resource Defaults
 - Operation Defaults
 - Nodes
 - Resources
 - Constraints
 - ACLs
 - Management

Name	Status	Details
Cluster	● have quorum	Openais & Pacemaker
SLES11 SP2-IDM1	● online (dc)	
SLES11 SP2-IDM2	● online	
Resources	●	
base-clone	● clone	
base-group:0	● group	
dlm:0	● running on [SLES11 SP2-IDM1]	ocf::pacemaker:controld
o2cb:0	● running on [SLES11 SP2-IDM1]	ocf::ocfs2:o2cb
ocfs2-1:0	● running on [SLES11 SP2-IDM1]	ocf::heartbeat:Filesystem
base-group:1	● group	
dlm:1	● running on [SLES11 SP2-IDM2]	ocf::pacemaker:controld
o2cb:1	● running on [SLES11 SP2-IDM2]	ocf::ocfs2:o2cb
ocfs2-1:1	● running on [SLES11 SP2-IDM2]	ocf::heartbeat:Filesystem
stonith_sbd	● running on [SLES11 SP2-IDM2]	stonith::external/sbd
eDir_group	● group	
clusterip	● running on [SLES11 SP2-IDM2]	ocf::heartbeat:IPAddr
eDirectory	● running on [SLES11 SP2-IDM2]	ocf::heartbeat:eDir88

