NetIQ Identity Manager

Setup Guide

February 2017

NetIQ

Legal Notice

For information about NetIQ legal notices, disclaimers, warranties, export and other use restrictions, U.S. Government restricted rights, patent policy, and FIPS compliance, see https://www.netiq.com/company/legal/.

Copyright (C) 2017 NetIQ Corporation. All rights reserved.

Contents

About this Book and the Library 17
About NetIQ Corporation 19

Part I Introduction 21

1 Overview of the Components of Identity Manager 23

2 Creating and Maintaining Your Identity Manager Environment 25

Designer for Identity Manager . . . 25
Analyzer for Identity Manager . . . 25
Role Administration . . . 26
iManager . . . 26

3 Managing Data in the Identity Manager Environment 27

Understanding Data Synchronization . . . 27
Understanding Auditing, Reporting, and Compliance . . . 27
Understanding the Components for Synchronizing Your Identity Data . . . 28
- Identity Vault . . . 28
- Identity Manager Engine . . . 28
- Remote Loader . . . 28
- Identity Reporting . . . 29

4 Provisioning Users for Secure Access 31

Understanding the Attestation Process in Identity Manager . . . 31
Understanding the Self-Service Process in Identity Manager . . . 32
Understanding the Components for Managing User Provisioning . . . 33
- User Application and Roles Based Provisioning Module . . . 33
- Identity Manager Dashboard . . . 34

Using Self-Service Password Management in Identity Manager . . . 35
- Understanding the Default Self-Service Process . . . 35
- Understanding the Legacy Password Management Provider . . . 36

Using Single Sign-on Access in Identity Manager . . . 37
- Understanding Authentication with One SSO Provider . . . 37
- Understanding the Keystore for One SSO Provider . . . 38
- Understanding Audit Events for One SSO Provider . . . 38

Part II Planning to Install Identity Manager 39

5 Planning Overview 41

Planning Checklist . . . 41
Understanding the Integrated and Standalone Installation Processes . . . 43
- Understanding the Integrated Installation Process . . . 43
- Understanding the Standalone Installation Process . . . 44

Recommended Installation Scenarios and Server Setup . . . 44

Send Events to an Auditing Service without Reporting in Identity Manager . . . 44
Send Events to Identity Manager and Generate Reports . . . 45
Send Events to an External Service Before Pushing Events to Identity Manager . . . 45
Recommended Server Setup . . . 46
Selecting an Operating System Platform for Identity Manager . . . 47
Understanding Licensing and Activation . . . 49
Understanding Identity Manager Communication . . . 49
Understanding Language Support . . . 51
Translated Components and Installation Programs . . . 51
Special Considerations for Language Support . . . 52
Downloading the Installation Files . . . 52

6 Considerations and Prerequisites for Installation 53

Ensuring High Availability for Identity Manager . . . 53
Minimum Space Requirement on Linux Servers . . . 54
Installing Identity Manager on SLES 12 SP1 or Later Servers . . . 55
Installing Identity Manager on RHEL 6.x or 7.x Servers . . . 55
Prerequisites . . . 55
Running a Prerequisite Check . . . 56
Ensuring that the Server has Dependent Libraries . . . 56
Creating a Repository for the Installation Media . . . 57

Part III Installing the Identity Vault 59

7 Planning to Install the Identity Vault 61

Checklist for Installing the Identity Vault . . . 61
Prerequisites and Considerations for Installing the Identity Vault . . . 62
Prerequisites for Installing the Identity Vault . . . 62
Prerequisites for Installing the Identity Vault as a Non-root User . . . 64
Prerequisites for Installing Identity Vault on a Windows Server . . . 64
Prerequisites for Installing the Identity Vault in a Clustered Environment . . . 65
Understanding Identity Manager Objects in eDirectory . . . 66
Replicating the Objects that Identity Manager Needs on the Server . . . 66
Using Scope Filtering to Manage Users on Different Servers . . . 68
Understanding the Linux Packages in the Identity Vault Installation Kit . . . 69
System Requirements for the Identity Vault . . . 71

8 Preparing to Install the Identity Vault 73

Using Escape Characters when a Container Name Includes a Period (“.”) . . . 73
Using OpenSLP or hosts.nds for Resolving Tree Names . . . 73
Using a hosts.nds File to Resolve Tree Names . . . 74
Understanding OpenSLP . . . 75
Configuring SLP for the Identity Vault . . . 77
Improving Identity Vault Performance . . . 78
Using IPv6 Addresses on the Identity Vault Server . . . 79
Using IPv6 Addresses on Linux Servers . . . 79
Using IPv6 Addresses on Windows Servers . . . 80
Using LDAP to Communicate with the Identity Vault . . . 80
Installing NICI Manually on Workstations that have Management Utilities . . . 81
Installing NICI on Linux Servers . . . 81
Installing NICI on Windows Servers . . . 82
Installing NMAS Client Software . . . 83
Installing and Configuring NMAS Client Software on Linux Servers . . . 83

Installing NMAS Client Software on Windows Servers . . . 84
Working with eDirectory 9.0.2 or Later . . . 84
Features That Can be Enabled on the Identity Vault Server . . . 84
Changing the NICI Configuration to a Non-FIPS Mode in eDirectory . . . 85

9 Installing the Identity Vault on a Linux Server 87

Installing the Identity Vault as Root . . . 87
Installing the Identity Vault as a Non-root User . . . 89

10 Installing the Identity Vault on a Windows Server 91

Using the Wizard to Install the Identity Vault on a Windows Server . . . 91
Silently Installing and Configuring the Identity Vault on a Windows Server . . . 92
Editing the response.ni File . . . 93
Performing a Silent or Unattended Installation . . . 98
Performing a Silent Configuration . . . 99
Performing a Silent Installation Combined with Configuration . . . 99

11 Applying Hotfix 2 to the Identity Vault 101

Prerequisites for Installing the Hotfix . . . 101
Installing the Hotfix as a Root User or an Administrator . . . 101
Installing the Hotfix as a Non-root User . . . 103

12 Configuring the Identity Vault after Installation 105

Modifying the eDirectory Tree and Replica Server with the ndsconfig Utility . . . 105
Understanding the ndsconfig Utility Parameters . . . 106
Adding SecretStore to the Identity Vault Schema . . . 109
Configuring the Identity Vault in a Specific Locale . . . 110
Adding a New Tree to the Identity Vault . . . 110
Adding a Server to an Existing Tree . . . 111
Removing the Identity Vault and its Database from the Server . . . 111
Removing an eDirectory Server Object and Directory Services from a Tree . . . 111
Configuring Multiple Instances of the Identity Vault . . . 111
Managing Instances with the ndsmanage Utility . . . 112
Listing Identity Vault Instances . . . 112
Creating a New Instance in the Identity Vault . . . 112
Configuring and Deconfiguring an Instance in the Identity Vault . . . 112
Invoking a Utility for an Instance in the Identity Vault . . . 113
Starting and Stopping Instances in the Identity Vault . . . 113

Part IV Installing and Managing Sentinel Log Management for Identity Governance and Administration 115

13 Planning to Install Sentinel Log Management for IGA 117

Checklist for Installing SLM for IGA . . . 117
Deciding When to Install SLM for IGA . . . 118
Overview of Changes . . . 118
Recommended Installation Scenarios . . . 119
Understanding the Installation Process . . . 124
Prerequisites for Installing SLM for IGA . . . 125
System Requirements . . . 126

14 Installing SLM for IGA 127

Performing an Interactive Installation . . . 127
Standard Installation . . . 127
Custom Installation. . . . 128
Performing a Silent Installation . . . 129
Customizing your Configuration . . . 129

Part V Installing the Identity Manager Engine, Drivers, and Plug-ins 131

15 Planning to Install the Engine, Drivers, and Plug-ins 133

Checklist for Installing the Identity Manager Engine, Drivers, and Plug-ins . . . 133
Understanding the Installation Program . . . 134
Prerequisites and Considerations for Installing the Identity Manager Engine. . . . 135
Considerations for Installing the Identity Manager Engine . . . 135
Considerations for Installing Drivers with the Identity Manager Engine . . . 136
System Requirements for the Identity Manager Engine . . . 136

16 Preparing to Install the Engine, Drivers, and Plug-ins 139

Verifying Environment Variables (UNIX / Linux) for the Identity Manager Installation. . . . 139
Stopping and Starting Identity Manager Drivers . . . 139
Stopping the Drivers. . . . 139
Starting the Drivers . . . 140

17 Installing the Engine, Drivers, and iManager Plug-ins 143

Using the Wizard to Install the Components. . . . 143
Installing as a Root or Administrative User . . . 143
Installing as a Non-root User . . . 144
Performing a Silent Installation . . . 146
Installing on a Server with Multiple Instances of Identity Vault . . . 147
Completing a Non-root Installation . . . 149
Assigning the Password Policy Object to Driver Sets . . . 149
Creating the Default Notification Collection Object in the Identity Vault. . . . 151
Adding Support for Graphics in Email Notifications . . . 152

Part VI Installing and Managing the Remote Loader 153

18 Planning to Install the Remote Loader 155

Checklist for Installing the Remote Loader . . . 155
Understanding the Remote Loader. . . . 156
Understanding Shims. . . . 157
Determining When to Use the Remote Loader . . . 157
Understanding the Java Remote Loader . . . 158
Understanding the Installation Program . . . 158
Using 32-bit and 64-bit Remote Loader on the Same Computer . . . 158
Prerequisites and Considerations for Installing the Remote Loader. . . . 158
System Requirements for the Remote Loader . . . 161
Remote Loader 32-bit and 64-bit . . . 161
.NET Remote Loader . . . 162
Java Remote Loader . . . 163

19 Installing Remote Loader **165**

Using the Wizard to Install the Remote Loader . . . 165
Performing a Silent Installation of the Remote Loader . . . 166
Installing Java Remote Loader on Linux . . . 167
Installing Java Remote Loader on Windows . . . 168
Installing .NET Remote Loader on Windows . . . 169

20 Configuring the Remote Loader and Drivers **171**

Creating a Secure Connection to the Identity Manager Engine . . . 171
Understanding the Communication Process . . . 171
Managing Self-Signed Server Certificates . . . 172
Creating a Keystore File when Using SSL Connections . . . 173
Understanding the Configuration Parameters for the Remote Loader . . . 174
Configuration Parameters for the Driver Instances in the Remote Loader . . . 175
Understanding the Names for the Java -class Parameter . . . 182
Configuring the Remote Loader for Driver Instances on UNIX or Linux . . . 183
Configuring the Remote Loader for Driver Instances on Windows . . . 185
Creating a New Driver Instance in the Remote Loader on Windows . . . 185
Modifying an Existing Driver Instance in the Remote Loader on Windows . . . 187
Configuring the Java Remote Loader for Driver Instances . . . 187
Configuring the .NET Remote Loader for Driver Instances on Windows . . . 189
Creating a New Driver Instance in the .NET Remote Loader on Windows . . . 189
Modifying an Existing Driver Instance in the .NET Remote Loader on Windows . . . 191
Configuring Identity Manager Drivers to Work with the Remote Loader . . . 191
Configuring Mutual Authentication with the Identity Manager Engine . . . 192
Exporting Certificates for the Identity Manager Engine and the Remote Loader . . . 192
Enabling a Driver for Mutual Authentication . . . 195
Verifying the Configuration . . . 199

21 Starting and Stopping the Remote Loader **201**

Starting a Driver Instance in the Remote Loader . . . 201
Starting Driver Instances on UNIX or Linux . . . 201
Starting Driver Instances on Windows . . . 202
Stopping a Driver Instance in the Remote Loader . . . 203

Part VII Installing iManager **205**

22 Planning to Install iManager **207**

Checklist for Installing iManager . . . 207
Understanding the Server and Client Versions of iManager . . . 208
Understanding Installation for iManager Plug-ins . . . 209
Prerequisites and Considerations for Installing iManager . . . 209
Considerations for Installing iManager . . . 210
Considerations for Installing iManager on a Linux Platform . . . 210
Considerations for Installing iManager on a Windows Platform . . . 211
Considerations for Installing iManager Workstation on Linux Clients . . . 212
Considerations for Installing iManager Workstation on Windows Clients . . . 213
System Requirements for iManager Server . . . 213
System Requirements for iManager Workstation (Client Version) . . . 214

23 Installing iManager Server and Workstation 217

Installing iManager and iManager Workstation on Linux . . . 217
Installing iManager on Linux . . . 217
Installing iManager Workstation on Linux Clients. . . . 220
Installing iManager and iManager Workstation on Windows . . . 221
Installing iManager on Windows . . . 221
Installing iManager Workstation on Windows. . . . 224
Installing iManager Silently . . . 224
Editing the Properties File for a Customized Silent Installation . . . 225
Running a Silent Installation for iManager . . . 226

24 Post-Installation Tasks for iManager 227

Replacing the Temporary Self-Signed Certificates for iManager . . . 227
Replacing the iManager Self-Signed Certificates on Linux . . . 227
Replacing the iManager Self-Signed Certificates on Windows . . . 229
Configuring iManager for IPv6 Addresses after Installation . . . 231
Specifying an Authorized User for eDirectory . . . 231

Part VIII Installing Designer for Identity Manager 233

25 Planning to Install Designer 235

Checklist for Installing Designer . . . 235
Prerequisites for Installing Designer . . . 236
System Requirements for Designer . . . 236

26 Installing Designer 239

Using the Installation Command on Linux . . . 239
Running the Windows Executable File . . . 239
Using the Silent Installation Process. . . . 239
Modifying an Installation Path that Includes a Space Character. . . . 240

Part IX Installing PostgreSQL and Tomcat for Identity Manager 241

27 Planning to Install PostgreSQL and Tomcat 243

Checklist for Installing Tomcat and PostgreSQL. . . . 243
Understanding the Installation Process for PostgreSQL and Tomcat . . . 244
Prerequisites for Installing PostgreSQL . . . 244
Prerequisites for Installing Tomcat . . . 245
System Requirements for PostgreSQL. . . . 245
System Requirements for Tomcat. . . . 245

28 Installing PostgreSQL and Tomcat 247

Using the Wizard to Install PostgreSQL and Tomcat . . . 247
Silently Installing Tomcat and PostgreSQL for Identity Manager . . . 249
Safeguarding the Passwords for a Silent Installation. . . . 249
Silently Installing Tomcat and PostgreSQL . . . 250

Part X Installing the Single Sign-on Component 251

29 Planning to Install Single Sign-on for Identity Manager 253

Checklist for Single Sign-on Component 253
Prerequisites for Installing One SSO Provider 254
System Requirements for One SSO Provider. 254
Using the Apache Log4j Service to Log Sign-on. 254

30 Installing Single Sign-on for Identity Manager 257

Using the Wizard to Install One SSO Provider 257
Silently Installing One SSO Provider 260
Configuring Single Sign-on Access. 260

Part XI Installing the Password Management Component 263

31 Planning to Install Password Management for Identity Manager 265

Checklist for Installing Password Management Components. 265
Prerequisites for Installing Self Service Password Reset 266
System Requirements for Self Service Password Reset 266
Using the Apache Log4j Service for Password Event. 266

32 Installing Password Management for Identity Manager 267

Using the Wizard to Install Self Service Password Request. 267
Silently Installing Self Service Password Reset 270
Post-Installation Tasks 271
Ensuring Error-Free Installation 271
Assigning the Universal Password Policy to a User Container 272
. . . . . Granting Rights to pwmResponseSet Attributes 272
Configuring OSP and SSPR for Clustering. 273
Configuring SSPR to Support Clustering 273
Configuring Tasks on Cluster nodes. 273

Part XII Installing the Identity Applications 277

33 Planning to Install the Identity Applications 279

Checklist for Installing the Identity Applications 279
Understanding the Installation Files for the Identity Applications 281
Prerequisites and Considerations for Installing the Identity Applications 282
Installation Considerations for the Identity Applications. 282
Configuration and Usage Considerations for the Identity Applications 283
Prerequisites and Considerations for the Application Server. 284
Prerequisites for Installing the Identity Applications in a Cluster Environment. 285
Prerequisites for Installing the Database for the Identity Applications 286
System Requirements for the Identity Applications. 287

34 Preparing the Identity Vault for the Identity Applications 291

Adding the User Application Schema to your Audit Server as a Log Application 291
Assign Rights to Identity Vault Administrator and User Application Administrator Account. 292

35 Configuring the Database for the Identity Applications 295

Configuring an Oracle Database. 295
Checking Compatibility Level of Databases. 295
Configuring the Character Set 296
Configuring the Admin User Account 296
Configuring a PostgreSQL Database 296
Configuring a SQL Server Database. 297
Configuring the Character Set 297
Configuring the Admin User Account 297

36 Preparing Your Environment for the Identity Applications 299

Specifying a Location for the Permission Index 299
Enabling the Permission Index for Clustering 300
Preparing Your Application Server for the Identity Applications 300
Preparing a Tomcat Environment. 300
Preparing a Cluster for the Identity Applications 301
Understanding Cluster Groups in Tomcat Environments 301
Setting System Properties for Workflow Engine IDs 302
Using the Same Master Key for Each User Application in the Cluster. 302

37 Installing the Identity Applications 303

Checklist for Installing the Identity Applications 303
Using the Guided Process to Install the Identity Applications 304
Silently Installing the Identity Applications 310
Setting Passwords in the Environment for a Silent Installation 310
Editing the Silent Properties File 310
Importing eDirectory Certificates into Identity Applications 315
Executing a Silent Installation of the Identity Applications 316
Post-Installation Steps 316
Configuring the User Application Driver for Clustering. 316
Passing the preferIPv4Stack Property to JVM 317
Checking the Health of the Server 317
Monitoring the Health Statistics 317
Creating Compound Indexes 318
Disabling the Prevent HTML Framing Setting for Integrating Identity Manager with SSPR 319
Starting the Identity Applications. 319
Starting the User Application on a Tomcat Server 319

38 Creating and Deploying the Drivers for the Identity Applications 323

Creating the User Application Driver. 323
Configuring the User Application Driver for Clustering 324
Creating the Role and Resource Service Driver 324
Deploying the Drivers for the User Application 325

39 Completing the Installation of the Identity Applications 327

Checking the Health of the Server in a Clustered Environment 327
Manually Creating the Database Schema 327

Using the SQL File to Generate the Database Schema . . . 327
Manually Creating the SQL File to Generate the Database Schema . . . 328
Recording the Master Key . . . 329
Configuring the Identity Vault for the Identity Applications . . . 329
Pre-installation Tasks for Non-Root Users . . . 329
Changing the Default Context Name for User Application . . . 330
Reconfiguring the WAR File for the Identity Applications . . . 333
Configuring Forgotten Password Management . . . 333
Using Self Service Password Reset for Forgotten Password Management . . . 333
Using the Legacy Provider for Forgotten Password Management . . . 335
Using an External System for Forgotten Password Management . . . 336
Updating SSPR Links in the Dashboard for a Distributed or Clustered Environment . . . 338

40 Configuring the Settings for the Identity Applications 339

Running the Identity Applications Configuration Utility . . . 339
User Application Parameters . . . 340
Identity Vault Settings . . . 340
Identity Vault DNs . . . 341
Identity Vault User Identity . . . 343
Identity Vault User Groups . . . 344
Identity Vault Certificates . . . 345
Email Server Configuration . . . 345
Trusted Key Store . . . 347
NetIQ Sentinel Digital Signature Certificate & Key . . . 347
Miscellaneous . . . 348
Container Object . . . 349
Authentication Parameters . . . 349
Authentication Server . . . 350
Authentication Configuration . . . 350
Authentication Method . . . 351
Password Management . . . 352
Novell Audit Digital Signature Certificate and Key . . . 353
SSO Clients Parameters . . . 354
Landing . . . 354
Dashboard . . . 355
IDM Dashboard . . . 357
RBPM . . . 357
Reporting . . . 358
DCS Driver . . . 359
Catalog Administrator . . . 359
Self Service Password Reset . . . 360
Reporting Parameters . . . 361
Email Delivery Configuration . . . 361
Report Retention Values . . . 361
Modify Locale . . . 362
Role Configuration . . . 362

Part XIII Installing Identity Reporting 363

41 Planning to Install Identity Reporting 365

Checklist for Installing Identity Reporting . . . 365
Understanding the Installation Process for the Identity Reporting Components . . . 366
Prerequisites for Installing the Identity Reporting Components . . . 367
Prerequisites for Identity Reporting . . . 367
System Requirements for Identity Reporting . . . 368

42 Installing Identity Reporting **371**

Using the Guided Process to Install Identity Reporting . . . 371
Configuring Create_rpt_roles_and_schemas.sql Schema against Oracle Database . . . 376
Installing Identity Reporting Silently . . . 378
Manually Generating the Database Schema . . . 379
Connecting to a Remote PostgreSQL Database . . . 380

43 Configuring Identity Reporting **383**

Running Reports on an Oracle Database . . . 383
Deploying REST APIs for Identity Reporting . . . 383

44 Managing the Drivers for Reporting **385**

Configuring Drivers for Identity Reporting . . . 385
Installing the Driver Packages for Identity Reporting . . . 385
Configuring the Managed System Gateway Driver . . . 386
Configuring the Driver for Data Collection Service . . . 387
Configuring Identity Reporting to Collect Data from the Identity Applications . . . 390
Deploying and Starting Drivers for Identity Reporting . . . 391
Deploying the Drivers . . . 391
Verifying that the Managed Systems are Working . . . 391
Starting the Drivers for Identity Reporting . . . 394
Configuring the Runtime Environment . . . 395
Configuring the Data Collection Services Driver to Collect Data from the Identity Applications . . . 396
Migrating the Data Collection Service Driver . . . 397
Adding Support for Custom Attributes and Objects . . . 399
Adding Support for Multiple Driver Sets . . . 401
Configuring the Drivers to Run in Remote Mode with SSL . . . 403
Setting Auditing Flags for the Drivers . . . 404
Setting Audit Flags in Identity Manager . . . 404
Setting Audit Flags in eDirectory . . . 405

Part XIV Installing Analyzer for Identity Manager **409**

45 Planning to Install Analyzer **411**

Checklist for Installing Analyzer . . . 411
Prerequisites for Installing Analyzer . . . 411
System Requirements for Installing Analyzer . . . 412

46 Installing Analyzer **413**

Using the Wizard to Install Analyzer . . . 413
Installing Analyzer Silently . . . 414
Adding XULrunner to Analyzer.ini on Linux Platforms . . . 414
Installing an Audit Client for Analyzer . . . 415

Part XV Configuring Single Sign-on Access in Identity Manager 417

47 Preparing for Single Sign-on Access 419

48 Using One SSO Provider for Single Sign-on Access in Identity Manager 421

Preparing eDirectory for Single Sign-on Access . . . 421
Modifying the Basic Settings for Single Sign-on Access . . . 421
Configuring Self Service Password Reset to Trust OSP . . . 422

49 Using SAML Authentication with NetIQ Access Manager for Single Sign-on 423

Understanding Third-Party Authentication and Single Sign-On . . . 423
Creating and Installing SSL Certificates . . . 423
- Creating an SSL Certificate for Access Manager . . . 424
- Installing the Access Manager Certificate in the Identity Manager Trust Store . . . 424
- Installing the SSL Server Certificate in the Access Manager Trust Store . . . 425

Configuring Identity Manager to Trust Access Manager . . . 425
Configuring Access Manager to Work with Identity Manager . . . 426
- Copying the Metadata for Identity Manager . . . 426
- Creating an Attribute Set for SAML . . . 426
- Adding Identity Manager as a Trusted Service Provider . . . 427

Updating the Login Pages for Access Manager . . . 427

50 Using Kerberos for Single Sign-On 429

Configuring the Kerberos User Account in Active Directory . . . 429
Configuring the Identity Applications Server . . . 430
Configure the End-User Browsers to Use Integrated Windows Authentication . . . 432

51 Verifying Single Sign-on Access for the Identity Applications 433

52 Using SSL for Secure Communication 435

Checklist for Ensuring SSL Connections . . . 435
Creating a Keystore and Certificate Signing Request . . . 435
Enabling SSL with a External CA Signed Certificate . . . 437
Enabling SSL with a Self-signed Certificate . . . 438
- Exporting the Certificate Authority . . . 438
- Generating the Self-signed Certificate . . . 439

Enabling SSL Between Sentinel and Identity Manager Components . . . 440
- Enabling SSL between Sentinel and Identity Manager Engine/Remote Loader . . . 440
- Enabling SSL between Sentinel and User Application . . . 442

Updating the SSL Settings for the Application Server . . . 444
Updating the SSL Settings in the Configuration Utility . . . 445
Updating the SSL Settings for Self Service Password Reset . . . 446

53 Post-Installation Tasks 447

Configuring a Connected System . . . 447
Creating and Configuring a Driver Set . . . 447
- Creating Driver Set . . . 447
- Assigning the Default Password Policy to Driver Sets . . . 448
- Creating the Password Policy Object in the Identity Vault . . . 448
- Creating a Custom Password Policy . . . 449

Creating the Default Notification Collection Object in the Identity Vault . . . 449
Creating a Driver . . . 450
Defining Policies . . . 450
Managing Driver Activities . . . 450
Configuring Sentinel Log Management for IGA . . . 451
Checking for Sentinel Events . . . 451
Configuring the Collector Instances in Sentinel . . . 451
Configuring Event Data Retention . . . 451
Configuring Disk Space Usage for Sentinel . . . 452
Configuring Raw Data Retention Policy in Sentinel . . . 452
Configuring the Sentinel Link Connection . . . 452
Activating Identity Manager . . . 453
Installing a Product Activation Credential . . . 453
Reviewing Product Activations for Identity Manager and Drivers . . . 454
Activating Identity Manager Drivers . . . 454
Activating Specific Identity Manager Components . . . 455

Part XVI Upgrading Identity Manager 457

54 Preparing to Upgrade Identity Manager 459

Checklist for Upgrading Identity Manager . . . 459
Understanding Upgrade and Migration . . . 461
Upgrade Order . . . 463
Supported Upgrade Paths . . . 463
Upgrading from Versions Lower Than 4.5.4 . . . 464
Upgrading from Identity Manager 4.0.2 . . . 464
Backing Up the Current Configuration . . . 465
Exporting the Designer Project . . . 465
Exporting the Configuration of the Drivers . . . 466

55 Upgrading Identity Manager Components 469

Upgrading Designer . . . 469
Upgrading iManager . . . 470
Upgrading iManager on Linux . . . 470
Upgrading iManager on Windows . . . 472
Upgrading iManager Silently . . . 473
Updating Role-Based Services . . . 473
Re-installing or Migrating Plug-ins for Plug-in Studio . . . 474
Updating iManager Plug-ins after an Upgrade or Re-installation . . . 475
Upgrading the Remote Loader . . . 475
Upgrading the Identity Manager Engine . . . 476
Performing a Guided Upgrade . . . 476
Performing a Silent Upgrade . . . 476
Upgrading Identity Applications and Supporting Components . . . 477
Understanding the Upgrade Program . . . 478
Prerequisites and Considerations for Upgrade . . . 478
Upgrading the PostgreSQL Database . . . 479
Changing the Custom Context Name for User Application . . . 483
System Requirements . . . 483
Using the Guided Process to Upgrade . . . 483
Silently Upgrading the Identity Manager Applications . . . 485
Post-Upgrade Tasks . . . 486
Upgrading Identity Reporting . . . 489
Upgrading the Driver Packages for Identity Reporting . . . 489
Migrating from Event Auditing Service to Sentinel Log Management for IGA . . . 489

Upgrading Identity Reporting . . . 498
Changing the References to reportRunner in the Database . . . 498
Verifying the Upgrade for Identity Reporting . . . 498
Upgrading Analyzer . . . 499
Upgrading the Identity Manager Drivers . . . 499
Creating a New Driver . . . 499
Replacing Existing Content with Content from Packages . . . 500
Keeping the Current Content and Adding New Content with Packages . . . 500
Adding New Servers to the Driver Set . . . 501
Adding the New Server to the Driver Set . . . 501
Removing the Old Server from the Driver Set . . . 501
Restoring Custom Policies and Rules to the Driver . . . 502
Using Designer to Restore Custom Policies and Rules to the Driver . . . 502
Using iManager to Restore Custom Policies and Rules to the Driver . . . 503

56 Switching from Advanced Edition to Standard Edition 505

57 Applying a Software Update to Identity Manager Components 507

Applying a Service Pack to Identity Manager Engine and Remote Loader . . . 507
Prerequisites for Installing the Service Pack . . . 507
Installing the Service Pack as a Root User in GUI Mode . . . 508
Installing the Service Pack as a Non-Root User in GUI Mode . . . 509
Silently Installing the Service Pack . . . 509
Applying a Patch for an Identity Manager Driver . . . 510
Applying the Identity Manager Driver Patch as a Root User . . . 510
Applying the Identity Manager Driver Patch as a Non-Root User . . . 510

Part XVII Migrating Identity Manager Data to a New Installation 513

58 Preparing to Migrate Identity Manager 515

Checklist for Performing a Migration . . . 515
Stopping and Starting Identity Manager Drivers during Migration . . . 516

59 Migrating Identity Manager to a New Server 517

Checklist for Migrating Identity Manager . . . 517
Preparing Your Designer Project for Migration . . . 518
Copying Server-specific Information for the Driver Set . . . 519
Copying the Server-specific Information in Designer . . . 519
Changing the Server-specific Information in iManager . . . 520
Changing the Server-specific Information for the User Application . . . 520
Migrating the Identity Manager Engine to a New Server . . . 520
Migrating the User Application Driver . . . 521
Importing a New Base Package . . . 521
Upgrading an Existing Base Package . . . 521
Deploying the Migrated Driver . . . 522
Migrating from Websphere or JBoss to Tomcat Web Application Server . . . 522
Upgrading the Identity Applications . . . 523
Completing the Migration of the Identity Applications . . . 524
Preparing an Oracle Database for the SQL File . . . 524
Flushing the Browser Cache . . . 525
Using the Legacy Provider or an External Provider for Managing Passwords . . . 525
Updating the Maximum Timeout Setting for the SharedPagePortlet . . . 525
Disabling the Automatic Query Setting for Groups . . . 525

60 Uninstalling Identity Manager Components 527

Removing Objects from the Identity Vault . . . 527
Uninstalling the Identity Manager Engine . . . 527
Uninstalling the Identity Manager Engine on Linux/UNIX . . . 528
Uninstalling the Identity Manager Engine as a Non-root User . . . 528
Uninstalling the Identity Manager Engine on Windows . . . 528
Uninstalling the Remote Loader . . . 528
Uninstalling the Remote Loader on Linux/UNIX . . . 528
Uninstalling the Remote Loader as a Non-root User . . . 529
Uninstalling the Remote Loader on Windows . . . 529
Uninstalling the Roles Based Provisioning Module . . . 529
Deleting the Drivers for the Roles Based Provisioning Module . . . 529
Uninstalling the User Application on Linux/UNIX . . . 530
Uninstalling the User Application on Windows . . . 530
Uninstalling the Identity Reporting . . . 530
Deleting the Reporting Drivers . . . 531
Uninstalling Identity Reporting . . . 531
Uninstalling Sentinel . . . 531
Uninstalling eDirectory . . . 532
Uninstalling Analyzer . . . 533
Uninstalling iManager . . . 533
Uninstalling iManager on Linux . . . 534
Uninstalling iManager on Windows . . . 534
Uninstalling iManager Workstation . . . 534
Uninstalling Designer . . . 534

61 Troubleshooting 535

Troubleshooting the User Application and RBPM Installation . . . 535
Troubleshooting Uninstallation . . . 536
Troubleshooting Login . . . 537
Troubleshooting SSPR Page Request Error . . . 537
Troubleshooting an Issue When server.xml file Is Not Updated with a Non-Default Port Specified During Identity Reporting Installation . . . 537

A Sample Identity Manager Cluster Deployment Solution on SLES 539

Sample Cluster Deployment on SLES 12 SP1 . . . 540
Prerequisites . . . 540
Installation Procedure . . . 540
Sample Cluster Deployment on SLES 12 SP2 . . . 549
Prerequisites . . . 549
Installation Procedure . . . 549

B Sample Identity Manager Cluster Deployment Solution on Windows 557

Prerequisites . . . 557
Configuring NetIQ Identity Manager on eDirectory Cluster . . . 557
Clustering Remote Loader . . . 558

C Sample Identity Applications Cluster Deployment Solution on Tomcat Application Server 559

Prerequisites . . . 560
Installation Procedure . . . 561

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.

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 website.

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
Website:	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
Website:	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 website in HTML and PDF formats on a page that does not require you to log in. 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.

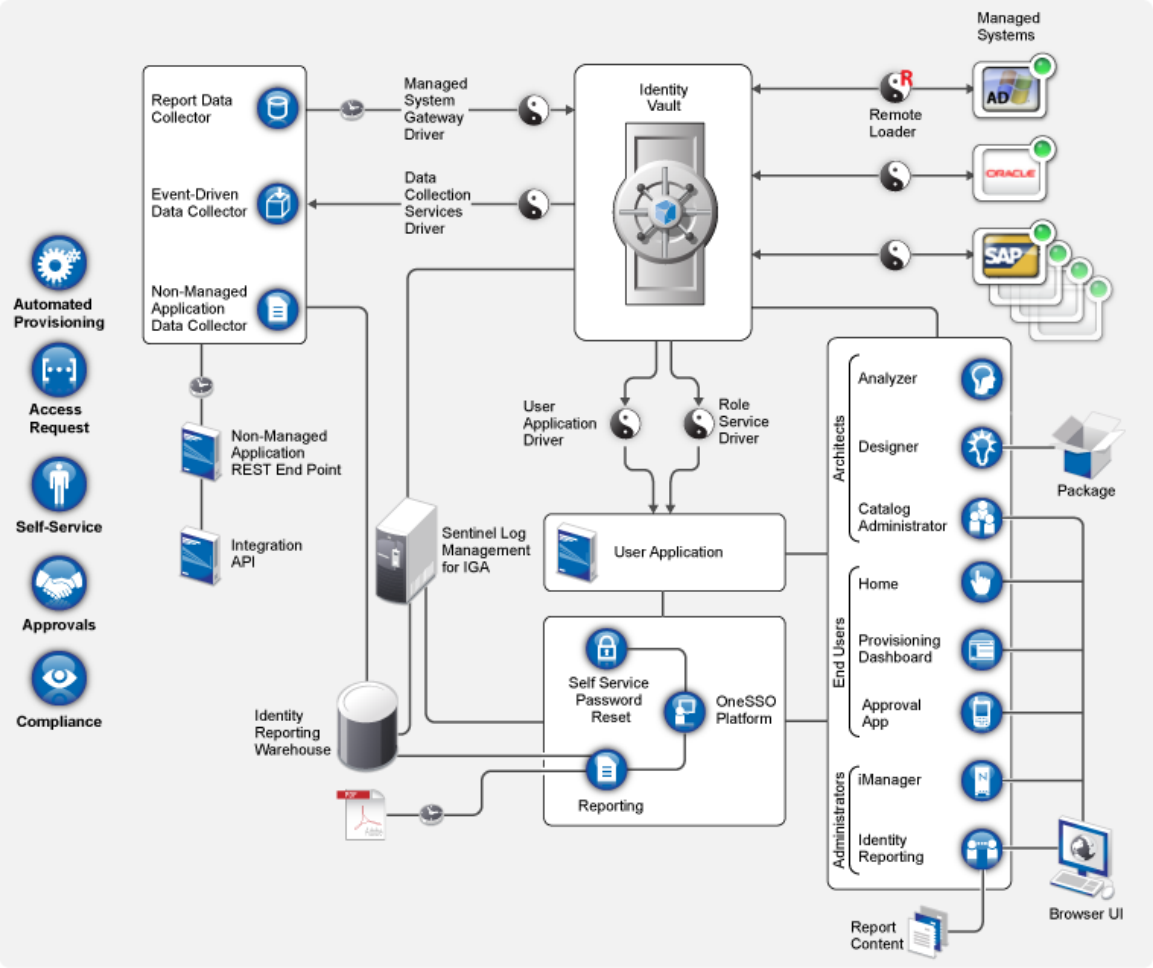
In general, you can group the components that comprise Identity Manager into the following functions:

- Creating and maintaining the Identity Manager environment. For more information, see Chapter 2, “Creating and Maintaining Your Identity Manager Environment,” on page 25.
- 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, “Overview of the Components of Identity Manager,” on page 23.

1 Overview of the Components 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 view of the components that support the Identity Manager capabilities. Some of these components can be installed on the same server, depending on the size of your identity management solution. However, some components, such as the identity applications, 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:

- "Designer for Identity Manager" on page 25
- "Analyzer for Identity Manager" on page 25
- "Role Administration" on page 26
- "iManager" on page 26

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.

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 *NetIQ Designer for Identity Manager Administration Guide*.

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 *NetIQ Analyzer for Identity Manager Administration Guide*.

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.

Business analysts can use **NetIQ Identity Manager Catalog Administrator** (Catalog 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.

Catalog Administrator pulls role information from the User Application driver and requires access to the Identity Vault and the Dashboard for the identity applications . For more information, see the *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*.

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 Reporting
- Identity Manager drivers
- Connected Systems

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, NetIQ 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.

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.

Understanding the Components for Synchronizing Your Identity Data

- "Identity Vault" on page 28
- "Identity Manager Engine" on page 28
- "Remote Loader" on page 28
- "Identity Reporting" on page 29

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.

The Identity Vault uses a NetIQ eDirectory database. For more information about using eDirectory see the *NetIQ eDirectory 8.8 Administration Guide*.

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.

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 servers that have Tomcat and the Identity Manager server.

For more information about Remote Loader, see the "Understanding the Remote Loader" on page 156.

Identity Reporting

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 for Identity Manager" on page 29
- "Data Collection Service" on page 29
- "Managed System Gateway Driver" on page 30

Identity Reporting for Identity Manager

The Identity Information Warehouse stores its information in the SIEM database of the Sentinel Log Management for IGA. The **Identity Reporting** component 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 Identity Reporting 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 Identity Reporting makes it easy to schedule reports to run at off-peak times for optimized performance. For more information about Identity Reporting, see the *Administrator Guide to NetIQ Identity Reporting*.

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

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:

- Identity Manager Dashboard
- Catalog Administrator
- User Application

The Dashboard provides a single access point for all Identity Manager users and administrators. It allows access to all existing Catlog Administrator and User Application functionality. As of Identity Manager v4.6, the Dashboard replaces Identity Manager Home and Provisioning Dashboard.

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.

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 have 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 have 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.

Understanding the Components for Managing User Provisioning

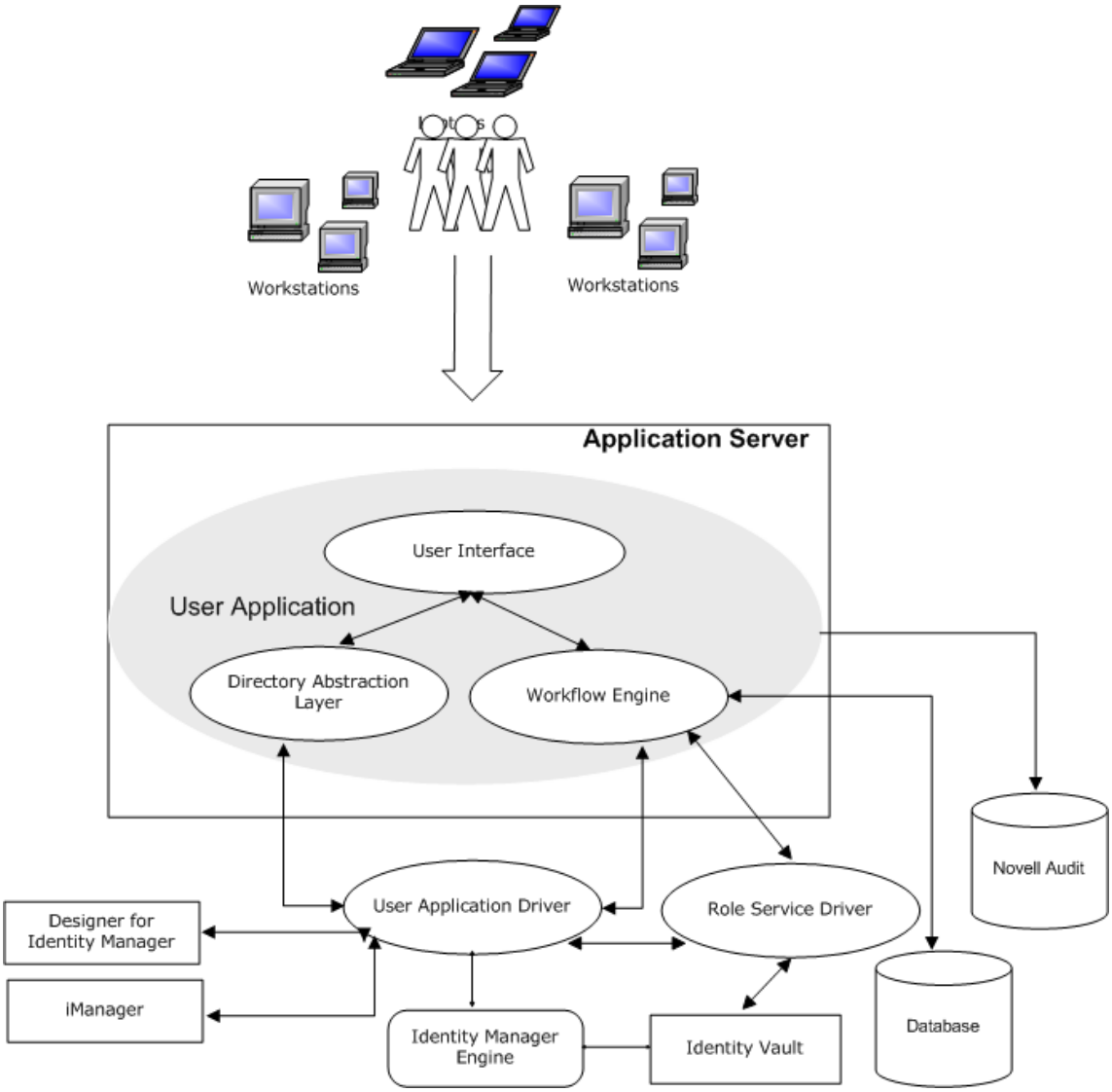
This section explains the purpose of the following components:

- "User Application and Roles Based Provisioning Module" on page 33
- "Identity Manager Dashboard" on page 34

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 Identity Manager - Administrator's Guide to the Identity Applications*.

Identity Manager Dashboard

The **Identity Manager Dashboard** (the Dashboard) includes a personalized view of each user's permissions, tasks, and requests. This helps users focus on the following basic areas of functionality:

I want something.

If you 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, you can request that item.

I need to do something.

If you want to know what tasks you need to manage, **My Tasks** page shows all of your pending approval or provisioning tasks in the Identity Manager system.

What do I have?

If you want to see your current permissions, the **My Permissions** page provides a list of the roles and resources to which you have access.

How did I get it?

If you want to see a list of past requests, the **Requests History** page shows everything that you have requested recently, as well as the status of your pending requests.

If you have an administrative role for the identity applications, you can customize the **Applications** page in the Dashboard for all users. You can configure the page to show items and links that your users need to see, organized into categories that make sense for your enterprise. You can include the following types of items:

- Identity Manager functions, such as creating groups or running reports
- Permissions that most users need to request
- Links to commonly accessed websites or web-based applications
- REST endpoints
- Badges, such as the number of items of a certain type that a user can access

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 - Administrator's Guide to the Identity Applications*.

Using Self-Service Password Management in Identity Manager

Identity Manager includes NetIQ Self Service Password Reset (SSPR) to help users who have access to the identity applications to reset their passwords without administrative intervention. The installation process enables SSPR by default when you install or upgrade to the latest version of Identity Manager. In a new installation, SSPR uses a proprietary protocol for managing authentication methods. However, after an upgrade, you can instruct SSPR to use the NetIQ Modular Authentication Services (NMAS) that Identity Manager traditionally has used for its legacy password management program.

Depending on whether you want to use complex password management, you can configure one of the following providers:

SSPR

NetIQ Self Service Password Reset is the default option when you install or upgrade Identity Manager. For more information, see "Understanding the Default Self-Service Process" on page 35.

Legacy Provider for Password Management

Uses the password management process from Identity Manager 4.0.2, which supports the use of multiple password policies. For more information, see "Understanding the Legacy Password Management Provider" on page 36.

Third-Party Provider Password Management

You can use an third-party program for managing forgotten passwords. You need to modify some configuration settings for Identity Manager. For more information, see "Using an External System for Forgotten Password Management" on page 336.

Understanding the Default Self-Service Process

SSPR automatically integrates with the single sign-on process for the identity applications and Identity Reporting. It is the default password management program for Identity Manager, even when you do not install SSPR. When a user requests a password reset, SSPR requires the user to answer the challenge-response question. If the answers are correct, SSPR responds in one of the following ways:

- Allow users to create a new password
- Create a new password and send it to the user
- Create a new password, send it to the user, and mark the old password as expired.

You configure this response in the SSPR Configuration Editor. After upgrading to a new version of Identity Manager, you can configure SSPR to use the NMAS method that Identity Manager traditionally has used for password management. However, SSPR does not recognize your existing password policies for managing forgotten passwords. To continue using your policies, see "Understanding the Legacy Password Management Provider" on page 36.

You also can configure SSPR to use its proprietary protocol instead of NMAS. If you make this change, you cannot return to using NMAS without resetting your password policies.

For more information about...	See...
Installing SSPR	Chapter 32, “Installing Password Management for Identity Manager,” on page 267
Configuring password management for the identity applications	“Using Self Service Password Reset for Forgotten Password Management” on page 333
Managing and configuring SSPR	*NetIQ Self Service Password Reset Administration Guide*

The `.iso` image for Identity Manager and the Identity Manager Integrated Installer application include the SSPR installation program.

Understanding the Legacy Password Management Provider

NOTE: The Legacy Password Self-Service feature of the User Application is deprecated with this release. NetIQ strongly recommends that you start using SSPR for all password-specific tasks. The installation process enables SSPR by default. For more information, see “Understanding the Self-Service Process in Identity Manager” on page 32.

When you upgrade from an older version of Identity Manager, the identity applications default to SSPR as the password management program. SSPR can use the NMAS method that Identity Manager traditionally has used for password management. However, SSPR does not recognize your existing password policies for managing forgotten passwords. You can bypass SSPR and use the legacy password management provider.

When a user requests a password reset, the legacy provider compares the user’s credentials to the password policies that you set. For example, it might requires the user to answer a challenge-response question. Based on the policy applied to that user, the program responds in one of the following ways:

- Resets the password
- Shows the password hint
- Emails the password hint to the user
- Emails a new password to the user

Use the legacy provider if your enterprise uses multiple or complex password policies. For example, your password policies are based on user roles. An intern might simply need a auto-generated password without a challenge response. For a manager who can access secure data, you might have more stringent requirements. This user might need to regularly reset the password. In both cases, you want the users to have self-service for password requests.

To use the legacy provider, modify the configuration settings for the identity applications after you install or upgrade Identity Manager. You do not need to reconfigure your password policies after the upgrade.

For more information about...	See...
Configuring Identity Manager to use the legacy provider	“Using the Legacy Provider for Forgotten Password Management” on page 335
Using the legacy provider for password management	*NetIQ Identity Manager Password Management Guide*

Using Single Sign-on Access in Identity Manager

To provide single sign-on access (SSO), Identity Manager uses the authentication service, NetIQ One SSO Provider (OSP). You must use OSP for the following components:

- Catalog Administrator
- Identity Manager Dashboard
- Identity Reporting
- Self-Service Password Reset
- User Application

Both the `.iso` image for Identity Manager and the Identity Manager Integrated Installer program include a method for installing OSP. For more information about installing OSP, see Chapter 32, “Installing Password Management for Identity Manager,” on page 267.

Understanding Authentication with One SSO Provider

OSP supports the OAuth2 specification and requires an LDAP authentication server. By default, Identity Manager uses Identity Vault (eDirectory). OSP can communicate other types of **authentication sources**, or **identity vaults**, to handle the authentication requests. You can configure the type of authentication that you want OSP to use: userID and password, Kerberos, or SAML. However, OSP does not support MIT-style Kerberos or SAP login tickets.

How do OSP and SSO work?

If you use the Identity Vault as your authentication service and the specified containers in the Identity Vault have CNs and passwords, authorized users can log in to Identity Manager immediately after installation. Without these login accounts, only the administrator that you specify during installation can log in immediately.

When a user logs in to one of the browser-based components, the process redirects the user’s name/password pair to the OSP service, which queries the authentication server. The server validates the user credentials. Then OSP issues an OAuth2 access token to the component and browser. The browser uses the token during the user’s session to provide SSO access to any of the browser-based components.

If you use Kerberos or SAML, OSP accepts authentication from the Kerberos ticket server or SAML IDP then issues an OAuth2 access token to the component where the user logged in.

How does OSP work with Kerberos?

OSP and Kerberos ensure that users can log in once to create a session with one of the identity applications and Identity Reporting. If the user’s session times out, authorization occurs automatically and without user intervention. After logging out, users should always close the browser to ensure that their sessions end. Otherwise, the application redirects the user to the login window and OSP reauthorizes the user session.

How do I set up Authentication and Single Sign-on Access?

For OSP and SSO to function, you must install OSP. Then specify the URLs for client access to each component, the URL that redirects validation requests to OSP, and settings for the authentication server. You can provide this information during installation or afterward with the RBPM configuration utility. You can also specify the settings for your Kerberos ticket server or SAML IDP.

For more information about configuring authentication and single sign-on access, see Part XV, “Configuring Single Sign-on Access in Identity Manager,” on page 417. In a cluster, the configuration settings must be identical for all members of the cluster.

Understanding the Keystore for One SSO Provider

Identity Manager uses a keystore that supports `http` and `https` communication between the OSP service and the authentication server. You create the keystore when you install OSP. You also create a password that the OSP service uses for authorized interactions with the authentication server. For more information, see Chapter 32, “Installing Password Management for Identity Manager,” on page 267.

Understanding Audit Events for One SSO Provider

OSP generates a single event to represent when a user logs in or out of the User Application or Identity Reporting:

- 003E0204 for login
- 003E0201 for logout

XDAS taxonomy then interprets these OSP events either as a successful login/logout or SOAP call to the User Application or as “other than success.”

Planning to Install Identity Manager

This section provides valuable information for planning your Identity Manager environment. To review the prerequisites and system requirements for the computers where you want to install each Identity Manager component, see the installation sections for those components.

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.

- Chapter 5, “Planning Overview,” on page 41
- Chapter 6, “Considerations and Prerequisites for Installation,” on page 53

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.

- "Planning Checklist" on page 41
- "Understanding the Integrated and Standalone Installation Processes" on page 43
- "Recommended Installation Scenarios and Server Setup" on page 44
- "Understanding Licensing and Activation" on page 49
- "Understanding Identity Manager Communication" on page 49
- "Understanding Language Support" on page 51
- "Downloading the Installation Files" on page 52

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
❑	1. Review product architecture information to learn about Identity Manager components. For more information, see Part I, "Introduction," on page 21.
❑	2. Determine which type of installation program that you want to use. For more information, see "Understanding the Integrated and Standalone Installation Processes" on page 43.
❑	3. Determine which operating system platforms best suit your installation. For more information, see "Selecting an Operating System Platform for Identity Manager" on page 47. **NOTE:** The Sentinel Log Management for IGA can be installed only on a Linux server. However, you can use a different auditing service if your identity solution is Windows only.
❑	4. (Conditional) When installing components in a Red Hat Enterprise Linux 6.*x* or 7.*x* environment, ensure that the server has the correct libraries. For more information, see "Installing Identity Manager on RHEL 6.x or 7.x Servers" on page 55
❑	5. Determine the order of component installation and where you want to install each component. For more information, see "Recommended Installation Scenarios and Server Setup" on page 44.
❑	6. Ensure that you have a license for running Identity Manager. For more information, see "Understanding Licensing and Activation" on page 49.
❑	7. Review the default ports for each Identity Manager component to determine whether you need to customize the installation settings. For more information, see "Understanding Identity Manager Communication" on page 49.

	Checklist Items
❑	8. Determine whether you can run the installation programs in your preferred language. For more information, see "Understanding Language Support" on page 51.
❑	9. Ensure that you have the files for installing Identity Manager. For more information, see "Downloading the Installation Files" on page 52. **IMPORTANT:** For a hassle-free installation on Windows, do not run any CPU-intensive applications while installing the Identity Manager components.
❑	10. (Conditional) To install Identity Manager in a cluster, ensure that your environment meets the requirements. For more information, see "Ensuring High Availability for Identity Manager" on page 53.
❑	11. 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.
❑	12. Ensure that the computers on which you are installing the Identity Manager components meet the specified requirements. For more information, see the following sections: ◆ **Analyzer**: (Optional) "Planning to Install Analyzer" on page 411 ◆ **Designer**: "Planning to Install Designer" on page 235 ◆ **Sentinel Log Management for IGA**: "Installing and Managing Sentinel Log Management for Identity Governance and Administration" on page 115 ◆ **Identity Applications for Role and Resource Management**: "Planning to Install the Identity Applications" on page 279 ◆ **Identity Manager Engine**: "Planning to Install the Engine, Drivers, and Plug-ins" on page 133 ◆ **Identity Vault**: "Installing the Identity Vault" on page 59 ◆ **iManager**: (Optional) "Planning to Install iManager" on page 207 ◆ **Password Reset (SSPR)**: "Planning to Install Password Management for Identity Manager" on page 265 ◆ **PostgreSQL**: "Planning to Install PostgreSQL and Tomcat" on page 243 ◆ **Remote Loader**: "Planning to Install the Engine, Drivers, and Plug-ins" on page 133 ◆ **Reporting**: "Planning to Install Identity Reporting" on page 365 ◆ **Single Sign-on Access (OSP)**: "Planning to Install Password Management for Identity Manager" on page 265 ◆ **Tomcat**: "Planning to Install PostgreSQL and Tomcat" on page 243 **NOTE:** NetIQ recommends that you make a note of each account that you create during the installation process.
❑	13. To install Identity Manager with default settings, see the *NetIQ Identity Manager Integrated Installation Guide*.
❑	14. Activate your Identity Manager components. For more information, see "Activating Identity Manager" on page 453.

Understanding the Integrated and Standalone Installation Processes

NetIQ provides two ways to install and configure Identity Manager in your environment: the Integrated Installation program and the standalone installation programs. This section helps you determine which process to use for your environment.

- "Understanding the Integrated Installation Process" on page 43
- "Understanding the Standalone Installation Process" on page 44

Understanding the Integrated Installation Process

NetIQ recommends using this process when you want to evaluate Identity Manager or create a test environment. The Integrated Installation program bundles all necessary components into one installation process. The process has the following capabilities:

- Applies the default values for most settings, including a predefined tree structure for the Identity Vault
- Installs all components on one computer or in a small, distributed environment
- Installs all drivers and creates the driver set as a separate partition when you specify settings for the Identity Manager engine
- Installs all iManager plug-ins
- Uses PostgreSQL for all databases
- Uses Apache Tomcat as an application server
- Checks the platform of the server to ensure it is a supported version
- Can be run on Red Hat Enterprise Linux (RHEL) 7.3 or later, SUSE Linux Enterprise Server (SLES) 12 SP1 or later, or Windows 2012 R2 platforms
- Cannot be used to install Identity Manager on the following operating systems:
  - Open Enterprise Server 2015 SP1
  - Open Enterprise Server 11 SP3
  - Redhat Enterprise Linux 6.x
  - SUSE Linux Enterprise Server 11
- Cannot be used to install Identity Manager Standard Edition
- Cannot be used in a clustered environment
- Cannot be used in a production environment
- Cannot be used to upgrade a previous version of Identity Manager

For more information, see the *NetIQ Identity Manager Integrated Installation Guide*.

Understanding the Standalone Installation Process

NetIQ recommends using this option for the staging and production environments of your identity management solution. The standalone installation programs give you more flexibility in setting up your environment. For example, many of the Identity Manager components are data-intensive, such as the Identity Vault, and should be installed on separate servers.

The standalone installation process provides the following capabilities:

- Allows you to customize component settings, including the tree structure in the Identity Vault
- Allows you to install in distributed and clustered environments
- Allows you to select the drivers and create driver sets that you want to add to your identity management solution
- Allows you to select the iManager plug-ins that you want to add to your identity management solution
- Allows you use a non-`root` account to install some components
- Supports multiple database platforms
- Uses Apache Tomcat for all supported operating systems
- Creates a supported production environment
- Can be used to upgrade a previous version of Identity Manager

For best results, run the standalone installation programs in the order specified by your identity management solution. For more information, see "Recommended Installation Scenarios and Server Setup" on page 44.

Recommended Installation Scenarios and Server Setup

When you perform a standalone installation, you should install the components in a specific order and on specific servers. The installation programs for some components require information about previously installed components.

This section helps you determine installation order and server types, according to specific scenarios for auditing and reporting.

- "Send Events to an Auditing Service without Reporting in Identity Manager" on page 44
- "Send Events to Identity Manager and Generate Reports" on page 45
- "Send Events to an External Service Before Pushing Events to Identity Manager" on page 45
- "Recommended Server Setup" on page 46
- "Selecting an Operating System Platform for Identity Manager" on page 47

Send Events to an Auditing Service without Reporting in Identity Manager

In this scenario, you plan to use Sentinel to audit events that occur in Identity Manager. You have no plans for generating reports in Identity Manager. Install the components in the following order:

1. Sentinel Log Management for IGA
2. Identity Vault

3. Identity Manager engine, drivers, and iManager plug-ins
4. (Optional) iManager
5. Designer
6. Tomcat and PostgreSQL
7. OSP
8. SSPR
9. Identity Applications
10. (Optional) Analyzer

Send Events to Identity Manager and Generate Reports

In this scenario, you plan to use the Sentinel Log Management for IGA that ships with Identity Manager to audit Identity Manager. You might also generate reports for those events. Install the components in the following order:

1. Identity Vault
2. Sentinel Log Management for IGA
3. Identity Manager engine, drivers, and iManager plug-ins
4. (Optional) iManager
5. Designer
6. Tomcat and PostgreSQL
7. OSP
8. SSPR
9. Identity Applications
10. Identity Reporting
11. (Optional) Analyzer

Send Events to an External Service Before Pushing Events to Identity Manager

In this scenario, you plan to use a service such as Sentinel to audit Identity Manager. Install the components in the following order:

1. External auditing service, such as Sentinel
2. Identity Vault
3. Identity Manager engine, drivers, and iManager plug-ins
4. (Optional) iManager
5. Designer
6. Tomcat and PostgreSQL
7. OSP
8. SSPR
9. Identity Applications
10. Identity Reporting
11. (Optional) Analyzer

Recommended Server Setup

In a typical production environment, you might install Identity Manager on seven or more servers, as well as on client workstations. For example:

Computer setup	Component setup
Servers 1 and 2 (two-server directory replica)	◆ Identity Vault ◆ Identity Manager Engine
Servers 3 and 4 (two-server cluster)	◆ Identity applications ◆ iManager ◆ One SSO Provider ◆ Remote Loader ◆ Self Service Password Reset
Server 5 (or a cluster of servers)	Identity Manager databases: ◆ Identity applications ◆ Identity Reporting
Server 6 (not in a cluster)	Identity Reporting
Server 7	Sentinel Log Management for IGA
Client workstations (1+)	◆ Designer ◆ iManager Workstation ◆ Internet browsers that access the identity applications and reporting

Selecting an Operating System Platform for Identity Manager

You can install the Identity Manager components on a variety of operating system platforms. The following table helps you determine which servers you might want to use for your identity management solution.

Platform	Component
Open Enterprise Server (OES)	Identity applications Identity Manager engine Identity Reporting Identity Vault iManager (server) One SSO Provider PostgreSQL Remote Loader Self Service Password Reset Tomcat **NOTE:** You cannot use the integrated installation process on a system running Open Enterprise Server 11 SP3 or Open Enterprise Server 2015 SP1.
openSUSE	Analyzer Designer iManager Workstation (client)
Red Hat Linux Server (RHEL)	Identity applications Identity Manager engine Identity Reporting Identity Vault iManager (server) One SSO Provider PostgreSQL Remote Loader Self Service Password Reset Sentinel Log Management for IGA Tomcat
SUSE Linux Enterprise Desktop (SLED)	Designer

Platform	Component
SUSE Linux Enterprise Server (SLES)	Analyzer
	Designer
	Identity applications
	Identity Manager engine
	Identity Reporting
	Identity Vault
	iManager (server)
	One SSO Provider
	PostgreSQL
	Remote Loader
	Self Service Password Reset
	Sentinel Log Management for IGA
	Tomcat
Windows desktop	Designer
	iManager Workstation (client)
	Browser access to the identity applications and Identity Reporting
Windows Server	Analyzer
	Designer
	Identity applications
	Identity Manager engine
	Identity Reporting
	Identity Vault
	iManager (server)
	.NET Remote Loader
	One SSO Provider
	PostgreSQL
	Remote Loader
	Self Service Password Reset
	Tomcat

For more information about system requirements and prerequisites, see the following sections:

- “Planning to Install Analyzer” on page 411
- “Planning to Install Designer” on page 235
- “Planning to Install iManager” on page 207

- “Installing the Identity Vault” on page 59
- “Planning to Install the Engine, Drivers, and Plug-ins” on page 133
- “Planning to Install the Identity Applications” on page 279
- “Planning to Install Password Management for Identity Manager” on page 265
- “Planning to Install PostgreSQL and Tomcat” on page 243

Understanding Licensing and Activation

Identity Manager comprises of a broad spectrum of functionality. In order to meet different customer needs, Identity Manager functionality is delivered in Advanced and Standard Editions. Identity Manager includes the complete set of functionality in Advanced Edition. Standard Edition includes a subset of the features provided in Advanced Edition. For a comparison of features available in Advanced and Standard Editions, see Identity Manager Version Comparison. NetIQ provides different licensing models for each edition.

Prior to Identity Manager 4.6, Identity Manager Advanced and Standard Editions were provided in separate ISO files. With Identity Manager 4.6, NetIQ delivers both editions in a single ISO file to improve its delivery of new features, patches, documentation, and support, while allowing customers to select the solution capabilities that best match their needs.

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, “Activating Identity Manager” on page 453.

Depending on which edition you purchase, NetIQ will provide you with the appropriate license keys to enable the right functionality within Identity Manager. To purchase an Identity Manager product license, see the NetIQ Identity Manager How to Buy website. After you purchase a product license, NetIQ sends you a Customer ID. The email also contains a URL to the NetIQ website 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.

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.

NOTE: If a default port is already in use, ensure that you specify a different port for the Identity Manager component.

Port Number	Component Computer	Port Use
389	Identity Vault	Used for LDAP communication in clear text with Identity Manager components
435	Identity Reporting	Used for communication with the SMTP mail server
524	Identity Vault	Used for NetWare Core Protocol (NCP) communication

Port Number	Component Computer	Port Use
636	Identity Vault	Used for LDAP with TLS/SSL communication with Identity Manager components
5432	Identity Applications	Used for communication with the identity applications database
7707	Identity Reporting	Used by the Managed System Gateway driver to communicate with the Identity Vault
8000	Remote Loader	Used by the driver instance for TCP/IP communication **NOTE:** Each instance of the Remote Loader should be assigned a unique port.
8005	Identity Applications	Used by Tomcat to listen for shutdown commands
8009	Identity Applications	Used by Tomcat for communication with a web connector using the AJP protocol instead of HTTP
8028	Identity Vault	Used for HTTP clear text communication with NCP communication
8030	Identity Vault	Used for HTTPS communication with NCP communication
8080	Identity Applications iManager	Used by Tomcat for HTTP clear text communication
8090	Remote Loader	Used by the Remote Loader to listen for TCP/IP connections from the remote interface shim **NOTE:** Each instance of the Remote Loader should be assigned a unique port.
8109	Identity Applications	Applies only when using the integrated installation process Used by Tomcat for communication with a web connector using the AJP protocol instead of HTTP
8180	Identity Applications	Used for HTTP communications by the Tomcat application server on which the identity applications run
8443	Identity Applications iManager	Used by Tomcat for HTTPS (SSL) communication or redirecting requests for SSL communication
8543	Identity Applications	*Not listening, by default* Used by Tomcat to redirect requests that require SSL transport when you do not use TLS/SSL protocol
9009	iManager	Used by Tomcat for MOD_JK
15432	Identity Reporting	Used for the PostgreSQL database Sentinel
45654	User Application	Used by the server on which the database for the identity applications are installed to listen for communications, when running Tomcat with a cluster group

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, set the LANG variable in the profile or through the command line.

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. If the component is not translated to the language of the operating system, the program defaults to English. Also, the End User License Agreement in the installation program might not be available in all supported languages.

Locale	Designer	Identity Manager Engine	iManager	iManager plug-ins	Identity Applications
Chinese Simplified	Yes	Yes	Yes	Yes	Yes
Chinese Traditional	Yes	Yes	Yes	Yes	Yes
Danish	–	–	–	–	Yes
Dutch	Yes	–	–	–	Yes
English	Yes	Yes	Yes	Yes	Yes
French	Yes	Yes	Yes	Yes	Yes
German	Yes	Yes	Yes	Yes	Yes
Italian	Yes	–	Yes	–	Yes
Japanese	Yes	Yes	Yes	Yes	Yes
Portuguese (Brazilian	Yes	–	Yes	–	Yes
Russian	–	–	Yes	–	Yes
Spanish	Yes	–	Yes	–	Yes
Swedish	–	–	–	–	Yes

Identity applications represents the Dashboard, Catalog Administrator, Identity Reporting, Identity Approvals, and the User Application.

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.

Downloading the Installation Files

NetIQ provides ISO files that contain all components for a full Identity Manager installation. Each file includes the 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 website.
2. In the **Product or Technology** menu, select **Identity Manager**, then click **Search**.
3. On the NetIQ 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.

6 Considerations and Prerequisites for Installation

This section lists general prerequisites 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.

An Identity Manager implementation can vary based on the needs of your IT environment, so you should contact NetIQ Consulting Services or any of the NetIQ Identity Manager partners prior to finalizing the Identity Manager architecture for your environment.

For information about the recommended hardware, supported operating systems, and browsers, see the NetIQ Identity Manager Technical Information website.

- "Ensuring High Availability for Identity Manager" on page 53
- "Minimum Space Requirement on Linux Servers" on page 54
- "Installing Identity Manager on SLES 12 SP1 or Later Servers" on page 55
- "Installing Identity Manager on RHEL 6.x or 7.x Servers" on page 55

Ensuring High Availability for Identity Manager

High availability ensures efficient manageability of critical network resources including data, applications, and services. NetIQ supports high availability for your Identity Manager solution through clustering or Hypervisor clustering, such as VMWare Vmotion. When planning a high-availability environment, the following considerations apply:

- You can install the following components in a high-availability environment:
  - Identity Vault
  - Identity Manager engine
  - Remote Loader
  - Identity applications, except Identity Reporting
- To manage the availability of your network resources for your Identity Manager environment, use the SUSE Linux Enterprise High Availability Extension with SUSE Linux Enterprise Server (SLES) 11 SP4 or later with the latest patches installed.
- When you run the Identity Vault (eDirectory) in a clustered environment, the Identity Manager engine is also clustered.

For more information about...	See...
Determining the server configuration for Identity Manager components	"Recommended Server Setup" on page 46
Configuring the SLES High Availability Extension	*SUSE Linux Enterprise High Availability Extention 11.SP4*

For more information about...	See...
Setting up a high-availability environment on SLES	Appendix A, “Sample Identity Manager Cluster Deployment Solution on SLES,” on page 539
Running the Identity Vault in a cluster	“Prerequisites for Installing the Identity Vault in a Clustered Environment” on page 65
	Deploying eDirectory on High Availability Clusters in the *NetIQ eDirectory Installation Guide*
Running the identity applications in a cluster	“Configuring OSP and SSPR for Clustering” on page 273
	“Prerequisites for Installing the Identity Applications in a Cluster Environment” on page 285
	“Enabling the Permission Index for Clustering” on page 300
	“Preparing a Cluster for the Identity Applications” on page 301
	“Configuring the User Application Driver for Clustering” on page 324
	“Updating SSPR Links in the Dashboard for a Distributed or Clustered Environment” on page 338
Setting up the identity applications in a cluster on SLES/RHEL	Appendix C, “Sample Identity Applications Cluster Deployment Solution on Tomcat Application Server,” on page 559

Minimum Space Requirement on Linux Servers

The Identity Manager components have minimum space requirements.

The Table 6-1 on page 54 contains the minimum safe space required for different components:

Table 6-1 *Minimum Safe Space Requirement*

Path	Component	Minimum Safe Space Required
/opt	IDM	3GB
/var	IDM	5 GB for dib of 100,000 object
/etc	IDM	5 MB
/opt	iManager	700 MB
/var	iManager	3 GB
/etc	iManager	10 MB
/opt	Identity Applications server	5 GB
/var	Identity Applications server	100 MB

During installation ensure that the `/temp` folder is mounted as exec, has a free space of 5 GB, and has write permissions.

Installing Identity Manager on SLES 12 SP1 or Later Servers

Your SLES 12 SP1 or later server must have specific packages already installed for a guided installation of Identity Manager components using the individual component installers or the integration installation program.

- `libXtst6-32bit-1.2.1-4.4.1.x86_64`
- `libXrender1-32bit`
- `libXi6-32bit`

NOTE: NetIQ recommends you to obtain the dependent packages from your operating system subscription service to ensure continued support from your operating system vendor. If you do not have a subscription service, you can find the recent packages from a website such as http://rpmfind.net/linux.

Installing Identity Manager on RHEL 6.x or 7.x Servers

To install Identity Manager on a server running Red Hat Enterprise Linux 6.*x* or 7.*x* operating systems, ensure that the server meets a specific set of prerequisites.

- "Prerequisites" on page 55
- "Running a Prerequisite Check" on page 56
- "Ensuring that the Server has Dependent Libraries" on page 56
- "Creating a Repository for the Installation Media" on page 57

Prerequisites

NetIQ recommends that you review the following prerequisites:

- If you have a loopback address alias to the hostname of the system in an `/etc/hosts` entry, it must be changed to the hostname or IP address. That is, if you have an entry similar to the one below in your `/etc/hosts` file, it needs to be changed to the correct entry given in second example below.

  The following example has problems when any utility tries to resolve to the ndsd server:

  ```
  127.0.0.1 test-system localhost.localdomain localhost
  ```

  The following is a correct example entry in `/etc/hosts`:

  ```
  127.0.0.1 localhost.localdomain localhost
  10.77.11.10 test-system
  ```

  If any third-party tool or utility resolves through localhost, it needs to be changed to resolve through a hostname or IP address and not through the localhost address.
- Install the appropriate libraries on the server. For more information, see "Ensuring that the Server has Dependent Libraries" on page 56.

Running a Prerequisite Check

You can generate a report of the missing prerequisites for each Identity Manager component. Run the `./II-rhel-Prerequisite.sh` script, located in the `<Identity Manager build extracted location>\install\utilities` directory of the installation kit.

Ensuring that the Server has Dependent Libraries

On a 64-bit platform, the required libraries for RHEL vary according to your chosen method of installation. Install the dependent libraries or rpms in the listed order.

NOTE: To add a `ksh` file, you can enter the following command:

```
yum -y install ksh
```

- **Guided installation (GUI)**:
  - `libXau-*.i686.rpm`
  - `libxcb-*.i686.rpm`
  - `libX11-*.i686.rpm`
  - `libXext-*.i686.rpm`
  - `libXi-*.i686.rpm`
  - `libXtst-*.i686.rpm`
  - `glibc-*.i686.rpm`
  - `libstdc++-*.i686.rpm`
  - `libgcc-*.i686.rpm`
  - `compat-libstdc++-33-*.x86_64.rpm`
  - `compat-libstdc++-33-*.i686.rpm`
  - `libXrender-*.i686.rpm`
- **Command line installation (console or silent)**:
  - `glibc-*.i686.rpm`
  - `libstdc++-*.i686.rpm`
  - `libgcc-*.i686.rpm`
  - `compat-libstdc++-33-*.x86_64.rpm`
  - `compat-libstdc++-33-*.i686.rpm`
  - `libXtst-*.i686.rpm`
  - `libXrender-*.i686.rpm`

NOTE: NetIQ recommends you to obtain the dependent packages from your operating system subscription service to ensure continued support from your operating system vendor. If you do not have a subscription service, you can find the recent packages from a website such as http://rpmfind.net/linux.

Creating a Repository for the Installation Media

If your RHEL 6.x or 7.x server needs a repository for the installation media, you can manually create one.

NOTE

- Your RHEL server must also have the appropriate libraries installed. For more information, see "Ensuring that the Server has Dependent Libraries" on page 56.
- Ensure that the `unzip` rpm is installed before installing Identity Manager. This applies to all Linux platforms.

To set up a repository for the installation:

1. Create a mount point in your local server.

   Example: `/mnt/rhel (mkdir –p /mnt/rhel)`

2. If you use an installation media, you can mount using the following command:

   ```
   # mount -o loop /dev/sr0 /mnt/rhel
   ```

   OR

   Mount the RHEL 7 installation ISO to a directory like `/mnt/rhel`, using the following command:

   ```
   # mount -o loop RHEL7.x.iso /mnt/rhel
   ```

   Download RHEL 6.x or 7.x iso and mount the same.

   For example: `mount -o loop <path_to_downloaded rhel*.iso> /mnt/rhel`

3. Copy the `media.repo` file from the root of the mounted directory to `/etc/yum.repos.d/` and set the required permissions.

   For example:

   ```
   # cp /mnt/rhel/media.repo /etc/yum.repos.d/rhel7dvd.repo
   # chmod 644 /etc/yum.repos.d/rhel7dvd.repo
   ```

4. Edit the new repo file by changing the `gpgcheck=0` setting to `1` and add the following:

   ```
   enabled=1
   baseurl=file:///mnt/rhel/
   gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
   ```

   In the end, the new repo file would look like the following (though the mediaid would be different depending on the RHEL version):

   ```
   [InstallMedia]
   name=DVD for Red Hat Enterprise Linux 7.1 Server
   mediaid=1359576196.686790
   metadata_expire=-1
   gpgcheck=1
   cost=500
   enabled=1
   baseurl=file:///mnt/rhel
   gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
   ```

5. To install the 32-bit packages, change "exactarch=1" to "exactarch=0" in the `/etc/yum.conf` file.

6 To install the required packages for Identity Manager on RHEL 6.x, create an `install.sh` file and add the following contents to the file:

```
#!/bin/bash
yum clean all
yum repolist
yum makecache

PKGS="ksh gettext.x86_64 libXrender.i686 libXau.i686 libxcb.i686 libX11.i686
libXext.i686 libXi.i686 libXtst.i686 glibc.x86_64 libstdc++.i686
libstdc++.x86_64 libgcc.x86_64 compat-libstdc++-33.x86_64"

for PKG in $PKGS;
do
yum -y install "$PKG"
done
```

NOTE: The script cannot locate libstdc++.i686 library in the 64-bit repository unless you have modified the 64-bit repository to 32-bit repository (Refer to step 6).

---

7 To install the required packages for Identity Manager on RHEL7.x, create an `install.sh` file and add the following contents to the file:

```
#!/bin/bash
yum clean all
yum repolist
yum makecache

PKGS="ksh gettext.x86_64 libXrender.i686 libXau.i686 libxcb.i686 libX11.i686
libXext.i686 libXi.i686 libXtst.i686 glibc.x86_64 libstdc++.i686
libstdc++.x86_64 libgcc.x86_64"

for PKG in $PKGS;
do
yum -y install "$PKG"
done
```

NOTE: As the installation media does not contain `compat-libstdc++-33-*.i686.rpm` and compat-libstdc++-33-*.x86_64.rpm. It needs to be downloaded from the Red Hat portal.

Example: To install the `compat-libstdc++-33-*.x86_64.rpm`, run the following command:

```
yum -y install compat-libstdc++-33-*.x86_64.rpm
```

---

8 Run the `install.sh` file created in Step 8 or Step 7 depending on the RHEL version.

9 To confirm if the prerequisites are met, run the script mentioned "Running a Prerequisite Check" on page 56.

10 Install Identity Manager 4.6.

III 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.

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/eDirectory`
- **Windows**: `C:\Novell\Directory`

NetIQ recommends that you review the installation process before beginning. For more information, see Chapter 7, “Planning to Install the Identity Vault,” on page 61.

7 Planning to Install the Identity Vault

This section provides the prerequisites, considerations, and system setup needed to install the Identity Vault. First, consult the checklist to understand the installation process.

- "Checklist for Installing the Identity Vault" on page 61
- "Prerequisites and Considerations for Installing the Identity Vault" on page 62
- "Understanding Identity Manager Objects in eDirectory" on page 66
- "Replicating the Objects that Identity Manager Needs on the Server" on page 66
- "Using Scope Filtering to Manage Users on Different Servers" on page 68
- "Understanding the Linux Packages in the Identity Vault Installation Kit" on page 69
- "System Requirements for the Identity Vault" on page 71

Checklist for Installing the Identity Vault

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

	Checklist Items
❑	1. Learn about the interaction among Identity Manager components. For more information, see "Identity Vault" on page 28.
❑	2. Decide which servers you want to use for your Identity Manager components. For more information, see "Recommended Server Setup" on page 46.
❑	3. Decide whether you should install an Sentinel before installing the Identity Vault. For more information, see "Recommended Installation Scenarios and Server Setup" on page 44.
❑	4. Review the considerations for installing the Identity Vault to ensure that the computers meet the prerequisites. For more information, see "Prerequisites and Considerations for Installing the Identity Vault" on page 62.
❑	5. Review the hardware and software requirements for the computers that will host the Identity Vault. For more information, see "System Requirements for the Identity Vault" on page 71.
❑	6. Understand how to use escape characters when the names of containers in the Identity Vault include a period (“.”). For more information, see "Using Escape Characters when a Container Name Includes a Period (“.”)" on page 73.
❑	7. Understand how to use the Identity Vault in an environment that uses IPv6 addresses. For more information, see "Using IPv6 Addresses on the Identity Vault Server" on page 79.
❑	8. Understand the ports required for LDAP communications. For more information, see "Using LDAP to Communicate with the Identity Vault" on page 80.
❑	9. Ensure that you have installed a Service Location Protocol (SLP) service and that SLPDAs are stable or that you have configured a `hosts.nds` file. For more information, see "Using OpenSLP or hosts.nds for Resolving Tree Names" on page 73.
❑	10. (Conditional) To install the Identity Vault as a non-root user, ensure that your environment meets the conditions for installation. For more information, see "Prerequisites for Installing the Identity Vault as a Non-root User" on page 64.

	Checklist Items
❑	11. (Conditional) To install on a Linux server, see one of the following sections: ◆ To install as `root`, see "Installing the Identity Vault as Root" on page 87. ◆ To install as a non-`root` user, see "Installing the Identity Vault as a Non-root User" on page 89.
❑	12. (Conditional) To install on a Windows server, see one of the following sections: ◆ For a guided installation (wizard), see "Using the Wizard to Install the Identity Vault on a Windows Server" on page 91. ◆ For a silent installation (unattended), "Silently Installing and Configuring the Identity Vault on a Windows Server" on page 92.
❑	13. Apply Hofix 2 on the Identity Vault. For more information, see Chapter 11, "Applying Hotfix 2 to the Identity Vault," on page 101.
❑	14. Configure NetIQ SecretStore. For more information, see "Adding SecretStore to the Identity Vault Schema" on page 109.
❑	15. (Optional) Exclude the DIB directory on your eDirectory server from any antivirus or backup software process.
❑	16. (Optional) Back up your DIB directory. For more information, see "Backing Up and Restoring NetIQ eDirectory" in the *NetIQ eDirectory Administration Guide*.
❑	17. Install the Identity Manager engine. For more information, see Chapter 16, "Preparing to Install the Engine, Drivers, and Plug-ins," on page 139.

Prerequisites and Considerations 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 the framework for the Identity Vault.

- "Prerequisites for Installing the Identity Vault" on page 62
- "Prerequisites for Installing the Identity Vault as a Non-root User" on page 64
- "Prerequisites for Installing Identity Vault on a Windows Server" on page 64
- "Prerequisites for Installing the Identity Vault in a Clustered Environment" on page 65

Prerequisites 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 NetIQ 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 "Using OpenSLP or hosts.nds for Resolving Tree Names" on page 73.

- (Conditional) 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.
- (Conditional) For a guided installation on a server running SLES 12 SP1 or later platforms, ensure that the server has `libXtst6-32bit-1.2.1-4.4.1.x86_64`, `libXrender1-32bit`, and `libXi6-32bit` libraries installed.
- 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 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 secured - 636
  - HTTP clear text - 8028
  - HTTP secured - 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" in the *NetIQ eDirectory Installation Guide*.
- (Conditional) NICI 2.7 and eDirectory 8.8.x support key sizes up to 4096 bits. To use a 4 KB key size, you must upgrade every server to the supported version of eDirectory. 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 a supported version of eDirectory, 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 the upgraded eDirectory 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 "Using Escape Characters when a Container Name Includes a Period (".")" on page 73.
- To support LDAP search with Virtual List View (VLV) and Server Side Sort (SSS) controls, apply Hotfix 2 to eDirectory 9.0.2 or eDirectory 8.8.8 Patch 9. For more information, see Chapter 11, "Applying Hotfix 2 to the Identity Vault," on page 101.

  This hotfix is not needed if you installed eDirectory with the integrated installation program. The integrated installer installs an updated version of eDirectory that has this hotfix applied.

Prerequisites 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.
- 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 NOVLsubag_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:$LD_LIBRARY_PATH
  export PATH=/etc/opt/novell/eDirectory/conf:$PATH
  export MANPATH=/opt/novell/man:$MANPATH
  ```

  For example:

  ```
  rpm -ivh --nodeps novell-NOVLsubag-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.

Prerequisites 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, `vcredist_x86.exe` and `vcredist_x64.exe` are located in the `eDirectory\Windows\x64\redist_pkg` folder.
  - Novell International Cryptographic Infrastructure (NICI) for both 32-bit and 64-bit. By default, the installation files are located in the `eDirectory/Windows/`*`processor_type/`*`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 "Understanding OpenSLP" on page 75.

Prerequisites 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 NICI (NetIQ International Cryptographic Infrastructure) data so that server-specific keys are replicated among the cluster nodes. NICI 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 about installing the Identity Vault in a clustered environment, see Deploying eDirectory on High Availability Clusters in the *NetIQ eDirectory Installation Guide*.

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 Identity Manager 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.

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. NetIQ 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 68.
  - **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 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.

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.

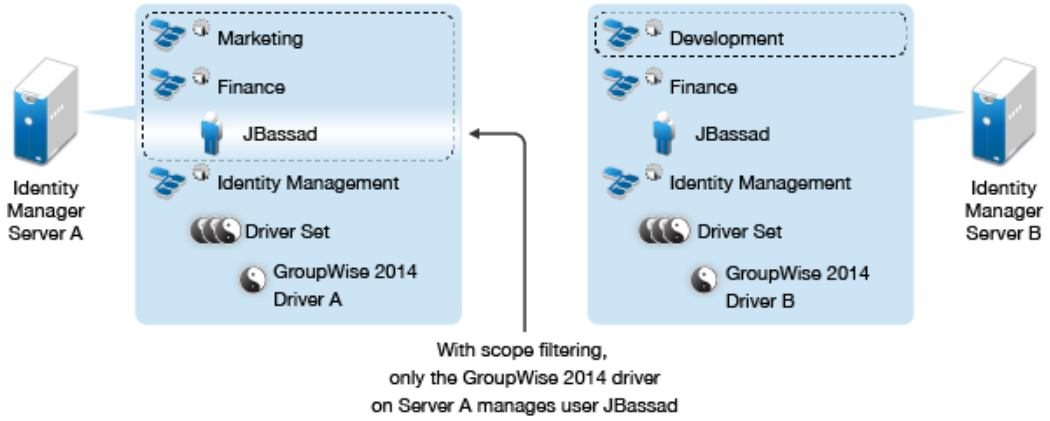
- You want an Identity Manager driver to synchronize all users, but you don't want all users to be replicated on the same server.

  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 7-1 on page 68 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 7-1 *Scope Filtering Defines Which Drivers Synchronize Each Container*



The administrator wants all the users in the tree to be synchronized by the GroupWise 2014 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 2014 driver, one on each server. He installs Identity Manager and sets up the GroupWise 2014 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 2014 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 2014 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 2014 Driver A and GroupWise 2014 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 *NetIQ Identity Manager Understanding Policies Guide*.

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.

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 NICI. 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 `NOVLmgnt`, `NOVLxis`, and `NLDAPbase` packages.
`NOVbase`	Represents the Directory User Agent. This package depends on the NICI package. This package contains the following items: ◆ 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.

Package	Description
NDScommon	Contains the man pages for the eDirectory configuration file, install, and uninstall utilities. This package depends on the NDSbase package.
NDSmasv	Contains the libraries required for mandatory access control (MASV).
NDSserv	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: ◆ 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, NDSD, and NLDAP. ◆ Man pages.
NDSrepair	Contains the runtime libraries and the utility that corrects problems in the eDirectory database. This package depends on the NDSbase package.
NLDAPbase	Contains LDAP libraries, extensions to LDAP libraries, and the following LDAP tools: ◆ ldapdelete ◆ ldapmodify ◆ ldapmodrdn ◆ ldapsearch This package is dependent on the NLDAPsdk package.
NOVLnmas	Contains all the NMAS libraries and the nmasinst binaries needed for NMAS server. This package depends on the NICI and NDSmasv packages.
NLDAPsdk	Contains NetIQ extensions to LDAP runtime and Security libraries (Client NICI).
NOVLsubag	Contains the runtime libraries and utilities for the eDirectory SNMP subagent. This package depends on the NICI, NDSbase, and NLDAPbase packages.
NOVLpkit	Provides PKI Services which do not require eDirectory. This package depend on the NICI and NLDAPsdk packages.
NOVLpkis	Provides PKI Server Service. This package depends on the NICI, NDSbase, and NLDAPsdk packages.
NOVLsnmp	The runtime libraries and utilities for SNMP. This package depends on the NICI package.
NDSdexvnt	Contains the library that manages events generated in NetIQ eDirectory to other databases.

Package	Description
`NOVLpkia`	Provides PKI services. This package depends on the `NICI`, `NDSbase`, and `NLDAPsdk` packages.
`NOVLembox`	Provides the eMBox infrastructure and eMTools.
`NOVLlmgnt`	Contains runtime libraries for NetIQ Language Management.
`NOVLxis`	Contains the runtime libraries for NetIQ XIS.
`NOVLsas`	Contains the NetIQ SAS libraries.
`NOVLntls`	Contains NetIQ TLS library. This package is also identified as `ntls`.
`NOVLldif2`	Contains the NetIQ Offline Bulkload utility and depends on the `NDSbase`, `NDSserv`, `NOVLntls`, `NOVLlmgnt`, and `NICI` packages.
`NOVLncp`	Contains the NetIQ Encrypted NCP Services for Linux. This package depends on the `NDScommon` package.

System Requirements for the Identity Vault

This section provides the minimum requirements for the server(s) where you want to install the Identity Vault. Ensure that you review the prerequisites and considerations for installation, particularly those related to the operating system.

Category	Requirement
Processor	1 GHz
Disk space	◆ 300 MB for the Identity Vault ◆ 150 MB of additional disk space for every 50,000 users
Memory	2 GB
Operating system (certified)	One of the following 64-bit operating systems: ◆ Open Enterprise Server 2015 SP1 ◆ Open Enterprise Server 11 SP3 ◆ Red Hat Enterprise Linux 7.3 ◆ Red Hat Enterprise Linux 6.8 ◆ SUSE Linux Enterprise Server 12 SP1 ◆ SUSE Linux Enterprise Server 11 SP4 ◆ Windows Server 2012 R2 ◆ Windows Server 2012 NetIQ recommends that you apply the latest operating system patches according to the manufacturer's automated update facility before you install Identity Manager. **NOTE:** *Certified* means that the operating system has been fully tested and is supported.

Category	Requirement
Operating system (supported)	Latest versions of service packs for the certified operating systems **NOTE:** *Supported* means that the operating system has not yet been tested but is expected to work
Virtualization system	◆ Hyper-V Server 2012 R2 ◆ VMWare ESX 5.0 and later ◆ Windows Server 2012 R2 Virtualization with Hyper-V (supported) NetIQ supports Identity Manager on enterprise-class virtualization systems that provide official support for the operating systems where NetIQ products are running. As long as the vendors of the virtualization systems officially support these operating systems, NetIQ supports the entire Identity Manager stack on them.
Directory services	NetIQ eDirectory 8.8.8 Patch 9 Hotfix 2 (runs with iManager 2.7.7 Patch 9 or later) or NetIQ eDirectory 9.0.2 Hotfix 2 (runs with iManager 3.0.2 Patch 1 or later) **NOTE:** NetIQ applies certain restrictions on installing eDirectory 9.0.2 as an Identity Vault. For more information, see "Working with eDirectory 9.0.2 or Later" on page 84.
Web browser	Any of the following browsers, at a minimum: ◆ Google Chrome 51 ◆ Microsoft Internet Explorer 11 ◆ Mozilla Firefox 46

8 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.

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 ldapconfig. 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`.

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:

- "Using a hosts.nds File to Resolve Tree Names" on page 74
- "Understanding OpenSLP" on page 75
- "Configuring SLP for the Identity Vault" on page 77

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. Do not use `localhost`.
- **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
     CORPSERVER 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.

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.

The interface provided by OpenSLP source code is an implementation of another IETF standard for programmatically accessing SLP functionality, documented in RFC 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 and the SourceForge websites. The OpenSLP website 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 75
- "User Agents" on page 76
- "Service Agents" on page 76
- "Directory Agents" on page 77

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 76.

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.

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 DAAdvert 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 tri-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.

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 user 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
	4 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.

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.

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 "Modifying the eDirectory Tree and Replica Server with the ndsconfig Utility" on page 105.

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 79
- "Adding LDAP URLS for IPV6 on the LDAP Server Object" on page 80

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:abc
   d: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 `ndsd` 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**.

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 10, “Installing the Identity Vault on a Windows Server,” on page 91.

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

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 TLS/SSL 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`. After eDirectory 8.7.3, the installation program loads `nldap`, 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 does not 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" in the *NetIQ eDirectory 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" in the *NetIQ eDirectory Administration Guide*.

Installing NICI Manually on Workstations that have Management Utilities

You must install NICI on every workstation that uses a management utility such as iManager. For more information about using NICI with the Identity Vault, see "Prerequisites for Installing the Identity Vault" on page 62.

Installing NICI on Linux Servers

Use `nds-install` and select the NICI option. By default, you can find the installation file in the `products\eDirectory\`*`processor_type`*`\setup\` directory. NetIQ recommends installing NICI as `root` because the required NICI 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 NICI 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 NICI.

This section describes the following activities:

- "Installing NICI as Root User" on page 82
- "Installing NICI as a Non-root User" on page 82

Installing NICI as Root User

To install NICI, perform the following steps:

1. Execute both of the following commands:

   ```
   32-bit: rpm -ivh NICI_rpm_absolute_path/nici-2.7.7-0.02.i586.rpm
   64-bit: rpm -ivh NICI_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.

2. Verify that NICI is set to server mode. Enter the following command:

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

   This is a mandatory step to ensure eDirectory configuration does not fail.

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 in 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
   ```

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.

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.

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" in the *NetIQ eDirectory Administration Guide*.

Installing NMAS Client Software on Windows Servers

1. Log in to the Windows client workstation with an administrator account.
2. Run the `nmasinstall.exe` program from the installation directory, by default `IDM4.5_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.

Working with eDirectory 9.0.2 or Later

In addition to eDirectory 8.8.8 Patch 3, you can install eDirectory 9.0.2 or later as an Identity Vault and as a connected system with Identity Manager 4.6. Before using eDirectory 9.0.2 or later as an Identity Vault, NetIQ recommends that you review the following sections:

- "Features That Can be Enabled on the Identity Vault Server" on page 84
- "Changing the NICI Configuration to a Non-FIPS Mode in eDirectory" on page 85

Features That Can be Enabled on the Identity Vault Server

Review the following table to understand which features of eDirectory 9.0.1 or later can be enabled with Identity Manager. None of these restrictions apply when eDirectory 9.0.1 or later is used as a connected system.

Feature	Can be enabled (Yes/No)	Description
TLS 1.2	Yes	Can enable all TCP communication using TLS 1.2 protocol.
Suite B Configuration	Yes	Can configure stronger ciphers for SSL communication as specified by Suite B.
AES 256-bit SDI Key	Yes	No impact on Identity Manager
LDAP and HTTP Services	Yes	The Identity Manager services continue to use the RSA certificate.
Authentication	Yes	No impact on Identity Manager
NPKI (NetIQ Certificate Server)	Yes	No impact on Identity Manager

Feature	Can be enabled (Yes/No)	Description
NICI in FIPS Mode	No	NICI is disabled in FIPS mode by default. If you enable it, the Identity Manager engine does not start and reports an error. For information about changing the NICI configuration to a non-FIPS mode, see "Changing the NICI Configuration to a Non-FIPS Mode in eDirectory" on page 85.
Container Readiness	Yes	No impact on Identity Manager
Enhanced Nested Groups	Yes	Not supported by Identity Manager engine and drivers
Proxied Authorization Control	Yes	No impact on Identity Manager
Monitoring	Yes	No support extended for monitoring Identity Manager components
Enhanced Data Replication	Yes	No impact on Identity Manager
Improved Data Synchronization	Yes	No impact on Identity Manager
Optimized Janitor Thread of Inherited ACL Calculation	Yes	No impact on Identity Manager

For detailed information about the new features of eDirectory 9.0.1 and 9.0.2, see the appropriate Release Notes at eDirectory Documentation site.

Changing the NICI Configuration to a Non-FIPS Mode in eDirectory

Identity Manager 4.6 does not support eDirectory 9.0.1 or later with NICI enabled in FIPS mode. For Identity Manager to work properly, you must disable the FIPS mode for NICI in the NICI configuration in one of the following ways:

- **Linux:** Navigate to `/etc/opt/novell/nici64.cfg` and change **RestrictionLevel** to **0**.
- **Windows:** Navigate to the `HKLM\SOFTWARE\Novell\Windows` registry and change this setting to **0** in the `nici_x64` key. Make this change in the `nici_x64` key on each server in the tree.

9 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. For more information about the additional packages that you can use to support eDirectory on a Linux server, see "Linux Packages for NetIQ eDirectory" in the *NetIQ eDirectory 9.0 SP2 Installation 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.

If you are installing eDirectory 9.0 or later version where the latest 64-bit Remote Loader is already installed, then the eDirectory installation fails and Remote Loader stops working. To ensure that the Remote Loader works properly, perform the below steps before installing eDirectory 9.0 or later:

1. Stop Remote Loader and its instances.
2. Uninstall `novell-DXMLopensslx` RPM.
3. Install eDirectory.

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 `non-root` user and specify a custom installation path, you might want to use the tarball format for installation. For more information, see "Installing the Identity Vault as a Non-root User" on page 89.

To install the Identity Vault as `root`:

1. Log in 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, located by default in the `products/eDirectory/`*`processor_type`*`/setup` directory:

   ```
   ./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" in the *NetIQ eDirectory 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, and HTTP services. If you do not specify the module name, all the modules are installed.

NOTE: You must install and configure NetIQ SecreStore (`ss`). For more information, see "Adding SecretStore to the Identity Vault Schema" on page 109.

-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/etc/opt/novell/eDirectory/conf/ndspath
```

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

For example:

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

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

```
. /etc/opt/novell/eDirectory/conf/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 in or open a new shell.

7 To support LDAP search with VLV (Virtual List View) and SSS (Server Side Sort) controls, apply Hotfix 2 to the Identity Vault. For more information, see Chapter 11, "Applying Hotfix 2 to the Identity Vault," on page 101.

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 "Prerequisites for Installing the Identity Vault as a Non-root User" on page 64.

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 in as a `sudo` user with the appropriate rights to the computer where you want to install the Identity Vault.

NOTE: You can also log in 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/etc/opt/novell/eDirectory/conf/ndspath
utility_name_with_parameters
```

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

```
. custom_location/eDirectory/etc/opt/novell/eDirectory/conf/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 in or open a new shell.

5 To support LDAP search with VLV (Virtual List View) and SSS (Server Side Sort) controls, apply Hotfix 2 to the Identity Vault. For more information, see Chapter 11, "Applying Hotfix 2 to the Identity Vault," on page 101.

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

6a 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 "Understanding the ndsconfig Utility Parameters" on page 106.
- 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`.
- You must install and configure NetIQ SecreStore (`ss`). For more information, see "Adding SecretStore to the Identity Vault Schema" on page 109.

6b Use the ndsmanage utility to configure a new instance. For more information, see "Creating a New Instance in the Identity Vault" on page 112.

Run the `ndsstat` command to verify the eDirectory version.

10 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 Administration Guide*. For more information on the Client, see the Novell Client for Windows 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 "Prerequisites for Installing Identity Vault on a Windows Server" on page 64.

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

1. Log in 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 `IDM`*`version`*`_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.

  Specify **Tree name, Server Context name, admin name,** and **context**.

  For example: Tree name: `WIND2K`; Server Context name: `<hostname><context>` example: `WIND2K-NDS.sa.system`; admin name: `admin`; context: `sa.system.`

  For more information, see "NWI:NDS" on page 93.

- 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*.
- (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 "Using LDAP to Communicate with the Identity Vault" on page 80.
- 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" in the *NetIQ eDirectory Administration Guide*.
- You must install and configure NetIQ SecreStore (`ss`). For more information, see "Adding SecretStore to the Identity Vault Schema" on page 109.

7 Follow the instructions in the wizard until you finish installing the Identity Vault.

8 To support LDAP search with VLV (Virtual List View) and SSS (Server Side Sort) controls, apply Hotfix 2 to the Identity Vault. For more information, see Chapter 11, "Applying Hotfix 2 to the Identity Vault," on page 101.

9 To use the NMAS login methods, install the NMAS client software on each client workstation. For more information, see "NMAS Considerations" in the *NetIQ eDirectory Administration Guide*.

10 (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" in the *NetIQ eDirectory Administration Guide*.

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.

NOTE: You must install and configure NetIQ SecreStore (`ss`). For more information, see "Adding SecretStore to the Identity Vault Schema" on page 109.

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 93
- “NWI:NMAS (NMAS Methods)” on page 95
- “eDir:HTTP (Ports)” on page 96
- “Novell:Languages:1.0.0 (Language Settings)” on page 96
- “Initialization” on page 97
- “NWI:SNMP” on page 97
- “EDIR:SLP” on page 97
- “Novell:ExistingTree:1.0.0” on page 97
- “Selected Nodes” on page 98
- “Novell:NOVELL_ROOT:1.0.0” on page 98

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 wan 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 97.

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 97.

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 93.

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.

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 “Prerequisites for Installing Identity Vault on a Windows Server” on page 64. Also, create the `response.ni` file to use as a template for the installation. For more information, see “Editing the response.ni File” on page 93.

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 “Editing the response.ni File” on page 93.
2. Log in 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
```

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 "Editing the response.ni File" on page 93.

2 Log in 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 /nopleasewait /template=Response file
```

For example:

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

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 "Prerequisites for Installing Identity Vault on a Windows Server" on page 64. 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 "Editing the response.ni File" on page 93.

2 Log in 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 /
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 Applying Hotfix 2 to the Identity Vault

The Identity Manager installation package includes the files for applying Hotfix 2 to the Identity Vault for eDirectory 8.8.8 Patch 9 and eDirectory 9.0.2 versions. You can install the hotfix as a root user or an administrator, or as a non-root user.

Prerequisites for Installing the Hotfix

Before installing the hotfix, complete the following steps:

- Stop the Identity Vault.
- (Conditional) On Windows, stop the Identity Vault and SNMP services.

Installing the Hotfix as a Root User or an Administrator

To install the hotfix to the Identity Vault as a root user, complete the following steps:

1. Ensure that you have completed the prerequisites for installing the hotfix.
2. On the server where you want to run the hotfix, log in as `root` or administrator.
3. Navigate to the hotfix installation files directory of the `.iso` image file.
   - **eDirectory 9.0.2 HotFix 2:** `products/eDirectory/eDir902_HF2`
   - **eDirectory 8.8.8 Patch 9 HotFix 2:** `products/eDirectory-888x/eDir8889_HF2`
4. Depending on your platform, run one of the following commands:
   - **Linux:** Run the following commands in a terminal window:
     - **eDirectory 9.0.2:** Run the following commands:

       ```
       rpm -Uvh novell-NDSserv-9.0.2-2.x86_64.rpm
       rpm -Uvh novell-AUDTplatformagent-2.0.2-80.x86_64.rpm
       rpm -Uvh novell-AUDTedirinst-9.0.2-2.x86_64.rpm
       rpm -Uvh novell-eba-9.0.2-2.x86_64.rpm
       rpm -Uvh novell-nmas-server-9.0.2-2.x86_64.rpm
       ```

     - **eDirectory 8.8.8 Patch 9**: Run the following commands:

       ```
       rpm -Uvh  novell-NDSserv-8.8.8.9-2.x86_64.rpm
       rpm -Uvh novell-AUDTedirinst-8.8.8.9-62.x86_64.rpm
       rpm -Uvh novell-AUDTplatformagent-2.0.2-80.x86_64.rpm
       rpm -Uvh novell-nmas-8.8.8.9-20170112.x86_64.rpm
       ```

- **Windows:** Perform the following steps:
  1. Copy the following files from the hotfix directory to your current directory. For example: `C:\Novell\Directory`:
     - `nldap.dlm`
     - `ebasrv.dlm`
     - `nauditds.dlm`
     - `nmas.dlm`
  2. Install `Novell_Audit_PlatformAgent_Win64.exe` file.

5 Start the eDirectory instance.

- **Linux:** To start all instances, enter the following command at the command line:

  ```
  ndsmanage startall
  ```

  To start a single instance, enter the following command:

  ```
  ndsmanage start --config-file configuration_file_of_the_instance
  ```

- **Windows:** Open a terminal and navigate to the `NDSCons.exe` utility located in the eDirectory installation folder by default:
  1. Run the following command:

     ```
     NDSCons.exe
     ```

  2. In the NDSCons utility, click **Startup** to start all eDirectory services.
  3. Click **Yes** to confirm.
  4. Verify that all eDirectory services are running, then close the NDSCons utility.

  Alternatively, click **Start > Control Panel > Novell eDirectory Services**.

6 (Conditional) To verify that the hotfix has been successfully applied, check the modification date for the files updated by the hotfix installer.

- **Linux:** Run the following commands depending on your eDirectory version:
  - **eDirectory 9.0.2:** Run the following commands:

    ```
    rpm -qa | grep -i novell-NDSserv
    rpm -qa | grep -i novell-AUDTedirinst
    rpm -qa | grep -i novell-AUDTplatformagent
    rpm -qa | grep -i novell-eba
    rpm –qa | grep –i nmas
    ```

  - **eDirectory 8.8.8 Patch 9:** Run the following commands:

    ```
    rpm -qa | grep -i novell-NDSserv
    rpm -qa | grep -i novell-AUDTedirinst
    rpm -qa | grep -i novell-AUDTplatformagent
    rpm -qa | grep -i nmas
    ```

- **Windows:** Perform the following steps:
  1. Right click the `nldap.dlm` file from your eDirectory installation folder.
  2. Select the `Details` tab in the Properties window.

3. Verify the value in the version for the updated components.
   - `nmas` and `EBAServ` is `9.0.2.2`
   - `nldap` is `4.4.56.0`

Installing the Hotfix as a Non-root User

To install the Hotfix to Identity Vault as a non-root user, complete the following steps:

1. Ensure that you have completed the prerequisites for installing the hotfix.
2. On the server where you want to run the hotfix, log in as a non-root user.
3. Navigate to the hotfix installation files directory of the `.iso` image file.
   - **eDirectory 9.0.2 HotFix 2:** `products/eDirectory/eDir902_HF2`
   - **eDirectory 8.8.8 Patch 9 HotFix 2:** `products/eDirectory-888x/eDir8889_HF2`
4. Create a temporary directory on your Linux machine and extract the files from the `nonroot.tar.gz` file to this directory.
5. Copy the `opt` directory from this temporary directory location to eDirectory installed location using the following command:

   ```
   cp –rp opt/
   ```

   For example, eDirectory installation location: `/home/user/eDirectory`
6. Create another temporary directory to extract filer form RPM.
7. Navigate to the temporary directory and run the following commands based on your current eDirectory version:
   - **eDirectory 9.0.2 HotFix 2:** Run the following commands:

     ```
     rpm2cpio ../novell-AUDTedirinst-9.0.2-2.x86_64.rpm | cpio –idmv
     ```
   - **eDirectory 8.8.8 Patch 9 HotFix 2:** Run the following commands:

     ```
     rpm2cpio ../novell-AUDTedirinst-8.8.8.9-62.x86_64.rpm | cpio –idmv
     ```
8. Copy the `opt` directory from the temporary directory location to eDirectory installed location using the following command:

   ```
   cp –rp opt/
   ```

   Example eDirectory installation location: `/home/user/eDirectory`
9. Start eDirectory.
   - To start all instances, enter the following command at the command line:

     ```
     ndsmanage startall
     ```
   - To start a single instance, enter the following command:

     ```
     ndsmanage start --config-file configuration_file_of_the_instance
     ```
10. Upgrade your tree configuration using the following command:

    ```
    ndsconfig upgrade
    ```
11. Restart eDirectory.
    - To start all instances, enter the following command at the command line:

```
ndsmanage startall
```

- To start a single instance, enter the following command:

  ```
  ndsmanage start --config-file configuration_file_of_the_instance
  ```

12 (Conditional) To verify if the hotfix is successfully applied, run the following command:

```
strings <installed location>/opt/novell/eDirectory/lib64/nds-modules/
libnldap.so | grep –i version
```

Verify that the value in the version is `40004.56.5` for eDirectory 9.0.2 and `20810.25.5` for eDirectory 8.8.8 Patch 9.

12 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.

Modifying the eDirectory Tree and Replica Server with the ndsconfig Utility

After installing the Identity Vault, you can use the ndsconfig utility to configure the 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 12, “Configuring the Identity Vault after Installation,” on page 105.

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” in the *NetIQ eDirectory Administration Guide*.

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

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 "Using Escape Characters when a Container Name Includes a Period (".")" on page 73.

-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://1.2.3.4:389,ldaps://1.2.3.4:636,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 80.

-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 ndsd for the new value to take effect. You do not need to restart ndsd 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.

Adding SecretStore to the Identity Vault Schema

You must extend the Identity Vault schema to support SecretStore functionality. The identity applications need SecretStore to connect to the vault.

1. To extend the schema for the Identity Vault, enter the following command:

   For x64bit

   ```
   ice -S SCH -f /opt/novell/eDirectory/lib64/nds-schema/sssv3.sch -D LDAP -s
   serverIP -d adminDN
   ```

   For example:

   For x32bit

   ```
   ice -S SCH -f /var/opt/novell/eDirectory/lib/nds-schema/sssv3.sch -D LDAP -s
   192.0.2.1 -d cn=admin,o=administrators
   ```

2. (Conditional) To configure SecretStore on a Linux server, complete the following steps:

   2a Navigate to the `conf` directory, by default `/etc/opt/novell/eDirectory/conf`.

   2b To run the configuration file, enter `ssscfg -c`.

   2c Specify the configuration settings for Secret Store, then close the utility.

   2d In a text editor, open `ndsmodules.conf`.

   2e Add the following entry to the file:

   ```
   ssncp
   ```

   This entry loads the SecretStore module when eDirectory starts.

3 (Conditional) To configure SecretStore on a Windows server, complete the following steps:

3a Navigate to the `conf` directory, by default `Program Files/novell/eDirectory/conf`.

3b Enter the following command:

```
ssscfg.exe -c
```

3c Specify the configuration settings for SecretStore, then close the utility.

3d Run NDSCons.exe.

3e In the utility, specify `auto` for the `ssncp.dlm` module.

3f Close the utility.

For more information, see "SecretStore Configuration for eDirectory Server" in the *NetIQ eDirectory Administration Guide* (https://www.netiq.com/documentation/edirectory-9/edir_admin/data/bookinfo.html).

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
```

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]
```

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
```

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]
   ```

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
```

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" 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).

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.

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.

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.

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`.

Invoking a Utility for an Instance in the Identity Vault

You can run utilities, such as DSTrace, against an instance. For example, you want to run the DSTrace 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.

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 and Managing Sentinel Log Management for Identity Governance and Administration

This section guides you through the process of installing Sentinel Log Management for IGA (SLM for IGA), which is the default auditing service for Identity Manager. Identity Reporting requires this version of Sentinel or a third-party auditing service such as NetIQ Sentinel.

The installation files are located in the `products/Sentinel` directory within the `.iso` image file for the Identity Manager installation package. By default, the installation program installs the components in the `/opt/novell/sentinel` location.

Identity Reporting communicates with SLM for IGA for auditing. To log events, Identity Reporting uses the data synchronization policy created by SLM for IGA. The events that you filter using the data synchronization policy will reach the Reporting database. For more information about creating the data synchronization policy and filtering the policy, see "Creating the Data Synchronization Policy" on page 494.

The PostgreSQL that is bundled with Identity Manager installer can be used. If you have installed PostgreSQL on a separate server, then you need to migrate your EAS data to a new server. For more information, see "Migrating from Event Auditing Service to Sentinel Log Management for IGA" on page 489.

NetIQ recommends that you review the installation process before beginning. For more information, see Chapter 13, "Planning to Install Sentinel Log Management for IGA," on page 117.

13 Planning to Install Sentinel Log Management for IGA

This section provides guidance for preparing to install Sentinel Log Management for IGA (SLM for IGA), which is the default auditing service for Identity Manager.

- "Checklist for Installing SLM for IGA" on page 117
- "Deciding When to Install SLM for IGA" on page 118
- "Understanding the Installation Process" on page 124
- "Prerequisites for Installing SLM for IGA" on page 125
- "System Requirements" on page 126

Checklist for Installing SLM for IGA

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

	Checklist Items
❑	1. Learn about when you want to install SLM for IGA. For more information, see "Deciding When to Install SLM for IGA" on page 118.
❑	2. Review the system requirements before installation to ensure that the computers meet the requirements. For more information, see "System Requirements" on page 126.
❑	3. (Conditional) For computers running a SLES 12 SP1 or later operating system, ensure that you have installed the appropriate set of libraries for a guided installation. For more information, see "Installing Identity Manager on SLES 12 SP1 or Later Servers" on page 55.
❑	4. (Conditional) For computers running an RHEL 6.x or RHEL 7.x operating system, ensure that you have installed the appropriate set of libraries. For more information, see "Installing Identity Manager on RHEL 6.x or 7.x Servers" on page 55.
❑	5. Determine whether you want to install SLM for IGA or use an existing Sentinel server for auditing purposes in your environment. For more information, see "Deciding When to Install SLM for IGA" on page 118.
❑	6. Learn about the important changes in the auditing infrastructure and Identity Reporting. For more information, see "Deciding When to Install SLM for IGA" on page 118.
❑	7. Decide how you want to install SLM for IGA. For more information, see the following sections: ◆ Performing an Interactive Installation ◆ Performing a Silent Installation
❑	8. (Conditional) If you choose to migrate your data from EAS to SLM for IGA, see "Migrating from Event Auditing Service to Sentinel Log Management for IGA" on page 489.
❑	9. (Conditional) Set up a new database for reporting. For more information, see "Setting up the Reporting Server" on page 493.

	Checklist Items
❑	10. Install Identity Reporting on the same server that has the migrated database server. For more information, see "Using the Guided Process to Install Identity Reporting" on page 371.
❑	11. Run the data synchronization utility to enable event forwarding from SLM for IGA to the reporting database. For more information, see "Creating the Data Synchronization Policy" on page 494.
❑	12. Log in to Event Source Management (Live View) and check if SLM for IGA is receiving events. For more information, see "Checking for Sentinel Events" on page 451.
❑	13. Configure the iManager, OSP, and SSPR collector instances. For more information, see "Configuring the Collector Instances in Sentinel" on page 451
❑	14. Configure the event retention and disk space usage. For more information, see "Configuring Event Data Retention" on page 451 and "Configuring Disk Space Usage for Sentinel" on page 452.
❑	15. Download the reports and views for SLM for IGA. For more information, see Using the Download Page to Download Report Definitions and Views in the Administrator Guide to NetIQ Identity Reporting.
❑	16. (Conditional) Configure the Sentinel link to forward events from Sentinel to SLM for IGA. For more information, see "Configuring the Sentinel Link Connection" on page 452.

Deciding When to Install SLM for IGA

Sentinel is the preferred audit event destination for Identity Manager. Identity Manager provides event forwarding capabilities to Sentinel by configuring Sentinel Link using Sentinel Event Source Management (ESM).

If you are already using Sentinel for auditing or as an integration framework for tracking identities, you might choose to use your existing Sentinel for auditing events instead of installing SLM for IGA. Regardless of whether you choose to reuse your existing installation or perform a new installation of SLM for IGA shipped with Identity Manager, you must create a synchronization policy on the Sentinel server for auditing events. The Identity Reporting installation directory includes Data Synchronization utility. The utility creates a synchronization policy on Sentinel that synchronizes events to an external SQL database. For more information, see "Creating the Data Synchronization Policy" on page 494.

NOTE: Sentinel Log Management for IGA does not support all features of Sentinel, such as Correlation, Distributed Search, Scalable Storage Routing, Security Intelligence, and all collectors that are not related to Novell and NetIQ products.

Overview of Changes

The following list includes the important changes made to the auditing framework:

- SLM for IGA 8.0.1 replaces Event Auditing Service (EAS) as an event auditing service for Identity Reporting.
- The Data Synchronization utility sets up a data synchronization policy in SLM for IGA or an existing Sentinel server.
- The Data Synchronization policy synchronizes the filtered event data from a Sentinel server or SLM for IGA with the Identity Reporting database.

- The Data Synchronization utility synchronizes data to a new table, `sentinel_events`, in the public schema of the PostgresSQL Reporting database. This table is located in `IDM_RPT_DATA user` in the Oracle database.
- The synchronization utility provides an option to delete the existing Report Data Definitions (RDD) on a SLM for IGA server. However, you must not delete RDDs on an external Sentinel server or on an identity tracking solution.

Also, the Reporting views have been simplified. The following list includes the important changes made to Identity Reporting:

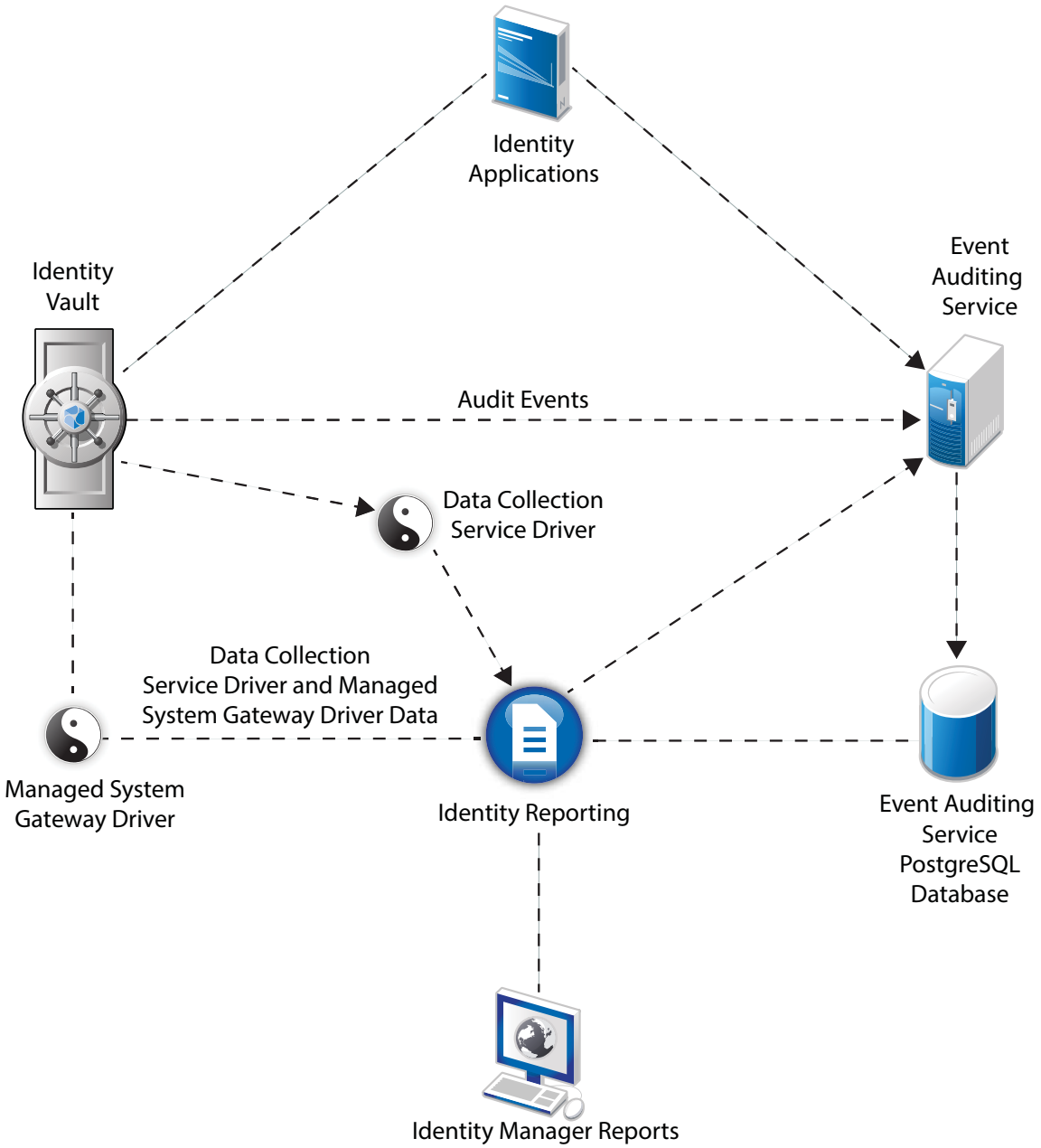
- The following new views have been created:
  - idmrpt_auth_by_serv_v
  - idmrpt_auth_by_user_v
  - idmrpt_events_v2
  - idmrpt_self_pass_change_v
- The following views are modified:
  - idmrpt_identity_cs_v
  - idmrpt_identity_v
  - idmrpt_idv_acct_v
  - idmrpt_res_trust_v
  - idmrpt_user_parameter_v
- Reporting data (excluding event data) migrated from Identity Manager 4.5 can be used with the reports supported with this version of Identity Manager.
- This version of Identity Reporting uses `sentinel_events` table. Therefore, it does not use audit data from a prior version of Identity Manager.

Recommended Installation Scenarios

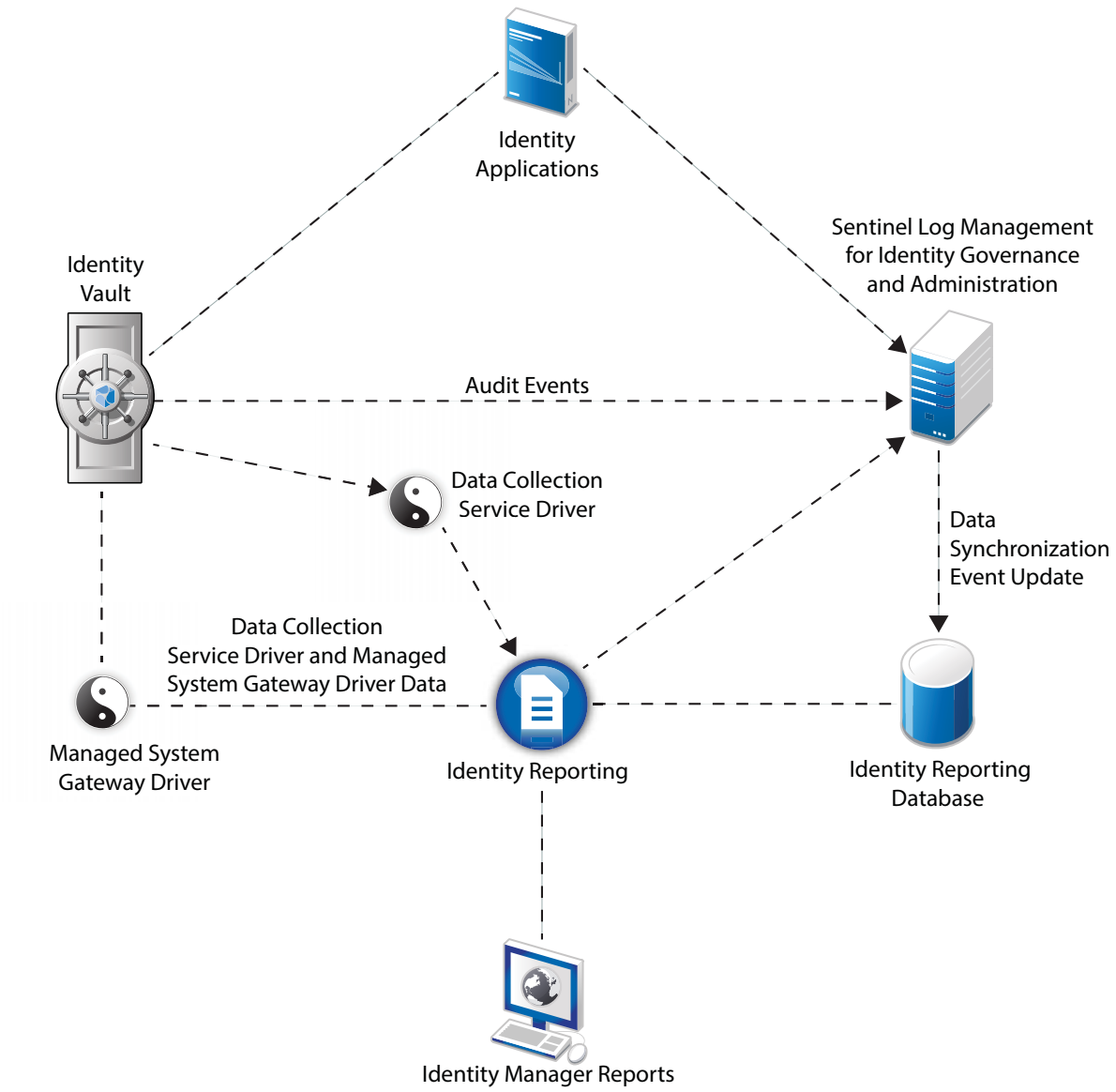
The following scenarios help you evaluate if a new installation of SLM for IGA is required for your environment:

Scenario I: Environment with Event Auditing Service and Identity Reporting

This is the most common scenario where you have only EAS installed and you do not have an existing installation of Sentinel or an identity tracking solution in your environment. The following figure illustrates this scenario:



You must install SLM for IGA that ships with Identity Manager because EAS is not supported with this version of Identity Manager as depicted in the following figure:



Follow these high-level steps to configure auditing in this environment:

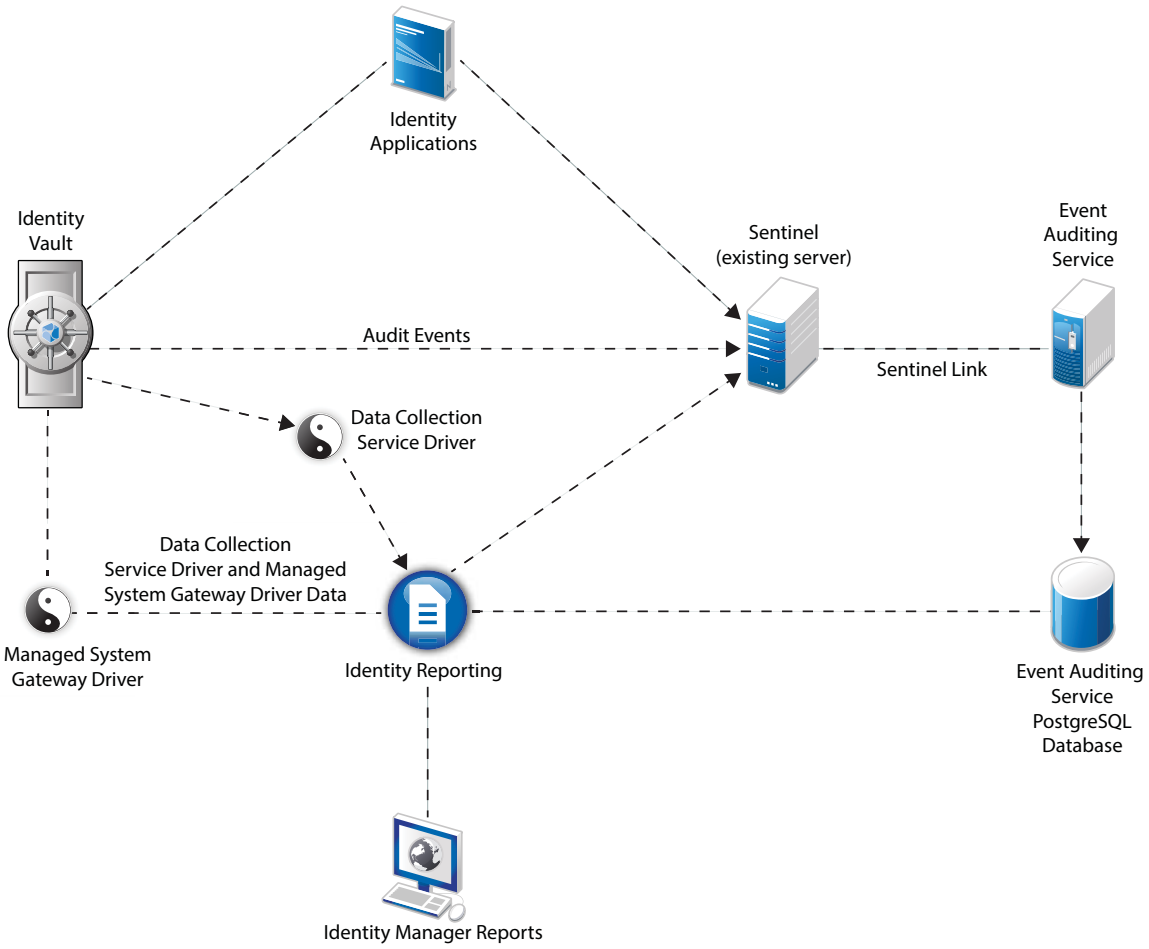
1 Migrate the existing Reporting data to another standalone PostgreSQL instance. For more information, see "Migrating from Event Auditing Service to Sentinel Log Management for IGA" on page 489.

2 To generate reports in Identity Manager, perform a new installation of Identity Reporting. For more information, see Part XIII, "Installing Identity Reporting," on page 363.

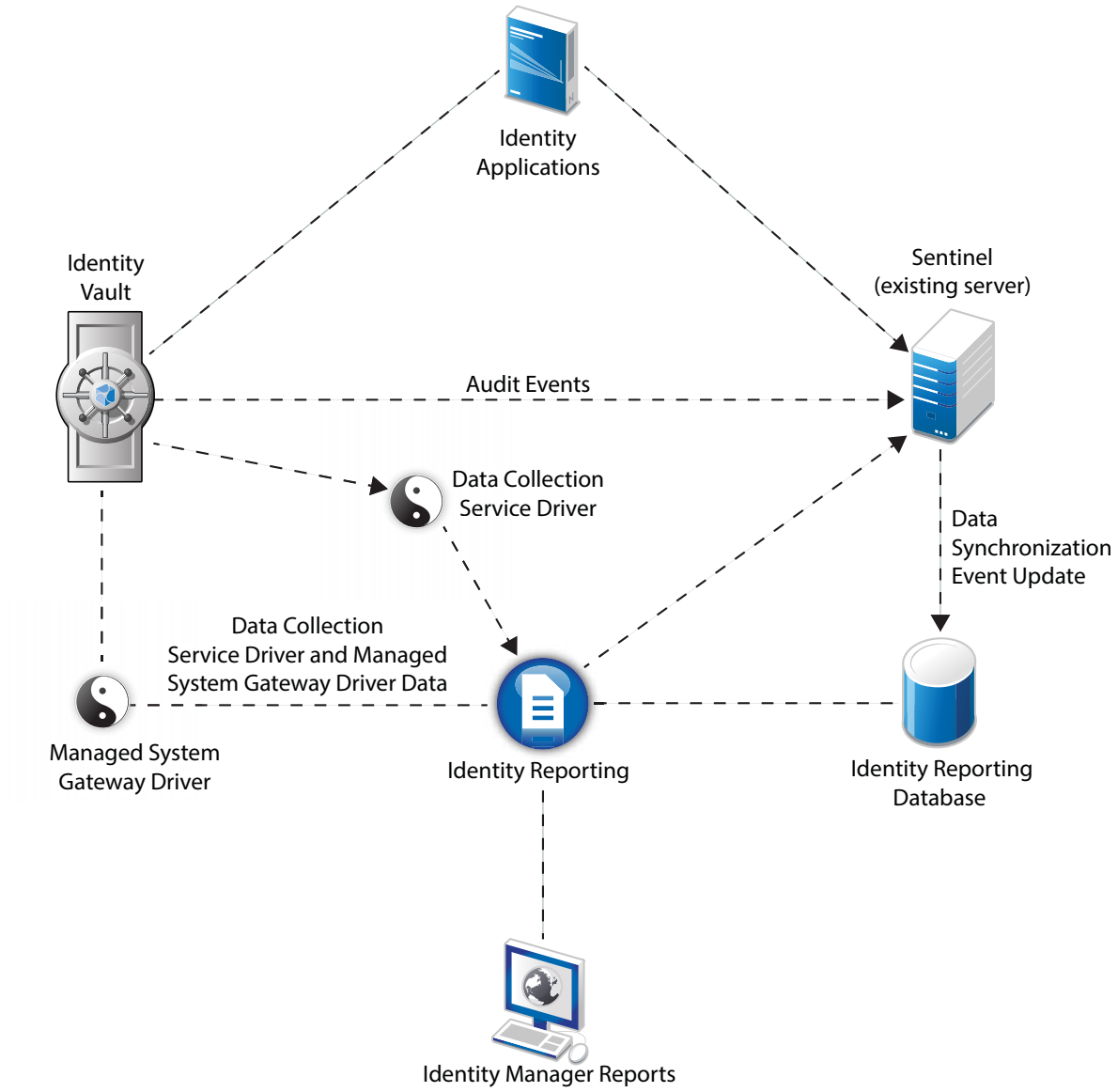
3 Run the data synchronization utility to create a policy in SLM for IGA that synchronizes the Identity Manager events with the Identity Reporting database. For more information, see "Creating the Data Synchronization Policy" on page 494.

Scenario II: Environment with Event Auditing Service, an existing Sentinel server, and Identity Reporting

This configuration includes EAS, an existing installation of Sentinel or an identity tracking solution, and Identity Reporting. The following figure illustrates this scenario:



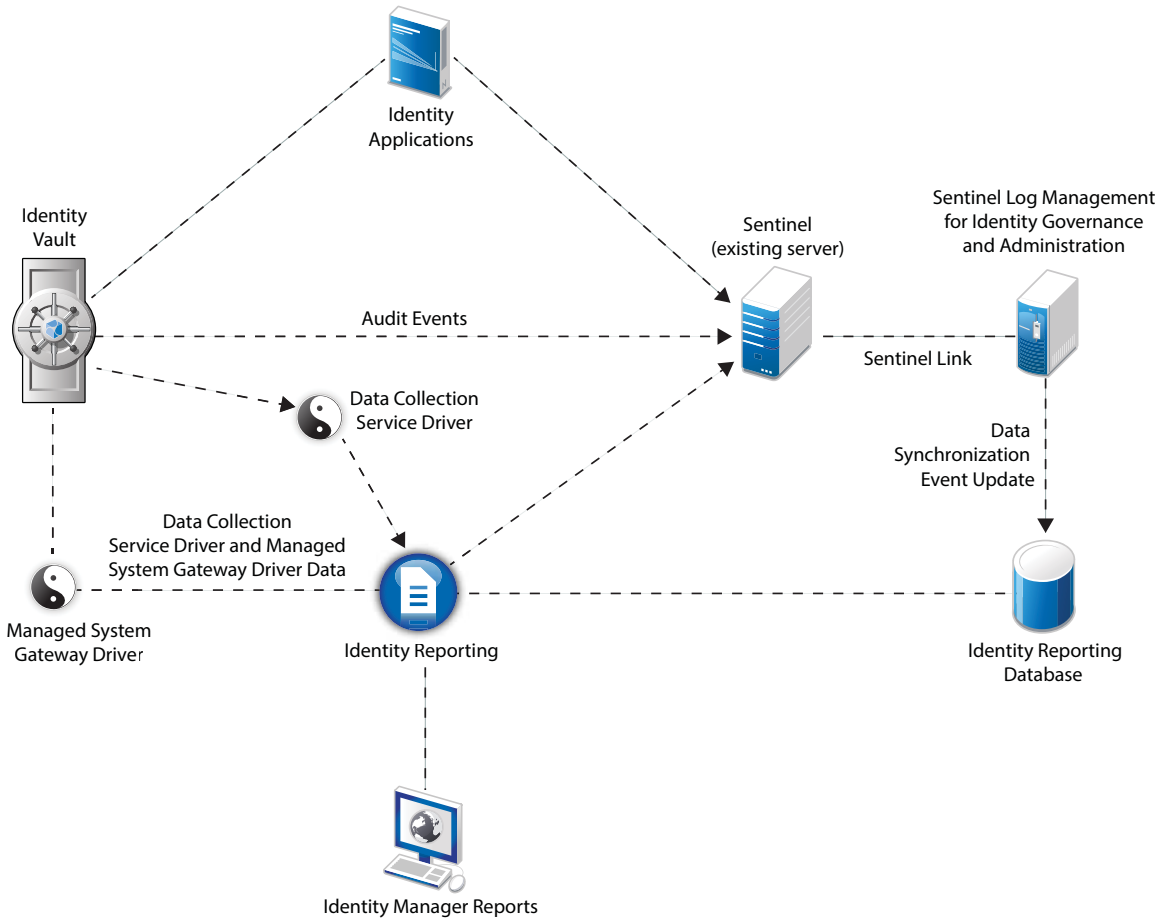
If you choose to use the existing Sentinel server, configure this server as a source of audit data instead of EAS as depicted in the following figure:



Follow these high-level steps to configure auditing in this environment:

1. Migrate the existing Reporting data to another standalone PostgreSQL instance. For more information, see "Migrating from Event Auditing Service to Sentinel Log Management for IGA" on page 489.
2. To generate reports in Identity Manager, perform a new installation of Identity Reporting. For more information, see Part XIII, "Installing Identity Reporting," on page 363.
3. Create a policy in the existing Sentinel server to synchronize the audit data from the Identity Manager components with the Identity Reporting database. You must use it as a source of audit data instead of EAS. For more information, see "Creating the Data Synchronization Policy" on page 494.

If you want to use SLM for IGA instead of an existing Sentinel server, install SLM for IGA that ships with Identity Manager and then configure it as the source of audit data as depicted in the following figure:



Follow these high-level steps to configure auditing in this environment:

1 Migrate the existing reporting data to another standalone PostgreSQL instance. For more information, see "Migrating from Event Auditing Service to Sentinel Log Management for IGA" on page 489.

2 To generate reports in Identity Manager, perform a new installation of Identity Reporting. For more information, see Part XIII, "Installing Identity Reporting," on page 363.

3 Forward Identity Manager events from SLM for IGA to the existing Sentinel server by configuring Sentinel Link between these servers. For more information on configuring Sentinel Link, see the *Sentinel Link Overview Guide*.

4 Create a policy in the SLM for IGA server to synchronize the audit data from Identity Manager components with the Identity Reporting database. For more information, see "Creating the Data Synchronization Policy" on page 494.

Understanding the Installation Process

The installation program for SLM for IGA performs the following functions:

- Installs and optionally configures the service
- Creates the user account that can perform administration tasks for the service (**admin**)
- Creates the database administrator account used by the service to interact with the database (**dbauser**)

Prerequisites for Installing SLM for IGA

Ensure that you have completed the following tasks before starting the installation:

- Verify that your hardware and software meet the system requirements listed in "System Requirements" on page 126.
- Ensure that the following RPMs are installed on the system before installing SLM for IGA:
  - `bash`
  - `bc`
  - `coreutils`
  - `gettext`
  - `glibc`
  - `grep`
  - `libgcc`
  - `libstdc`
  - `lsof`
  - `net-tools`
  - `openssl`
  - `python-libs`
  - `sed`
  - `zlib`
- If you are using Sentinel or an identity tracking solution and have not upgraded to SLM for IGA 8.0.0.1, you must apply the latest JDBC patch:
  1. Stop the SLM for IGA service.

     ```
     rcsentinel stop
     ```
  2. Back up the `postgresql-9.4-1201-jdbc4.jar` file present in the `$ESEC_HOME$/lib` directory.
  3. Navigate to the `/products/SentinelLogManagementforIGA/patches` and copy the `postgresql-9.4-1212-jdbc4.jar` to the `$ESEC_HOME$/lib` directory.
  4. Assign the required permissions to the `postgresql-9.4-1212-jdbc4.jar`:

     ```
     chown novell:novell postgresql-9.4-1212-jdbc4.jar
     chmod 600 postgresql-9.4-1212-jdbc4.jar
     ```
  5. Edit the `server.conf` to add an entry for `postgresql-9.4-1212-jdbc4.jar`:

     ```
     vi $ESEC_HOME$/config/server.conf
     wrapper.java.classpath.7=%ESEC_HOME%/lib/postgresql-9.4-1212-jdbc4.jar
     ```
  6. Start the SLM for IGA service.

     ```
     rcsentinel start
     ```

System Requirements

This section provides the minimum requirements for the server(s) where you want to install. For more information, see the NetIQ Sentinel Technical Information website.

Also, ensure that you review the prerequisites and considerations for installation, particularly those related to the operating system.

Category	Requirement
Processor	4 to 8 CPU cores
Disk space	200 GB
Memory	8 to 15 GB
Operating system (certified)	One of the following 64-bit operating systems: ◆ Red Hat Enterprise Linux 7.3 ◆ Red Hat Enterprise Linux 7.2 ◆ Red Hat Enterprise Linux 6.8 ◆ Red Hat Enterprise Linux 6.7 ◆ SUSE Linux Enterprise Server 12 SP1 ◆ SUSE Linux Enterprise Server 11 SP4 NetIQ recommends that you apply the latest operating system patches according to the manufacturer's automated update facility before you install Identity Manager. **NOTE:** *Certified* means that the operating system has been fully tested and is supported.
Operating system (supported)	Latest versions of service packs for the certified operating systems **NOTE:** *Supported* means that the operating system has not yet been tested but is expected to work

14 Installing SLM for IGA

You can install SLM for IGA in the following ways:

- Performing an Interactive Installation
- Performing a Silent Installation

Performing an Interactive Installation

You can install SLM for IGA in an interactive mode or silently. The interactive mode allows you to perform a standard or custom installation. In the standard installation, you install SLM for IGA with default values for ports, licenses, and passwords. To change the port assignments, licenses, and, passwords during installation, use custom installation.

After completing the installation, migrate your EAS data to SLM for IGA if you are upgrading to Identity Manager 4.6. For more information, see "Migrating from Event Auditing Service to Sentinel Log Management for IGA" on page 489.

You can install SLM for IGA using the interactive mode in two ways:

Standard Installation

1. Log in as administrative user to the computer where you want to install SLM for IGA.
2. From the directory that contains the installation files, execute the following command:

   ```
   ./install-logmanager
   ```

3. Specify the language that you want to use for installation, then press `Enter`.
4. Press the `Spacebar` to read through the license agreement.
5. Enter `yes` or `y` to accept the license agreement and continue with the installation.

   The installation might take a few seconds to load the installation packages.
6. When prompted, specify `1` to proceed with the standard configuration.

   Installation proceeds with the default evaluation license key included with the installer. At any time during or after the evaluation period, you can replace the evaluation license with a license key you have purchased.
7. Specify the password for the administrator user `admin`.
8. Confirm the password again.

   This password is used by `admin`, `dbauser`, and `appuser`.

   The installation finishes and the server starts. It might take a few minutes for all services to start after installation because the system performs a one-time initialization. Wait until the installation finishes before you log in to the server.

To access the SLM for IGA main interface, specify the following URL in your web browser:

```
https://<IP_Address/DNS_SLM for IGA_server>:8443/SLM for IGA/views/main.html
```

Where <*IP_Address/DNS_SLM for IGA_server*> is the IP address or DNS name of the SLM for IGA server and *8443* is the default port for the SLM for IGA server.

Custom Installation

1. Log in as administrative user to the computer where you want to install SLM for IGA.
2. From the directory that contains the installation files, execute the following command:

   ```
   ./install-logmanager
   ```

3. Specify the language that you want to use for installation, then press `Enter`.
4. Press the `Spacebar` to read through the license agreement.
5. Enter `yes` or `y` to accept the license agreement and continue with the installation.

   The installation might take a few seconds to load the installation packages.
6. Specify `2` to perform a custom configuration of SLM for IGA.
7. Enter `1` to use the default evaluation license key.

   or

   Enter `2` to enter a purchased license key for SLM for IGA.
8. Specify the password for the administrator user `admin` and confirm the password again.
9. Specify the password for the database user `dbauser` and confirm the password again.

   The `dbauser` account is the identity used by SLM for IGA to interact with the database. The password you enter here can be used to perform database maintenance tasks, including resetting the admin password if the admin password is forgotten or lost.
10. Specify the password for the application user `appuser` and confirm the password again.
11. Change the port assignments for Sentinel services by entering the required number.

    For example, the default port for Database Service is 8443. To modify the port number for Database Service, specify `4`. Enter the new port value for database service, for example, 8643.
12. After you have changed the ports, specify 7 for done.
13. Enter `1` to authenticate users using only the internal database.

    or

    If you have configured an LDAP directory in your domain, enter `2` to authenticate users by using LDAP directory authentication.

    The default value is `1`.
14. Enter `n` when you are prompted to enable FIPS 140-2 mode.
15. Enter `n` when you are prompted to enable scalable storage.

The SLM for IGA installation finishes and the server starts. It might take few minutes for all services to start after installation because the system performs a one-time initialization. Wait until the installation finishes before you log in to the server.

To access the SLM for IGA main interface, specify the following URL in your web browser:

```
https://<IP_Address/DNS_SLM for IGA_server>:<port>/SLM for IGA/views/main.html
```

Where <*IP_Address/DNS_SLM for IGA_server*> is the IP address or DNS name of the SLM for IGA server and <*port*> is the port for the SLM for IGA server.

NOTE: Once you have configured the Identity Reporting server, you need to create the data synchronization utility for forwarding events from SLM for IGA to the Reporting database.

For information on installing Identity Reporting, see Chapter 42, “Installing Identity Reporting,” on page 371.

For information on creating a data synchronization policy, see “Creating the Data Synchronization Policy” on page 494.

Performing a Silent Installation

To run a silent installation of SLM for IGA, create a properties files with the parameters required to complete the installation. The Identity Manager media includes a sample `silent.properties` file.

1. In the installation directory, create a properties file or edit the sample `silent.properties` file.
2. In a text editor, specify the required parameters in the file.
3. Specify the following command to perform installation in silent mode:

   ```
   ./install-logmanager -u <full path of the silent.properties file>
   ```

Customizing your Configuration

After installing SLM for IGA, if you want to enter the valid license key, change the password, or modify any of the assigned ports, you can run the `configure.sh` script to accomplish this. The script is available in the `/setup` folder.

1. Shut down SLM for IGA using the following command:

   ```
   rcsentinel stop
   ```

2. Run the `configure.sh` script by executing the following command at the command line:

   ```
   ./configure.sh
   ```

3. Specify `1` to perform a standard configuration or specify `2` to perform a custom configuration of SLM for IGA.
4. Press the `Spacebar` to read through the license agreement.
5. Enter `yes` or `y` to accept the license agreement and continue with the installation.

   The installation might take a few seconds to load the installation packages.
6. Enter `1` to use the default evaluation license key.

   or

   Enter `2` to enter a purchased license key for SLM for IGA.
7. Decide whether you want to keep the existing password for the `admin` administrator user.
   - If you want to keep the existing password, enter `1`.
   - If you want to change the existing password, enter `2`, specify the new password, then confirm the password.

   The `admin` user is the identity used to perform administration tasks through the SLM for IGA Main interface, including the creation of other user accounts.

8 Decide whether you want to keep the existing password for the `dbauser` database user.

- If you want to keep the existing password, enter `1`.
- If you want to change the existing password, enter `2`, specify the new password, then confirm the password.

The `dbauser` account is the identity that SLM for IGA uses to interact with the database. The password you enter here can be used to perform database maintenance tasks, including resetting the admin password if the admin password is forgotten or lost.

9 Decide whether you want to keep the existing password for the `appuser` database user.

- If you want to keep the existing password, enter `1`.
- If you want to change the existing password, enter `2`, specify the new password, then confirm the password.

The `appuser` account is an internal identity, which SLM for IGA Java process uses to establish connection and interact with the database. The password you enter here is used to perform database tasks.

10 Change the port assignments for the Sentinel services by entering the desired number, then specifying the new port number.

11 After you have changed the ports, specify `7` for done.

12 Enter `1` to authenticate users using only the internal database.

or

If you have configured an LDAP directory in your domain, enter `2` to authenticate users by using LDAP directory authentication.

The default value is `1`.

V Installing the Identity Manager Engine, Drivers, and Plug-ins

This section provides information about installing some of the basic framework for your Identity Manager server. This installation program allows you to install the following components:

- Identity Manager drivers
- Identity Manager engine
- iManager plug-ins for Identity Manager

NetIQ bundles the components in the same installation program for your convenience. You can choose to install them on the same server or install them individually. 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/netiq`
- **Windows**: `C:\netiq`

NetIQ recommends that you review the installation process before beginning. For more information, see "Checklist for Installing the Identity Manager Engine, Drivers, and Plug-ins" on page 133.

NOTE: This installation program also can install the Remote Loader. For more information, see Part VI, "Installing and Managing the Remote Loader," on page 153.

---

15 Planning to Install the Engine, Drivers, and Plug-ins

This section provides the prerequisites, considerations, and system setup needed to install the Identity Vault. First, consult the checklist to understand the installation process.

- "Checklist for Installing the Identity Manager Engine, Drivers, and Plug-ins" on page 133
- "Understanding the Installation Program" on page 134
- "Prerequisites and Considerations for Installing the Identity Manager Engine" on page 135
- "System Requirements for the Identity Manager Engine" on page 136

NOTE: This installation program also can install the Remote Loader. For more information, see Part VI, "Installing and Managing the Remote Loader," on page 153.

Checklist for Installing the Identity Manager Engine, Drivers, and Plug-ins

Before beginning the installation process, NetIQ recommends that you review the following steps.

	Checklist Items
❑	1. Learn about the interaction among Identity Manager components. For more information, see "Identity Manager Engine" on page 28.
❑	2. Decide which servers you want to use for your Identity Manager components. For more information, see "Recommended Installation Scenarios and Server Setup" on page 44.
❑	3. 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 9, "Installing the Identity Vault on a Linux Server," on page 87.
❑	4. Review the considerations for installing the Identity Manager engine to ensure that the computers meet the prerequisites. For more information, see "Prerequisites and Considerations for Installing the Identity Manager Engine" on page 135.
❑	5. Review the hardware and software requirements for the computers that will host the Identity Manager engine. For more information, see "System Requirements for iManager Server" on page 213 and "System Requirements for iManager Workstation (Client Version)" on page 214.
❑	6. Learn which drivers automatically become activated after installing the Identity Manager engine. For more information, see "Considerations for Installing Drivers with the Identity Manager Engine" on page 136.
❑	7. (Conditional) For computers running a SLES 12 SP1 or later operating system, ensure that you have installed the appropriate set of libraries for a guided installation. For more information, see "Installing Identity Manager on SLES 12 SP1 or Later Servers" on page 55.
❑	8. (Conditional) For computers running an RHEL 6.x or RHEL 7.x operating system, ensure that you have installed the appropriate set of libraries. For more information, see "Installing Identity Manager on RHEL 6.x or 7.x Servers" on page 55.

	Checklist Items
❑	9. Learn about the options in the installation program. For more information, see "Understanding the Installation Program" on page 134.
❑	10. Ensure that your UNIX/Linux environment meets the requirements for the Identity Manager engine. For more information, see "Verifying Environment Variables (UNIX / Linux) for the Identity Manager Installation" on page 139.
❑	11. (Conditional) For a guided installation process (wizard) of the Identity Manager engine, see one of the following sections: ◆ "Installing as a Root or Administrative User" on page 143 ◆ "Installing as a Non-root User" on page 144
❑	12. (Conditional) To install the components in a single command, see "Performing a Silent Installation" on page 146.
❑	13. (Conditional) To install the Remote Loader, see Part VI, "Installing and Managing the Remote Loader," on page 153.
❑	14. (Conditional) If you perform a non-root install, update the driverset to support graphics in email notifications. For more information, see "Adding Support for Graphics in Email Notifications" on page 152.
❑	15. Start the driver instance in the Remote Loader. For more information, see Chapter 20, "Configuring the Remote Loader and Drivers," on page 171.
❑	16. Install the rest of the Identity Manager components, including the identity applications and Identity Reporting.

Understanding the Installation Program

As a convenience, this installation program bundles several of the components that provide the underlying framework for your Identity Manager solution. You can choose to install all components on the same server, or on individual servers. For more information about server requirements, see the Planning to Install the Engine, Drivers, and Plug-ins for each component, the guide for the individual driver, and the latest Release Notes.

The installation program provides the following options for component installation:

Identity Manager Server

Installs the Identity Manager engine, schema, NetIQ Audit Agent, and XDAS (Distributed Audit services).

Connected System Server

Installs the Remote Loader service and the driver instances in the loader. The Remote Loader allows you to run Identity Manager drivers on connected systems that do not host the Identity Vault and Identity Manager engine.

In the installation program, you can select the drivers that you want to install with the Remote Loader on the connected system. On Linux servers, you can choose to install either a 32-bit or 64-bit version of the service, or both. On Windows servers, you can install the .NET Remote Loader.

iManager Plug-ins for Identity Manager

Installs the iManager plug-ins that allow you to use iManager to manage Identity Manager drivers that have structured Global Configuration Values (GCVs). Select this option if you previously installed iManager on the server.

Fanout Agent

Installs the Fan-Out agent for the JDBC Fan-Out driver. The JDBC Fan-Out driver uses the Fan-Out agent to create multiple JDBC Fan-Out driver instances. The Fan-Out agent loads the JDBC driver instances based on the configuration of the connection objects in the Fan-Out driver. For more information, see NetIQ Identity Manager Driver for *NetIQ Identity Manager Driver for JDBC Fanout Implementation Guide*.

Drivers

Identity Manager drivers synchronize identity information among several types of directories, databases, and business applications and the Identity Vault. You can configure the driver to synchronize the data in a single direction or in both directions.

In the installation program, you can select the drivers that you want to install with the other components. You might want to install some of the drivers on a server that does not host the Identity Manager engine. In this case, you would also need to install the Remote Loader service on that server.

Prerequisites and Considerations for Installing the Identity Manager Engine

This section provide information for installing the Identity Manager engine and drivers.

- "Considerations for Installing the Identity Manager Engine" on page 135
- "Considerations for Installing Drivers with the Identity Manager Engine" on page 136

Considerations for Installing the Identity Manager Engine

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

- (Conditional) For a guided installation of the Identity Manager engine on a server running SLES 12 SP1 or later platforms, ensure that the server has `libXtst6-32bit-1.2.1-4.4.1.x86_64`, `libXrender1-32bit`, and `libXi6-32bit` libraries installed.
- 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.
- Install the Identity Manager engine on the same server that hosts the Identity Vault.
- (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 "Prerequisites and Considerations for Installing the Remote Loader" on page 158.
- (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.

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, the number of drivers running on the server depends on the load that the drivers place on the server. Some drivers process a large quantity of objects while other drivers do not.
- If you plan to synchronize millions of objects with each driver, limit the number of drivers on the server. For example, deploy fewer than 10 drivers of these drivers.
- 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 Driver Administration Guide*.

For more information about activating Identity Manager drivers after installation, see "Activating Identity Manager" on page 453.

System Requirements for the Identity Manager Engine

This section provides the minimum requirements for the server(s) where you want to install the Identity Manager engine. Ensure that you review the prerequisites and considerations for installation, particularly those related to the operating system.

Category	Requirement
Processor	1 GHz
Disk space	◆ 300 MB ◆ 150 MB of additional disk space for every 50,000 users
Memory	◆ 2 GB for the Identity Manager engine ◆ 2 GB for Identity Manager Drivers

Category	Requirement
Operating system (certified)	One of the following 64-bit operating systems: ◆ Open Enterprise Server 2015 SP1 ◆ Open Enterprise Server 11 SP3 ◆ Red Hat Enterprise Linux 7.3 ◆ Red Hat Enterprise Linux 6.8 ◆ SUSE Linux Enterprise Server 12 SP1 ◆ SUSE Linux Enterprise Server 11 SP4 ◆ Windows Server 2012 R2 ◆ Windows Server 2012 NetIQ recommends that you apply the latest operating system patches according to the manufacturer's automated update facility before you install Identity Manager. **NOTE:** *Certified* means that the operating system has been fully tested and is supported.
Operating systems (supported)	Latest versions of service packs for the certified operating systems **NOTE:** *Supported* means that the operating system has not yet been tested but is expected to work
Virtualization system	◆ Hyper-V Server 2012 R2 ◆ VMWare ESX 5.0 and later ◆ Windows Server 2012 R2 Virtualization with Hyper-V (supported) NetIQ supports Identity Manager on enterprise-class virtualization systems that provide official support for the operating systems where NetIQ products are running. As long as the vendors of the virtualization systems officially support these operating systems, NetIQ supports the entire Identity Manager stack on them.
Additional software	◆ NetIQ eDirectory 8.8.8 Patch 9 Hotfix 2 ◆ NetIQ eDirectory 9.0.2 Hotfix 2 ◆ iManager 2.7.7 Patch 9 (for eDirectory 8.8.8 Patch 9 or later) ◆ iManager 3.0.2 Patch 1 (for eDirectory 9.0.2 or later)

16 Preparing to Install the Engine, Drivers, and Plug-ins

The Identity Manager engine processes the data changes that occur in the Identity Vault and connected applications. The engine has also been called the Metadirectory engine. Drivers connect the Identity Manager engine to the connected applications. The Remote Loader loads drivers and communicates with the Identity Manager engine on behalf of drivers installed on remote servers.

- "Verifying Environment Variables (UNIX / Linux) for the Identity Manager Installation" on page 139
- "Stopping and Starting Identity Manager Drivers" on page 139

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:

```
. /etc/opt/novell/eDirectory/conf/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" in the *NetIQ eDirectory Installation Guide*.

Stopping and Starting Identity Manager Drivers

You might need to start or stop the Identity Manager drivers to ensure that an installation or upgrade process can modify or replace the correct files. This section explains the following activities:

- "Stopping the Drivers" on page 139
- "Starting the Drivers" on page 140

Stopping the Drivers

Before you modify any files for a driver, it is important to stop the drivers.

- "Using Designer to Stop the Drivers" on page 140
- "Using iManager to Stop the Drivers" on page 140

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.

Starting the Drivers

After all of the Identity Manager components are updated, restart the drivers. NetIQ recommends that you test the drivers after they are running to verify that all of the policies still work.

- "Using Designer to Start the Drivers" on page 140
- "Using iManager to Start the Drivers" on page 141

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 *NetIQ Identity Manager - Using Designer to Create Policies*.

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.

17 Installing the Engine, Drivers, and iManager Plug-ins

This section describes the installation process for the Identity Manager engine, drivers, iManager plug-ins, and the Remote Loader. You can install these programs on the same server or separate servers. For example, you might want to a driver on a connected system, rather than on the same server as the Identity Manager engine. In this case, you also would install the Remote Loader on that connected system.

NetIQ provides both a guided installation process and a silent installation.

- "Using the Wizard to Install the Components" on page 143
- "Performing a Silent Installation" on page 146
- "Installing on a Server with Multiple Instances of Identity Vault" on page 147
- "Completing a Non-root Installation" on page 149

Using the Wizard to Install the Components

The installation program guides you through the configuration settings for the Identity Manager engine. You can run the installation in the console or in the GUI. On UNIX and Windows computers, the installation program automatically defaults to wizard mode.

To prepare for the installation, see "Checklist for Installing the Identity Manager Engine, Drivers, and Plug-ins" on page 133. Also see the Release Notes accompanying the release. To perform an unattended installation, see "Performing a Silent Installation" on page 146.

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.

Installing as a Root or Administrative User

This section describes the guided process for using the installation wizard or console to install the Identity Manager engine as a `root` user or as an administrator on a Windows computer. Use the following installation program for your platform:

- **Linux:** `/products/IDM/install.bin`
- **Windows:** `\products\IDM\windows\setup\idm_install.exe`

NOTE: On a Linux platform, when you install the Identity Manager engine as a `root` user, the installation files are located under the `/tmp` directory. If the `/tmp` directory does not exist, the install program will create it. The installation files are not required to run Identity Manager. You can delete the files after installation.

To install the Identity Manager engine as a `root` or administrative user:

1. Log in as `root` or administrator on the computer where you want to install the Identity Manager engine.
2. From the directory that contains the installation files, complete one of the following actions:
   - **Linux (console)**: Enter `./install.bin -i console`
   - **Linux (GUI)**: Enter `./install.bin`
   - **Windows**: Run `idm_install.exe`
3. Accept the license agreement, and then click **Next**.
4. In the Select Components window, specify the components that you want to install.

   For more information about the options, see "Understanding the Installation Program" on page 134.
5. (Optional) To select specific drivers for the individual components, complete the following steps:
   - **5a** Click **Customize the selected components**, and then click **Next**.
   - **5b** Expand **Drivers** under the component that you want to install.
   - **5c** Select the drivers that you want to install.
6. Click **Next**.
7. In the Activation Notice window, click **OK**. For more information, see "Activating Identity Manager" on page 453.
8. For Authentication, 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=admin,o=company`.
9. For Pre-Installation Summary, verify the settings.
10. Click **Install**.
11. Activate Identity Manager. For more information, see "Activating Identity Manager" on page 453.
12. To create and configure your driver objects, consult the specific guide for that driver. For more information, see Identity Manager Drivers documentation website.
13. (Optional) For the default installation locations, see `/tmp/idmInstall.log`.

Installing 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 "Installing Java Remote Loader on Linux" on page 167.
- **NetIQ Sentinel Platform Agent:** Install the Novell Audit Platform Agent package from NetIQ Sentinel Plug-ins download page after installing the engine as a non-root user.
- **UNIX/Linux Account Driver:** Requires `root` privileges to function.

NOTE: On a Linux platform, when you install the Identity Manager engine as a non-root user, the installation files are located under the non-root users directory (Example: `/home/user`; where user is non-root). The installation files are not required to run Identity Manager. You can delete the files after installation.

To install the Identity Manager engine as a non-root user:

1 Log in as the non-`root` user that you used to install the Identity Vault.
   - Create a sudo user and a directory.
   - The user account must have administrator rights to the directories and files of the non-`root` Identity Vault (eDirectory) installation. To provide administrator rights, run the following command:

     ```
     chown <non-root user name>/home/<non-root directory> –R
     ```

     For example, `chown test/home/mkdir/home/test –R`
   - Provide sudo password for the newly created user.

2 Install NICI as root user. For more information, see "Installing NICI as a Non-root User" on page 82.

3 Log in as non-root user using the `>systemctl start user@< non-root user >.service` command. Copy the Identity Vault file to the non-root home directory, using the `do gunzip` command.

4 Perform the steps (step 2 to step 6) mentioned in "Installing the Identity Vault as a Non-root User" on page 89.

5 Execute the installation program:

   `IDM`*`version`*`_Lin/products/IDM/linux/setup/idm-nonroot-install`

6 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 `/etc/opt/novell/eDirectory/conf/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 for a Windows server, copy the utilities from the Identity Manager installation media to the Identity Manager server. All utilities are found in the `IDM`*`version_platform`*`/product/IDM/`*`platform`*`/setup/utilities` directory.

7 To support auditing, install the latest software update for Novell Audit Platform Agent from NetIQ Sentinel Plug-ins download (https://www.netiq.com/support/sentinel/plugins/) page.

8 To complete the installation process, continue to "Completing a Non-root Installation" on page 149.

9 Activate Identity Manager. For more information, see "Activating Identity Manager" on page 453.

10 To create and configure your driver objects, consult the specific guide for that driver. For more information, see Identity Manager Drivers documentation website.

Performing a Silent Installation

To run a silent installation of Identity Manager, create a properties files with the parameters required to complete the installation. The Identity Manager media includes a sample properties file:

- **Linux:** `/products/IDM/linux/setup/silent.properties`
- **Windows:** `\products\IDM\windows\setup\silent.properties`

To perform a silent installation:

1 In the installation directory, create a properties file or edit the sample `silent.properties` file.

2 In a text editor, specify the following parameters in the file:

EDITION_INPUT_RESULTS

Specifies the edition of the Identity Manager server. For example, `Advanced Edition` or `Standard Edition`. The installation program uses this information to configure the specified Identity Manager edition.

EDIR_USER_NAME

Specifies the LDAP distinguished name of the Administrator account for the Identity Vault. For example, `c=admin,o=netiq`. The installation program uses this account to connect the Identity Manager engine to the Identity Vault.

You might need to add this parameter to the sample `silent.properties` file.

EDIR_USER_PASSWORD

Specifies the password for the Administrator account for the Identity Vault. For example, `netiq123`. You might need to add this parameter to the sample `silent.properties` file.

If you do not want to include the password value in the file, leave the field empty. The installation program then reads the value from the `EDIR_USER_PASSWORD` environment variable. Ensure that you have an environment variable for `EDIR_USER_PASSWORD`.

METADIRECTORY_SERVER_SELECTED

Specifies whether you want to install the Identity Manager server and drivers.

CONNECTED_SYSTEM_SELECTED

Specifies whether you want to install the 32-bit Remote Loader service and drivers. You can install both 32-bit and 64-bit versions on the same server.

FANOUTAGENT_SELECTED

Specifies whether you want to install the Fan-Out agent for the JDBC driver.

X64_CONNECTED_SYSTEM_SELECTED

Specifies whether you want to install the 64-bit Remote Loader service and drivers. You can install both 32-bit and 64-bit versions on the same server.

WEB_ADMIN_SELECTED

Applies when you have previously installed iManager.

Specifies whether you want to install iManager plug-ins.

UTLITIES_SELECTED

Specifies whether you want to install the Utilities and system components for the Remote Loader.

DOT_NET_REMOTELOADER_SELECTED

Specifies whether you want to install the .NET Remote Loader service and drivers on the Windows server.

EDIR_NDS_CONF

Specifies the path to the `nds.conf` file, which is the configuration file for the Identity Vault. For example, `/etc/opt/novell/eDirectory/nds.conf`.

If you have multiple instances of the Identity Vault, specify the appropriate value for each instance.

EDIR_IP_ADDRESS

Specifies the IP address for the Identity Vault.

If you have multiple instances of the Identity Vault, specify the address for each instance.

EDIR_NCP_PORT

Specifies the port number of the Identity Vault.

If you have multiple instances of the Identity Vault, specify the port for each instance.

3 To run the silent installation, issue one of the following commands from the directory for the properties file:

- **Linux**: `install.bin -i silent -f filename.properties`
- **Windows**: `install.exe -i silent -f filename.properties`

4 (Optional) For default installed locations, see `/tmp/idmInstall.log`.

5 (Conditional) If you ran the installation as a non-`root` user, continue to "Completing a Non-root Installation" on page 149.

Installing on a Server with Multiple Instances of Identity Vault

Identity Manager supports this installation as a root user and in a silent mode. This procedure requires you to create a `silent.properties` file for each Identity Vault instance where you want to install Identity Manager.

Perform the following steps to install Identity Manager in the silent mode:

1 Review the prerequisites and system requirements in Chapter 15, "Planning to Install the Engine, Drivers, and Plug-ins," on page 133.

2 Follow the instructions from "Performing a Silent Installation" on page 146.

2a Ensure that the silent.properties file includes the following settings:

```
EDITION_INPUT_RESULTS=Advanced Edition
EDIR_USER_NAME=cn=admin_name,o=organization_name
EDIR_USER_PASSWORD=identity_vault_password
METADIRECTORY_SERVER_SELECTED=true
CONNECTED_SYSTEM_SELECTED=false
X64_CONNECTED_SYSTEM_SELECTED=false
WEB_ADMIN_SELECTED=false
UTILITIES_SELECTED=false
FANOUTAGENT_SELECTED=false
EDIR_NCP_PORT=<ncp_port>
EDIR_NDS_CONF=</path/to/edir/conf>
EDIR_IP_ADDRESS=ip_address_for_identity_vault

# For Customization use the following properties
CUSTOM_SELECTED=true
# engine custom list engine and drivers jdbc and delim
CHOSEN_INSTALL_FEATURE_LIST_SERVER=ENGINE,JDBC,DELIM,additional_value
```

2b You can include the following additional values to customize the engine list:

- Server_DRIVERS
- AD
- EBSHR
- EBSTCA
- EBSUM
- DELIM
- EDIR
- BIEDIR
- JDBC
- JMS
- LDAP
- NXSET
- NOTES
- PS
- REMEDY
- SAPUMJ
- SAPHR
- SAPBL
- SAPPORTAL
- SOAP
- REST
- SFORCE
- SENTREST
- BLACK
- BANNER
- GOOGLE
- AR

- NPUM
- TSS
- RACF
- AFC2
- UAD
- RRSD

3 (Conditional) To verify whether the installation was successful, look for the following lines in the `/tmp/idmInstall.log` file.

```
NDS schema extension complete.
exitValue=0
Schema extended
SCHEMA_EXTENDED=true
==== UpdateIDMConfigureStatus ==============================
stateFile: /root/idm/Uninstall_Identity_Manager/idmconfigure_state.conf
INSTALL_SUCCESS: SUCCESS
enter loop:
==== Complete ==============================================
INSTALL_SUCCESS=SUCCESS
```

Completing a Non-root Installation

When you install the Identity Manager engine and plug-ins as a non-`root` user, the process performs all intended installation activities. This section guides you through the manual process required to complete the installation.

- "Assigning the Password Policy Object to Driver Sets" on page 149
- "Creating the Default Notification Collection Object in the Identity Vault" on page 151
- "Adding Support for Graphics in Email Notifications" on page 152

Assigning the Password Policy Object to Driver Sets

You must assign the DirMXL-PasswordPolicy object to each driver set in the Identity Vault. The Identity Manager Default Universal Password Policy package includes this policy object. The default policy installs and assigns a universal password policy to control how the Identity Manager engine automatically generates random passwords for drivers.

Alternatively, to use a custom password policy, you must create the password policy object and the policy. For more information, see "Creating a Custom Password Policy" on page 151.

- "Creating a Container for Password Policies" on page 150
- "Creating the Password Policy Object in the Identity Vault" on page 150
- "Assigning the Password Policy Object" on page 151
- "Creating a Custom Password Policy" on page 151

Creating a Container for Password Policies

Identity Manager requires password policy objects in the Identity Vault. However, the non-`root` installation process does not create a container for password policies.

1. Log in to the Identity Manager tree in iManager.
2. Navigate to the security container in eDirectory.
3. Create a container for password policies.

   For more information about creating a container in eDirectory, see the *eDirectory Administration Guide*.

Creating the Password Policy Object in the Identity Vault

After creating the container for password policies, you must create the `DirMXL-PasswordPolicy` object in the Identity Vault using Designer or the ldapmodify utility. For more information about how to do this in Designer, see "Configuring Driver Sets" in *NetIQ Designer for Identity Manager Administration Guide*. To use the ldapmodify utility, use the following procedure:

1. In a text editor, create an LDAP Data Interchange Format (LDIF) file with the following attributes:

```
dn: cn=DirXML-PasswordPolicy,cn=Password Policies,cn=Security
changetype: add
nsimPwdRuleEnforcement: FALSE
nspmSpecialAsLastCharacter: TRUE
nspmSpecialAsFirstCharacter: TRUE
nspmSpecialCharactersAllowed: TRUE
nspmNumericAsLastCharacter: TRUE
nspmNumericAsFirstCharacter: TRUE
nspmNumericCharactersAllowed: TRUE
nspmMaximumLength: 64
nspmConfigurationOptions: 596
passwordUniqueRequired: FALSE
passwordMinimumLength: 1
passwordAllowChange: TRUE
objectClass: nspmPasswordPolicy

dn: cn=DirXML-PasswordPolicy,cn=Password Policies,cn=Security
changetype: modify
add: nsimAssignments
nsimAssignments: <driverset LDAP dn>
```

   NOTE: Copying the content as is might insert some hidden special characters in the file. If you receive a `ldif_record() = 17` error message when you add these attributes to the Identity Vault, insert an extra space between the two DNs.

2. To add the DirMXL-PasswordPolicy object in the Identity Vault, import the attributes from the file by performing one of the following actions:

   Linux:

   From the directory containing the ldapmodify utility, enter the following command:

```
ldapmodify -x -c -h hostname_or_IP_address -p 389 -D
"cn=admin,ou=sa,o=system" -w password -f path_to_ldif_file
```

For example:

```
ldapmodify -x -ZZ -c -h server1.test.com -p 389 -D
"cn=admin,ou=sa,o=system" -w test123 -f /root/dirxmlpasswordpolicy.ldif
```

The ldapmodify utility is located by default in the `/etc/opt/novell/eDirectory/conf` directory.

Windows:

Run `ldapmodify.exe` from the `install/utilities` directory of the Identity Manager installation kit.

Assigning the Password Policy Object

You must assign the `DirMXL-PasswordPolicy` object to each driver set in a tree.

1. Open your project in Designer.
2. In the Outline pane, expand your project.
3. Expand **Package Catalog > Common > Common Settings** to verify whether the Default Universal Password Policy package exists.
4. (Conditional) If the password policy package is not already listed in Designer, complete the following steps:
   - **4a** Right-click **Package Catalog**.
   - **4b** Select **Import Package**.
   - **4c** Select **Identity Manager Default Universal Password Policy**, and then click **OK**.

     To ensure that the table displays all available packages, you might need to deselect **Show Base Packages Only**.
5. Select each driver set and assign the password policy.

Creating a Custom Password Policy

Rather than using the default password policy in Identity Manager, you can create a new policy based on your organizational requirements. You can assign a password policy to the entire tree structure, a partition root container, a container, or a specific user. To simplify management, NetIQ recommends that you assign password policies as high in the tree as possible. For more information, see Creating Password Policies in the *Password Management 3.3.2 Administration Guide*.

NOTE: You must also assign the DirXML-PasswordPolicy object to the driver sets. For more information, see "Assigning the Password Policy Object" on page 151.

Creating the Default Notification Collection Object in the Identity Vault

The Default Notification Collection is an Identity Vault object that contains a set of e-mail notification templates and an SMTP server that is used when sending e-mails generated from the templates. The non-`root` installation process does not create the Default Notification Collection object in the Identity Vault. You must use Designer to create the object.

- "Creating a Container for Notification Templates" on page 152
- "Creating the Default Notification Collection Object" on page 152

Creating a Container for Notification Templates

Identity Manager requires default notification templates in the Identity Vault. However, the non-`root` installation process does not create a container for notification templates.

1. Log in to the Identity Manager tree in iManager.
2. Navigate to the security container in eDirectory.
3. Create a container for notification templates.

   For more information about creating a container in eDirectory, see the *eDirectory Administration Guide*.

Creating the Default Notification Collection Object

1. Open your project in Designer.
2. In the Outline pane, expand your project.
3. Right-click the Identity Vault, then click Identity Vault **Properties**.
4. Click **Packages**, then click the **Add Packages** icon.
5. Select all the notification templates packages, and then click **OK**.
6. Click **Apply** to install the packages with the **Install** operation.
7. Deploy the notification templates to the Identity Vault.

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.

VI Installing and Managing the Remote Loader

In this section, you will install the Remote Loader, .NET Remote Loader, or the Java Remote Loader and configure driver instances in the loader.

The installation program for the Remote Loader is bundled with the Identity Manager engine. The 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/netiq`
- **Windows**: `C:\netiq`

NetIQ recommends that you review the installation process before beginning. For more information, see "Checklist for Installing the Remote Loader" on page 155.

18 Planning to Install the Remote Loader

This section provides information that helps you prepare for installing the Remote Loader and the Java Remote Loader.

- "Checklist for Installing the Remote Loader" on page 155
- "Understanding the Remote Loader" on page 156
- "Understanding the Installation Program" on page 158
- "Using 32-bit and 64-bit Remote Loader on the Same Computer" on page 158
- "Prerequisites and Considerations for Installing the Remote Loader" on page 158
- "System Requirements for the Remote Loader" on page 161

Checklist for Installing the Remote Loader

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

	Checklist Items
❑	1. Learn about the interaction among Identity Manager components. For more information, see "Remote Loader" on page 28.
❑	2. Decide which servers you want to use for your Identity Manager components. For more information, see "Recommended Installation Scenarios and Server Setup" on page 44.
❑	3. Ensure that the Identity Manager engine has been installed. For more information, see Part V, "Installing the Identity Manager Engine, Drivers, and Plug-ins," on page 131.
❑	4. Review the considerations for installing the Remote Loader to ensure that the computers meet the prerequisites. For more information, see "Prerequisites and Considerations for Installing the Remote Loader" on page 158.
❑	5. Review the hardware and software requirements for the computers that will host the Remote Loader. For more information, see "System Requirements for the Remote Loader" on page 161.
❑	6. (Conditional) For computers running a SLES 12 SP1 or later operating system, ensure that you have installed the appropriate set of libraries for a guided installation. For more information, see "Installing Identity Manager on SLES 12 SP1 or Later Servers" on page 55.
❑	7. (Conditional) For computers running an RHEL 6.x or RHEL 7.x operating system, ensure that you have installed the appropriate set of libraries. For more information, see "Installing Identity Manager on RHEL 6.x or 7.x Servers" on page 55.
❑	8. (Conditional) To install the Remote Loader on a server that does not host the Identity Manager engine, ensure that you can establish a secure connection to the engine. For more information, see "Creating a Secure Connection to the Identity Manager Engine" on page 171.
❑	9. Decide whether you want to install a 32-bit or 64-bit version of the Remote Loader. For more information, see "Using 32-bit and 64-bit Remote Loader on the Same Computer" on page 158.

	Checklist Items
❑	10. Decide whether you should use the Remote Loader or Java Remote Loader. For more information, see "Understanding the Java Remote Loader" on page 158.
❑	11. Install the Remote Loader: ◆ For a guided installation, see "Using the Wizard to Install the Remote Loader" on page 165. ◆ For a silent installation, see "Performing a Silent Installation of the Remote Loader" on page 166.
❑	12. (Conditional) To install the Java Remote Loader, see "Installing Java Remote Loader on Linux" on page 167.
❑	13. (Conditional) To install the .NET Remote Loader, see "Installing .NET Remote Loader on Windows" on page 169.
❑	14. Review the parameters for configuring a driver instance. For more information, see "Understanding the Configuration Parameters for the Remote Loader" on page 174.
❑	15. To configure a driver instance in the Remote Loader, see one of the following sections: ◆ "Configuring the Remote Loader for Driver Instances on UNIX or Linux" on page 183 ◆ "Configuring the Remote Loader for Driver Instances on Windows" on page 185 ◆ "Configuring the Java Remote Loader for Driver Instances" on page 187 ◆ "Configuring the .NET Remote Loader for Driver Instances on Windows" on page 189
❑	16. Prepare your drivers for the Remote Loader. For more information, see "Configuring Identity Manager Drivers to Work with the Remote Loader" on page 191.
❑	17. Start the driver instance in the Remote Loader. For more information, see "Starting a Driver Instance in the Remote Loader" on page 201.
❑	18. (Conditional) To configure mutual authentication between the Remote Loader and the Identity Manager engine, see "Configuring Mutual Authentication with the Identity Manager Engine" on page 192.
❑	19. Verify that the Remote Loader and driver are communicating with the Identity Manager engine and the connected system. For more information, see "Verifying the Configuration" on page 199.
❑	20. Install the rest of the Identity Manager components, including the identity applications and Identity Reporting.

Understanding the Remote Loader

The Remote Loader allows you to run Identity Manager drivers on connected systems that do not host the Identity Vault and Identity Manager engine. The .Net Remote Loader works on Windows-based systems only.

The Remote Loader is capable of hosting Identity Manager application shims contained in platform-specific files through JNI, as well as the more-common Identity Manager application shims contained in platform-agnostic JAR files. The Remote Loader can run on any platform. However, platform-specific shims must be run on their native platform (for example, `.so` files on Linux/Unix).

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.

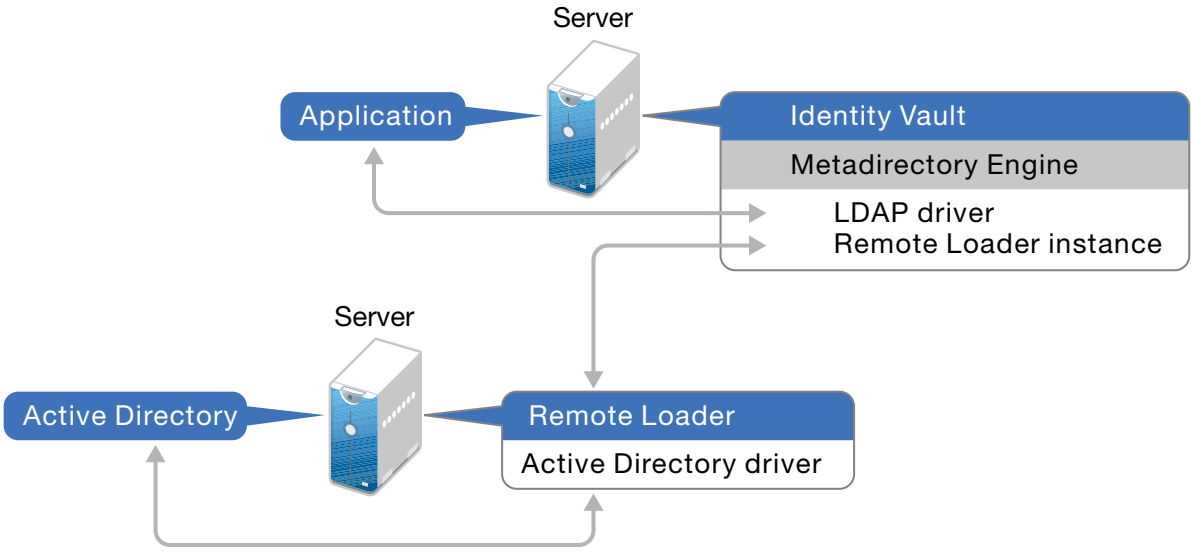
For more information, see Chapter 20, “Configuring the Remote Loader and Drivers,” on page 171.

Determining When to Use the Remote Loader

You can install the Identity Manager engine, Identity Vault, and the driver shim on the same server. The Identity Manager engine runs as part of an eDirectory process. The Identity Manager drivers can run on the server with the Identity Manager. They also can run as part of the same process as the Identity Manager engine. However, in the following scenarios, you might want the Identity Manager driver to run as a separate process on the server that hosts the Identity Manager engine:

- To protect the Identity Vault from any exceptions encountered by the driver shim.
- To improve the performance of the server running the Identity Manager engine, by offloading driver commands to the remote application or database.
- To run additional drivers on servers that do not host the Identity Manager engine.

In these scenarios, the Remote Loader provides a communication channel between the Identity Manager engine and the driver. For example, you install an LDAP driver on the same server as the Identity Manager engine and the Identity Vault. Then you install the Active Directory (AD) driver on a different server with the Remote Loader. To allow the drivers to access the application and communicate with the Identity Vault, install the Remote Loader on both servers, as shown in the following figure:



NetIQ recommends that you use the Remote Loader configuration for use with your drivers where possible. Use the Remote Loader even in cases where the application is on the same server as the Identity Manager engine.

Understanding the Java Remote Loader

The Java Remote Loader provides the flexibility to load a driver shim on computers with UNIX or Linux servers that the native Remote Loader does not support. The Java Remote Loader is a Java application. You can use the Java Remote Loader with any publicly supported version of Java.

To open the application, run the shell script named `dirxml_jremote`. For more information, see "Configuring the Java Remote Loader for Driver Instances" on page 187.

Understanding the Installation Program

As a convenience, this installation program bundles several of the components that provide the underlying framework for your Identity Manager solution. You can choose to install all components on the same server or on individual servers. In addition to the Remote Loader, you can select the drivers that you want to install on the connected system. The installation kit provides the following installation options, depending on the operating system of the target server:

Linux or UNIX servers

- Remote Loader 32-bit version, 64-bit version, or both
- Java Remote Loader

Wiindows servers

.NET Remote Loader on the supported operating systems

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.

Prerequisites and Considerations for Installing the Remote Loader

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

- (Conditional) For a guided installation of the Remote Loader on a server running SUSE Linux Enterprise Server (SLES) 12 SP1 or later platforms, ensure that the server has `libXtst6-32bit-1.2.1-4.4.1.x86_64`, `libXrender1-32bit`, and `libXi6-32bit` libraries installed.
- 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.
- You can install both 32-bit and 64-bit Remote Loader on the same computer.
- Ensure that your Linux operating system has the following kernel versions:
  - 4.4.59-92.42.2 or later on SLES 12 SP2
  - 3.12.74-60.64.48.1 or later on SLES 12 SP1
  - 3.12.61-52.80.1 or later on SLES 12
  - 3.0.101-107.1 or later on SLES 11 SP4
  - 3.0.101-0.47.105.1 or later on SLES 11 SP3
  - 2.6.32-696.6.3 or later on Red Hat 6.9
- You can install Java Remote Loader on platforms that do not support the native Remote Loader. For more information about supported platforms, see "System Requirements for the Remote Loader" on page 161.
- (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 shim in the Remote Loader configuration, the following advantages apply:
  - Memory and processing isolation between driver shims allows for better performance and monitoring of the Identity Manager solution.
  - Patching and upgrading the driver shim does not impact eDirectory or other drivers.
  - Protects eDirectory from fatal issues that could occur in the driver shim.
  - Distributes the load from the driver shims to other servers.
- The following drivers support the Remote Loader capability:
  - Active Directory
  - Access Review
  - ACF2
  - Banner
  - Blackboard
  - Data Collection Service
  - Delimited Text
  - GoogleApps
  - REST
  - GroupWise 2014 (for 32-bit Remote Loader)
  - JDBC
  - JMS
  - LDAP

    - Linux/UNIX Settings
    - Lotus Notes
    - Managed System Gateway
    - Manual Task Services
    - Null and Loopback
    - Office 365
    - Oracle EBS HRMS
    - Oracle EBS TCA
    - Oracle EBS User Management
    - PeopleSoft 5.2
    - Privileged User Management
    - Remedy
    - SalesForce.com
    - SAP Business Logic
    - SAP Portal
    - SAP HR (not supported with Java Remote Loader)
    - SAP User Management (not supported with Java Remote Loader)
    - ServiceNow
    - Integration Module V2.0 for Sentinel
    - SharePoint
    - SOAP
    - Top Secret
    - WorkOrder
  - The following drivers do not support Remote Loader:
    - Bidirectional eDirectory
    - eDirectory
    - Entitlements Services
    - Role Service
    - User Application

For more information about the Identity Manager Remote Loader, see “The Many Faces of Remote Loader in Identity Manager”.

System Requirements for the Remote Loader

This section provides the minimum requirements for the server(s) where you want to install the Remote Loader, .NET Remote Loader, and Java Remote Loader.

Ensure that you review the prerequisites and considerations for installation, particularly those related to the operating system..

Remote Loader 32-bit and 64-bit

Category	Requirement
Processor	Pentium* III 600MHz processor
Memory	512 MB
Operating system (certified)	One of the following 64-bit operating systems: ◆ Open Enterprise Server 2015 SP1 ◆ Open Enterprise Server 11 SP3 ◆ Red Hat Enterprise Linux 7.3 ◆ Red Hat Enterprise Linux 6.8 ◆ SUSE Linux Enterprise Server 12 SP1 ◆ SUSE Linux Enterprise Server 11 SP4 ◆ Windows Server 2016 ◆ Windows Server 2012 R2 ◆ Windows Server 2012 ◆ Windows Server 2008 R2 For a 32-bit operating system: ◆ Windows Server 2008 SP2 **IMPORTANT:** The Lotus Notes Client is only supported on the workstation platforms. A Remote Loader running on Windows XP, Windows 7 and 8, SLED 32-bit, RHEL 6 Client 32-bit is only supported for the Lotus Notes driver integration. In normal Identity Manager installations, the Remote Loader is supported only on the server platforms. NetIQ recommends that you apply the latest operating system patches according to the manufacturer's automated update facility before you install Identity Manager. **NOTE:** *Certified* means that the operating system has been fully tested and is supported.
Operating system (supported)	Latest versions of service packs for the certified operating systems **NOTE:** *Supported* means that the operating system has not yet been tested but is expected to work

Category	Requirement
Virtualization system	◆ Hyper-V Server 2012 R2 ◆ VMWare ESX 5.0 and later ◆ Windows Server 2012 R2 Virtualization with Hyper-V (supported) NetIQ supports Identity Manager on enterprise-class virtualization systems that provide official support for the operating systems where NetIQ products are running. As long as the vendors of the virtualization systems officially support these operating systems, NetIQ supports the entire Identity Manager stack on them.

.NET Remote Loader

The .NET Remote Loader is designed for use with Windows-based servers.

Category	Requirement
Processor	Pentium* III 600MHz processor
Memory	512 MB
Operating system (certified)	One of the following 64-bit operating systems: ◆ Windows Server 2016 ◆ Windows Server 2012 R2 ◆ Windows Server 2012 ◆ Windows Server 2008 R2 For a 32-bit operating system: ◆ Windows Server 2008 SP2 NetIQ recommends that you apply the latest operating system patches according to the manufacturer's automated update facility before you install Identity Manager. **NOTE:** *Certified* means that the operating system has been fully tested and is supported.
Operating system (supported)	Latest versions of service packs for the certified operating systems **NOTE:** *Supported* means that the operating system has not yet been tested but is expected to work
Virtualization system	◆ Hyper-V Server 2012 R2 ◆ VMWare ESX 5.5 ◆ Windows Server 2012 R2 Virtualization with Hyper-V (supported) NetIQ supports Identity Manager on enterprise-class virtualization systems that provide official support for the operating systems where NetIQ products are running. As long as the vendors of the virtualization systems officially support these operating systems, NetIQ supports the entire Identity Manager stack on them.
.NET Framework	4.x

Java Remote Loader

The Java Remote Loader runs on any connected system with a compatible JRE and Java Sockets.

Category	Requirement
Processor	Pentium* III 600MHz, at a minimum
Memory	512 MB for the Remote Loader
JRE	Java8u112, at a minimum
Platform Agent	Platform Agent 2011.1r5, at a minimum

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.

- "Using the Wizard to Install the Remote Loader" on page 165
- "Performing a Silent Installation of the Remote Loader" on page 166
- "Installing Java Remote Loader on Linux" on page 167
- "Installing Java Remote Loader on Windows" on page 168
- "Installing .NET Remote Loader on Windows" on page 169

Using the Wizard to Install the Remote Loader

The installation program guides you through the configuration settings for the Remote Loader. You can run the installation in the console or in the GUI. On UNIX and Windows computers, the installation program automatically defaults to wizard mode.

To prepare for the installation, see "Checklist for Installing the Remote Loader" on page 155. Also see the Release Notes accompanying the release. To perform an unattended installation, see "Performing a Silent Installation" on page 146.

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.

- **Linux:** `/products/IDM/install.bin`
- **Windows:** `\products\IDM\windows\setup\idm_install.exe`

To install the Remote Loader as a `root` or administrative user:

1. Log in as `root` or administrator on the computer where you want to install the Remote Loader.

   NOTE: You can install the Java Remote Loader as a non-`root` user.

   ---

2. From the directory that contains the installation files, complete one of the following actions:
   - **Linux (console)**: Enter `./install.bin -i console`
   - **Linux (GUI)**: Enter `./install.bin`
   - **Windows**: Run `idm_install.exe`
3. Accept the license agreement, and then click **Next**.
4. In the Select Components window, specify the Remote Loader components that you want to install.

For more information about the options, see "Understanding the Installation Program" on page 134.

5 (Optional) To select specific drivers for the individual components, complete the following steps:

   5a Click **Customize the selected components**, and then click **Next**.

   5b Expand **Drivers** under the component that you want to install.

   5c Select the drivers that you want to install.

6 Click **Next**.

7 In the Activation Notice window, click **OK**. For more information, see "Activating Identity Manager" on page 453.

8 For Authentication, 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=admin,o=company`.

9 For Pre-Installation Summary, verify the settings.

10 Click **Install**.

11 Activate Identity Manager. For more information, see "Activating Identity Manager" on page 453.

12 Configure the Remote Loader to connect with the drivers and Identity Manager. For more information, see Chapter 20, "Configuring the Remote Loader and Drivers," on page 171.

13 To create and configure your driver objects, consult the specific guide for that driver. For more information, see Identity Manager Drivers documentation website.

14 (Optional) For the default installation locations, see `/tmp/idmInstall.log`.

Performing a Silent Installation of the Remote Loader

To run a silent installation of the Remote Loader, create a properties files with the parameters required to complete the installation. The Identity Manager media includes a sample properties file:

- **Linux:** `/products/IDM/linux/setup/silent.properties`
- **Windows:** `\products\IDM\windows\setup\silent.properties`

To perform a silent installation:

1 In the installation directory, create a properties file or edit the sample `silent.properties` file.

2 In a text editor, specify the following parameters in the file:

CONNECTED_SYSTEM_SELECTED

Specifies whether you want to install the 32-bit Remote Loader service and drivers. You can install both 32-bit and 64-bit versions on the same server.

X64_CONNECTED_SYSTEM_SELECTED

Specifies whether you want to install the 64-bit Remote Loader service and drivers. You can install both 32-bit and 64-bit versions on the same server.

UTLITIES_SELECTED

Specifies whether you want to install the Utilities and system components for the Remote Loader.

DOT_NET_REMOTELOADER_SELECTED

Specifies whether you want to install the .NET Remote Loader service and drivers on the Windows server.

3 To run the silent installation, issue one of the following commands from the directory for the properties file:
   - **Linux**: `install.bin -i silent -f filename.properties`
   - **Windows**: `install.exe -i silent -f filename.properties`
4 (Optional) For default installed locations, see `/tmp/idmInstall.log`.

Installing Java Remote Loader on Linux

In general, you install the Java Remote Loader, `dirxml_jremote`, on computers where the operating system is not compatible with the native Remote Loader. However, the Java Remote Loader can also run on the same servers where you might install the native Remote Loader. Identity Manager uses the Java Remote Loader 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 with any publicly supported version of Java (JRE 5.0 minimum).

1 On the server that hosts the Identity Manager engine, copy the application shim `.iso` or `.jar` files, located by default in the `/opt/novell/eDirectory/lib/dirxml/classes` directory.
2 Log in to the computer where you want to install the Java Remote Loader (the target computer).
3 Verify that the target computer has a supported version of JRE.
4 To access the installation program, complete one of the following steps:
   - **4a** (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`.
   - **4b** (Conditional) If you downloaded the Java Remote Loader installation files from the NetIQ Downloads website, complete the following steps:
     - **4b1** Navigate to the `.tgz` file for the downloaded image.
     - **4b2** Extract the contents of the file to a folder on the local computer.
5 Copy the `dirxml_jremote_dev.tar.gz` file to the desired location on the target computer. For example, copy the file to `/usr/idm`.
6 Copy one of the following files to the desired location on the target computer:
   - `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.
7 On the target computer, unzip and extract the `.tar.gz` files.

   For example, enter `gunzip dirxml_jremote.tar.gz` or `tar -xvf dirxml_jremote_dev.tar`.
8 Place the `.so` or `.jar` files for the application shim that you copied in Step 1 in the `dirxml/classes` directory under the `lib` directory.
9 To customize the `dirxml_jremote` script so the Java executable is reachable through the `RDXML_PATH` environment variable, complete one of the following steps:
   - **9a** Enter one of the following commands to set the environment variable `RDXML_PATH`:
     - `set RDXML_PATH=path`
     - `export RDXML_PATH`
   - **9b** Edit the `dirxml_jremote` script and prepend the path to the Java executable on the script line that executes Java.

10 You must specify the location of the jar files in the `dirxml_jremote` script from the lib subdirectory of the untarred `dirxml_jremote.tar.gz` directory. For example, `/lib/*.jar`.

11 Configure the sample configuration file `config8000.txt` for use with your application shim.

The sample file is located by default in the `/opt/novell/dirxml/doc` directory. For more information, see Chapter 20, “Configuring the Remote Loader and Drivers,” on page 171.

Installing Java Remote Loader on Windows

Identity Manager uses the Java Remote Loader 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 java remote loader - dirxml_jremote on any supported Windows platform that has a compatible JRE (1.8.0 minimum) and Java Sockets.

1 On the server that hosts the Identity Manager engine, copy the application shim `.iso` or `.jar` files, in the default location. For example, `C:\NetIQ\IdentityManager\NDS\lib` directory.

2 Log in to the computer where you want to install the Java Remote Loader (the target computer).

3 Verify that the target computer has a supported version of JRE.

4 To access the installation program, complete one of the following steps:

4a (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`.

4b (Conditional) If you downloaded the Java Remote Loader installation files from the NetIQ Downloads website, complete the following steps:

4b1 Navigate to the `.tgz` file for the downloaded image.

4b2 Extract the contents of the file to a folder on the local computer.

5 Copy the `dirxml_jremote_dev.tar.gz` file to the desired location on the target computer. For example, copy the file to `C:\NetIQ\IdentityManager`.

6 Copy one of the following files to the desired location on the target computer:

- `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.

7 On the target computer, unzip and extract the `.tar.gz` files.

For example, use 7-Zip or supported software to unzip `.tar.gz` files.

8 Set the `CLASSPATH` environment variable to all jars that are present in `lib` folder. If you have dependent jars specific to any driver, copy those jar files to `lib` folder, then set the `CLASSPATH` environment variable to these jars also.

For example, set:

```
CLASSPATH=E:\RL\JAVARL\lib\activation.jar;E:\RL\JAVARL\lib\commondrivershim.ja
r;E:\RL\JAVARL\lib\delimitedtextshim.jar;E:\RL\JAVARL\lib\delimitedtextutil.ja
r;E:\RL\JAVARL\lib\dirxml.jar;E:\RL\JAVARL\lib\dirxml_misc.jar;E:\RL\JAVARL\li
b\dirxml_remote.jar;E:\RL\JAVARL\lib\jco3environment.jar;E:\RL\JAVARL\lib\mail
.jar;E:\RL\JAVARL\lib\mapdb.jar;E:\RL\JAVARL\lib\nxsl.jar;E:\RL\JAVARL\lib\shi
mwrapper.jar;E:\RL\JAVARL\lib\xds.jar;E:\RL\JAVARL\lib\xp.jar
```

9 Set the `PATH` environment variable to `bin` folder of JDK or JRE for `Java.exe`.

10 You must specify the location of the jar files in the `dirxml_jremote` script from the lib subdirectory of the untarred `dirxml_jremote.tar.gz` directory. For example, `/lib/*.jar`.

11 Configure the sample configuration file `config8000.txt` for use with your application shim.

The `dirxml_jremote.tar.gz` jar file contains this file. For more information, see Chapter 20, "Configuring the Remote Loader and Drivers," on page 171.

12 Launch the Remote Loader using following commands:

12a To specify a Remote Loader password:

```
java.exe -classpath %CLASSPATH%
com.novell.nds.dirxml.remote.loader.RemoteLoader -config <config file name>
-sp <Remote Loader Password> <Object Driver Password>
```

For example,

```
java.exe -classpath %CLASSPATH%
com.novell.nds.dirxml.remote.loader.RemoteLoader -config
e:\RL\JAVARL\config8000.txt -sp novell novell
```

12b To start the Remote Loader:

```
java.exe -classpath %CLASSPATH%
com.novell.nds.dirxml.remote.loader.RemoteLoader -config <config file name>
```

For example,

```
java.exe -classpath %CLASSPATH%
com.novell.nds.dirxml.remote.loader.RemoteLoader -config
e:\RL\JAVARL\config8000.txt
```

12c To stop the Remote Loader:

```
java.exe -classpath %CLASSPATH%
com.novell.nds.dirxml.remote.loader.RemoteLoader -config <config file name>
-unload
```

For example,

```
java.exe -classpath %CLASSPATH%
com.novell.nds.dirxml.remote.loader.RemoteLoader -config
e:\RL\JAVARL\config8000.txt -unload
```

Installing .NET Remote Loader on Windows

To install the .NET Remote Loader as an administrative user:

1 Log in as administrator on the computer where you want to install the .NET Remote Loader.

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 .NET Remote Loader installation files, located by default in \products\IDM\windows\setup\idm_install.exe.

2b (Conditional) If you downloaded the .NET Remote Loader installation files from the NetIQ Downloads website, complete the following steps:

- Navigate to the .tgz file for the downloaded image.
- Extract the contents of the file to a folder on the local computer.

3 Run the idm_install.exe program from the installation directory.

4. Accept the license agreement, and then click **Next**.
5. In the Select Components window, specify the .NET Remote Loader.

   For more information about the options, see "Understanding the Installation Program" on page 134.
6. (Optional) To select specific drivers for the individual components, complete the following steps:
   - **6a** Click **Customize the selected components**, and then click **Next**.
   - **6b** Expand Drivers under the component that you want to install.
   - **6c** Select the drivers that you want to install.
7. Click **Next**.
8. In the Activation Notice window, click **OK**.

   For more information, see "Activating Identity Manager" on page 453.
9. Select the .NET Remote Loader installation directory on your computer.
10. Review the Summary page, then click **Install** to complete the installation.

20 Configuring the Remote Loader and Drivers

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.

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 "Understanding Shims" on page 157.

- "Creating a Secure Connection to the Identity Manager Engine" on page 171
- "Understanding the Configuration Parameters for the Remote Loader" on page 174
- "Configuring the Remote Loader for Driver Instances on UNIX or Linux" on page 183
- "Configuring the Remote Loader for Driver Instances on Windows" on page 185
- "Configuring the Java Remote Loader for Driver Instances" on page 187
- "Configuring the .NET Remote Loader for Driver Instances on Windows" on page 189
- "Configuring Identity Manager Drivers to Work with the Remote Loader" on page 191
- "Configuring Mutual Authentication with the Identity Manager Engine" on page 192
- "Verifying the Configuration" on page 199

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 or KMO. 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.

Understanding the Communication Process

The Remote Loader opens a client 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 "Managing Self-Signed Server Certificates" on page 172.
- **For a Java driver**, you must create a keystore. For more information, see "Creating a Keystore File when Using SSL Connections" on page 173.
- **For a .NET driver**, point to a base64 encoded certificate. For more information, see "Managing Self-Signed Server Certificates" on page 172.

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.

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. For additional security, you can configure stronger ciphers for SSL communication as specified by Suite B. This communication requires the use of ECDSA (Elliptic Curve Digital Signature Algorithm) certificates for encrypting the data. When Suite B is enabled, Remote Loader uses TLS 1.2 as a communication protocol. For more information about Suite B, see Suite B Cryptography.

You can export a newly created certificate or use an existing certificate.

NOTE: When a server joins a tree, eDirectory creates the following default certificates:

- SSL CertificateIP
- SSL CertificateDNS
- Suite B compliant certificates

---

1. Log in to NetIQ iManager.
2. To create a new certificate, complete the following steps:
   - **2a** Click **NetIQ 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** Select the certificate creation method, then click **Next**.

You have the following options:

- **Standard:** This option creates a server certificate object using the largest possible key size and signs the public key certificate with your Organizational CA.
- **Custom:** This option creates a server certificate object using the settings you specify. It allows you to set a number of customized settings for the Server Certificate object. Select this option to create ECDSA certificates for Suite B communication.
- **Import:** This option creates a server certificate object using the keys and certificates from a PKCS12 (PFX) file. You can use this option in conjunction with the Export feature to backup and restore a Server Certificate or to move a Server Certificate object from one server to another.

2e Specify the certificate parameters.

2f Accept the rest of the certificate defaults.

2g Review the summary, click **Finish**, then click **Close**.

3 To export a certificate, complete the following steps:

3a In iManager, navigate to **Roles and Tasks** > **NetIQ Certificate Access > Server Certificates**.

3b Browse and select the created certificate or the server created certificate (for example, SSL CertificateDNS).

3c Click **Export**.

3d Select the **CA Certificate** as **OU=organization CA.O=TREEANAME** from the drop down menu.

3e Select the **Export Format** as **BASE64** from the drop down menu.

NOTE: When the Remote Loader is running on a Windows 2012 R2 64-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.

3f Click **Next**.

3g Click **Save**, then click **Close**.

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 173
- "Creating a Keystore on Linux" on page 174
- "Creating a Keystore on Windows" on page 174

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 Linux

In 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.

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**: “Configuring the Remote Loader for Driver Instances on UNIX or Linux” on page 183
- **Windows**: “Configuring the Remote Loader for Driver Instances on Windows” on page 185.

Configuration Parameters for the Driver Instances in the Remote Loader

You can configure a driver instance from the command line or in a configuration file. NetIQ provides a sample file `config8000.txt` to help you configure the Remote Loader and drivers for use with your application shim. The sample file is located by default in the `/opt/novell/dirxml/doc` directory. For example, the configuration file might include the following lines:

```
-commandport 8000
-connection "port=8090 rootfile=/dirxmlremote/root.pem"
-module $DXML_HOME/dirxmlremote/libcskeldrv.so.0.0.0
-trace 3
```

Use the following parameters:

-assembly

(Conditional) When using a .NET Remote Loader, specifies the path where the driver .dll is located. Ensure that the configuration file includes this parameter. For example:

```
-assembly C:\Novell\remoteloader.NET\DXMLMADDriver.dll
```

-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 "Understanding the Names for the Java -class Parameter" on page 182.

-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
```

secureprotocol=*TLS version*

Specifies the version of the TLS protocol that the Remote Loader uses to connect to the Identity Manager engine. For example:

```
secureprotocol=TLSv1_2
```

Identity Manager supports TLSv1 and TLSv1_2. By default, the Remote Loader uses TLSv1_2. To use TLSv1, specify this version in the parameter.

enforceSuiteB=*true/false*

(Conditional) Applies only when you want the Remote Loader to communicate with the Identity Manager engine using Suite B cryptographic algorithms.

To use Suite B for communication, specify `true`. This communication is supported only on TLS 1.2 protocol.

If you try to connect a Suite B-enabled engine with a Remote Loader that does not support TLSv1.2, the handshake fails and the communication is not established. For example, Remote Loader 4.5.3, which does not support TLS v1.2.

useMutualAuth=*true/false*

(Conditional) Applies only when want the Remote Loader and the Identity Manager engine to authenticate each other by verifying the public key certificate or digital certificate issued by the trusted Certificate Authorities (CAs) or self-signed certificates. For example:

```
useMutualAuth=true
```

keystore=*filename*

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=keystore filename
```

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*

Specifies the name of the file that contains the trusted root certificate of the issuer of the certificate that the remote interface shim uses. The certificate file must be in Base 64 format (PEM). For example:

```
rootfile=trustedcert
```

Usually, the file will be the Certificate Authority of the tree that is hosting the remote interface shim.

storepass=*password*

Specifies password for the Java keystore that you entered for the `keystore` parameter. For example:

```
storepass=mypassword
```

For 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
```

NOTE: Do not use this parameter with the Java Remote Loader.

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_OPTIONS

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 netiq4
```

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 netiq4 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.

Understanding the 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.dcsshim.DCSShim	Driver for Data Collection Service
com.novell.nds.dirxml.driver.delimitedtext.DelimitedTextDriver	Delimited Text 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.rest.shim.GWdriverShim	GroupWise 2014 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

Java Class Name	Driver
com.novell.nds.dirxml.driver.ldap.LDAPDriverShim	LDAP Driver
com.novell.nds.dirxml.driver.loopback.LoopbackDriverShim	Loopback Driver
com.novell.nds.dirxml.driver.ebs.user.EBSUserDriver	Oracle User Management Driver
com.novell.nds.dirxml.driver.ebs.hr.EBSHRDriver	Oracle HR Driver
com.novell.nds.dirxml.driver.ebs.tca.EBSTCADriver	Oracle TCA Driver
com.novell.nds.dirxml.driver.msgateway.MSGatewayDriverShim	Managed System Gateway Driver
com.novell.nds.dirxml.driver.manualtask.driver.ManualTaskDriver	Manual Task Driver
com.novell.nds.dirxml.driver.nisdriver.NISDriverShim	NIS Driver
com.novell.nds.dirxml.driver.notes.NotesDriverShim	Notes Driver
com.novell.nds.dirxml.driver.psoftshim.PSOFTDriverShim	PeopleSoft Driver
com.netiq.nds.dirxml.driver.pum.PUMDriverShim	Privileged User Management 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

Configuring the Remote Loader for Driver Instances on UNIX or Linux

The Remote Loader can host the Identity Manager application shims contained in `.dll`, `.so`, or `.jar` files. 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 174.

To create a configuration file:

1. In a text editor, create a new file.

   NetIQ provides a sample file `config8000.txt` to help you configure the Remote Loader and drivers for use with your application shim. The sample file is located by default in the `/opt/novell/dirxml/doc` directory.

2. Add the following configuration parameters to the file:
   - -description (optional)
   - -commandport
   - connection parameters:
     - port (mandatory)
     - address
     - fromaddress
     - handshaketimeout
     - rootfile
     - keystore
     - storepass
     - localaddress
     - hostname
     - kmo
     - secureprotocol
     - enforceSuiteB
     - useMutualAuth
   - trace file parameters (optional):
     - -trace
     - -tracefile
     - -tracefilemax
   - -javaparam
   - -class or -module

   For more information about specifying values for these parameters, see "Understanding the Configuration Parameters for the Remote Loader" on page 174.

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.

Configuring the Remote Loader for Driver Instances on Windows

The Remote Loader can host the Identity Manager application shims contained in `.dll`, `.so`, or `.jar` files. For the Remote Loader to run, the application needs a configuration file, such as `LDAPShim.txt`. 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 "Understanding the Configuration Parameters for the Remote Loader" on page 174.

This section provides instructions for the following activities:

- "Creating a New Driver Instance in the Remote Loader on Windows" on page 185
- "Modifying an Existing Driver Instance in the Remote Loader on Windows" on page 187

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\`*`nn`*`bit`.

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 driver, select **ADDriver.dll**. For more information about the class names for each driver, see "Understanding the Names for the Java -class Parameter" on page 182.

5. For **Config File**, specify the path to the file where Remote Loader stores its configuration parameters. The default value is `C:\novell\remoteloader\`*`nn`*`bit\`*`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** (base64 format file), specify the exported self-signed certificate from the eDirectory tree's Organization Certificate Authority. For more information, see "Creating a Secure Connection to the Identity Manager Engine" on page 171 and "Understanding the Configuration Parameters for the Remote Loader" on page 174.

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:\novell\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**.

NOTE: If the SSL connection fails due to `handshaketimeout` when Remote Loader establishes connection with Identity Manager engine then, update the default `handshaketimeout` variable to 10000 and restart both driver and remote loader.

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 For Suite B communication, specify `enforceSuiteB=true`. This communication is supported only on TLS 1.2 protocol.

For more information, see "Creating a Secure Connection to the Identity Manager Engine" on page 171 and "Understanding the Configuration Parameters for the Remote Loader" on page 174.

10f Click **OK**.

11 (Optional) To allow the Remote Loader to use the secure protocol while connecting to the Identity Manager engine, specify the secure protocol version in the Remote Loader configuration file. For example: `secureprotocol=TLSv1_2`

For more information, see "Understanding the Configuration Parameters for the Remote Loader" on page 174.

NOTE: Skip this step if you already configured the secure protocol version on the driver.

---

12 (Optional) To allow the Remote Loader communication to use the protocols specified by Suite B, specify `enforceSuiteB=true` in the Remote Loader configuration file. This communication is supported only on TLS 1.2 protocol.

For more information, see "Understanding the Configuration Parameters for the Remote Loader" on page 174.

NOTE: Skip this step if you already enabled Suite B communication on the driver.

---

13 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 185.
6. To save the changes, click **OK**.

Configuring the Java Remote Loader for Driver Instances

The Java Remote Loader hosts only Java driver shims. It does not load or host a native (C++) driver shim.

To configure a new instance for the Java Remote Loader on Linux 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 174.

1. In a text editor, create a new file.

   NetIQ provides a sample file `config8000.txt` to help you configure the Remote Loader and drivers for use with your application shim. The sample file is located by default in the `/opt/novell/dirxml/doc` directory.

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 (mandatory)
  - address
  - fromaddress
  - handshaketimeout
  - rootfile
  - keystore
  - storepass
  - localaddress
  - hostname
  - kmo
  - secureprotocol
  - enforceSuiteB
  - useMutualAuth
- -java (conditional)
- -javadebugport
- -password
- -service
- -setpasswords
- trace file parameters (optional):
  - -trace
  - -tracefile
  - -tracefilemax

NOTE: For more information about the parameters, see "Understanding the Configuration Parameters for the Remote Loader" on page 174.

---

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/jremote` 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:

```
dirxml_jremote -config filename
```

Configuring the .NET Remote Loader for Driver Instances on Windows

The Remote Loader can host the Identity Manager application shim contained in `.dll` file. For the Remote Loader to run, the application needs a configuration file, such as `LDAPShim.txt`. 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.net`. 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 "Understanding the Configuration Parameters for the Remote Loader" on page 174.

This section provides instructions for the following activities:

- "Creating a New Driver Instance in the .NET Remote Loader on Windows" on page 189
- "Modifying an Existing Driver Instance in the .NET Remote Loader on Windows" on page 191

Creating a New Driver Instance in the .NET 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.net`.

---

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 appropriate driver.dll.

5 For **Config File**, specify the path to the file where Remote Loader stores its configuration parameters. The default value is `C:\novell\remoteloader.net\`*`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** (base64 format file), specify the exported self-signed certificate from the eDirectory tree's Organization Certificate Authority. For more information, see "Creating a Secure Connection to the Identity Manager Engine" on page 171 and "Understanding the Configuration Parameters for the Remote Loader" on page 174.

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:\novell\remoteloader.net\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**.

NOTE: If the SSL connection fails due to `handshaketimeout` when Remote Loader establishes connection with Identity Manager engine then, update the default `handshaketimeout` variable to 10000 and restart both driver and remote loader.

10 (Optional) To allow the Remote Loader to use the secure protocol while connecting to the Identity Manager engine, specify the secure protocol version in the Remote Loader configuration file. For example: `secureprotocol=TLSv1_2`

For more information, see "Understanding the Configuration Parameters for the Remote Loader" on page 174.

NOTE: Skip this step if you already configured the secure protocol version on the driver.

11 (Optional) To allow the Remote Loader communication to use the protocols specified by Suite B, specify `enforceSuiteB=true` in the Remote Loader configuration file. This communication is supported only on TLS 1.2 protocol.

For more information, see "Understanding the Configuration Parameters for the Remote Loader" on page 174.

NOTE: Skip this step if you already enabled Suite B communication on the driver.

12 Click **OK**.

Modifying an Existing Driver Instance in the .NET 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 .NET Remote Loader on Windows" on page 189.
6 To save the changes, click **OK**.

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. You must set up an Identity Manager application shim for use with the Remote Loader.

NOTE: 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 website.

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 174.

1 From **Overview**, select the Identity Manager Driver object.
2 In the properties of the Driver object, complete the following steps:
   2a For **Driver Module**, select **Connect to Remote Loader**.
   2b 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 in the Remote Loader.
   2c 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. For example, `hostname=192.168.0.1`.

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. For example, `kmo=remotecert`.

localaddress

Specifies the source IP address if more than one IP addresses are configured on the server that hosts the Identity Manager engine.

2d For **Remote Loader Password**, specify the password required for the Identity Manager engine (or Remote Loader shim) to authenticate to the Remote Loader.

3 Define a security-equivalent user.

4 Click **Next**, then click **Finish**.

NOTE: If you delete a driver or clean the DirXML-DriverStorage attribute, you must also delete the state file created by the driver. The state file is named `state<name of driver>.xml`. It is located in the Remote Loader directory.

Configuring Mutual Authentication with the Identity Manager Engine

You can configure mutual authentication to ensure secure communication between the Remote Loader and the Identity Manager engine. Mutual authentication uses certificates for handshake instead of passwords. The Remote Loader and the Identity Manager engine authenticate each other by exchanging and validating the public key certificate or digital certificate issued by the trusted Certificate Authorities (CAs) or self-signed certificates. If mutual authentication succeeds, the Remote Loader authenticates to the engine. Synchronization traffic occurs after both the Remote Loader and the Identity Manager engine establish trust that they are communicating with an authorized entity.

Perform the following tasks to configure mutual authentication:

- "Exporting Certificates for the Identity Manager Engine and the Remote Loader" on page 192
- "Enabling a Driver for Mutual Authentication" on page 195

Exporting Certificates for the Identity Manager Engine and the Remote Loader

For mutual authentication to work properly, you need a server certificate for the engine and a client certificate for the Remote Loader. You can export the certificates from eDirectory or import them from a third-party vendor. In most cases, you will export a server certificate from eDirectory with no further investment. In some cases, you might want to export a third-party client certificate for the Remote Loader.

- "Exporting a Certificate from eDirectory" on page 193
- "Exporting a Third-Party Certificate for Remote Loader" on page 194

Exporting a Certificate from eDirectory

A certificate object in the Identity Vault is called Key Material Object (KMO). This object securely contains both the certificate data including the public key and the private key associated with the certificate used for SSL connections. For mutual authentication, you need two KMOs, each for the engine and the Remote Loader.

You can export an existing KMO or create a new KMO and then export it. The process of creating a client KMO and a server KMO is different.

Creating KMOs

To create a server KMO:

1. Log in to NetIQ iManager.
2. In the left side pane, click **NetIQ Certificate Server**, then select the server certificate.
3. Select the server to own the certificate that you created.
4. Specify a nickname for the certificate. For example, `serverkmo`.
5. Select **Standard** in the certificate creation method, then click **Next**.
6. Review the summary, click **Finish**, then click **Close**.

To create a client KMO:

1. Log in to NetIQ iManager.
2. In the left side pane, click **NetIQ Certificate Server**, then select the server certificate.
3. Select the server to own the certificate that you created.
4. Specify a nickname for the certificate. For example, `clientkmo`
5. Select **Custom** in the certificate creation method, then click **Next**.
6. Leave the default **Organizational Certificate Authority** unchanged, then click **Next**.
7. Unselect **Enable Extended key usage**, then click **Next**.
8. Accept the rest of the certificate defaults.
9. Review the summary, click **Finish**, then click **Close**.

Exporting KMOs

Export the KMOs from eDirectory that the engine and the Remote Loader will use for authenticating with each other.

To export the KMO for the Identity Manager engine, run the DirXML Command Line (dxcmd) utility:

```
dxcmd -user <admin DN> -password <password of admin> -exportcerts <kmoname>
<server|client> <java|native|dotnet> <output dir>
```

where

- `user` specifies the name of a user with administrative rights to the driver.
- `password` specifies the password of the user with administrative rights to the driver.
- `exportcerts` exports the certificates and private/public keys from eDirectory. You must specify whether you are exporting a server or a client certificate, the type of driver that will use the certificate, and a destination folder where the command will store this information.

For example, `dxcmd -user admin.sa.system -password novell -exportcerts serverkmo server java '/home/certs'`

This command generates the `serverkmo_server.ks` file in the `/home/certs/` directory. The default password for the keystore is `dirxml.`

When running the dxcmd command for exporting the KMO for the Remote Loader, the following considerations apply:

- The dxcmd utility runs in LDAP mode. When you use it for the first time, it prompts for specifying the choice of trusting the certificate from eDirectory. Depending on your environment, you can choose to trust the certificate only for the current session, for the current and future sessions, trust all certificates, or select not to trust the certificate.
- If the Remote Loader is running on the Identity Manager server, run the command in either LDAP or dot format. If the Remote Loader is installed on a separate server, run the command only in LDAP format.
- Specify the `-host` parameter in the command to resolve the server IP address or hostname to be able to authenticate with the Identity Manager server.

Run the command using the following syntax:

```
dxcmd -dnform ldap -host <IP address of the host> -user <admin DN> -password
<password of admin> -exportcerts <kmoname> <client> <java|native|dotnet> <output
dir>
```

Table 20-1 *Examples for different types of drivers*

Type of Driver	Command	Output
Java Driver	`dxcmd -dnform ldap -host 194.99.90.218 -user cn=admin,ou=sa,o=system -password novell -exportcerts clientkmo client java '/home/certs'`	`clientkmo_client.ks` file in the `/home/certs/` directory The default password for the keystore is `dirxml.`
Native Driver	`dxcmd -dnform ldap -host 194.99.90.218 -user cn=admin,ou=sa,o=system -password novell -exportcerts clientkmo client native 'C:\certs'`	`clientkmo_clientcert.pem`, `clientkmo_clientkey.pem`, and `trustedcert.b64` files in the `C:\certs` directory
.NET Driver	`dxcmd -dnform ldap -host 194.99.90.218 -user cn=admin,ou=sa,o=system -password novell -exportcerts clientkmo client dotnet 'C:\certs'`	`clientkmo_clientcert.pfx` and `trustedcert.b64` files in the `C:\certs` directory

Exporting a Third-Party Certificate for Remote Loader

To use third party certificates with the Remote Loader, you need to export a certificate in the `.pfx` file and a trusted root file in Base 64 format and then convert the `.pfx` certificate to the format that the driver uses. For example, a native driver requires the private key and the certificate key in `.pem` format while a Java driver requires the keystore in `.jks` format. The .NET driver uses the file in `.pfx` format. So you need not convert the file for a .NET driver.

Native driver

Complete the following steps:

1. Retrieve the private key in `.pem` format from the `.pfx` file.

Enter a command, such as `openssl pkcs12 -in servercert.pfx -nocerts -out serverkey.pem –nodes`

2. Retrieve the certificate key in `.pem` format from the `.pfx` file.

   Enter a command, such as `openssl pkcs12 -in servercert.pfx -nokeys -out servercert.pem`

Java driver

Create a Java keystore from the `.pfx` file. Enter a command, such as `keytool -importkeystore -srckeystore servercert.pfx -srcstoretype pkcs12 -destkeystore servercert.jks -deststoretype JKS`.

As a final step, specify the information in the Remote Loader configuration file depending on the type of the driver. For more information, see Enabling a Driver for Mutual Authentication.

Enabling a Driver for Mutual Authentication

You enable a driver communication for mutual authentication by performing the following tasks:

- "Configuring a Driver Using KMO or Keystore" on page 195
- "Configuring the Remote Loader for Driver Instances" on page 197

Configuring a Driver Using KMO or Keystore

You can configure the driver by using KMO or keystore in Designer or iManager.

In Designer, you can configure the driver during the initial driver creation process or configure it after creating the driver.

To configure a driver in Designer:

1. Open your project in Designer.
2. In the palette of the Modeler view, select the driver that you want to create.
3. Drag the icon for the driver onto the Modeler view.
4. Follow the steps in the installation wizard.
5. In the Remote Loader window, select **yes**.

   5a **Host name:** Specify the hostname or IP address of the server where the driver's Remote Loader service is running. For example, enter hostname=192.168.0.1. If you do not specify a value for this parameter, the value defaults to localhost.

   5b **Port:** Specify the port number where the Remote Loader is installed and is running for this driver. The default port number is 8090.

   5c **KMO:** Specify the Key Name of the KMO that contains the keys and certificate that the Remote Loader uses for an SSL connection. For example, enter kmo=`serverkmo`. If you are configuring mutual authentication using KMO, you must specify a value for this parameter. You also need to specify a value for the **Root File** parameter in the Other parameters section. **Root File** should contain the trusted root certificate of Remote Loader in `b64` format.

   5d **Other parameters:** Specify the settings for the Remote Loader that you want to use. You include information about mutual authentication communication in this parameter. Any parameters specified must use a key-value pair format, as follows:`paraName1=paraValue1 paraName2=paraValue2`

   For example, use the following syntax for keystore:

```
UseMutualAuth=true keystore='/home/certs/serverkmo_server.ks'
storepass='dirxml' keypass='dirxml' key='serverkmo'
```

For example, use the following syntax for kmo:

```
useMutualAuth=true rootFile='/home/cacert.b64'
```

IMPORTANT: Ensure that the `rootFile` generated is in `b64` format.

5e **Set Password:** Enables you to set or change an application password.

5f **Delete Password:** Deletes the password to the application.

6 Click **Next**.

7 Follow the rest of the instructions in the wizard until you finish installing the driver.

8 Review the summary of tasks that will be completed to create the driver, then click **Finish**.

Alternatively, you can configure the driver after creating it by performing the following steps:

1 In the Outline view of Designer, right-click the driver.

2 Select **Properties**.

3 In the navigation pane, select **Driver Configuration**.

4 Select **Authentication**.

5 Under **Remote Loader authentication** section, specify the information required to configure mutual authentication between the Remote Loader and the Identity Manager engine.

Use the following syntax for kmo:

```
hostname=xxx.xxx.xxx.xxx port=xxxx useMutualAuth=true kmo=certificatename
rootFile=<absolute path to the file>
```

For example:

```
hostname=192.168.0.1 port=8090 useMutualAuth=true kmo=serverkmo rootFile='/
home/cacert.b64'
```

Use the following syntax for keystore:

```
hostname=xxx.xxx.xxx.xxx port=xxxx useMutualAuth=true keystore=<absolute path
to the keystore file> storepass=<keystore password> key=<alias name> keypass=
<password for the key>
```

For example:

```
hostname=192.99.90.17 port=8097 useMutualAuth=true keystore='/home/certs/
serverkmo_server.ks' storepass='dirxml' key='serverkmo' keypass='dirxml'
```

To modify the configuration in iManager:

1 Launch iManager.

2 From Overview, select the Identity Manager Driver object.

3 In the properties of the Driver object, complete the following steps:

3a For **Driver Module**, select **Connect to Remote Loader**.

3b For **Driver Object Password**, specify the password that the Remote Loader uses to authenticate with the engine.

This password must match the password for the driver object defined in the Remote Loader.

3c For **Remote Loader Connection Parameters**, specify the information required to connect to the Remote Loader.

Use the following syntax for kmo:

```
hostname=xxx.xxx.xxx.xxx port=xxxx useMutualAuth=true kmo=certificatename
rootFile=<absolute path to the file>
```

For example:

```
hostname=192.168.0.1 port=8090 useMutualAuth=true kmo=serverkmo rootFile='/
home/cacert.b64'
```

Use the following syntax for keystore:

```
hostname=xxx.xxx.xxx.xxx port=xxxx useMutualAuth=true keystore=<absolute
path to the keystore file> storepass=<keystore password> key=<alias name>
keypass= <password for the key>
```

For example:

```
hostname=192.99.90.17 port=8097 useMutualAuth=true keystore='/home/certs/
serverkmo_server.ks' storepass='dirxml' key='serverkmo' keypass='dirxml'
```

3d (Optional) For **Remote Loader Password**, specify the password required for the Identity Manager engine (or Remote Loader shim) to authenticate to the Remote Loader.

3e Click **Apply**, then click **OK**.

Configuring the Remote Loader for Driver Instances

You must configure the driver instance in the Remote Loader configuration file. Ensure that you specify the absolute path to the directory that stores the key file, certificate file, and the root file in the Remote Loader configuration file for a driver.

Configuring on UNIX or Linux

Modify the Remote Loader configuration file for a driver to include the content for enabling mutual authentication. The file is located in the `/opt/novell/dirxml/doc` directory.

To modify the configuration:

1. Log in to the server where you installed the driver and Remote Loader.
2. Stop the Remote Loader.

   For example, enter the following command:

   ```
   rdxml -config /home/drivershim.conf -u
   ```

3. In a text editor, open the Remote Loader configuration file for the driver.
4. Add the content required for enabling mutual authentication to the file.
   - For example, for a Java driver, add this entry:

     ```
     -connection "port=8090 useMutualAuth=true keystore='/home/certs/
     clientkmo_client.ks' storepass='dirxml' key='clientkmo' keypass='dirxml'"
     ```

   - For example, for a Native driver, add this entry:

     ```
     -connection "useMutualAuth=true port=8090 rootfile='/home/certs/
     trustedcert.b64' certfile='/home/certs/clientkmo_clientcert.pem'
     keyfile='/home/certs/clientkmo_clientkey.pem' keypass='dirxml'
     certform=PEM keyform=PEM"
     ```

5 Save and close the file.

6 Restart the driver.

Configuring on Windows

1 In the Remote Loader Console, select the driver instance from **Description** column.

2 Click **Stop**.

3 Enter the password for the Remote Loader, then click **OK**.

4 Click **Edit**.

5 To modify the configuration information for enabling mutual authentication, complete the following steps:

5a Select **Mutual Authentication**.

5b **For a native driver**, specify the path to the key file that stores the certificate for authentication. The key file must be in Base 64 format.

Key File

Specifies the path to the file that stores the key for authentication. The key file must be in Base 64 format. For example, `clientkmo_clientkey.pem` file in the `C:\certs\` directory created by `dxcmd` in "Exporting a Certificate from eDirectory" on page 193.

Key Password

Specifies the password for the private key used for authentication.

Certificate File

Specifies the file where the certificates are stored. The certificate file must be in Base 64 format. For example, `clientkmo_clientcert.pem` in the `C:\certs\` directory created by `dxcmd` in "Exporting a Certificate from eDirectory" on page 193.

Trusted Root File

Specifies the name of the file that contains the trusted root certificate of the issuer of the certificate that the remote interface shim uses. The trusted root file must be in Base 64 format. For example, trustedcert.b64 files in the `C:\certs\` directory created by `dxcmd` in "Exporting a Certificate from eDirectory" on page 193.

5c **For a Java driver**, specify the path of the keystore file that contains the certificate. The keystore file must contain at least one public/private key pair.

Keystore File

Specifies the path to the Java keystore file you want to use for authentication. The keystore file contains encryption keys and certificates. The keystore file must contain at least one public/private key pair. For example, `clientkmo_client.ks` in the `C:\certs\` directory created by `dxcmd` in "Exporting a Certificate from eDirectory" on page 193.

Key Alias

Specifies the name of the public/private key pair in the keystore file that you want to use for symmetric key generation. For example, `clientkmo`.

Keystore Password

Specifies the password used to load the keystore file.

Private Key Password

Specifies the password for the private key stored in the keystore. Identity Manager uses this key for encrypting the SSL communication.

5d **For a .NET driver**, specify the path to the key file that stores the certificate for authentication.

Key File

Specifies the path to the file that stores the key for authentication. For example, `clientkmo_clientcert.pfx` in the in the `C:\certs\` directory created by `dxcmd` in "Exporting a Certificate from eDirectory" on page 193.

Key Password

Specifies the password for the private key used for authentication.

Trusted Root File

Specifies the name of the file that contains the trusted root certificate of the issuer of the certificate that the remote interface shim uses. The trusted root file must be in Base 64 format. For example, `trustedcert.b64` file in the `C:\certs\` directory created by `dxcmd` in "Exporting a Certificate from eDirectory" on page 193.

5e Click **OK**.

6 Click **OK**.

Verifying the Configuration

For more information about starting and stopping the Remote Loader, see Chapter 21, "Starting and Stopping the Remote Loader," on page 201.

1. Start the Remote Loader. For example:

```
dirxml_remote -config config.txt
```

2. Start the remote interface shim using iManager.
3. Confirm that the Remote Loader is operating properly.
4. Stop the Remote Loader. For example:

```
dirxml_remote -config config.txt -u
```

5. Install the Remote Loader as a Win32 service. For example:

```
dirxml_remote -config config.txt -service install
```

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.

- "Starting a Driver Instance in the Remote Loader" on page 201
- "Stopping a Driver Instance in the Remote Loader" on page 203

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.

- "Starting Driver Instances on UNIX or Linux" on page 201
- "Starting Driver Instances on Windows" on page 202

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 201
- "Using the Command Line to Start Driver Instances on UNIX or Linux" on page 201

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 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 174.

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:
   - **Linux/UNIX:** `rdxml -config filename -sp Remote Loader password Driver Object` *`password`*
   - **Java Remote Loader:** `dirxml_jremote -config` *`filename`* `-sp Remote Loader password Driver Object` *`password`*

3 To start the driver instance, enter the following command:

```
rdxml -config filename
```

4 Log in to iManager, then start the driver.

5 Confirm that the Remote Loader is working properly.

- **Linux**: Use the `ps` command or a trace file to determine whether the command and connection ports are listening.
- **UNIX**: Monitor the 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.

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 202
- "Using the Console to Start Driver Instances on Windows" on page 202
- "Using the Command Line to Start Driver Instances on Windows" on page 203

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.

During installation, if you created 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\`*nn*`bit`.

2 Select a driver instance, then click **Edit**.

3 Select **Establish a Remote Loader service for this driver instance**.

4 Save your changes, and then close the console.

Using the Console to Start Driver Instances on Windows

1 Open the Remote Loader Console.

During installation, if you created 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\`*nn*`bit`.

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 174.

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 in 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
   ```

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 174.

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:

Linux/UNIX

Enter the `rdxml -config` *`filename`* `-u` command. For example:

```
rdxml -config config.txt -u
```

Windows

Use the Remote Loader Console.

During installation, if you created 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\`*`nn`*`bit`.

Java Remote Loader

Enter the `dirxml_jremote -config` *`filename`* `-u` command. For example:

```
dirxml_jremote -config config.txt -u
```

VII 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`
- **Windows**: `C:\Novell`

NetIQ recommends that you review the installation process before beginning. For more information, see Chapter 22, “Planning to Install iManager,” on page 207.

22 Planning to Install iManager

This section provides the prerequisites, considerations, and system setup needed to install iManager. First, consult the checklist to understand the installation process.

- "Checklist for Installing iManager" on page 207
- "Understanding the Server and Client Versions of iManager" on page 208
- "Understanding Installation for iManager Plug-ins" on page 209
- "Prerequisites and Considerations for Installing iManager" on page 209
- "System Requirements for iManager Server" on page 213
- "System Requirements for iManager Workstation (Client Version)" on page 214

Checklist for Installing iManager

Before beginning the installation, NetIQ recommends that you review the following steps:

	Checklist Items
❑	1. Learn about the interaction among Identity Manager components. For more information, see Chapter 1, "Overview of the Components of Identity Manager," on page 23.
❑	2. Decide which servers you want to use for your Identity Manager components. For more information, see "Recommended Installation Scenarios and Server Setup" on page 44.
❑	3. Understand the difference between iManager and iManager Workstation. For more information, see "Understanding the Server and Client Versions of iManager" on page 208.
❑	4. (Conditional) To ensure that Linux computers meet the prerequisites for installing iManager and iManager Workstation, review the following considerations: ◆ For iManager, see "Considerations for Installing iManager on a Linux Platform" on page 210 ◆ For iManager Workstation, see "Considerations for Installing iManager Workstation on Linux Clients" on page 212
❑	5. (Conditional) To ensure that Windows computers meet the prerequisites for installing iManager and iManager Workstation, review the following considerations: ◆ For iManager, see "Considerations for Installing iManager on a Windows Platform" on page 211 ◆ For iManager Workstation, see "Considerations for Installing iManager Workstation on Windows Clients" on page 213
❑	6. Review the hardware and software requirements for the computers that will host iManager: ◆ For iManager, see "System Requirements for iManager Server" on page 213 ◆ For iManager Workstation, see "System Requirements for iManager Workstation (Client Version)" on page 214

	Checklist Items
❑	7. (Conditional) For computers running a SLES 12 SP1 or later operating system, ensure that you have installed the appropriate set of libraries for a guided installation. For more information, see "Installing Identity Manager on SLES 12 SP1 or Later Servers" on page 55.
❑	8. (Conditional) For computers running an RHEL 6.x or RHEL 7.x operating system, ensure that you have installed the appropriate set of libraries. For more information, see "Installing Identity Manager on RHEL 6.x or 7.x Servers" on page 55.
❑	9. Access the installation files for iManager, located by default in the `products/iManager/installs/`*`server_platform`*`/` directory within the `.iso` image file for the Identity Manager installation package. Alternatively, download the installation files from the NetIQ Downloads website. Search for iManager products, select the iManager version that you want, then download the `.tgz` and `tar.bz2` or `win.zip` file to a directory on your server. For example, `iMan_277_linux.tgz` and `iMan_277_workstation_linux.tar.bz2` or `iMan_277_win.zip`.
❑	10. (Optional) To learn more about the process for installing plug-ins, see "Understanding Installation for iManager Plug-ins" on page 209.
❑	11. (Optional) To review actions that you can perform after installing iManager, see Chapter 24, "Post-Installation Tasks for iManager," on page 227.
❑	12. To install iManager and iManager Workstation, see the following sections: ◆ For Linux computers, see "Installing iManager and iManager Workstation on Linux" on page 217 ◆ For Windows computers, see "Installing iManager and iManager Workstation on Windows" on page 221 ◆ For a silent installation, see "Installing iManager Silently" on page 224

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.

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/consoles/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:

- **Linux**: “Installing iManager and iManager Workstation on Linux” on page 217
- **Windows**: “Installing iManager and iManager Workstation on Windows” on page 221
- **Silent installation**: “Installing iManager Silently” on page 224

For more information about customizing the process for downloading and installing plug-ins, see “Downloading and Installing Plug-in Modules” in the *NetIQ iManager Installation Guide*.

Prerequisites and Considerations for Installing iManager

This section provide information for installing server and workstation versions of iManager.

- “Considerations for Installing iManager” on page 210
- “Considerations for Installing iManager on a Linux Platform” on page 210
- “Considerations for Installing iManager on a Windows Platform” on page 211
- “Considerations for Installing iManager Workstation on Linux Clients” on page 212
- “Considerations for Installing iManager Workstation on Windows Clients” on page 213

Considerations for Installing iManager

Before installing iManager, review the following considerations:

- Identity Manager 4.6 supports two versions of eDirectory. Depending on the version you install, you must install a compatible version of iManager.
  - eDirectory 9.0.2 with Hotfix 2: Use iManager 3.0.2 Patch 1. For more information, see NetIQ iManager Installation Guide.
  - eDirectory 8.8.8 Patch 9 with Hotfix 2: Use iManager 2.7.7 Patch 9. For more information, see NetIQ iManager Installation Guide.
- 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 Server setup program detects a previously installed version of iManager, you can stop the installation process or remove the existing iManager, JRE, and Tomcat installations. For example, iManager 2.7.7 detects 2.7.x version.
- 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.

Considerations for Installing iManager on a Linux Platform

Your Linux server must have specific packages already installed before you install iManager. In general, you can download the `.rpm` files from a website such as http://rpmfind.net/linux.

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-`*`version`*`.el6.i686.rpm` (RHEL 6 or 7 32-bit)
- `compat-libstdc++-33-`*`version`*`.el6.i686.rpm` (RHEL 6 or 7 64-bit)
- `compat-libstdc++-33-`*`version`*`.el6.x86_64.rpm` (RHEL 6 or 7 64-bit)

- `libstdc++-4.4.`*`version`*`.el6.i686.rpm` (RHEL 6 or 7 64-bit)
- `libstdc++-4.4.`*`version`*`.el6.x86_64.rpm` (RHEL 6 or 7 64-bit for GUI installation mode)
- `glibc-2.12-`*`version`*`.el6.i686` (RHEL 6 or 7 64-bit)
- `libXau-`*`version`*`.el6.i686.rpm` (RHEL 6 or 7 64-bit)
- `libxcb-`*`version`*`.el6.i686.rpm` (RHEL 6 or 7 64-bit))
- `libX11-`*`version`*`.el6.i686.rpm` (RHEL 6 or 7 64-bit)
- `libXext-`*`version`*`.el6.i686.rpm` (RHEL 6 or 7 64-bit)
- `libXi-`*`version`*`.el6.i686.rpm` (RHEL 6 or 7 64-bit)
- `libXtst-`*`version`*`.el6.i686.rpm` (RHEL 6 or 7 64-bit)
- `libstdc++-`*`version`*`.el6.i686.rpm` (RHEL 6 or 7 64-bit)
- `libgcc-`*`version`*`.el6.i686.rpm` (RHEL 6 or 7 64-bit)
- `libXrender-0.9.5-1.el6.i686.rpm` (RHEL 6 or 7 64-bit)

SUSE Linux Enterprise Server (64-bit)

You must install the following packages.

- `libstdc++33-32bit`
- (Conditional) For a guided installation of iManager on a server running SUSE Linux Enterprise Server (SLES) 12 SP1 or later platforms, ensure that the server has `libXtst6-32bit-1.2.1-4.4.1.x86_64`, `libXrender1-32bit`, and `libXi6-32bit` libraries installed.

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`)

SUSE Linux Enterprise Server (32-bit)

You must install the following packages.

- `libstdc++33`
- `libstdc++43`

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`)

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.

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)

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 NetIQ 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.

System Requirements for iManager Server

This section provides the minimum requirements for the server(s) where you want to install iManager. For more information about the server version of iManager, see "Understanding the Server and Client Versions of iManager" on page 208.

Also ensure that you review the prerequisites and considerations for installation, particularly those related to the operating system.

Category	Requirement
Processor	Pentium* III 600MHz
Disk space	**Linux**: 200 MB **Windows**: 500 MB
Memory	512 MB (1 GB recommended) 80 MB for iManager Plug-ins
Operating system	Identity Manager 4.6 supports two versions of eDirectory. Depending on the version you install, you must install a compatible version of iManager. ◆ iManager 3.0.2 Patch 1: For more information, see NetIQ iManager Installation Guide. ◆ iManager 2.7.7 Patch 9: For more information, see NetIQ iManager Installation Guide. **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.
Operating system hotfixes	NetIQ recommends that you apply the latest operating system patches according to the manufacturer's automated update facility.

Category	Requirement
Web browser	Any of the web browsers listed for your version of iManager in the NetIQ iManager Installation Guide. ◆ iManager 3.0.2 Patch 1: For more information, see NetIQ iManager Installation Guide. ◆ iManager 2.7.7 Patch 9: For more information, see NetIQ iManager Installation Guide.
Application server	Tomcat 8.5.x, or the version supplied with iManager **NOTE:** You can manually integrate an existing IIS or Apache web server infrastructure with iManager on a Windows server.
Directory services	NetIQ eDirectory 8.8.8 Patch 9 Hotfix 2 for iManager 2.7.7 Patch 9 or NetIQ eDirectory 9.0.2 Hotfix 2 for iManager 3.0.2 Patch 1
Default ports	8080, 8443, and 9009

System Requirements for iManager Workstation (Client Version)

This section provides the minimum requirements for the server(s) where you want to install iManager Workstation. For more information about the client version of iManager, see "Understanding the Server and Client Versions of iManager" on page 208.

Also ensure that you review the prerequisites and considerations for installation, particularly those related to the operating system.

Category	Requirement
Processor	Pentium* III 600MHz
Disk space	200 MB
Memory	256 MB (512 MB recommended)
Operating system	Identity Manager 4.6 supports two versions of eDirectory. Depending on the version you install, you must install a compatible version of iManager. ◆ iManager 3.0.2 Patch 1: For more information, see NetIQ iManager Installation Guide. ◆ iManager 2.7.7 Patch 9: For more information, see NetIQ iManager Installation Guide.
Web browser	Any of the web browsers listed for your version of iManager in the NetIQ iManager Installation Guide. ◆ iManager 3.0.2 Patch 1: For more information, see NetIQ iManager Installation Guide. ◆ iManager 2.7.7 Patch 9: For more information, see NetIQ iManager Installation Guide.

Category	Requirement
Operating system hotfixes	NetIQ recommends that you apply the latest operating system patches according to the manufacturer's automated update facility.
Application server	Tomcat 8.5.x, bundled with iManager Workstation
Software	Java 1.8.0_x or later, bundled with iManager Workstation
Default ports	8080, 8443, and 9009

23 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 “Prerequisites and Considerations for Installing iManager” on page 209.

To review the full installation process, see the “Planning to Install iManager” on page 207.

- “Installing iManager and iManager Workstation on Linux” on page 217
- “Installing iManager and iManager Workstation on Windows” on page 221
- “Installing iManager Silently” on page 224

Installing iManager and iManager Workstation on Linux

This section provides the steps for installing iManager and iManager Workstation on Linux servers and clients.You are recommended to install iManager on a separate workstation different from the Identity Manager server. To prepare for the installation, review the prerequisites and system requirements:

- **iManager**: “Considerations for Installing iManager on a Linux Platform” on page 210 and “System Requirements for iManager Server” on page 213
- **iManager Workstation**: “Considerations for Installing iManager Workstation on Linux Clients” on page 212 and “System Requirements for iManager Workstation (Client Version)” on page 214.
- Also see the Release Notes accompanying the release.

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 “Installing iManager Silently” on page 224.

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 “Installing iManager Silently” on page 224.

To install iManager on Linux:

1. Log in 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.

   For example, iManager 3.0.2 Patch 1 is located in the `<iso_extracted_directory>/products/iManager/installs/linux` directory and iManager 2.7.7 Patch 9 is located in the `<iso_extracted_directory>/products/iManager277/installs/linux` directory.
3. (Conditional) If you downloaded the iManager installation files from the NetIQ Downloads website, 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/products/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 "Configuring iManager for IPv6 Addresses after Installation" on page 231.
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 "Understanding Installation for iManager Plug-ins" on page 209.

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) 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 "Specifying an Authorized User for eDirectory" on page 231.
- 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, an then log in. For more information, see "Accessing iManager" in the *NetIQ iManager 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 "Installing iManager and iManager Workstation on Windows" on page 221.

---

23 Use the `chmod` command to change the permissions on the following InstallAnywhere files to `644` (read) to prevent modifications:

`/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.

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.

For example, iManager 3.0.2 Patch 1 is located in the `<iso_extracted_directory>/products/iManager/installs/win` directory and iManager 2.7.7 Patch 9 is located in the `<iso_extracted_directory>/products/iManager277/installs/win` directory.

2 (Conditional) If you downloaded the iManager installation files from the NetIQ Downloads website, 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_version_workstation_linux.tar.bz2
```

For example,

```
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 in 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" in the *NetIQ iManager 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.

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**: "Considerations for Installing iManager on a Linux Platform" on page 210.
- **iManager Workstation**: "Considerations for Installing iManager Workstation on Linux Clients" on page 212.
- Also see the Release Notes accompanying the release.

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 "Installing iManager Silently" on page 224.

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 in 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 NetIQ Downloads website, 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 \products\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" in the *NetIQ iManager 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 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 "Configuring iManager for IPv6 Addresses after Installation" on page 231.

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 "Understanding Installation for iManager Plug-ins" on page 209.

   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/products/iManager/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. Do not use `localhost`. 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 "Specifying an Authorized User for eDirectory" on page 231.
- 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, an then log in. For more information, see "Accessing iManager" in the *NetIQ iManager 2.7.7 Administration Guide*.

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 NetIQ Downloads website, 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" in the *NetIQ iManager 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.

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**: "Considerations for Installing iManager on a Linux Platform" on page 210.

- **iManager Workstation**: "Considerations for Installing iManager Workstation on Linux Clients" on page 212.
- Also see the Release Notes accompanying the release.

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 "Understanding Installation for iManager Plug-ins" on page 209.

`$LAUNCH_BROWSER$`

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 website.
- If you do not define a version for a module, the setup program installs any module that matches the `.npm` name.

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**: `./iManagerInstall`*`platform`*`.bin -i silent`
- **Windows**: `iManagerInstall.exe -i silent`

24 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.

- "Replacing the Temporary Self-Signed Certificates for iManager" on page 227
- "Configuring iManager for IPv6 Addresses after Installation" on page 231
- "Specifying an Authorized User for eDirectory" on page 231

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 NetIQ Certificate Server and to replace the temporary certificate. If you are using eDirectory, you can use NetIQ 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.

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/tomcat8/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 in to iManager.
   - **1b** Click **NetIQ 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-tomcat8 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/tomcat8/server.xml`. For example:

   ```
   <Connector className="org.apache.coyote.http11.Http11AprProtocol"
    port="8443" minProcessors="5" maxProcessors="75" enableLookups="true"
    acceptCount="100" debug="0" scheme="https" secure="true"
    useURIValidationHack="false" disableUploadTimeout="true">
      <Factory className="org.apache.coyote.http11.Http11AprProtocol"
    clientAuth="false" protocol="TLS" keystoreType="PKCS12"  keystoreFile="/var/
   opt/novell/novlwww/newtomcert.p12" keystorePass="password" />
   </Connector>
   ```

   Or,

```
<Connector className="org.apache.coyote.http11.Http11NioProtocol"
 port="8443" minProcessors="5" maxProcessors="75" enableLookups="true"
 acceptCount="100" debug="0" scheme="https" secure="true"
 useURIValidationHack="false" disableUploadTimeout="true">
   <Factory className="org.apache.coyote.http11.Http11NioProtocol"
 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-tomcat8 start
```

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 in to iManager.

   1b Click **NetIQ 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 website. 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 "Replacing the Temporary Self-Signed Certificates for iManager" on page 227.

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-tomcat8 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.http11.Http11AprProtocol"
 port="8443" minProcessors="5" maxProcessors="75" enableLookups="true"
 acceptCount="100" debug="0" scheme="https" secure="true"
 useURIValidationHack="false" disableUploadTimeout="true">
   <Factory className="org.apache.coyote.tomcat7.CoyoteServerSocketFactory"
 clientAuth="false" protocol="TLS" keystoreType="PKCS12"
 keystoreFile="/conf/ssl/newtomcert.p12" keystorePass="password" />
```

Or,

```
<Connector className="org.apache.coyote.http11.Http11NioProtocol"
 port="8443" minProcessors="5" maxProcessors="75" enableLookups="true"
 acceptCount="100" debug="0" scheme="https" secure="true"
 useURIValidationHack="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.

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/tomcat8/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.

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" in the *NetIQ iManager Administration Guide*.

1. Log in to iManager.
2. In the Configure view, select **iManager Server** > **Configure iManager** > **Security**.
3. Update the user credentials and tree name.

VIII Installing Designer for Identity Manager

This section guides you through the process of installing Designer for Identity Manager. By default, the installation program installs the components in the following locations:

- **Linux**: `/opt/netiq`
- **Windows**: `C:\NetIQ`

NetIQ recommends that you review the installation process before beginning. For more information, see Chapter 25, “Planning to Install Designer,” on page 235.

25 Planning to Install Designer

This section provides the prerequisites, considerations, and system setup needed to install Designer. First, consult the checklist to understand the installation process.

- "Checklist for Installing Designer" on page 235
- "Prerequisites for Installing Designer" on page 236
- "System Requirements for Designer" on page 236

Checklist for Installing Designer

Before beginning the installation, NetIQ recommends that you review the following steps:

	Checklist Items
❑	1. Review product architecture information to learn about the interaction among Identity Manager components. For more information, see "Designer for Identity Manager" on page 25.
❑	2. Decide which servers you want to use for your Identity Manager components. For more information, see "Recommended Installation Scenarios and Server Setup" on page 44.
❑	3. Review the considerations for installing Designer to ensure that the computer meets the prerequisites. For more information, see "Prerequisites for Installing Designer" on page 236.
❑	4. Ensure that the computer on which you are installing Designer meets the specified software and hardware requirements. For more information, see "System Requirements for Designer" on page 236.
❑	5. (Conditional) For computers running a SLES 12 SP1 or later operating system, ensure that you have installed the appropriate set of libraries for a guided installation. For more information, see "Installing Identity Manager on SLES 12 SP1 or Later Servers" on page 55.
❑	6. To install Designer, see one of the following sections: ◆ "Using the Installation Command on Linux" on page 239 ◆ "Running the Windows Executable File" on page 239 ◆ "Using the Silent Installation Process" on page 239
❑	7. Install the rest of the Identity Manager components.
❑	8. (Optional) To start a project for your Identity Manager solution, see the *NetIQ Designer for Identity Manager Administration Guide*.

Prerequisites for Installing Designer

This section provides the considerations and system requirements 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, 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 "Understanding Language Support" on page 51.
- (Conditional) For a guided installation on a server running SLES 12 SP1 or later platforms, ensure that the server has `libXtst6-32bit-1.2.1-4.4.1.x86_64`, `libXrender1-32bit`, and `libXi6-32bit` libraries installed.
- You cannot use Designer 2.1*x* 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.x workspaces are installed in the following directories by default:
  - **Linux**: `$HOME/designer_workspace`
  - **Windows 10 and Windows 7**: `%UserProfile%\designer_workspace` directory for
- To upgrade Designer and you are running workflow provisioning and provisioning with roles, review the upgrade procedure in "Migrating the User Application Driver" on page 521.

System Requirements for Designer

This section provides the minimum requirements for the server(s) where you want to install Designer. Ensure that you review the prerequisites and considerations for installation, particularly those related to the operating system.

Category	Requirement
Processor	1 GHz
Disk space	1 GB
Memory	1 GB

Category	Requirement
Operating system (certified)	One of the following 64-bit operating systems: **Servers** ◆ OpenSUSE 13.2 ◆ SUSE Linux Enterprise Server 12 SP1 ◆ SUSE Linux Enterprise Server 11 SP4 ◆ Windows Server 2012 R2 ◆ Windows Server 2012 ◆ Windows Server 2008 R2 ◆ Windows Server 2008 **Desktops** ◆ SUSE Linux Enterprise Desktop 11 SP4 ◆ SUSE Linux Enterprise Desktop 12 SP1 ◆ Windows 10 ◆ Windows 8 ◆ Windows 7 NetIQ recommends that you apply the latest operating system patches according to the manufacturer's automated update facility before you install Identity Manager. **NOTE:** *Certified* means that the operating system has been fully tested and is supported.
Operating system (supported)	Latest versions of service packs for the certified operating systems **NOTE:** *Supported* means that the operating system has not yet been tested but is expected to work
Virtualization system	◆ Hyper-V Server 2012 R2 ◆ VMWare ESX 5.0 and later ◆ Windows Server 2012 R2 Virtualization with Hyper-V (supported) NetIQ supports Identity Manager on enterprise-class virtualization systems that provide official support for the operating systems where NetIQ products are running. As long as the vendors of the virtualization systems officially support these operating systems, NetIQ supports the entire Identity Manager stack on them.
Web browser	Any of the following browsers, at a minimum: ◆ Internet Explorer 11 ◆ Chrome 51 ◆ Firefox 46

26 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. Use the installation program, located by default in the following directories:

- **Linux computers**: `/products/Designer/install`
- **Windows computers**: `\products\Designer\install.exe`

This section provides information about installing Designer in a new environment. For more information about upgrading Designer, see "Upgrading Designer" on page 469.

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

- "Using the Installation Command on Linux" on page 239
- "Running the Windows Executable File" on page 239
- "Using the Silent Installation Process" on page 239
- "Modifying an Installation Path that Includes a Space Character" on page 240

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`

Running the Windows Executable File

1. Log in 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.

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 in 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 *`Path_to_unzipped_Designer_files`*`/products/Designer` directory.

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`

Modifying an Installation Path that Includes a Space Character

You can install Designer to a location that includes spaces in the directory names. However, after you install Designer, you must modify the `StartDesigner.sh` and `Designer.ini` files to ensure that Designer functions properly. Manually replace the space with an escape character (“\”). For example:

Change

```
root/designer installation
```

to

```
root/designer\ installation
```

IX Installing PostgreSQL and Tomcat for Identity Manager

In this section, you will install the following application server and database programs that are used by most of the Identity Manager components:

- Apache Tomcat
- PostgreSQL

The installation files are located in the `products/RBPM/` directory in the Identity Manager installation package. By default, the installation program installs the applications in their respective directories in the following locations:

- **Linux**: `/opt/netiq/idm/apps/`
- **Windows**: `C:\netiq\idm\apps\`

NetIQ recommends that you review the installation process before beginning. For more information, see "Checklist for Installing Tomcat and PostgreSQL" on page 243.

27 Planning to Install PostgreSQL and Tomcat

Identity Manager 4.6 supports only Apache Tomcat as an application server. If your company provides a supported version of Tomcat, you can use it with Identity Manager.

Alternatively, NetIQ bundles Tomcat and PostgreSQL in the same installation program for your convenience. This installer lets you install these applications without downloading them separately. NetIQ does not provide updates for these components, or administration, configuration, or tuning information beyond what is outlined in the NetIQ Identity Manager documentation.

- "Checklist for Installing Tomcat and PostgreSQL" on page 243
- "Understanding the Installation Process for PostgreSQL and Tomcat" on page 244
- "Prerequisites for Installing PostgreSQL" on page 244
- "Prerequisites for Installing Tomcat" on page 245
- "System Requirements for PostgreSQL" on page 245
- "System Requirements for Tomcat" on page 245

Checklist for Installing Tomcat and PostgreSQL

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

	Checklist Items
❑	1. Learn about the interaction among Identity Manager components. For more information, see the following sections: ◆ "Using Single Sign-on Access in Identity Manager" on page 37 ◆ "Using Self-Service Password Management in Identity Manager" on page 35
❑	2. Decide which servers you want to use for your Identity Manager components. For more information, see "Recommended Server Setup" on page 46.
❑	3. Decide whether you should install NetIQ Sentinel before installing Tomcat or PostgreSQL. For more information, see "Recommended Installation Scenarios and Server Setup" on page 44.
❑	4. Review the considerations for installing the applications to ensure that the computers meet the requirements: ◆ "Prerequisites for Installing Tomcat" on page 245 ◆ "Prerequisites for Installing PostgreSQL" on page 244
❑	5. (Conditional) For computers running a SLES 12 SP1 or later operating systemFor computers running a SLES 12 SP1 or later operating system, ensure that you have installed the appropriate set of libraries for a guided installation. For more information, see "Installing Identity Manager on SLES 12 SP1 or Later Servers" on page 55.

	Checklist Items
❑	6. (Conditional) For computers running an RHEL 6.x or RHEL 7.x operating system, ensure that you have installed the appropriate set of libraries. For more information, see "Installing Identity Manager on RHEL 6.x or 7.x Servers" on page 55.
❑	7. Install the applications: ◆ For a guided installation, see "Using the Wizard to Install PostgreSQL and Tomcat" on page 247. ◆ For a silent installation, see "Silently Installing Tomcat and PostgreSQL for Identity Manager" on page 249.
❑	8. Install the rest of the Identity Manager components.

Understanding the Installation Process for PostgreSQL and Tomcat

You can choose to install one or both of the applications. For example, you might not need PostgreSQL because you already have a supported version of the application on the server. The following considerations apply to the individual installations:

PostgreSQL

The installation process installs the database for the identity applications and creates an administrative user called `idmadmin` to own the database. However, the installation does not create the schema in the database for the identity applications. Schema information gets added when you install the identity applications.

If you already have a supported version of PostgreSQL running on the server, the installation program prompts you for the password for the default `postgres` user. The program then creates the `idmadmin` user and assigns it the same password as for `postgres`.

At the end of the process, the installation program starts the database instance. The instance must be running when you install other Identity Manager components that use the database, such as the User Application.

You are not required to use PostgreSQL for the database for identity applications.

Tomcat

The installation process creates the IDM Apps Tomcat Service. To support the Tomcat application server, the installation program also installs Apache ActiveMQ and Oracle JRE. These items help Tomcat send email notifications.

The installation program does not start Tomcat upon completion. Tomcat must be stopped before you install other Identity Manager components, such as Identity Reporting.

Prerequisites for Installing PostgreSQL

Review the following considerations before planning the PostgreSQL installation:

- You can install the version of PostgreSQL bundled with Identity Manger in an environment that runs an older version of the database program. To ensure that the new installation does not overwrite the previous version, specify a different directory for the files.

- The identity applications apply some prerequisites to the database they use, such as PostgreSQL. For more information, see "Prerequisites for Installing the Database for the Identity Applications" on page 286.
- (Conditional) On Windows, you cannot install more than one version of PostgreSQL because the service account for Postgres does not handle both instances. Uninstall the old version before installing this version of Postgres.

Prerequisites for Installing Tomcat

Review the following considerations before planning the Tomcat installation:

- You can install Tomcat and PostgreSQL on the same server or on separate servers.
- The installation process installs supported versions of Oracle JRE and Apache ActiveMQ.
- The installation process also installs the files required for the Apache Log4j service to audit Tomcat events.
- You can use your own Tomcat installation program instead of the one provided in the Identity Manager installation kit. However, to use the Apache Log4j service with your version of Tomcat, ensure that you have the appropriate files installed. For more information, see "Using the Apache Log4j Service to Log Sign-on" on page 254. This requirement applies to using Tomcat for OSP, the identity applications, and Identity Reporting.
- To have guaranteed delivery of email notifications with ActiveMQ, install MQServer.
- The identity applications apply some prerequisites to the Tomcat application server on which they run. For more information, see "Prerequisites and Considerations for the Application Server" on page 284.
- The installation process sets the JRE location in the `setenv.sh` file, located by default in the `/opt/netiq/idm/apps/tomcat/bin/` directory. When you install the identity applications and Identity Reporting on Tomcat, the process updates the `JAVA_OPTs` or `CATALINA_OPTS` entries in the `setenv.sh` file.
- Do not run Tomcat as `root`. The installation process creates a user account for the Tomcat service, which should not be `root`.

System Requirements for PostgreSQL

PostgreSQL has the same computer requirements as for the identity applications. For more information, see "System Requirements for the Identity Applications" on page 287. Also see the release notes for the latest version of Identity Manager and the PostgreSQL documentation.

System Requirements for Tomcat

Tomcat has the same computer requirements as for the identity applications. For more information, see "System Requirements for the Identity Applications" on page 287. Also see the release notes for the latest version of Identity Manager and the Apache documentation.

28 Installing PostgreSQL and Tomcat

This section guides you through the process of installing Tomcat and PostgreSQL.

- "Using the Wizard to Install PostgreSQL and Tomcat" on page 247
- "Silently Installing Tomcat and PostgreSQL for Identity Manager" on page 249

Using the Wizard to Install PostgreSQL and Tomcat

The following procedure describes how to install Tomcat and PostgreSQL on a Linux or Windows platform using a guided process, either in the GUI format or from the console. To perform a silent, unattended installation, see "Silently Installing Tomcat and PostgreSQL for Identity Manager" on page 249.

To prepare for the installation, review the considerations and system requirements listed in the following sections:

- "Prerequisites for Installing Tomcat" on page 245
- "Prerequisites for Installing PostgreSQL" on page 244
- Release Notes accompanying the release

NOTE: Whether you install PostgreSQL or use an existing version of PostgreSQL, you must specify passwords for the database. However, this installation program does not support passwords that include a `"` or `$` character. To use these special characters, change the password after you complete the installation process.

To perform a guided installation:

1. Log in as `root` or an administrator to the computer where you want to install the applications.
2. Ensure that the planned installation path does not include directories with any of the following names:
   - tomcat
   - postgres
   - activemq
   - jre
3. (Conditional) If you have the `.iso` image file for the Identity Manager installation package, navigate to the directory containing the installation files:
   - **Linux**: `products/RBPM/postgre_tomcat_install/`
   - **Windows**: `products/RBPM/postgre_tomcat_install`
4. (Conditional) If you downloaded the installation files from the NetIQ Downloads website, complete the following steps:
   - **4a** Navigate to the `.tgz` or `win.zip` file for the downloaded image.
   - **4b** Extract the contents of the file to a directory on the local computer.

5 From the directory that contains the installation files, complete one of the following actions:
   - **Linux (console)**: Enter `./TomcatPostgreSQL.bin -i console`
   - **Linux (GUI)**: Enter `./TomcatPostgreSQL.bin`
   - **Windows**: Run `TomcatPostgreSQL.exe`
6 In the installation program, specify the language that you want to use for installation, and then click **OK**.
7 Review the introductory information, and then click **Next**.
8 Accept the License Agreement, and then click **Next**.
9 Specify whether you want to install Tomcat, PostgreSQL, or both.
10 To complete the guided process, specify values for the following parameters:
   - **Tomcat parent folder**

     Applies only when installing Tomcat.

     Specifies the directory where you want to install the Tomcat files.
   - **Tomcat details**

     Applies only when installing Tomcat.

     Represents the ports needed for Tomcat.

     Tomcat shutdown port

     Specifies the port that you want to use for cleanly shutting down all webapps and Tomcat. The default is 8005.

     Tomcat http port

     Specifies the port that you want the Tomcat server to use for communication with client computers. The default is 8080. To use SSL, the default is 8443.

     Tomcat redirect port

     (Conditional) When you do not use TLS/SSL protocols, specifies the port to which the application server redirects requests that require SSL transport. The default value is 8443.

     Tomcat ajp port

     (Optional) Specifies the port that you want the application server to use for communication with a web connector using the AJP protocol instead of `http`. The default value is 8009.

     Use this parameter when you want the application server to manage the static content contained in the web application, and/or utilize the application server's SSL processing.
   - **PostgreSQL parent folder**

     Applies only when installing PostgreSQL.

     Represents the directory where you want to install the PostgreSQL files.
   - **PostgreSQL details**

     Applies only when installing PostgreSQL.

     Represents the settings for the PostgreSQL database for the identity applications.

     NOTE: If you already have a supported version of PostgreSQL running on the server, the installation program prompts you for the password for the default `postgres` user. The program then creates the `idmadmin` user and assigns it the same password as for `postgres`.

     This installation program does not support passwords that include a `"` or `$` character.

Database name

Specifies the name of the database. The default value is `idmuserappdb`.

Database admin

Specifies the `idmadmin` account, which is a database administrator that can create database tables, views, and other artifacts.

This account is not the same as the default postgres user.

Password for admin user

Specifies the password for the database administrator and the default `postgres` user.

This installation program does not support passwords that include a `"` or `$` character.

PostgreSQL port

Specifies the port of the server that hosts the Postgres database. The default value is 5432.

11 Review the pre-installation summary.

12 Start the installation process.

13 When the installation process completes, click *Done*.

Silently Installing Tomcat and PostgreSQL for Identity Manager

A silent (non-interactive) installation does not display a user interface or ask the user any questions. Instead, InstallAnywhere uses information from a default `silent.properties` file. You can run the silent installation with the default file or edit the file to customize the installation process. For a guided installation, see "Using the Wizard to Install PostgreSQL and Tomcat" on page 247.

To prepare for the installation, review the considerations and system requirements listed in the following sections:

- "Prerequisites for Installing Tomcat" on page 245
- "Prerequisites for Installing PostgreSQL" on page 244
- "Safeguarding the Passwords for a Silent Installation" on page 249
- Release Notes accompanying the release

Safeguarding the Passwords for a Silent Installation

If you do not want to specify the passwords in the `silent.properties` file for the 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 installation:

- NETIQ_DB_PASSWORD
- NETIQ_DB_PASSWORD_CONFIRM

Linux

Use the `export` command. For example:

```
export NETIQ_DB_PASSWORD_CONFIRM=myPassWord
```

Windows

Use the `set` command. For example:

```
set NETIQ_DB_PASSWORD_CONFIRM=myPassWord
```

The installation program does not support passwords that include a " for $ character. To use these special characters, change the password after installing PostgreSQL.

Silently Installing Tomcat and PostgreSQL

1. Log in to the computer where you want to install the applications.
2. (Conditional) If you have the `.iso` image file for the Identity Manager installation package, navigate to the directory containing the installation files:
   - **Linux**: `products/RBPM/postgre_tomcat_install`
   - **Windows**: `products/RBPM/postgre_tomcat_install`
3. (Conditional) If you downloaded the installation files from the NetIQ Downloads website, 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 directory on the local computer.
4. To specify the installation parameters, complete the following steps:
   - **4a** Ensure that the `silent.properties` file is located in the same directory as the execution file for installation.
   - **4b** In a text editor, open the `silent.properties` file.
   - **4c** Specify the parameter values. For a description of the parameters, see Step 10 on page 248.

     NOTE: To use an existing PostgreSQL database for your User Application on a Linux server, specify `installed` for `NETIQ_USE_INSTALLED_POSTGRES`. The database instance must be run by a supported version of PostgreSQL. Also, you do not need to configure the database.

   - **4d** Save and close the file.
5. To launch the installation process, enter one of the following commands:
   - **Linux**: `TomcatPostgreSQL.bin -i silent -f silent.properties`
   - **Windows**: `install -i silent -f silent.properties`

NOTE: If the `silent.properties` file resides in a different directory from the installation 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.

X Installing the Single Sign-on Component

In this section, you will install One SSO Provider (OSP) to support single sign-on access to the identity applications and Identity Reporting.

The installation files are located in the `products/RBPM/osp_install` directory in the Identity Manager installation package. By default, the installation program installs the components in the following locations:

- **Linux**: `/opt/netiq/idm/apps/osp`
- **Windows**: `C:\netiq\idm\apps\osp`

NetIQ recommends that you review the installation process before beginning.

29 Planning to Install Single Sign-on for Identity Manager

This section provides information prerequisites, considerations, and system setup that are needed to install One SSO Provider (OSP).

- "Checklist for Single Sign-on Component" on page 253
- "Prerequisites for Installing One SSO Provider" on page 254
- "System Requirements for One SSO Provider" on page 254
- "Using the Apache Log4j Service to Log Sign-on" on page 254

Checklist for Single Sign-on Component

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

	Checklist Items
❑	1. Learn about the interaction among Identity Manager components. For more information, see "Using Single Sign-on Access in Identity Manager" on page 37.
❑	2. Decide which servers you want to use for your Identity Manager components. For more information, see "Recommended Installation Scenarios and Server Setup" on page 44.
❑	3. Ensure that Tomcat has been installed. For more information, see Chapter 28, "Installing PostgreSQL and Tomcat," on page 247.
❑	4. (Conditional) To use the Apache Log4j service to record events in Tomcat, ensure that you have the appropriate files. For more information, see "Using the Apache Log4j Service to Log Sign-on" on page 254.
❑	5. (Conditional) For computers running a SLES 12 SP1 or later operating system, ensure that you have installed the appropriate set of libraries for a guided installation. For more information, see "Installing Identity Manager on SLES 12 SP1 or Later Servers" on page 55.
❑	6. (Conditional) For computers running an RHEL 6.x or RHEL 7.x operating system, ensure that you have installed the appropriate set of libraries. For more information, see "Installing Identity Manager on RHEL 6.x or 7.x Servers" on page 55.
❑	7. Install OSP: ◆ For a guided installation, see "Using the Wizard to Install One SSO Provider" on page 257. ◆ For a silent installation, see "Silently Installing One SSO Provider" on page 260.
❑	8. Install Self Service Password Reset (SSPR) to manage user passwords for Identity applications. For more information, see Part XI, "Installing the Password Management Component," on page 263.
❑	9. Install and configure the identity applications to use single sign-on access. For more information, see Part XII, "Installing the Identity Applications," on page 277.

Prerequisites for Installing One SSO Provider

The following Identity Manager components require OSP for user authentication:

- Identity Applications
- Identity Reporting

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

- To run OSP, you can use your own Tomcat installation program instead of the one provided in the Identity Manager installation kit. However, to use the Apache Log4j service with your version of Tomcat, ensure that you have the appropriate files installed. For more information, see "Using the Apache Log4j Service to Log Sign-on" on page 254.
- You can configure OSP to work with NetIQ Access Manager 4.0 using SAML 2.0 authentication. For more information, see Chapter 49, "Using SAML Authentication with NetIQ Access Manager for Single Sign-on," on page 423.
- OSP requires trust certificates to ensure that the identity applications and reporting can communicate with the authentication server. The installation process automatically creates a certificate for TLS/SSL in the `osp.jks` file. You can also have the process create the Trusted Root Certificate for a SAML Assertion to eDirectory.

  NOTE: These certificates expire two years after their creation date. You must create new certificates when the original ones expire. For more information, see "Authentication Server" on page 350 and Part XV, "Configuring Single Sign-on Access in Identity Manager," on page 417.

System Requirements for One SSO Provider

OSP requires Apache Tomcat application server. The version of Tomcat must be the same as required for the identity applications.

All other server requirements match the server requirements for the identity applications. For more information, see "Prerequisites and Considerations for Installing the Identity Applications" on page 282 and the most recent Release Notes for this version.

Using the Apache Log4j Service to Log Sign-on

You can use either the Apache Log4j or java.util.logging service to record events that occur in Tomcat. The Tomcat installer in the Identity Manager installation kit includes the files that you need for Log4j. However, if you install your own version of Tomcat, you need the following files to use the Apache logging service:

- `log4j-1.2.16.jar`
- `tomcat-juli-adapters.jar`
- `tomcat-juli.jar`

To add the files to your Tomcat installation, complete the following steps:

1. Download the "JULI" files for Tomcat v8.5.x from the Apache website:
   - `tomcat-juli.jar`
   - `tomcat-juli-adapters.jar`
2. Download the `log4j-1.2.16.jar` file from the Apache website.

3 Place the following files in the `$TOMCAT_HOME/lib` directory:

- `log4j-1.2.16.jar`
- `tomcat-juli-adapters.jar`

4 Place the `tomcat-juli.jar` file in the `$TOMCAT_HOME/bin` directory.

5 Specify a value for `-Dlog4j.configuration` in `CATALINA_OPTS` or create a `log4j.properties` file in the `$TOMCAT_HOME/lib` directory.

30 Installing Single Sign-on for Identity Manager

- "Using the Wizard to Install One SSO Provider" on page 257
- "Silently Installing One SSO Provider" on page 260
- "Configuring Single Sign-on Access" on page 260

Using the Wizard to Install One SSO Provider

The following procedure describes how to install OSP 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 "Silently Installing One SSO Provider" on page 260. To prepare for the installation, review the prerequisites and system requirements listed in "Checklist for Single Sign-on Component" on page 253.

1. Log in as `root` or an administrator to the server where you want to install OSP.
2. Stop the Tomcat server.
3. (Conditional) If you have the `.iso` image file for the Identity Manager installation package, navigate to the directory containing the OSP installation files, located by default in the `products/rbpm/osp_install` directory.
4. (Conditional) If you downloaded the OSP installation files, complete the following steps:
   - **4a** Navigate to the `.tgz` or `win.zip` file for the downloaded image.
   - **4b** Extract the contents of the file to a directory on the local computer.
5. From the directory that contains the installation files, complete one of the following actions:
   - **Linux (GUI)**: Enter `./osp-install-linux.bin`
   - **Windows**: Run `osp-install.exe`
6. Read and accept the license agreement, and then click **Next**.
7. Specify a path for the installed files.
8. Complete the guided process, using the following parameters:
   - **Tomcat details**

     Represents the home directory for the Tomcat server. For example, `/opt/netiq/idm/apps/tomcat`. The installation process adds some files for OSP to this folder.
   - **Tomcat Java home**

     Represents the home directory for Java on the Tomcat server. For example, `/usr/lib/jvm/default-java`. The installation process adds some files for OSP to the directory.
   - **Application address**

     Represents the settings of the URL that users need to connect to OSP on the Tomcat server. For example, `https://myserver.mycompany.com:8543`.

     Protocol

     Specifies whether you want to use *http* or *https*. To use Secure Sockets Layer (SSL) for communications, specify `https`.

Host Name

Specifies the DNS name or IP address of the server where you are installing OSP. Do not use `localhost`.

Port

Specifies the port that you want the server to use for communication with client computers.

- **Login Screen Customization**

  Specifies the custom name that you want to display on user login screen. The default value is **NetIQ Access**.

NOTE: By default, `Latin1 Standard character set` is supported. To support extended characters, first complete the installation and then perform the steps from Customizing Strings for OSP.

- **Authentication details**

  Represents the requirements for connecting to the authentication server which contains the list of users who can log in to the application. For more information about the authentication server, see "Understanding Authentication with One SSO Provider" on page 37.

LDAP host

Specifies the DNS name or IP address of the LDAP authentication server. Do not use `localhost`.

LDAP port

Specifies the port that you want the LDAP authentication server to use for communication with Identity Manager. For example, specify `389` for a non-secure port or `636` for SSL connections.

Use SSL

Specifies whether you want to use Secure Sockets Layer protocol for connections between the Identity Vault and the authentication server.

JRE Trust store (cacerts) file

Applies only when you want to use SSL for the LDAP connection.

Specifies the path to the certificate. For example, `C:\netiq\idm\apps\jre\lib\security\cacerts`.

JRE Trust store password

Applies only when you want to use SSL for the LDAP connection.

Specifies the password for the `cacerts` file.

Admin DN

Applies only when installing a new authentication server.

Specifies the DN for an administrator account of the LDAP authentication server. For example, `cn=admin,ou=sa,o=system`.

Admin password

Applies only when installing a new authentication server.

Specifies the password for the administrator account of the LDAP authentication server.

User container

Applies only when installing a new authentication server.

Specifies the container in the LDAP authentication server where you store the user accounts that can log in to Access Review. For example, `o=data`.

Admin container

Applies only when installing a new authentication server.

Specifies the container in the LDAP authentication server where you store the administrator accounts. For example, `ou=sa,o=system`.

Identity Vault

Specifies your Identity Vault.

Keystore Password

Applies only when installing a new authentication server.

Specifies the password that you want to create for the new keystore for the LDAP authentication server.

The password must be a minimum of six characters.

- **Auditing details (OSP)**

Represents the settings for auditing OSP events that occur in the authentication server.

(Conditional) *Enable auditing for OSP*

Specifies whether you want to send OSP events to an auditing server.

If you select this setting, also specify the location for the audit log cache.

Audit log cache folder

Applies only when you enable auditing for OSP.

Specifies the location of the cache directory that you want to use for auditing. For example, `/var/opt/novell/naudit/jcache`.

Specify existing certificate / Generate a certificate

Indicates whether you want to use an existing certificate for the NAudit server or create a new one.

Enter Public key

Applies only when you want to use an existing certificate.

Lists the custom public key certificate that you want the NAudit service to use to authenticate audit messages.

Enter RSA Key

Applies only when you want to use an existing certificate.

Specifies the path to the custom private key file that you want the NAudit service to use to authenticate audit messages.

9 To install SSPR, continue to Part XI, “Installing the Password Management Component,” on page 263.

For more information about configuring forgotten password management, see “Configuring Forgotten Password Management” on page 333.

Silently Installing One SSO Provider

A silent (non-interactive) installation does not display a user interface or ask the user any questions.

1. Log in as `root` or an administrator to the computer where you want to install the components.
2. Stop Tomcat.
3. (Conditional) If you have the `.iso` image file for the Identity Manager installation package, navigate to the directory containing the OSP installation files, located by default in the `osp` directory.
4. (Conditional) If you downloaded the installation files from the NetIQ Downloads website, complete the following steps:
   - **4a** Navigate to the `.tgz` or `.zip` file for the downloaded image.
   - **4b** Extract the contents of the file to a folder on the local computer.
5. Copy the `osp.configure.properties` file on to the location where you have write access and edit this file.

   For more information about the settings for installation, see Step 7 and Step 8 on page 257.
6. To run the silent installation, issue one of the following commands:
   - **Linux**: `osp-install-linux.bin -i silent -f` *`path_to_silent.properties_file`*
   - **Windows**: `osp-install-win.exe -i silent -f` *`path_to_silent.properties_file`*

   In this command, specify the absolute path of the file. For example:
   - **Linux:** `osp-install-linux.bin -i silent -f` *`/tmp/osp.configure.properties`*
   - **Windows:** `osp-install-win.exe -i silent -f` *`c:\opt\netiq\idm\apps\osp\osp.configure.properties`*
7. Install SSPR. For more information, see Part XI, “Installing the Password Management Component,” on page 263.

Configuring Single Sign-on Access

You can perform some steps to configure single sign-on access immediately after installing OSP. However, the final configuration process requires that first you install the identity applications. For more information, see Part XV, “Configuring Single Sign-on Access in Identity Manager,” on page 417.

NOTE: While configuration the One SSO Provider in silent mode, ensure to specify the correct path for install, Java, Tomcat and SSL Keystore folders in the `osp.configure.properties` file. For example,

Install Folder:

- **Linux**: `USER_INSTALL_DIR=/opt/netiq/idm/apps/osp`
- **Windows**: `USER_INSTALL_DIR=C:\netiq\idm\apps\osp`

Tomcat Folder:

- **Linux**: `NETIQ_TOMCAT_HOME=/opt/netiq/idm/apps/tomcat`
- **Windows**: `NETIQ_TOMCAT_HOME=C:\netiq\idm\apps\tomcat`

Java Folder:

- **Linux**: `NETIQ_JAVA_HOME=/opt/netiq/idm/apps/jre`
- **Windows**: `NETIQ_JAVA_HOME=C:\netiq\idm\apps\jre`

SSL Keystore Folder:

- **Linux**: `NETIQ_SSL_KEYSTORE_FILE=/opt/netiq/idm/apps/jre/lib/security/cacerts`
- **Windows**: `USER_INSTALL_DIR=C:\netiq\idm\apps\jre\lib\security\cacerts`

XI Installing the Password Management Component

In this section, you will install Self Service Password Reset (SSPR) that helps you configure Identity Manager to allow users to reset their passwords.

SSPR integrates with the identity applications, identity reporting, and OSP to ensure that users who need to modify their passwords get directed to the appropriate web pages without performing any additional actions. After users complete their self-service activities, SSPR redirects users to the application that they original attempted to access.

NOTE: Identity Manager 4.6 and above version uses SSPR as a primary Password Management Tool.

Identity Manager does not require SSPR. You can use an alternative method for resetting user passwords.However, you might need to modify some configuration settings for Identity Manager. For more information, see "Configuring Forgotten Password Management" on page 333.

The installation files are located in the `products/RBPM/sspr_install` directory. By default, the installation program installs the components in the following locations:

- **Linux**: `/opt/netiq/idm/apps/sspr`
- **Windows**: `C:\netiq\idm\apps\sspr`

NetIQ recommends that you review the installation process before beginning.

31 Planning to Install Password Management for Identity Manager

This section provides information prerequisites, considerations, and system setup that are needed to install Self Service Password Reset (SSPR).

- "Checklist for Installing Password Management Components" on page 265
- "Prerequisites for Installing Self Service Password Reset" on page 266
- "System Requirements for Self Service Password Reset" on page 266
- "Using the Apache Log4j Service for Password Event" on page 266

Checklist for Installing Password Management Components

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

	Checklist Items
❑	1. Learn about the interaction among Identity Manager components. For more information, see "Using Self-Service Password Management in Identity Manager" on page 35.
❑	2. Decide which servers you want to use for your Identity Manager components. For more information, see "Recommended Installation Scenarios and Server Setup" on page 44.
❑	3. Ensure that Tomcat has been installed. For more information, see Chapter 28, "Installing PostgreSQL and Tomcat," on page 247.
❑	4. (Conditional) To use the Apache Log4j service to record events in Tomcat, ensure that you have the appropriate files. For more information, see "Using the Apache Log4j Service to Log Sign-on" on page 254.
❑	5. (Conditional) For computers running a SLES 12 SP1 or later operating system, ensure that you have installed the appropriate set of libraries for a guided installation. For more information, see "Installing Identity Manager on SLES 12 SP1 or Later Servers" on page 55.
❑	6. (Conditional) For computers running an RHEL 6.x or RHEL 7.x operating system, ensure that you have installed the appropriate set of libraries. For more information, see "Installing Identity Manager on RHEL 6.x or 7.x Servers" on page 55.
❑	7. Install SSPR: ◆ For a guided installation, see "Using the Wizard to Install Self Service Password Request" on page 267. ◆ For a silent installation, see "Silently Installing Self Service Password Reset" on page 270.
❑	8. Install and configure the identity applications to use single sign-on access and password management. For more information, see Part XII, "Installing the Identity Applications," on page 277.

Prerequisites for Installing Self Service Password Reset

Your installation of NetIQ Self Service Password Reset (SSPR) should match the server requirements for the identity applications, with the following considerations:

- SSPR requires TSL/SSL protocol for communication.
- SSPR requires a supported version of the Tomcat application server. For more information, see "Prerequisites for Installing Tomcat" on page 245 and the most recent Release Notes for this version.
- NetIQ recommends that you review the prerequisites and requirements listed in the *NetIQ Self Service Password Reset Administration Guide*.

System Requirements for Self Service Password Reset

SSPR requires Apache Tomcat application server. The version of Tomcat must be the same as required for the identity applications.

All other server requirements match the server requirements for the identity applications. For more information, see "Prerequisites and Considerations for Installing the Identity Applications" on page 282 and the most recent Release Notes for this version.

Using the Apache Log4j Service for Password Event

You can use either the Apache Log4j or java.util.logging service to record events that occur in Tomcat. The Tomcat installer in the Identity Manager installation kit includes the files that you need for Log4j. However, if you install your own version of Tomcat, you need the following files to use the Apache logging service:

- `log4j-1.2.16.jar`
- `tomcat-juli-adapters.jar`
- `tomcat-juli.jar`

To add the files to your Tomcat installation, complete the following steps:

1. Download the "JULI" files for Tomcat v8.5.x from the Apache website:
   - `tomcat-juli.jar`
   - `tomcat-juli-adapters.jar`
2. Download the `log4j-1.2.16.jar` file from the Apache website.
3. Place the following files in the `$TOMCAT_HOME/lib` directory:
   - `log4j-1.2.16.jar`
   - `tomcat-juli-adapters.jar`
4. Place the `tomcat-juli.jar` file in the `$TOMCAT_HOME/bin` directory.
5. Specify a value for `-Dlog4j.configuration` in `CATALINA_OPTS` or create a `log4j.properties` file in the `$TOMCAT_HOME/lib` directory.

32 Installing Password Management for Identity Manager

This section describes the installation process for SSPR. You can install these programs on the same server where OSP component is installed or on the separate server.

- "Using the Wizard to Install Self Service Password Request" on page 267
- "Silently Installing Self Service Password Reset" on page 270
- "Post-Installation Tasks" on page 271
- "Configuring OSP and SSPR for Clustering" on page 273

NOTE: If you use the legacy forgot password method, you do not need to install SSPR. For more information, see "Understanding the Legacy Password Management Provider" on page 36.

Using the Wizard to Install Self Service Password Request

The following procedure describes how to install SSPR 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 "Silently Installing Self Service Password Reset" on page 270. To prepare for the installation, review the prerequisites and system requirements listed in "Checklist for Installing Password Management Components" on page 265.

1. Log in as `root` or an administrator to the server where you want to install SSPR.
2. Stop the Tomcat server.
3. (Conditional) If you have the `.iso` image file for the Identity Manager installation package, navigate to the directory containing the SSPR installation files, located by default in the `products/rbpm/sspr_install` directory.
4. (Conditional) If you downloaded the SSPR installation files, complete the following steps:
   - **4a** Navigate to the `.tgz` or `win.zip` file for the downloaded image.
   - **4b** Extract the contents of the file to a directory on the local computer.
5. From the directory that contains the installation files, complete one of the following actions:
   - **Linux (GUI)**: Enter `./sspr-install-linux.bin`
   - **Windows**: Run `sspr-install.exe`
6. Read and accept the license agreement, and then click **Next**.
7. Specify a path for the installed files.
8. Complete the guided process, using the following parameters:
   - **Tomcat details**

     Represents the home directory for the Tomcat server. For example, `/opt/netiq/idm/apps/tomcat`. The installation process adds some files for SSPR to this folder.

- **Tomcat connection**

  Represents the settings of the URL that users need to connect to SSPR on the Tomcat server. For example, `https://myserver.mycompany.com:8080`.

  NOTE: You must also select **Connect to an external authentication server** and specify values for the external server if the following considerations are true:

  - You are installing SSPR.
  - OSP runs on a different instance of the supported application server than SSPR does.

  Protocol

  Specifies whether you want to use *http* or *https*. To use Secure Sockets Layer (SSL) for communications, specify `https`.

  Host Name

  Specifies the DNS name or IP address of the server where you are installing SSPR. Do not use `localhost`.

  Port

  Specifies the port that you want the server to use for communication with client computers.

  Connect to an external authentication server

  Specifies whether a different instance of Tomcat hosts the authentication server (OSP). The authentication server contains the list of users who can log in to SSPR.

  If you select this setting, also specify values for the authentication server's **Protocol**, **Host name**, and **Port**.

- **Tomcat Java home**

  Represents the home directory for Java on the Tomcat server. For example, `/opt/netiq/idm/jre`. The installation process adds some files for OSP to the directory.

- **Authentication details**

  Represents the requirements for connecting to the authentication server which contains the list of users who can log in to the application. For more information about the authentication server, see "Understanding Authentication with One SSO Provider" on page 37.

  LDAP host

  Specifies the DNS name or IP address of the LDAP authentication server. Do not use `localhost`.

  LDAP port

  Specifies the port that you want the LDAP authentication server to use for communication with Identity Manager. For example, specify `389` for a non-secure port or `636` for SSL connections.

  Use SSL

  Specifies whether you want to use Secure Sockets Layer protocol for connections between the Identity Vault and the authentication server.

  JRE Trust store (cacerts) file

  Applies only when you want to use SSL for the LDAP connection.

  Specifies the path to the certificate. For example, `C:\netiq\idm\apps\jre\lib\security\cacerts`.

JRE Trust store password

Applies only when you want to use SSL for the LDAP connection.

Specifies the password for the `cacerts` file.

Admin DN

Applies only when installing a new authentication server.

Specifies the DN for an administrator account of the LDAP authentication server. For example, `cn=admin,ou=sa,o=system`.

Admin password

Applies only when installing a new authentication server.

Specifies the password for the administrator account of the LDAP authentication server.

User container

Applies only when installing a new authentication server.

Specifies the container in the LDAP authentication server where you store the user accounts that can log in to Access Review. For example, `o=data`.

Admin container

Applies only when installing a new authentication server.

Specifies the container in the LDAP authentication server where you store the administrator accounts for Access Review. For example, `ou=sa,o=system`.

Keystore Password

Applies only when installing a new authentication server.

Specifies the password that you want to create for the new keystore for the LDAP authentication server.

The password must be a minimum of six characters.

- **SSPR details**

  Represents the settings required for configuring SSPR.

  Configuration password

  Specifies the password that you want to create for an administrator to use to configure SSPR.

  By default, SSPR does not have a configuration password. Without the password, any user who can log in to SSPR can also modify the configuration settings.

  SSPR redirect URL

  Specifies the absolute URL to which the client will redirect when actions such as password changes or challenge questions have been completed in SSPR. For example, forward to the Dashboard.

  Use the following format: `protocol://server:port/path`. For example, `http://idm_userapp_server_ip:port_no/idmdash/#/landing`.

- **Authentication server details**

  Represents the password that you want to create for the SSPR service to use when connecting to the OSP client on the server. Also referred to as the client secret.

  To modify this password after installation, use the RBPM Configuration utility.

- **Auditing details (SSPR)**

  Represents the settings for auditing SSPR events that occur in the authentication server.

(Conditional) ***Enable auditing for SSPR***

Specifies whether you want to send SSPR events to an auditing server.

If you select this setting, also specify the settings for the syslog server.

Syslog host name

Applies only when you enable auditing for SSPR.

Specifies the DNS or IP address of the server that hosts the syslog server. Do not use `localhost`.

Syslog port

Applies only when you enable auditing for SSPR.

Specifies the port of the server that hosts the syslog server.

9 To configure the identity applications and Identity Reporting to use SSPR, continue to Part XII, "Installing the Identity Applications," on page 277.

10 In Configuration Update Utility, update the SSO clients Parameters. For more information see, "Self Service Password Reset" on page 360.

For more information about configuring forgotten password management, see "Configuring Forgotten Password Management" on page 333.

Silently Installing Self Service Password Reset

A silent (non-interactive) installation does not display a user interface or ask the user any questions.

1 Log in as `root` or an administrator to the computer where you want to install the components.

2 Stop Tomcat.

3 (Conditional) If you have the `.iso` image file for the Identity Manager installation package, navigate to the directory containing the SSPR installation files, located by default in the `sspr` directory.

4 (Conditional) If you downloaded the installation files from the NetIQ Downloads website, complete the following steps:

4a Navigate to the `.tgz` or `.zip` file for the downloaded image.

4b Extract the contents of the file to a folder on the local computer.

5 Edit the `silent.properties` file for the SSPR installation, located by default in the same directory as the installation scripts.

For more information about the settings for installation, see Step 7 on page 267 and Step 8 on page 267.

6 To run the silent installation, issue one of the following commands:

- **Linux**: `sspr-install-linux.bin -i silent -f` *`path_to_silent.properties_file`*
- **Windows**: `sspr-install-win.exe -i silent -f` *`path_to_silent.properties_file`*

7 In Configuration Update Utility, update the SSO clients Parameters. For more information see, "Self Service Password Reset" on page 360.

Post-Installation Tasks

Ensuring Error-Free Installation

After you install SSPR, you can modify the configuration settings, such as change administrator permission of the LDAP group DN for the default profile or change the forward URL. Also, NetIQ recommends that you verify the URLs that the installation process created and change them if needed.

1. To open the SSPR login page, enter the following URL on your browser:

   `protocol://server:port/web-context`

   For example,

   `http://192.168.0.1:8080/sspr/`

2. On the top-right corner of the SSPR login page, select **Configuration Editor** from the list.
3. Specify the configuration password and click **Sign In**.
4. From the tree view, select **Default Settings** and ensure that **NetIQ IDM/OAuth Integration** is selected in the **LDAP Vendor Default Settings** list.
5. From the tree view, click **LDAP > LDAP Directories > default > Connection > LDAP Certificates**, then click **Import From Server** to import the certificates.

   (Conditional) Click **Test LDAP Profile** on the same page to ensure that all configured LDAP servers are reachable.

6. From the tree view, click **Modules > Authenticated > Administration** and ensure that the administrator permissions are assigned to the LDAP group DN for the default profile.

   If you are performing a fresh installation of SSPR, the list will be empty. You need to create a new group in iManager and add the `admin` user to the group.

7. Click **Settings > Application > Application**, and ensure that the **Forward URL** is set to `http://<Server:Port>/idmdash/#/landing`.

   For example, `http:/192.168.0.1:8080/idmdash/#/landing`.

8. From the tree view, click **Settings > UserInterface > Look & Feel** and change **Interface Theme** to **Micro Focus** if not already specified.
9. From the tree view, click **Settings > Single Sign On (SSO) Client > OAuth** and verify the values are correctly specified for the following parameters:

   OAuth Login URL

   Specifies the URL for OAuth server login. When user logs in, this URL to redirects the users for authentication with OSP.

   For example, `http://192.168.0.1:8080/osp/a/idm/auth/oauth2/grant`

   OAuth Code Resolve Service URL

   Specifies the URL for OAuth Code Resolve Service. SSPR uses this web service URL to resolve the artifact that the OAuth identity server returns.

   For example, `http://192.168.0.1:8080/osp/a/idm/auth/oauth2/authcoderesolve`

   OAuth Profile Service URL

   Specifies the URL for the web service that the Identity Manager provides to return attribute data from the user.

   For example, `http://192.168.0.1:8080/osp/a/idm/auth/oauth2/getattributes`

OAUTH Web Service Server Certificate

(Conditional) If HTTPS is enabled, import the certificate for the OAuth web service server.

OAuth Client ID

Specifies the client ID of the OAuth client. For example, `sspr`.

OAuth Shared Secret

Specifies a password for the OAuth shared secret. This password is shared between OSP and SSPR applications.

OAuth User Name/DN Login Attribute

Specifies the attribute of the user that SSPR uses to request OAuth server to authenticate user locally. For example, `name`.

10 Click from the top-right corner of the page to save your configuration.

11 On the top right corner of the SSPR login page, select **Configuration Manager** from the list.

12 Click **Restrict Configuration**.

Assigning the Universal Password Policy to a User Container

To assign the Universal Password policy to a user container:

1 Log in to iManager.

2 Select **Roles and Tasks > Password Policies**, then choose the password policy.

3 To select a user with administrative rights:

3a Click **Universal Password > Configuration Options > Universal Password Retrieval**.

3b Select **Allow admin to retrieve passwords** or **Allow the following to retrieve passwords** and click **OK**.

For example, `cn=uaadmin,ou=sa,o=data`

4 Click **Policy Assignment** and assign `container` to the container where the user resides.

For example, `o=data` or administrative users.

Granting Rights to pwmResponseSet Attributes

Users with authenticated rights perform operations based on the permissions associated with the user's connection. Authenticated users need the following rights for their own user entry:

- Browse rights to [Entry Rights]
- Read, Compare, and Write rights to pwmResponseSet

To grant rights to pwmResponseSet attribute, perform the following steps:

1 Log in to iManager.

2 Click .

3 Click **iManager Server** > **Configure iManager**.

4 Click **Misc** > **Enable [this]**.

5 Click .

6 From the **Tree** view, select the top level container of all users in the directory.

7 Click the **current level** check box and then click **Actions** > **Modify Trustees**.

8 Click **[This]** from the list and then click **Add Trustee**.

9 Click **Apply**.

10 Click **Assigned Rights** for **[This]** trustee.

11 Click **Add Property** and then select the **Show all properties in schema** check box.

12 Select **pwdResponseSet** from the list.

Ensure that Write, Compare, Read, and Inherited options are selected.

13 Click **Done**.

Configuring OSP and SSPR for Clustering

Identity Manager supports SSPR configuration in a Tomcat cluster environment.

Configuring SSPR to Support Clustering

Perform the following steps to configure SSPR that already exists on a separate computer:

1 Review the prerequisites and system requirements in "Checklist for Installing Password Management Components" on page 265.

2 Follow the instructions from "Using the Wizard to Install Self Service Password Request" on page 267 and ensure the following steps are considered during the installation process.

   a. In the Application Server connection page, select **Connect to external authentication server** and provide the DNS name of the server where the load balancer is installed.

   b. In the Authentication details page, provide the IP address and the port of the Identity Manager engine server. The password for the CA certificates is 'changeit'.

   c. After completing the SSPR installation, update the SSL settings. For more information, see "Updating the SSL Settings for Self Service Password Reset" on page 446.

3 To update the SSPR information in the first node of the cluster, launch the Configuration utility from `/opt/netiq/idm/apps/UserApplication/configupdate.sh`.

In the window that opens, click **SSO clients** > **Self Service Password Reset** and enter values for **Client ID**, **Password**, and **OSP Auth redirect URL** parameters.

Configuring Tasks on Cluster nodes

Perform the following configuration tasks on the cluster nodes:

1 To update the Forgotten Password link with the SSPR IP address, log in to the User Application on the first node and click **Administration** > **Forgot Password**.

For more information on SSPR configuration, see "Configuring Forgotten Password Management" on page 333.

2 To change the Change my password link, see "Updating SSPR Links in the Dashboard for a Distributed or Clustered Environment" on page 338.

3 Verify that the Forgot Password link and Change my password links are updated with the SSPR IP address on the other nodes in the cluster.

NOTE: If the Change Password and Forgot Password links are already updated with the SSPR IP address, no changes are required.

---

4 In the first node, stop Tomcat and generate a new `osp.jks` file by specifying the DNS name of the load balancer server by using the following command:

```
/opt/netiq/idm/jre/bin/keytool -genkey -keyalg RSA -keysize 2048 -keystore
osp.jks -storepass <password> -keypass <password> -alias osp -validity 1800 -
dname "cn=<loadbalancer IP/DNS>"
```

For example : `/opt/netiq/idm/jre/bin/keytool -genkey -keyalg RSA -keysize 2048 -keystore osp.jks -storepass changeit -keypass changeit -alias osp -validity 1800 -dname "cn=mydnsname"`

NOTE: Ensure that the key password is the same as the one provided during OSP installation. Alternatively, this can also be changed using Configuration Update utility including the keystore password.

---

5 (Conditional) To verify if the `osp.jks` file is updated with the changes, run the following command:

```
/opt/netiq/idm/jre/bin/keytool -list -v -keystore osp.jks -storepass changeit
```

6 Take backup of the original `osp.jks` file located at `/opt/netiq/idm/apps/osp` and copy the new `osp.jks` file to this location. The new `osp.jks` file was created in step 3.

7 Copy the new `osp.jks` file located at `/opt/netiq/idm/apps/osp/` from the first node to all other User Application nodes in the cluster.

8 Launch the Configuration utility in the first node and change all of the URL settings, such as URL link to landing page and OAuth redirect URL to the load balancer DNS name under the SSO Client tab.

8a Save the changes in the Configuration utility.

8b To reflect this change in all other nodes of the cluster, copy the `ism-configuration properties` file located in `/TOMCAT_INSTALLED_HOME/conf` from the first node to all other User Application nodes.

NOTE: You copied the `ism.properties` file from the first node to the other nodes in the cluster. If you specified custom installation paths during User Application installation, ensure that referential paths are corrected by using Configuration update utility in the cluster nodes.

In this scenario, both OSP and User Application are installed on the same server; therefore, the same DNS name is used for redirect URLs.

If OSP and User Application are installed on separate servers, change the OSP URLs to a different DNS name pointing to load balancer. Do this for all the servers where OSP is installed. This ensures that all OSP requests are dispatched through load balancer to the OSP cluster DNS name. This involves having a separate cluster for OSP nodes.

---

9 Perform the following actions in the `setenv.sh` file in the `/TOMCAT_INSTALLED_HOME/bin/` directory:

9a To ensure that the mcast_addr binding is successful, JGroups requires that the `preferIPv4Stack` property be set to **true**. To do so, add the JVM property "-Djava.net.preferIPv4Stack=true" in the `setenv.sh` file in all nodes.

9b Add "-Dcom.novell.afw.wf.Engine-id=Engine" in the `setenv.sh` file in the first node.

The engine name should be unique. Provide the name that was given during the installation of the first node. The default name is "Engine" in case no name was specified.

Similarly, add a unique engine name for other nodes in the cluster. For example, for second node, the engine name can be Engine2.

10 Enable clustering in the User Application. For more information see, Step 10 on page 320.

11 Enable the permission index for clustering. For more information see, “Enabling the Permission Index for Clustering” on page 300.

12 Enable Tomcat cluster. For more information see, Step 9 on page 301.

13 Restart Tomcat on all nodes.

14 Configure the User Application Driver for clustering. For more information see, “Configuring the User Application Driver for Clustering” on page 324.

XII Installing the Identity Applications

This section guides you through the process of installing the components and framework required for the identity applications:

- Catalog Administrator
- Identity Applications Dashboard
- Role and Resource Service driver
- User Application
- User Application driver

By default, the installation program installs these components in the following locations:

- **Linux**: `/opt/netiq/idm`
- **Windows**: `C:\netiq\idm\apps`

The identity applications 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 33, “Planning to Install the Identity Applications,” on page 279.

33 Planning to Install the Identity Applications

The identity applications installation includes the following components:

- Catalog Administrator
- Home and Provisioning Dashboard

  NOTE: Although Identity Manager v4.6 includes the Home and Provisioning Dashboard, this feature is being deprecated. When users log in to the identity applications, they will be directed to the Identity Applications Dashboard instead of to Home.

- Identity Manager Dashboard
- Role and Resource Service driver
- User Application

The installation does not include the two drivers required for the identity applications: User Application driver and Roles and Resource Services driver. You install these drivers with the Identity Manager engine. For more information, see Chapter 16, "Preparing to Install the Engine, Drivers, and Plug-ins," on page 139.

NOTE: Technically Identity Reporting could be considered an identity application because the component also uses SSPR and OSP, and you modify the settings with the RBPM configuration utility. However, Identity Reporting has its own installation program, can be installed on a separate server, and uses a different database. For more information, see "System Requirements for Identity Reporting" on page 368.

- "Checklist for Installing the Identity Applications" on page 279
- "Understanding the Installation Files for the Identity Applications" on page 281
- "Prerequisites and Considerations for Installing the Identity Applications" on page 282
- "System Requirements for the Identity Applications" on page 287

Checklist for Installing the Identity Applications

Before beginning the installation process, NetIQ recommends that you review the following steps:

	Checklist Items
❑	1. Learn about the interaction among Identity Manager components. For more information, see "User Application and Roles Based Provisioning Module" on page 33.
❑	2. Decide which servers you want to use for your Identity Manager components. For more information, see "Recommended Server Setup" on page 46.
❑	3. Decide whether you should install an Sentinel before installing the identity applications. For more information, see "Recommended Installation Scenarios and Server Setup" on page 44.

	Checklist Items
❑	4. Ensure that the Identity Vault includes the SecretStore module. For more information, see "Adding SecretStore to the Identity Vault Schema" on page 109.
❑	5. Ensure that the Identity Manager engine has been installed. For more information about installing the engine, see Chapter 16, "Preparing to Install the Engine, Drivers, and Plug-ins," on page 139.
❑	6. Review the considerations for installing the identity applications and their supporting framework to ensure that your servers meet the prerequisites. For more information, see "Prerequisites and Considerations for Installing the Identity Applications" on page 282.
❑	7. (Conditional) For computers running a SLES 12 SP1 or later operating system, ensure that you have installed the appropriate set of libraries for a guided installation. For more information, see "Installing Identity Manager on SLES 12 SP1 or Later Servers" on page 55.
❑	8. (Conditional) For computers running an RHEL 6.x or RHEL 7.x operating system, ensure that you have installed the appropriate set of libraries. For more information, see "Installing Identity Manager on RHEL 6.x or 7.x Servers" on page 55.
❑	9. Review the hardware and software requirements for the computers that will host the identity applications and their framework. For more information, see "System Requirements for the Identity Applications" on page 287.
❑	10. 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 "Adding the User Application Schema to your Audit Server as a Log Application" on page 291.
❑	11. Create a User Application Administrator account in the eDirectory identity vault. For more information, see "Assign Rights to Identity Vault Administrator and User Application Administrator Account" on page 292.
❑	12. Install and configure a database for the identity applications on the local computer or a connected server. ◆ To learn about the database, see "Prerequisites for Installing the Database for the Identity Applications" on page 286. ◆ To install the database, see Chapter 35, "Configuring the Database for the Identity Applications," on page 295.
❑	13. Prepare an application server on the local computer or in a cluster. ◆ To understand the requirements, see "Prerequisites and Considerations for the Application Server" on page 284. ◆ To prepare the cluster, see Chapter 36, "Preparing Your Environment for the Identity Applications," on page 299. ◆ To install an application server, see "Preparing Your Application Server for the Identity Applications" on page 300.
❑	14. (Conditional) To use the Apache Log4j service to record events in Tomcat, ensure that you have the appropriate files. For more information, see "Using the Apache Log4j Service to Log Sign-on" on page 254.
❑	15. Review the contents of the identity applications installation kit to determine which files are needed for your environment. For more information, see "Understanding the Installation Files for the Identity Applications" on page 281.

	Checklist Items
❑	16. Create and deploy the User Application driver and the Roles and Resource Service driver. For more information, see Chapter 38, "Creating and Deploying the Drivers for the Identity Applications," on page 323.
❑	17. Install the identity applications. For more information, see Chapter 37, "Installing the Identity Applications," on page 303.
❑	18. To perform the final tasks in the installation process, see Chapter 39, "Completing the Installation of the Identity Applications," on page 327.
❑	19. Ensure that you have configured the identity applications and single sign-on settings correctly. For more information, see Chapter 51, "Verifying Single Sign-on Access for the Identity Applications," on page 433.
❑	20. (Optional) To begin using the identity applications, see the *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*.

Understanding the Installation Files for the Identity Applications

The installation files for the identity applications are located in the `/products/RBPM/user_app_install` directory of the installation package.

File	Description
`configupdate.properties`	If you are going to perform a silent installation, you use this file to configure the Roles Based Provisioning Module. For more information, see "Silently Installing the Identity Applications" on page 310.
`IdmUserApp.exe` or `IdmUserApp.bin`	The installation program for the identity applications. There is a specific installer for the platform you are using.
`user_app.configure.properties`	If you are going to perform a silent installation, you use this file to configure the Identity Applications. For more information, see "Silently Installing the Identity Applications" on page 310.
`user_app.install.properties`	If you are going to perform a silent installation, you use this file to install the Identity Applications. For more information, see "Silently Installing the Identity Applications" on page 310.

The installation program does the following:

- Designates an existing version of an application server to use.
- Designates an existing version of a database to use. The database stores identity application data and configuration information.
- Configures the JDK's certificates file so that the identity application (running on Tomcat) 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 Tomcat.
- Enables logging through Sentinel or OpenXDAS auditing clients if you choose to do so.
- Enables you to import an existing master key to restore a specific installation of the identity applications and to support clusters.

Prerequisites and Considerations for Installing the Identity Applications

NetIQ recommends that you review the prerequisites and computer requirements for the identity applications before you begin the installation process. For more information about configuring the User Application environment, see *NetIQ Identity Manager - User's Guide to the Identity Applications*.

- "Installation Considerations for the Identity Applications" on page 282
- "Configuration and Usage Considerations for the Identity Applications" on page 283
- "Prerequisites and Considerations for the Application Server" on page 284
- "Prerequisites for Installing the Identity Applications in a Cluster Environment" on page 285
- "Prerequisites for Installing the Database for the Identity Applications" on page 286

Installation Considerations for the Identity Applications

The following considerations apply to the installation of the identity applications.

- Require a supported version of the following Identity Manager components:
  - Designer
  - Identity Vault
  - Identity Manager engine
  - Remote Loader
  - One SSO Provider

  For more information about required versions and patches for these components, see the latest Release Notes.
- Ensure that the Identity Vault includes the SecretStore module, and that the module is configured. For more information, see "Adding SecretStore to the Identity Vault Schema" on page 109.
- Ensure that the Identity Vault includes the created and deployed User Application and Roles and Resources service drivers. For more information, see Chapter 38, "Creating and Deploying the Drivers for the Identity Applications," on page 323.
- Install the following framework items before installing the identity applications:
  - An application server on the local computer. For more information, see "Prerequisites and Considerations for the Application Server" on page 284.
  - A database on the local computer or a connected server. For more information, see "Prerequisites for Installing the Database for the Identity Applications" on page 286.
- (Conditional) When installing the identity applications on SUSE Linux Enterprise Server (SLES) platforms, 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) For a guided installation on a server running SLES 12 SP1 or later platforms, ensure that the server has `libXtst6-32bit-1.2.1-4.4.1.x86_64`, `libXrender1-32bit`, and `libXi6-32bit` libraries installed.
- (Optional) NetIQ recommends that you enable Secure Sockets Layer (SSL) protocol for communication among the Identity Manager components. To use SSL protocol, you must enable SSL in your environment and specify **https** during the installation. For information about enabling SSL, see Configuring Security in the Identity Applications in the *NetIQ Analyzer for Identity Manager Administration Guide*.

- 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.
- Set the `JAVA_HOME` environment variable to point to the JDK that you plan to use with the identity applications. To override `JAVA_HOME`, manually specify the path during the installation.
- The installation process places the program files in the `C:\NetIQ\IDM` or `/opt/netiq/idm` directory by default. If you plan to install the User Application in a 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.
- 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 Tomcat on which you deploy the identity applications and the `IDMPwdMgt.war` file.
  - Ensure that the SSL port is open on your firewall.

  For more information about enabling SSL for Tomcat, see "Updating the SSL Settings for Self Service Password Reset" on page 446.

  For more information about the `IDMPwdMgt.war` file, see "Configuring Forgotten Password Management" on page 333.
- To support LDAP search with Virtual List View (VLV) and Server Side Sort (SSS) controls, apply Hotfix 2 to eDirectory 9.0.2 or eDirectory 8.8.8 Patch 9. For more information, see Chapter 11, "Applying Hotfix 2 to the Identity Vault," on page 101.

  This hotfix is not needed if you installed eDirectory with the integrated installation program. The integrated installer installs an updated version of eDirectory that has this hotfix applied.
- (Optional) To retrieve authorizations from managed systems, install one or more of the Identity Manager drivers.
  - 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 Identity Manager Drivers documentation website.
  - To manage the drivers, you must have previously installed Designer or the appropriate plug-ins for iManager. For more information, see "Understanding Installation for iManager Plug-ins" on page 209.

Configuration and Usage Considerations for the Identity Applications

The following considerations apply to the configurations and initial usage of the identity applications.

- Before users can access the identity applications, you must complete the following activities:
  - Ensure that all necessary Identity Manager drivers are installed.

    - Ensure that the indexes for the Identity Vault are in Online mode. For more information about configuring an index during installation, see "Miscellaneous" on page 348.
    - Enable cookies on all browsers. The applications do not work when cookies are disabled.
- Users cannot access the identity applications as a guest or anonymous user without being logged in to the identity applications. The users are prompted to log in to the user interface. For more information, see Part XV, "Configuring Single Sign-on Access in Identity Manager," on page 417.
- To ensure that Identity Manager enforces Universal Password functionality, configure the Identity Vault to use NMAS Login as the process for a user's first login.
    - **Linux**: Add the following commands to the end of the `/opt/novell/eDirectory/sbin/pre_ndsd_start` script:

      ```
      NDSD_TRY_NMASLOGIN_FIRST=true
      export NDSD_TRY_NMASLOGIN_FIRST
      ```

    - **Windows**: Add `NDSD_TRY_NMASLOGIN_FIRST` with the string value `true` to the HKLM\SYSTEM\CurrentControlSet\Control\SessionManager\Environment registry key.
- (Conditional) To run reports, you must have the components for Identity Reporting installed in your environment. For more information, see *Administrator Guide to NetIQ Identity Reporting*.
- 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 Identity Applications 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.
- (Conditional) To audit the identity applications, you must have the Identity Reporting and an auditing service installed in your environment and configured to capture the events. You must also configure the identity applications for auditing. For more information, see the
- (Optional) You can configure the identity applications to work with NetIQ Access Manager using SAML authentication. For more information, see Chapter 49, "Using SAML Authentication with NetIQ Access Manager for Single Sign-on," on page 423.

Prerequisites and Considerations for the Application Server

The identity applications require that Tomcat be installed with the following considerations:

- Tomcat must be running with the Java Development Kit (JDK) or Java Runtime Environment (JRE). For more information about supported versions, see "System Requirements for the Identity Applications" on page 287.
- 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 installation.
- (Conditional) You can use your own Tomcat installation program instead of the one provided in the Identity Manager installation kit. However, to use the Apache Log4j service with your version of Tomcat, ensure that you have the appropriate files installed. For more information, see "Using the Apache Log4j Service to Log Sign-on" on page 254.
- (Conditional) To preserve documents that you digitally sign, you must install the identity applications on a Tomcat 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 Setting Up Logging in the Identity Applications in the *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*.

- (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 identity applications. For more information about configuring for optimal performance, see Tuning the Performance of the Applications in the *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*.
- (Conditional) If you use a Tomcat application server, do not start the server until after you complete the installation process.
- (Conditional) To use external password management, you must do the following to enable the Secure Sockets Layer (SSL) protocol:
  - Enable SSL for Tomcat on which you deploy the identity applications and the `IDMPwdMgt.war` file.
  - Ensure that the SSL port is open on your firewall.

  For more information about the `IDMPwdMgt.war file`, see Configuring Forgotten Password Management and the *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*.
- The installation process does not modify the `JAVA_HOME` or `JRE_HOME` entries on a Tomcat server. By default, the convenience installer for Tomcat places the `setenv.sh` file in the `/opt/netiq/idm/apps/tomcat/bin/` directory. The installation also configures the JRE location in the file.

Prerequisites for Installing the Identity Applications in a Cluster Environment

You can install the database for the identity applications in an environment supported by Tomcat 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 identity applications database.
  - For each member of the cluster, you must specify the same hostname or IP address of the server hosting the identity applications database.
- You must synchronize the clocks of the servers in the 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 ins across browser tabs or browser sessions on the same host. Some browsers share cookies across tabs and processes, so allowing multiple logins might cause problems with HTTP session failover (in addition to risking unexpected authentication functionality if multiple users share a computer).
- The cluster nodes reside in the same subnet.
- A failover proxy or a load balancing solution is installed on a separate computer.

For more information about configuring the identity applications in a cluster environment, see Chapter 36, "Preparing Your Environment for the Identity Applications," on page 299.

Prerequisites for Installing the Database for the Identity Applications

The database stores the identity applications data and configuration information.

Before installing the database instance, review the following prerequisites:

- To configure a database for use with Tomcat, you must create a JDBC driver. The identity applications use standard JDBC calls to access and update the database. The identity applications use 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. The installation program for the User Application creates a data source entry for Tomcat in `server.xml` and `context.xml` which points to the database.
- 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 identity applications 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`.
  - 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 "Configuring the Character Set" on page 297 or "Configuring an Oracle Database" on page 295.
- To avoid duplicate key errors during migration, use case-sensitive collation. If a duplicate key error occurs, check the collation and correct it, then re-install the identity applications.
- (Conditional) To use the same database instance both for auditing purposes and for the identity applications, NetIQ recommends installing the database on a separate dedicated server from the server that hosts Tomcat running the identity applications.
- (Conditional) If you are migrating to a new version of the identity applications, you must use the same database that you used for the previous installation.
- 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:
  - By default, the maximum number of connections is set to 100. This value might be too low to handle the workflow request load in a cluster. 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 the `my.cnf` file to a higher value.
  - 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.

System Requirements for the Identity Applications

This section provides the minimum requirements for the server(s) where you want to install the identity applications. These requirements also apply to your installation of PostgreSQL, Tomcat, OSP, and SSPR.

Ensure that you review the prerequisites and considerations for installation, particularly those related to the operating system.

Category	Requirement
Processor	1 GHz
Disk space	1 GB
	NOTE: Enough space for the content of supporting applications, such as the database and application server logs.
Memory	512 MB (4 GB recommended)

Category	Requirement
Operating system (certified)	One of the following 64-bit operating systems: ◆ Open Enterprise Server 2015 SP1 ◆ Open Enterprise Server 11 SP3 ◆ Red Hat Enterprise Linux 7.3 ◆ Red Hat Enterprise Linux 7.2 ◆ Red Hat Enterprise Linux 7.1 ◆ Red Hat Enterprise Linux 7.0 ◆ Red Hat Enterprise Linux 6.8 ◆ SUSE Linux Enterprise Server 12 SP1 ◆ SUSE Linux Enterprise Server 11 SP4 ◆ Windows Server 2012 R2 ◆ Windows Server 2012 One of the following 32-bit operating systems: ◆ Open Enterprise Server 11 SP3 NetIQ recommends that you apply the latest operating system patches according to the manufacturer's automated update facility before you install Identity Manager. **NOTE:** *Certified* means that the operating system has been fully tested and is supported.
Operating system (supported)	Latest versions of service packs for the certified operating systems **NOTE:** *Supported* means that the operating system has not yet been tested but is expected to work
Virtualization system	◆ Hyper-V Server 2012 R2 ◆ VMWare ESX 5.5 and later ◆ Windows Server 2012 R2 Virtualization with Hyper-V (supported) NetIQ supports Identity Manager on enterprise-class virtualization systems that provide official support for the operating systems where NetIQ products are running. As long as the vendors of the virtualization systems officially support these operating systems, NetIQ supports the entire Identity Manager stack on them.
Database	◆ Microsoft SQL Server 2014 with JDBC 3.0 3.0.1119.0 ◆ Oracle 12c with JDBC 12.1.0.2 ◆ PostgreSQL 9.4.10 with JDBC 4.2 (SLES 11 SP4 only) ◆ PostgreSQL 9.6.1 with JDBC 4.2 (other supported platforms) **NOTE:** Do not include PostgreSQL versions (for example 8.x or 9.3.x) in Tomcat’s classpath. The Home page images might not load if these versions are specified.
Application server	Apache Tomcat 8.5.x

Category	Requirement
Java	Java Development Kit (JDK) or Java Runtime Environment (JRE) version 1.8.0_112 or later from Sun (Oracle)
Port	8180
Web browser	Any of the following browsers, at a minimum: ◆ Apple Safari 9 ◆ Google Chrome 51 ◆ Microsoft Edge ◆ Mozilla Firefox 46 ◆ Microsoft Internet Explorer 11 (except versions 11.1029.15063.0 and 11.0.9600.18952) **NOTE:** The Compatibility View option is not supported in the Internet Explorer browser. **NOTE:** The browser must have cookies enabled. If cookies are disabled, the product does not work.
Audit	One of the following auditing services: ◆ OpenXDAS 0.8.345 ◆ (Conditional) For servers running SLES SP4 with Open XDAS: ◆ openxdas-0.8.351-1.1.i586.rpm ◆ openxdas-0.8.351-1.1.x86_64.rpm ◆ Platform Agent 2011.1r5, at a minimum
Domain Services for Windows	Open Enterprise Server 11 SP3
Directory services	NetIQ eDirectory 8.8.8 Patch 9 Hotfix 2 or NetIQ eDirectory 9.0.2 Hotfix 2 **NOTE:** NetIQ applies certain restrictions on installing eDirectory 9.0.2 as an Identity Vault. For more information, see "Working with eDirectory 9.0.2 or Later" on page 84.

34 Preparing the Identity Vault for the Identity Applications

This section helps you prepare to install the identity applications. The applications run on a framework called the Roles Based Provisioning Module (RBPM). When you install the Identity Manager engine, the installation process automatically installs `netiq-DXMLuad-4.5.0-0.noarch` and `netiq-DXMLrrsd-4.5.0-0.noarc` RPMs that install the User Application driver, the Roles and Resource driver, and extend the eDirectory schema to interact with RBPM.

The installation files are located in the `products/RBPM/user_app_install` directory within the `.iso` image file for the Identity Manager installation package.

- "Adding the User Application Schema to your Audit Server as a Log Application" on page 291
- "Assign Rights to Identity Vault Administrator and User Application Administrator Account" on page 292

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/netiq/idm/apps/UserApplication`.

2. Use a web browser to access an iManager with the Novell Identity Audit plug-in installed, and log in as an administrator.
3. Navigate 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.

Assign Rights to Identity Vault Administrator and User Application Administrator Account

The Identity Vault Administrator is a user who has rights to configure the Identity Vault. This is a logical role that can be shared with other administrative user types.

The Identity Vault Administrator needs the following rights:

- Supervisor rights to the User Application driver and all the objects it contains. You can accomplish this by setting the rights at the driver container level and making them inheritable.
- Supervisor Entry rights to any of the users that are defined through the directory abstraction layer user entity definition. This should include Write attribute rights to objectClass and any of the attributes associated with the `DirXML-EntitlementRecipient`, `srvprvEntityAux` and `srvprvUserAux` auxiliary classes.
- Supervisor rights to the container object `cn=DefaultNotificationCollection`, `cn=Security`. This object persists email server settings used for automated provisioning emails. It can contain SecretStore credentials for authenticating to the email server itself.
- Supervisor rights to the container object `cn=Authorized Login Methods`, `cn=Security`. During the User Application installation the SAML Assertion object is created in this container.
- Ensure that you have supervisor rights to the `cn=Security` container before you install user application. During the User Application installation, the container `cn=RBPMTrustedRootContainer` is created under the `cn=Security` container.

  Alternatively, manually create the `cn=RBPMTrustedRootContainer`,`cn=Security` container (create an object called `Trusted Root Container` with object class `NDSPKI:Trusted Root` inside the `Security` container), and then assign supervisor rights to the container.

You must manually create a User Application Administrator account in the eDirectory Identity Vault for the Roles Based Provisioning Module to install correctly. The User Application Administrator account must be a trustee of the top container and must have Supervisor rights to the container.

When you create the User Application Administrator account, you must assign a password policy to this new user account. For more information, see "Creating Password Policies" in the *Password Management Administration Guide*.

The integrated installer for Identity Manager creates a default User Application Administrative account as `cn=uaadmin.ou=sa.o=data`. Designer pre-populates fields with this account name. When using the standalone installation program, you can create the same account name or use a different account name.

To create the permissions for the User Application Administrator account, run the following commands in an LDAP Data Interchange Format (LDIF) file:

```
dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 1#subtree#[Root]#[Entry Rights]
  dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 3#subtree#%%RBPM_USER_APP_CONTAINER_DN%%#description
  dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 3#subtree#%%RBPM_USER_APP_CONTAINER_DN%%#directReports
  dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
```

```
add: ACL
ACL: 3#subtree#%%RBPM_USER_APP_CONTAINER_DN%%#mail
  dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 3#subtree#%%RBPM_USER_APP_CONTAINER_DN%%#manager
  dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 3#subtree#%%RBPM_USER_APP_CONTAINER_DN%%#photo
  dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 3#subtree#%%RBPM_USER_APP_CONTAINER_DN%%#srvprvQueryList
  dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 3#subtree#%%RBPM_USER_APP_CONTAINER_DN%%#srvprvUserPrefs
  dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 3#subtree#%%RBPM_USER_APP_CONTAINER_DN%%#telephoneNumber
  dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 3#subtree#%%RBPM_USER_APP_CONTAINER_DN%%#title

dn: %%RBPM_USER_APP_CONTAINER_DN%%
changetype: modify
add: ACL
ACL: 17#subtree#%%RBPM_USER_APP_ADMIN_DN%%#[Entry Rights]
ACL: 35#subtree#%%RBPM_USER_APP_ADMIN_DN%%#[All Attributes Rights]
```

35 Configuring the Database for the Identity Applications

The database for the Identity Applications supports tasks such as storing configuration data and data for workflow activities. Before you can install the applications, the database must be installed and configured. For more information about supported databases, see "System Requirements for the Identity Applications" on page 287. For more information about considerations for the User Application database, see "Prerequisites for Installing the Database for the Identity Applications" on page 286.

NOTE: If you are migrating to a new version of RBPM and the Identity Applications, you must use the same database that you used for the previous installation. That is, the installation from which you are migrating.

- "Configuring an Oracle Database" on page 295
- "Configuring a PostgreSQL Database" on page 296
- "Configuring a SQL Server Database" on page 297

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 "System Requirements for the Identity Applications" on page 287.

Checking Compatibility Level of Databases

Databases from different releases of Oracle are compatible if they support the same features and those features perform the same way. If they are not compatible, certain features or operations might not work as expected. For example, creation of schema fails that does not allow you to deploy the identity applications.

To check the compatibility level of your database, perform the following steps:

1. Connect to the Database Engine.
2. After connecting to the appropriate instance of the SQL Server Database Engine, in **Object Explorer**, click the server name.
3. Expand **Databases**, and, depending on the database, either select a user database or expand **System Databases** and select a system database.
4. Right-click the database, and then click **Properties**.

   The **Database Properties** dialog box opens.
5. In the **Select a page** pane, click **Options**.

   The current compatibility level is displayed in the **Compatibility level** list box.
6. To check the **Compatibility Level**, enter the following in the query window and click **Execute**.

```
SQL> SELECT name, value FROM v$parameter
WHERE name = 'compatible';
```

The expected output is: 12.1.0.2

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 12c 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
```

NOTE: It is recommended to use JDBC JAR version `ojdbc6.jar`.

For more information about configuring a character set, see "Choosing an Oracle Database Character Set".

Configuring the Admin User Account

The User Application requires that the Oracle database user account have specific privileges. In the SQL Plus utility, enter the following commands:

```
CREATE USER idmuser IDENTIFIED BY password;
GRANT CREATE SESSION TO idmuser;
GRANT CREATE CLUSTER TO idmuser;
GRANT CREATE PROCEDURE TO idmuser;
GRANT CREATE SEQUENCE TO idmuser;
GRANT CREATE TABLE TO idmuser;
GRANT CREATE TRIGGER TO idmuser;
ALTER USER idmuser quota 100M on USERS;
```

where *`idmuser`* represents the user account.

Configuring a PostgreSQL Database

For your convenience, NetIQ provides an installation program for PostgreSQL, which fully supports the framework services and applications within Identity Manager. The installation program guides you through the configuration process. For more information, see Chapter 28, "Installing PostgreSQL and Tomcat," on page 247.

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 "System Requirements for the Identity Applications" on page 287.

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.

Configuring the Admin User Account

After installing Microsoft SQL Server 2014, 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`

NOTE: It is recommended to use JDBC JAR version `sqljdbc4.jar`.

---

36 Preparing Your Environment for the Identity Applications

The Identity Applications benefit from higher availability when you run them in a cluster. In addition, they support 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 section provides instructions for preparing your environment, including a cluster environment, to function with the identity applications. You must complete the steps in this chapter in conjunction with the instructions in one of the following sections:

- "Using the Guided Process to Install the Identity Applications" on page 304
- "Silently Installing the Identity Applications" on page 310

For more information about the requirements for a cluster environment, see "Prerequisites for Installing the Identity Applications in a Cluster Environment" on page 285 and "System Requirements for the Identity Applications" on page 287.

- "Specifying a Location for the Permission Index" on page 299
- "Enabling the Permission Index for Clustering" on page 300
- "Preparing Your Application Server for the Identity Applications" on page 300
- "Preparing a Cluster for the Identity Applications" on page 301

Specifying a Location for the Permission Index

When you install the identity applications, the process creates a permission index for Tomcat. If you do not specify a location for the index, the installation creates a folder in a temporary directory. For example: `/opt/netiq/idm/apps/tomcat/temp/permindex` on Tomcat.

In a test environment, the location usually does not matter. However, in a production or staging environment, you might not want to place the permission index in a temporary directory.

To specify a location for the index:

1. Stop Tomcat.
2. In a text editor, open the `ism-configuration.properties` file.
3. At the end of the file, add the following text:

   ```
   com.netiq.idm.cis.indexdir = path/permindex
   ```

   For example:

   ```
   com.netiq.idm.cis.indexdir = /opt/netiq/idm/apps/permindex
   ```

4. Save and close the file.
5. Delete the existing `permindex` folder in the temporary directory.
6. Start Tomcat.

Enabling the Permission Index for Clustering

This section provides instructions for enabling the permission index for clustering.

1. Log in to iManager in the first node of the cluster and navigate to **View Objects**.
2. Under **System**, navigate to the driver set containing the **User Application driver**.
3. Select **AppConfig** > **AppDefs** > **Configuration**.
4. Select the XMLData attribute and set the `com.netiq.idm.cis.clustered` property to **true**.

   For example:

   ```
   <property>
   <key>com.netiq.idm.cis.clustered</key>
   <value>true</value>
   </property>
   ```
5. Click **OK.**

Preparing Your Application Server for the Identity Applications

You should prepare Tomcat that will run the identity applications. For your convenience, NetIQ provides Apache Tomcat in the installation kit. For more information about using the applications in a cluster environment, also see "Preparing a Cluster for the Identity Applications" on page 301.

Preparing a Tomcat Environment

This section describes how to prepare an environment where you want to run the identity applications on Tomcat. The `.iso` for installing Identity Manager includes a program for installing Tomcat (and optionally PostgreSQL). For more information, see Chapter 28, "Installing PostgreSQL and Tomcat," on page 247.

You can use your own Tomcat installation program instead of using the convenience installer provided in the installation package. However, if you do use a different installation program, there are additional steps you must perform for Tomcat to function correctly with the Identity Applications.

Before you start the installation process, ensure that the versions of the components you are installing are supported with this version of the Identity Applications. For more information, see "Prerequisites and Considerations for Installing the Identity Applications" on page 282.

1. Install Apache Tomcat as a service on your server.

   For more information, see Tomcat Setup.
2. Install the following components on the same server where you installed Tomcat.
   - **Java Runtime Environment (JRE):** For more information, see the Java Platform Installation Guide.
   - **Apache ActiveMQ:** For more information, see ActiveMQ.
   - **PostgreSQL:** For more information, see PostgreSQL Manuals.
3. Copy the `activemq-all-5.14 jar` file to the *`TOMCAT_INSTALLED_HOME`*`/lib` folder for ActiveMQ.

4 Copy the following files to the *TOMCAT_INSTALLED_HOME*/lib folder for logging.
   - log4j.jar
   - log4j.properties
   - tomcat-juli-adapters.jar
5 Set the following properties in the setenv.bat (Windows) or setenv.sh (Linux) file.

```
JAVA_HOME
JRE_HOME
PATH (set Java path)
JAVA_OPTS="-Xms1024m -Xmx1024m"
```

6 Create a user with the name novlua and create a group with the name novlua.

   This allows you to run Tomcat as a non-root user. For more information, see *A Guide To Apache Tomcat Linux Installation and Set-Up*.
7 Make the novlua user and novlua group owners of the Tomcat files.
8 Copy the postgresql-9.4.1212jdbc42.jar file to the */TOMCAT_INSTALLED_HOME*/lib folder.
9 (Conditional) In a cluster environment, open the server.xml file located by default in the /TOMCAT_INSTALLED_HOME/conf/ directory in the first node of the cluster and uncomment this line:

   ```
   <Cluster className="org.apache.catalina.ha.tcp.SimpleTcpCluster"/>
   ```

   Do this for all nodes in the cluster.

   For advanced Tomcat clustering configuration, follow the steps from Apache Tomcat Documentation.

After you have installed Tomcat and the Identity Applications, you can tune Tomcat to function more effectively. For more information, see "Post-Installation Steps" on page 316.

Preparing a Cluster for the Identity Applications

The identity applications supports HTTP session replication and session failover. 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. Before installing the identity applications in a cluster, you should prepare the environment.

- "Understanding Cluster Groups in Tomcat Environments" on page 301
- "Setting System Properties for Workflow Engine IDs" on page 302
- "Using the Same Master Key for Each User Application in the Cluster" on page 302

Understanding Cluster Groups in Tomcat Environments

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 "Prerequisites and Considerations for Installing the Identity Applications" on page 282.

Setting System Properties for Workflow Engine IDs

Each server that hosts the identity applications in the cluster can run a workflow engine. 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 cache framework for the identity applications.

To ensure that your workflow engines run appropriately, you must set system properties for Tomcat.

1. Create a new JVM system property for each identity applications server in the cluster.
2. Name the system property `com.novell.afw.wf.`*`engine-id`* where the engine ID is a unique value.

Using the Same Master Key for Each User Application in the Cluster

The identity applications encrypt sensitive data using a master key. All identity applications in a cluster must use the same master key. This section helps you ensure that all identity applications in a cluster use the same master key.

For more information about creating the master key, see **Security - Master Key** in Step 6 on page 304. For more information about encrypting sensitive data in the identity applications, see Encrypting Sensitive Identity Applications Data in the *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*.

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 identity applications. By default, the file is in the installation directory.
3. Install the identity applications 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.

37 Installing the Identity Applications

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 Tomcat and Java, see "System Requirements for the Identity Applications" on page 287.

- "Checklist for Installing the Identity Applications" on page 303
- "Using the Guided Process to Install the Identity Applications" on page 304
- "Silently Installing the Identity Applications" on page 310
- "Post-Installation Steps" on page 316
- "Disabling the Prevent HTML Framing Setting for Integrating Identity Manager with SSPR" on page 319
- "Starting the Identity Applications" on page 319

Checklist for Installing the Identity Applications

Use the following checklist to guide you through the process of installing the identity applications.

	Checklist Items
❑	1. (Conditional) Review considerations for installing the identity applications on Tomcat in a cluster environment. For more information, see "Understanding Cluster Groups in Tomcat Environments" on page 301.
❑	2. Install a supported version of your application server and Java development kit or runtime environment. For more information, see "System Requirements for the Identity Applications" on page 287.
❑	3. Ensure that Tomcat has the correct settings. For more information, see "Preparing Your Application Server for the Identity Applications" on page 300.
❑	4. Configure a data source file and JDBC provider for the database.
❑	5. Install the identity applications. For more information, see one of the following sections: ◆ "Using the Guided Process to Install the Identity Applications" on page 304 ◆ "Silently Installing the Identity Applications" on page 310 **NOTE:** You can run a silent installation on Linux computers only.
❑	6. Configure Tomcat for the identity applications. For more information, see one of the following sections: ◆ "Post-Installation Steps" on page 316
❑	7. Deploy and start the identity applications. For more information, see "Starting the Identity Applications" on page 319.

Using the Guided Process to Install the Identity Applications

The following procedure describes how to install the identity applications using an installation wizard, either in GUI format or from the console. To perform a silent, unattended installation, see "Silently Installing the Identity Applications" on page 310.

To prepare for the installation, review the activities listed in "Checklist for Installing the Identity Applications" on page 303. Also see the Release Notes accompanying the release.

NOTE

- 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 Tomcat to this user. For example, the `idmapps_tomcat_init` script uses this user account to run Tomcat.

To install with the guided process:

1. Log in as a `root` or administrative user to the computer where you want to install the identity applications.
2. Stop Tomcat.
3. (Conditional) If you have the `.iso` image file for the Identity Manager installation package, navigate to the directory containing the installation files, located by default in the `products/RBPM/user_app_install` directory.
4. (Conditional) If you downloaded the installation files, complete the following steps:
   - **4a** Navigate to the `.tgz` or `win.zip` file for the downloaded image.
   - **4b** Extract the contents of the file to a directory on the local computer.
5. From the directory that contains the installation files, complete one of the following actions:
   - **Linux (console)**: Enter `./IdmUserApp.bin -i console`
   - **Linux (GUI)**: Enter `./IdmUserApp.bin`
   - **Windows**: Run `IdmUserApp.exe`
6. Complete the guided process, using the following parameters:
   - **Application Server Platform**

     Represents Tomcat for running the Identity Applications. Tomcat must already be installed.
   - **Installation Folder**

     Represents the path to a directory where the installation program creates the application files.
   - **Database Platform**

     Represents the platform of the User Application database. The database software must already be installed. However, you do not need to create the database schema during installation.

     For your convenience, NetIQ provides PostgreSQL.
   - **Database Host and Port**

     Represents the settings for the server that hosts the User Application database.

NOTE: In a cluster environment, you must specify the same database settings for each member in the cluster.

Host

Specifies the name or IP address of the server.

Port

Specifies the port that you want the server to use for communication with the User Application.

- **Database Username and Password**

Represents the settings for running the User Application database.

NOTE

- If you installed PostgreSQL as part of the installation for this version of Identity Manager, the installation process already created the database and database administrator. By default, the installed database is `idmuserappdb` and the database user is `idmadmin`. Specify the same values that you used for the PostgreSQL installation.
- In a cluster environment, you must specify the same database name, username, and password for each member in the cluster.

Database Name or SID

Specifies the name of the database according to the database platform. By default, the database name is `idmuserappdb`.

- For a PostgreSQL or SQL Server database, specify the name.
- For an Oracle database, specify the Security Identifier (SID) that you created with the database instance.

Database Username

Specifies the name of an account that allows the User Application to access and modify data in the databases.

Database Password

Specifies the password for the specified username.

Database Driver JAR File

Specifies 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, you might specify `postgresql-9.4-1212.jdbc42.jar`, by default in the `/opt/netiq/idm/apps/postgres/` folder.

NetIQ does not support driver JAR files from third-party vendors.

- **Database Administrator**

Optional

Represents the name and password for the database administrator.

This field automatically lists the same user account and password that you specified for Database Username and Password. To use that account, do not make any changes.

Database administrator

(Optional) Specifies the account for a database administrator that can create database tables, views, and other artifacts.

Password

(Optional) Specifies the password for the database administrator.

- **Create Database Tables**

  Indicates whether you want to configure your new or existing database as part of the installation process, or afterward.

  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

  Generates a SQL script that the database administrator can run to create the databases. If you choose this option, you must also specify a name for **Schema File**. The setting is in the **SQL Output File** configuration.

  You might select this option if you do not have permissions to create or modify a database in your environment. For more information about generating the tables with the file, see "Manually Creating the Database Schema" on page 327.

- **New Database or Existing Database**

  Specifies whether you want to use existing, empty databases or create new tables in the existing database. Use the following considerations:

  - New Database

    If the database used is new, click **New Database.** Ensure that a database exists before selecting this option.

  - Existing Database

    If database is existing and it has User Application tables from a previous installation, select **Existing Database.**

    If the existing database runs on an Oracle platform, you must prepare Oracle before updating the schema. For more information, see "Preparing an Oracle Database for the SQL File" on page 524.

  After selecting the database type, you need to specify, as to when the database tables should be created. The Create Database Tables screen gives you the option to create tables at installation time or at application startup. Alternatively, you can create a schema file at installation time, which the Database Administrator would use to create the tables later.

  If you want to generate a schema file, select the Write SQL to File button and provide a name for the file in the Schema Output File field.

- **Test Database Connection**

  Specifies whether you want the installer to connect to the database for creating tables directly or for creating the `.sql` file.

  The installation program attempt the connection when you click **Next** or press **Enter**.

  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 "Manually Creating the SQL File to Generate the Database Schema" on page 328.

- **Java Install**

Represents the path to the JRE file used to launch the installation program. For example, `/root/opt/java/jre7`.

- ***Application_Server* Configuration**

  Represents the path to the installation files for Tomcat. For example, `/opt/apache-tomcat-7.0.52`. The installation process adds some files to this folder.

- **IDM Configuration**

  Represents the settings for the identity application context used in URLs and for the workflow engine.

  Application Context

  Specifies a name that represents the Tomcat 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 Tomcat. 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 identity applications from a browser.

- **Select Audit Logging Type**

  Indicates whether you want to send log events to an auditing server. Specify **Yes** or **No**.

- **Audit Logging**

  Applies only when you specify Yes for Select Audit Logging Type.

  Indicates the type of logging that you want to enable.

  For more information about setting up logging, see the *User Application Administration Guide.*

  Novell Identity Audit or NetIQ Sentinel

  Enables logging through a Novell or NetIQ client for the User Application.

  NOTE: If you choose this option, you must also specify the hostname or IP address for the client server and the path to the log cache.These settings are in the **Novell Identity Audit or NetIQ Sentinel** configuration section.

  OpenXDAS

  Enables the User Application to send events to your OpenXDAS logging server.

- **Security - Master Key**

  Indicates whether you want to import an existing master key. The User Application uses the master key to access encrypted data. Specify **Yes** or **No**.

  You might want to import the master key in the following situations:

  - After installing the first instance of the identity applications in a cluster. Every instance of the User Application in a cluster must use the same master key. For more information, see "Using the Same Master Key for Each User Application in the Cluster" on page 302.
  - 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.
  - If you are restoring your User Application and you want to access the encrypted data stored by your previous version of the User Application.

  Yes

  Specifies that you want to import an existing master key.

No

Specifies that you want the installation program to create the key.

By default, the installation procedure writes the encrypted master key to the `master-key.txt` file in the installation directory.

- **Import Master Key**

  Applies only when you specify Yes for Security - Master Key.

  Specifies the master key that you want to use. You can copy the master key from the `master-key.txt` file.

- **Application server connection**

  Represents the settings of the URL that users need to connect to the identity applications on Tomcat. For example, `https:myserver.mycompany.com:8080`.

  NOTE: If OSP runs on a different instance of the Tomcat application server, you must also select **Connect to an external authentication server** and specify values for the OSP server.

  Protocol

  Specifies whether you want to use *http* or *https*. To use Secure Sockets Layer (SSL) for communications, specify `https`.

  Host Name

  Specifies the DNS name or IP address of the server hosting OSP. Do not use `localhost`.

  Port

  Specifies the port that you want the server to use for communication with client computers.

  Connect to an external authentication server

  Specifies whether a different instance of Tomcat hosts the authentication server (OSP). The authentication server contains the list of users who can log in to SSPR.

  If you select this setting, also specify values for the authentication server's **Protocol**, **Host name**, and **Port**.

- **Authentication server details**

  Specifies the password that you want the identity applications to use when connecting to the authentication server. Also referred to as the client secret. The installation process creates this password.

7 Configure the settings for the identity applications in the Config Update window.

7a Browse for the **Identity Vault DNs**.

7b Click **OK**.

NOTE

- Ensure that the User Application and the Roles and Resources Service drivers are already created and deployed to the Identity Vault. For more information, see "Installation Considerations for the Identity Applications" on page 282.

- If you click **Cancel**, the installer takes you back to the Application Server Connection window.
- 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 Chapter 40, "Configuring the Settings for the Identity Applications," on page 339.

---

8 (Conditional) In a GUI installation, to immediately configure the identity applications, complete the following steps in the Configure IDM window:

8a Click **Yes** and then click **Next**.

8b In Roles Based Provisioning Module Configuration, click **Show Advanced Options.**

8c Modify the settings as needed.

NOTE

- For more information about specifying the values, see Chapter 40, "Configuring the Settings for the Identity Applications," on page 339.
- 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.

8d Click **OK**.

9 (Conditional) In a console installation, to immediately configure the identity applications, complete the following steps:

9a Launch the configuration update utility from the command line:

- **Linux**: `configupdate.sh`
- **Windows:** `configupdate.bat`

NOTE: SSO Client tab of the configupdate utility displays `localhost:defaultport` when Self Service Password Reset (SSPR) and Identity Reporting are not installed as a part of the same Identity User Application server. You need to manually update the **Client ID**, **Password** and the **Redirect URL** of the SSPR and Reporting server in the User Application server.

9b (Optional) To create the NMAS certificate, navigate to **SSO Clients > RBPM**, and then change **RBPM to eDirectory SAML configuration** to **Auto**.

9c Specify values for other settings as described in Chapter 40, "Configuring the Settings for the Identity Applications," on page 339.

10 Click **Next**.

11 In the Pre-Installation Summary window, click **Install**.

12 (Optional) Review the installation log files. For results of the basic installation, see the `user_application_install_log.log` file in the `/opt/netiq/idm/apps/UserApplication/logs/` directory.

For information about the identity applications configuration, see the `NetIQ-Custom-Install.log` file in the `/opt/netiq/idm/apps/UserApplication/` directory.

13 (Optional) If you are using an external password management WAR, manually copy the WAR to the installation directory and to the remote application server deploy directory that runs the external password WAR functionality.

14 Continue with the post-installation tasks described in Chapter 39, “Completing the Installation of the Identity Applications,” on page 327.

Silently Installing the Identity Applications

This section describes how to perform a silent install of the identity applications. A silent installation requires no interaction during the installation and can save you time, especially when you install on more than one server. You can perform silent installations on supported Linux computers only.

To prepare for the installation, review the activities listed in “Checklist for Installing the Identity Applications” on page 303. Also see the Release Notes accompanying the release.

This process includes the following activities:

- “Setting Passwords in the Environment for a Silent Installation” on page 310
- “Editing the Silent Properties File” on page 310
- “Importing eDirectory Certificates into Identity Applications” on page 315
- “Executing a Silent Installation of the Identity Applications” on page 316

Setting Passwords in the Environment for a Silent Installation

Instead of specifying the configuration passwords in the `.properties` file, 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 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
```

Editing the Silent Properties File

You must edit the parameter values in the `.properties` file before performing the silent installation or configuration. The table in this section provides a list of the parameters. The parameters correspond to the basic installation parameters as well as for configuring RBPM and the identity applications. For

more information about specifying the parameter values, see "Using the Guided Process to Install the Identity Applications" on page 304 and Chapter 40, "Configuring the Settings for the Identity Applications," on page 339.

1 Log in as `root` to the computer where you want to install the identity applications
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.
3 Open the `user_app.configure.properties` file.
4 Modify the following parameters in the `.properties` file:

Parameter Name	Description
USER_INSTALL_DIR=	Specify the installation path for the User Application. For example: `/opt/netiq/idm/apps/UserApplication`
NOVL_APP_SERVER_TYPE_CHOICE=	Specify the application server hosting the User Application. This release of Identity Manager supports only Apache Tomcat.
NOVL_TOMCAT_BASE_FOLDER=	Specify the base folder location of the application server hosting the User Application. For example: `/opt/netiq/idm/apps/tomcat`
NOVL_APPLICATION_NAME=	Specify the application context name. By default, it contains `IDMProv` as an application context name.
NOVL_CREATE_DB=	Specify whether you want to configure new or existing database as part of the installation process, or afterward. Alternatively, you can create a schema file at installation time, which the Database Administrator would use to create the tables later. Depending on your requirement, specify one of the following options: ◆ **Now:** The installation program creates the database tables as part of the installation process. ◆ **File:** The installation program generates a SQL script that the database administrator can run to create the databases. If you choose this option, you must also set `NOVL_CONFIG_WRITE_TO_FILE` to `1`. You might select this option if you do not have permissions to create or modify a database in your environment. For more information about generating the tables with the file, see "Manually Creating the Database Schema" on page 327. ◆ **Startup:** The installation program leaves instructions to create the tables when the User Application starts for the first time.

Parameter Name	Description
NOVL_DATABASE_NEW=	Specify whether you want to use existing, empty databases, or create new tables in the existing database. To create a new database specify `true`. Ensure that a database exists before selecting this option. Otherwise, specify `false`.
NOVL_UPGRADE=	To upgrade your User Application using an existing database, specify `true`. If database is existing and it has User Application tables from a previous installation, specify `false`. If the existing database runs on an Oracle platform, you must prepare Oracle before updating the schema. For more information, see "Preparing an Oracle Database for the SQL File" on page 524.
NOVL_UPGRADE_PROPS_FILE=	If you are upgrading the User Application, specify the path of the properties file of the currently installed application.
NOVL_JDBC_DRIVER=	Specify the absolute path of the JDBC jar file.
NOVL_DB_JARFILE_NAME=	For example: `/opt/netiq/idm/apps/postgres/postgresql-9.4.1212.jdbc42.jar`

NOVL_DB_DRIVER_CLASS_NAME=	Specify the database driver class name for the database that is used for installation.
	
	◆ **PostgreSQL:**
	`liquibase.database.core.PostgresDatabase`
	◆ **Oracle:**
	`liquibase.database.ext.OracleUnicodeDatabase`
	◆ **MS SQL:**
	`liquibase.database.ext.MSSQLUnicodeDatabase`
	
	NOTE: MS SQL is supported on Windows only.

NOVL_DB_DRIVER_NAME=	Specify the database driver name. ◆ **PostgreSQL:** `org.postgresql.Driver` ◆ **Oracle:** `oracle.jdbc.driver.OracleDriver` ◆ **MS SQL:** `com.microsoft.sqlserver.jdbc.SQLServerDriver` **NOTE:** MS SQL is supported on Windows only.

Parameter Name	Description
NOVL_DB_JDBC_URL=	Specify the URL to connect to the database running the User Application. ◆ **PostgreSQL:** `jdbc:postgresql:// <database server IP address:port>/ idmuserappdb` For example, `jdbc:postgresql:// 192.168.0.1:5432/idmuserappdb` ◆ **Oracle:** `jdbc:oracle:thin:@<database server IP address:port>:idmuserappdb` For example, `jdbc:oracle:thin:@192.168.0.1:1521:idm userappdb` ◆ **MS SQL:** `jdbc:sqlserver://<database server IP address:port>;DatabaseName=idmuserappd b` For example, `jdbc:sqlserver:// 192.168.0.1: 1433;DatabaseName=idmuserappdb` **NOTE:** MS SQL is supported on Windows only.
NOVL_DB_TYPE	Select the valid database type. Your options are: PostgreSQL, SQL Server, and Oracle.
NOVL_DB_ORACLE_VERSION=	If you select `Oracle` in `NOVL_DB_TYPE`, specify the version of the database.
NOVL_DB_HOST=	Specify the hostname or IP address of the User Application database server. For example: `192.168.0.1`
NOVL_DB_PORT=	Specify the port that is used by the User Application database server. For example: `5432`
NOVL_DB_NAME=	Specify the name of your database. For example, `idmuserappdb`.
NOVL_DB_USER=	Specify the name of an account that allows the User Application to access and modify data in the databases. For example, `idmadmin`.
NOVL_DB_USER_PASSWORD= NOVL_DB_USER_PASSWORD_CONFIRM=	Specify and confirm the password for the username specified in `NOVL_DB_USER`.
NOVL_CONFIG_DBADMIN_NAME= NOVL_CONFIG_DBADMIN_PASSWORD= NOVL_CONFIG_DBADMIN_PASSWORD_CONFIRM =	Specify the name and password for the database administrator. You can use the same user account and password that you specified for `NOVL_DB_USER` and `NOVL_DB_USER_PASSWORD`. To use that account, do not make any changes.

Parameter Name	Description
NOVL_CONFIG_WRITE_TO_FILE=	By default, the value of this property is set to `0`. To write database to a file, change the value to `1`. You might select this option if you do not have permissions to create or modify a database in your environment. For more information about generating the tables with the file, see "Manually Creating the Database Schema" on page 327.
RUN_LDAPCONFIG=	Specify whether you want to configure LDAP settings now or later. The options are: ◆ **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.
NOVL_JAVA_HOME=	Specify the JAVA_HOME path for this attribute and specify the same path for `USER_MAGIC_FOLDER_1` attribute also. For example: `/opt/netiq/idm/apps/jre`
NOVL_AUDIT_OFF= NOVL_AUDIT_ON=	Specify whether you want to set up auditing for the User Application. By default auditing is enabled. If you choose this option, you must also set `NOVL_AUDIT_SERVER` and `NOVL_AUDIT_LOG_CACHE_DIR` properties.
NOVL_AUDIT_SERVER=	If auditing is enabled, specify the hostname or IP address of the Audit server. For example: `192.168.0.1`
NOVL_AUDIT_LOG_CACHE_DIR=	If auditing is enabled, specify the absolute path of audit cache. For example: `/var/opt/novell/audit`
NOVL_XDAS_OFF= NOVL_XDAS_ON=	Specify whether you want to use XDAS for auditing the User Application. If you choose this option, you must also set the following XDAS options: ◆ NOVL_XDAS_SERVER_NAME ◆ NOVL_XDAS_LOGGING_DIR ◆ NOVL_XDAS_LOGGING_DIR
NOVL_XDAS_SERVER_NAME=	If XDAS is enabled, specify the hostname or IP address of the XDAS server.
NOVL_XDAS_LOGGING_DIR=	If XDAS is enabled, specify the path of the XDAS directory.
NOVL_UA_OSP_PWD=	Specify the User Application and OSP password.

Parameter Name	Description
NOVL_USE_EXTERNAL_AUTH_SERVER=	If OSP is installed on a different server, you can configure that server for external authentication with the User Application. If you choose this option, you must also set the following properties: ◆ `NOVL_EXTERNAL_AUTH_PROTOCOL` ◆ `NOVL_EXTERNAL_AUTH_HOSTNAME` ◆ `NOVL_EXTERNAL_AUTH_PORT` By default, authenticating to an external server is disabled.
NOVL_EXTERNAL_AUTH_PROTOCOL=	If you are using an external server for authentication, specify the external authentication protocol. For example: `http/https`
NOVL_EXTERNAL_AUTH_HOSTNAME=	If you are using an external server for authentication, specify the hostname or IP address of the authentication server. For example: `192.168.0.1`
NOVL_EXTERNAL_AUTH_PORT=	If you are using an external server for authentication, specify the port value of the authentication server. For example: `8180` for `http`, `8443` for `https`
NOVL_CONFIG_UPDATE_FILE_PATH=	Specify the path for the configuration update properties file. For example: `/root/configupdate.properties`

Importing eDirectory Certificates into Identity Applications

To establish a trust connection between Identity Applications and eDirectory server, import the eDirecotry certificates into Identity Applications.

1. Export the eDirectory certificate from iManager:
   - **1a** Log in to iManager as an administrator.
   - **1b** Navigate to **Roles and Task > NetIQ Certificate Access > Server Certificates**.
   - **1c** Check the **SSL CertificateDNS** check box and click **Export**.
   - **1d** From **Certificates** drop-down list, select **SSL CertificateDNS** option, clear the **Export Private Key** check box, and select the export format as **DER**.
   - **1e** Click **Next**.
   - **1f** Click **Save the exported certificate**, and exported certificate is saved on to your local system.
2. Import the eDirectory certificate into Identity Applications:
   - **2a** Log in to the server as an administrator where you want to install Identity Applications.
   - **2b** Copy the eDirectory certificate which you have exported from iManager, run `keytool` command:

```
<java bin path>keytool -import -trustcacerts -file <Cerificate_Path> -alias
<ALIAS_NAME> -keystore <java security keystore path>
```

In `Certificate_Path`, specify the location of eDirectory certificate that is saved in your computer.

In `ALIAS_NAME`, specify any alias name for the certificate. For example,

```
/opt/netiq/idm/jre/bin/keytool -import -trustcacerts -file /opt/
Certificate_Import_Path/EdirCertificate -alias EDIR_CERT -keystore /opt/
netiq/idm/jre/lib/security/cacerts
```

Executing a Silent Installation of the Identity Applications

1. Log in as a root user to the computer where you want to install the identity applications.
2. Open a terminal session.
3. Specify the values for the installation. For more information, see "Editing the Silent Properties File" on page 310 and "Safeguarding the Passwords for a Silent Installation" on page 249.
4. To launch the installation program for your platform, enter the following command:
   - **Linux**: `./IdmUserApp.bin -i silent -f /yourdirectorypath/silent.properties`
   - **Windows**: `./IdmUserApp.exe -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.

Post-Installation Steps

This section provides information about updating your Tomcat environment after you install the identity applications.

- "Configuring the User Application Driver for Clustering" on page 316
- "Passing the preferIPv4Stack Property to JVM" on page 317
- "Checking the Health of the Server" on page 317
- "Monitoring the Health Statistics" on page 317
- "Creating Compound Indexes" on page 318

If you used the convenience installer for Tomcat, the installation programs for Identity Manager configure Tomcat for you. If you installed your own Tomcat program, consider the following issues:

- You can modify the Tomcat service to perform more effectively. For more information, see *So You Want High Performance*.
- You might want to add support for logging events. For more information, see "Using the Apache Log4j Service to Log Sign-on" on page 254.

Configuring the User Application Driver for Clustering

For more information see, "Configuring the User Application Driver for Clustering" on page 324.

Passing the preferIPv4Stack Property to JVM

The identity applications use 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`.

Checking the Health of the Server

Most loadbalancers provide a healthcheck feature for determining whether an HTTP server is up and listening. The User Application contains a URL that can be used for configuring HTTP healthchecks on your loadbalancer. The URL is:

```
http://<NodeIP>:port/IDMProv/jsps/healthcheck.jsp
```

Monitoring the Health Statistics

The new API allows you to retrieve information about the health of the User Application. The `REST API` can access the system for the currently running threads, memory consumption, cache, and cluster information and returns the information using the `GET` operation.

- **Memory information (JVM and system memory):** Reads the memory related information such as system memory and memory consumed by the JVM.

  For example,

  ```
  http://<ip_addr:port>/IDMProv/rest/monitoring/statistics/memoryinfo
  ```

- **Thread information:** Reads the information about the CPU-intensive threads and returns the list of top threads that cause heavy utilization of the CPU.

  For example,

  ```
  http://<ip_addr:port>/IDMProv/rest/monitoring/statistics/threadinfo
  ```

  To access the stack trace of threads in the JVM, set the stack parameter to **True**.

  For example,

  ```
  http://<ip_addr:port>/IDMProv/rest/monitoring/statistics/threadinfo?stack=true
  ```

  To specify the number of threads in the JVM, specify the value for the **thread-count** parameter.

  For example,

```
http://<ip_addr:port>/IDMProv/rest/monitoring/statistics/threadinfo?thread-count=1
```

- **Cache information:** Reads the cache information for the User Application.

  For example,

  ```
  http://<ip_addr:port>/IDMProv/rest/monitoring/statistics/cacheinfo
  ```

- **Cluster information:** Reads the cluster related information.

  For example,

  ```
  http://<ip_addr:port>/IDMProv/rest/monitoring/statistics/clusterinfo
  ```

NOTE: You need to be a Security Administrator to view the User Application health statistics by using the REST API.

Creating Compound Indexes

After installing or upgrading the identity applications, manually create the compound indexes for each attribute that you want to use to sort users in the Identity Manager Dashboard. You can create compound indexes using `ndsindex` utility which is located in the eDirectory installed path. You can specify multiple attributes separated using `$` sign for compound indexing. Following are the basic attributes that require compound indexing:

- Surname,Given Name
- Given Name,Surname
- cn,Surname
- Title,Surname
- Telephone Number,Surname
- Internet Email Address,Surname
- L,Surname
- OU,Surname

The following command helps you to create compound indexes using `ndsindex` utility:

```
ndsindex add [-h <hostname>] [-p <port>] -D <admin DN> -W|[-w <password>] -s
<eDirectory Server DN> [<indexName1>, <indexName2>.....]
```

For example, to sort users based on **Title**, execute the following command:

Linux

```
ndsindex add -h <hostname> -p <ldap port> -D <admin DN> -w <admin passwd> -s
<eDirectory Server DN> Title-SN\;Title\$Surname\;value
```

Windows

```
ndsindex add -h <hostname> -p <ldap port> -D <admin DN> -w <admin passwd> -s
<eDirectory Server DN> Title-SN;Title$Surname;value
```

You can also create compound indexes using Conversion Export Utility.

You must use an LDIF file to create indexes. After the LDIF file is imported, initiate the indexing activity by triggering Limber. Otherwise, indexing takes place when Limber triggers automatically.

Example LDIF file to create compound indexes to sort users on **Title** attribute:

```
dn: cn=osg-nw5-7, o=Novell

changetype: modify

add: indexDefinition

indexDefinition: 0$sntitleindex$0$0$0$1$Title$surname
```

For more information LDIF files, see LDIF Files in NetIQ eDirectory Administration Guide.

Disabling the Prevent HTML Framing Setting for Integrating Identity Manager with SSPR

This section discusses the configuration required for Identity Manager to integrate it with an existing SSPR 3.2 environment which is not deployed by Identity Manager 4.5. SSPR provides a configurable option, **Prevent HTML Framing**, that allows users to view SSPR in an inline frame for any application that includes the iframe html source code. If you select this option, SSPR is not included in the specified iFrame for the application. To disable this option for Identity Manager, run the following steps:

1. Go to http://*<IP/DNS name>:<port>/sspr.* This link takes you to the SSPR portal.
2. Log in as SSPR administrator.
3. Click **Configuration Editor** at the top of the page and specify the OSP configuration password.
4. Click **Settings > Security** > **Always Show Advanced Settings**, and do the following actions:
   - **4a** Browse for **Prevent HTML Framing,** de-select **Enabled** and then click **Save** to save the setting.
   - **4b** In the confirmation window, click **OK**.

Starting the Identity Applications

This section provides instructions for starting the identity applications and logging in the first time on an application server. In a cluster environment, start the procedure on the primary node. The identity applications should be installed and ready for deployment. For more information about post-installation tasks, see Chapter 39, “Completing the Installation of the Identity Applications,” on page 327.

- “Starting the User Application on a Tomcat Server” on page 319

Starting the User Application on a Tomcat Server

This section requires a startup script for Tomcat application server.

- **Linux**: `/etc/init.d/idmapps_tomcat_init start`
- **Windows**: `services.msc`

  From `services.msc`, start the Tomcat service. You can also use this file for stopping and restarting the Tomcat service.

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 61, “Troubleshooting,” on page 535.

To start the identity applications:

1. Start the database for the identity applications. 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 Tomcat. 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 Tomcat where you installed the identity applications.

   NOTE: In a cluster, start the primary node only.

4. At the command line, make the installation directory your working directory.
5. Execute the startup script.
6. To enable communication with the User Application driver, complete the following steps:
   - **6a** Log in to iManager.
   - **6b** Under **Roles and Tasks > Identity Manager** in the left navigation frame, click **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** Click **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 in to the User Application, enter the following URL in your web browser:

   `http://hostname:port/ApplicationName`

   hostname

   Represents the name of the application server (Tomcat). 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. For example, `IDMProv`.
9. In the upper right corner of the User Application landing page, click **Login**.
10. (Conditional) To enable the User Application in a cluster group, complete the following steps:
    - **10a** Click **Administration**.
    - **10b** In the Application Configuration portal, click **Caching**.
    - **10c** In the Caching Management window, select **True** for **Cluster Enabled**.

10d Click **Save**.

10e Restart the server.

10f (Conditional) To use local settings, repeat this procedure for each server in the cluster.

38 Creating and Deploying the Drivers for the Identity Applications

The process for installing RBPM adds the files for creating the drivers for the Identity Applications. 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 in Designer. When you create a new Identity Manager project, the user interface automatically prompts you to import several packages into the new project.

- "Creating the User Application Driver" on page 323
- "Configuring the User Application Driver for Clustering" on page 324
- "Creating the Role and Resource Service Driver" on page 324
- "Deploying the Drivers for the User Application" on page 325

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. In the **Modeler > Provisioning** 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**.
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**.

Configuring the User Application Driver for Clustering

In a clustered environment, you can use a single User Application driver with multiple instances of the User Application. The driver stores various kinds of information (such as workflow configuration and cluster information) that is application-specific. You must configure the driver to use the host name or IP address of the dispatcher or load balancer for the cluster.

1. Log in to the instance of iManager that manages your Identity Vault.
2. In the navigation frame, select **Identity Manager**.
3. Select **Identity Manager Overview**.
4. Use the search page to display the Identity Manager Overview for the driver set that contains your User Application driver.
5. Click the round status indicator in the upper right corner of the driver icon:
6. Select **Edit Properties**.
7. For **Driver Parameters**, change **Host** to the host name or IP address of the dispatcher.
8. Click **OK**.

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. In the **Modeler > Provisioning** 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**.
5. (Conditional) If this is the first driver you have installed in Designer, click **OK** to install the **Common Settings Advanced Edition** package.
   - **5a** Specify the URL for the User Application server.
   - **5b** Specify the eDirectory DN for the User Application Administrator.
   - **5c** Specify the LDAP DN for the User Application Provisioning Service account. It can be the same account as your User Application Administrator or a different account.

     If a Role or Resource provisioning request is initiated by this service account, then any approvals or provisioning workflows associated with this role or resource are bypassed.
6. (Optional) Specify the name of the driver.
7. Click **Next**.
8. In the User Application/Workflow Connection window, specify the User-Group base container DN 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.
9. Specify the URL for the User Application.
10. Specify the LDAP DN of the User Application Administrator account

    The User Application Administrator account authenticates to the User Application in order to start the Approval Workflow. For more information, see "Assign Rights to Identity Vault Administrator and User Application Administrator Account" on page 292.

11 Specify the password of the User Application Administrator account.

12 Click **Next**.

13 In the Confirm Installation Tasks window, click **Finish**.

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**.

39 Completing the Installation of the Identity Applications

This section provides instructions for activities that you might want to perform after installing identity application and their framework:

- "Checking the Health of the Server in a Clustered Environment" on page 327
- "Manually Creating the Database Schema" on page 327
- "Recording the Master Key" on page 329
- "Configuring the Identity Vault for the Identity Applications" on page 329
- "Changing the Default Context Name for User Application" on page 330
- "Reconfiguring the WAR File for the Identity Applications" on page 333
- "Configuring Forgotten Password Management" on page 333

Checking the Health of the Server in a Clustered Environment

For more information see, "Checking the Health of the Server" on page 317

Manually Creating the Database Schema

When you install the identity applications, you can postpone connecting to the database or creating tables in the database. If you do not have permissions to the database, you might need to choose this option. The installation program creates a SQL file that you can use to create the database schema. You can also recreate the database tables after installation without having to reinstall. To do so, you delete the database for the identity applications and create a new database with the same name.

Using the SQL File to Generate the Database Schema

This section assumes that the installation program created a SQL file that you can execute to generate the database schema. If you do not have the SQL file, see "Manually Creating the SQL File to Generate the Database Schema" on page 328.

NOTE: Do not use SQL*Plus to execute the SQL file. The line lengths in the file exceed 4000 characters.

---

1. Stop the Application Server.
2. Login to the Database Server.
3. Delete the database that is used by the identity applications.
4. Create a new database with the same name as the one that was deleted in Step 3.
5. Navigate to the SQL script that the installation process created, by default in the `/installation_path/userapp/sql` directory.

6 (Conditional) For an Oracle database, insert a backslash (/) after the definition of the function `CONCAT_BLOB`. For example:

```
  -- Changeset icfg-data-load.xml::700::IDMRBPM
CREATE OR REPLACE FUNCTION CONCAT_BLOB(A IN BLOB, B IN BLOB) RETURN BLOB AS
                C BLOB;
            BEGIN
                DBMS_LOB.CREATETEMPORARY(C, TRUE);
                DBMS_LOB.APPEND(C, A);
                DBMS_LOB.APPEND(C, B);
                RETURN c;
            END;
/
```

7 Have the database administrator run the SQL script to create and configure the User Application database.

8 Restart Tomcat.

Manually Creating the SQL File to Generate the Database Schema

You can recreate the database tables after installation without having to reinstall and without having the SQL file. This section helps you create the database schema in the event that you do not have the SQL file.

1 Stop Tomcat.

2 Log in to the server that hosts your identity applications database.

3 Delete the existing database.

4 Create a new database with the same name as the one that you deleted in Step 3.

5 In a text editor, open the `NetIQ-Custom-Install.log` file, located by default at the root of the installation directory for the identity applications. For example:

```
/opt/netiq/idm/apps/UserApplication
```

6 Search and copy the below command from the `NetIQ-Custom-Install.log` file:

```
/opt/netiq/idm/jre/bin/java -Xms256m -Xmx256m  -Dwar.context.name=IDMProv -
Ddriver.dn="cn=User Application Driver,cn=driverset1,o=system" -
Duser.container="o=data" -jar /opt/netiq/idm/apps/UserApplication/
liquibase.jar --databaseClass=liquibase.database.core.PostgresDatabase --
driver=org.postgresql.Driver --classpath=/opt/netiq/idm/apps/postgresql/
postgresql-9.4.1212jdbc42.jar opt/netiq/idm/apps/UserApplication/IDMProv.war -
-changeLogFile=DatabaseChangeLog.xml  --url="jdbc:postgresql://localhost:5432/
idmuserappdb" --contexts="prov,newdb" --logLevel=info --logFile=/opt/netiq/
idm/apps/UserApplication/db.out --username=******** --password=******** update
```

7 Log in to the server where you installed the database for the identity applications.

8 In a terminal, paste the command string that you copied.

NOTE: The command should be `updateSQL`. If it is `update`, change the command to `updateSQL`.

---

9 In the command, replace the asterisks (*) that represent the database username and password with the actual values required to authenticate. Also, ensure the name of the SQL file is unique.

10 Execute the command.

11 (Conditional) If the process generates a SQL file instead of populating the database, provide the file to your database administrator to import into the database server. For more information, see "Using the SQL File to Generate the Database Schema" on page 327.

12 After the database administrator imports the SQL file, start Tomcat.

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 identity applications on other members of the cluster.

If you installed the identity applications 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 `ism-configuration.properties` file.

1 Open the `ism-configuration.properties` 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.

Configuring the Identity Vault for the Identity Applications

The identity applications must be able to interact with the objects in your Identity Vault.

To improve the performance of the identity applications, the eDirectory Administrator should create value indexes for the manager, ismanager and srvprvUUID attributes. Without value indexes on these attributes, identity application users can experience impeded performance, particularly in a clustered environment.

You can create these value indexes automatically during installation by selecting Advanced > Create eDirectory Indexes in the RBPM Configuration utility. For more information about using Index Manager to create value indexes, see the *NetIQ eDirectory Administration Guide*.

Pre-installation Tasks for Non-Root Users

Perform the following steps before installing Identity Manager User Application as non-root user:

1 Import the eDirectory certificate into the User Application `JRE cacerts` file.

2 Ensure that the **Default Notification Collection** object is deployed.

3 Add SAML method to the eDirectory server using the following command:

```
nmasinst -addmethod <admin dn> <tree-name> <configuration file present in /
<eDirectory installed location>/nmas/NmasMethods/Novell/SAML> -h <hostname:NCP
port> -w <pawsswd>
```

For example on Linux:

```
nmasinst -addmethod admin.sa.system TREE /home/user1/eDirectory/nmas/
NmasMethods/Novell/SAML/config.txt -h 10.10.10.248:524 -w novell
```

For example on Windows:

```
nmasinst.exe -addmethod admin.sa.system tree
C:\Users\Administrator\Desktop\SAML\config.txt -h 10.10.10.248:524
```

4 Extend the required schema:

```
ndssch -h <hostname:port> -t <treename> <admin dn> authsaml.sch
ndssch -h <hostname:port> -t <treename> <admin dn> edirectory-schema.sch
ndssch -h <hostname:port> -t <treename> <admin dn> osp.sch
```

For example:

```
ndssch -h 10.10.10.248 -t TREE admin.sa.system authsaml.sch
```

5 Restart eDirectory.

Changing the Default Context Name for User Application

Instead of using the default context name, you can create a new context based on your organizational requirements. You can change the context name in the console or in the GUI by performing the following actions:

1 Stop the Tomcat service.

```
/etc/init.d/idmapps_tomcat_init stop
```

2 Navigate to the User Application directory located in `/opt/netiq/idm/apps/UserApplication`.

3 Launch the configupdate utility in GUI mode.

Ensure that the `use_console` option is set to `false` in `configupdate.sh.properties` or `configupdate.bat.properties` file.

Alternatively, launch the configupdate utility and pass an additional command line argument on Linux.

```
./configupdate.sh use_console=false
```

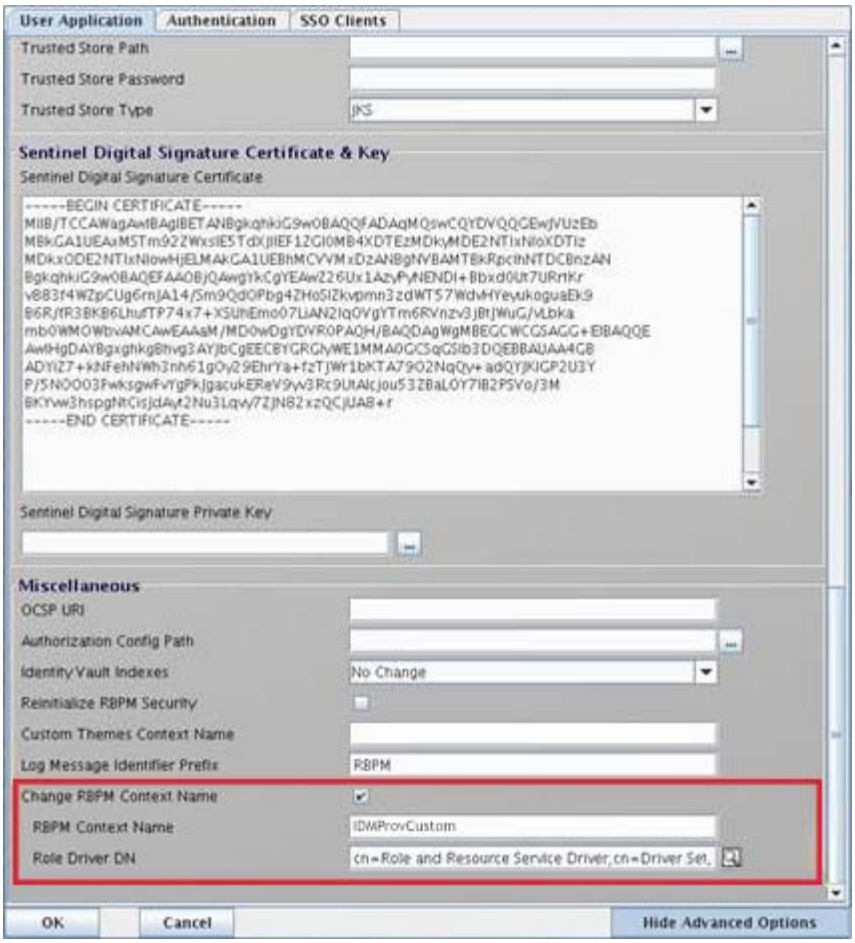
4 In the **User Application** tab, click **Show Advanced Options** and perform the following steps:

4a Select **Change RBPM Context Name**.

4b Specify the custom context name in **RBPM Context Name**. For example, `IDMProvCustom`.

4c Browse to and select the Roles Driver DN. For example, `cn=Role and Resource Service Driver,cn=Driver Set,o=system`.

4d Click **OK**.



5 Verify that the war file is renamed.

- Navigate to `/opt/netiq/idm/apps/tomcat/webapps` and check if `IDMProvCustom.war` entry is updated.
- Navigate to `ism-configuration` properties file located in `/TOMCAT_INSTALLED_HOME/conf` and check if `portal.context` entry specifies the new context name.

6 Update your database with the new context name by using the `update-context.sh` script located in `/opt/netiq/idm/apps/UserApplication`.

Execute the following command to run the `update-context.sh` script.

```
ua:/opt/netiq/idm/apps/UserApplication # vi update-context.sh
```

You should see the following entries on your screen:

```
# copy and paste or execute this script before changing context name

# Substitute your new context where indicated

#
```

```
/opt/netiq/idm/apps/jre/bin/java -Xms256m -Xmx256m  -Dwar.context.name=[New
Context Here] -Ddriver.dn=[UA Driver DN] -jar /opt/netiq/idm/apps/
UserApplication/liquibase.jar --
databaseClass=liquibase.database.core.PostgresDatabase  --
driver=org.postgresql.Driver  --classpath=/opt/netiq/idm/apps/postgres/
postgresql-9.4.1212.jdbc42.jar:/opt/netiq/idm/apps/tomcat/webapps/IDMProv.war
--changeLogFile=UpdateProducerId.xml   --url="jdbc:postgresql://
localhost:5432/idmuserappdb?compatible=true" --contexts="prov,updatedb" --
logLevel=debug --username=******** --password=******** update
```

For example, run the following script if you are using a PostgreSQL database:

```
/opt/netiq/idm/apps/jre/bin/java -Xms256m -Xmx256m  -
Dwar.context.name=IDMProvCustom  -Ddriver.dn= cn=Role and Resource Service
Driver,cn=driverset1,o=system -jar /opt/netiq/idm/apps/UserApplication/
liquibase.jar --databaseClass=liquibase.database.core.PostgresDatabase  --
driver=org.postgresql.Driver  --classpath=/opt/netiq/idm/apps/postgres/
postgresql-9.4.1212.jdbc42.jar:/opt/netiq/idm/apps/tomcat/webapps/IDMProv.war
--changeLogFile=UpdateProducerId.xml   --url="jdbc:postgresql://<Database
Server:5432/idmuserappdb?compatible=true" --contexts="prov,updatedb" --
logLevel=debug --–username=dbadmin --password=******** update
```

where

`-Dwar.context.name=IDMProvCustom` specifies the new context.

`-Ddriver.dn ="cn=User Application Driver,cn=driverset1,o=system"` specifies the User Application driver DN.

`--username=dbadmin` specifies the database administrator username that can create database tables, views, and other artifacts.

IMPORTANT: Do not change the database driver details in the script for other supported databases.

---

7 Verify that the database tables have the new context name.

Table Name	Column to Check
PORTALPRODUCERS	`producerid`
PORTALPRODUCERREGISTRY	`producerid`
PORTALREGISTRY	`producerid`
PORTALPORTLETSETTINGS	`producerid`
PORTALPORTLETHANDLES	`producerid`
PROFILEGROUPPREFERENCES	`elementid`

For example, run the following SQL command to verify the new context name in the `PORTALPRODUCERS` table:

```
Select * from PORTALPRODUCERS;
```

The command should return only the new context name.

8 Start the Tomcat service.

```
/etc/init.d/idmapps_tomcat_init start
```

Reconfiguring the WAR File for the Identity Applications

To update your WAR file for the identity applications, run the RBPM Configuration utility.

1. Run the utility in the install directory by executing `configupdate.sh` or `configupdate.bat`.

   For more information about utility parameters, see Chapter 40, "Configuring the Settings for the Identity Applications," on page 339.

2. Deploy the new WAR file to your application server.

   For Tomcat single server, the changes are applied to the deployed WAR.

Configuring Forgotten Password Management

The Identity Manager installation includes Self Service Password Reset to help you manage the process for resetting forgotten passwords. Alternatively, you can use an external password management system.

- "Using Self Service Password Reset for Forgotten Password Management" on page 333
- "Using the Legacy Provider for Forgotten Password Management" on page 335
- "Using an External System for Forgotten Password Management" on page 336
- "Updating SSPR Links in the Dashboard for a Distributed or Clustered Environment" on page 338

Using Self Service Password Reset for Forgotten Password Management

In most cases, you can enable the forgotten password management feature when you install SSPR and the identity applications. However, you might not have specified the URL of the landing page for the identity applications to which SSPR forwards users after a password change. You might also need to enable forgotten password management. This section provides the following information:

- "Configuring Identity Manager to Use Self Service Password Reset" on page 333
- "Configuring Self Service Password Reset for Identity Manager" on page 334
- "Locking the SSPR Configuration" on page 334

Configuring Identity Manager to Use Self Service Password Reset

This section provides information about configuring Identity Manager to use SSPR.

1. Log in to the server where you installed the identity applications.
2. Run the RBPM configuration utility. For more information, see "Running the Identity Applications Configuration Utility" on page 339.
3. In the utility, navigate to **Authentication > Password Management**.
4. For **Password Management Provider**, specify **SSPR**.
5. Select **Forgotten Password**.
6. Navigate to **SSO Clients > Self Service Password Reset**.

7 For **OSP client ID**, specify the name that you want to use to identify the single sign-on client for SSPR to the authentication server. The default value is `sspr`.

8 For **OSP client secret**, specify the password for the single sign-on client for SSPR.

9 For **OSP redirect URL**, specify the absolute URL to which the authentication server redirects a browser client when authentication is complete.

   Use the following format: `protocol://server:port/path`.For example, `http://10.10.10.48:8180/sspr/public/oauth.`

10 Save your changes and close the utility.

Configuring Self Service Password Reset for Identity Manager

This section provides information about configuring SSPR to work with Identity Manager. For example, you might want to modify the password policies and challenge response questions.

When you installed SSPR with Identity Manager, you specified a password that an administrator can use to configure the application. NetIQ recommends that you modify the SSPR settings, then specify an administrator account or group can configure SSPR. For more information about the configuration password, see Chapter 32, “Installing Password Management for Identity Manager,” on page 267.

1 Log in to SSPR by using the configuration password that you specified during installation.

2 In the Settings page, modify the settings for the password policy and challenge response questions. For more information about configuring the default values for SSPR settings, see Configuring Self Service Password Reset in the *NetIQ Self Service Password Reset Administration Guide*.

3 Lock the SSPR configuration file (`SSPRConfiguration.xml`). For more information about locking the configuration file, see “Locking the SSPR Configuration” on page 334.

4 (Optional) To modify SSPR settings after you lock the configuration, you must set the `configIsEditable` setting to `true` in the `SSPRConfiguration.xml` file.

5 Log out of SSPR.

6 For the changes to take effect, restart Tomcat.

Locking the SSPR Configuration

1 Go to **http://<IP/DNS name>:<port>/sspr**. This link takes you to the SSPR portal.

2 Log in to the Identity Manager with an administrator account or log in with your existing login credentials.

3 Click **Configuration Manager** at the top of the page and specify the configuration password that you specified during installation.

4 Click **Configuration Editor** and navigate to **Settings > LDAP Settings**.

5 Lock the SSPR configuration file (`SSPRConfiguration.xml`).

   5a Under the Administrator Permission section, define a filter in LDAP format for a user or a group that has administrator rights to SSPR in the Identity Vault. By default, the filter is set to `groupMembership=cn=Admins,ou=Groups,o=example`.

   For example, set it to `uaadmin` (`cn=uaadmin`) for the User Application administrator.

   This prevents users from modifying the configuration in SSPR except the SSPR admin user who has full rights to modify the settings.

   5b To ensure LDAP query returns results, click **View Matches**.

If there is any error in the setting, you cannot proceed to the next configuration option. SSPR displays the error details to help you troubleshoot the issue.

5c Click **Save**.

5d In the confirmation window that pops up, click **OK**.

When SSPR is locked, the admin user can see additional options in the Administration user interface such as Dashboard, User Activity, Data Analysis, and so on that were not available for him before SSPR lock down.

6. (Optional) To modify SSPR settings after you lock the configuration, you must set the `configIsEditable` setting to `true` in the `SSPRConfiguration.xml` file.
7. Log out of SSPR.
8. Log in to SSPR again as an admin user defined in Step 3.
9. Click **Close Configuration**, then click **OK** to confirm the changes.
10. For the changes to take effect, restart Tomcat.

Using the Legacy Provider for Forgotten Password Management

Instead of SSPR, you can use the legacy provider in Identity Manager for the Forgotten Password Management feature. If you choose the legacy provider, you do not need to install SSPR. However, you will need to reassign permissions for users to access the shared pages for password management. This section provides the steps to perform these activities:

- "Configuring the Legacy Provider for Forgotten Password Management" on page 335
- "Reassigning Permissions for the Password Management Pages" on page 336

For more information about the legacy provider, see "Understanding the Legacy Password Management Provider" on page 36. For more information about shared pages and permissions, see "Page Administration" in the *NetIQ Identity Manager - Administrator's Guide to the Identity Applications*.

Configuring the Legacy Provider for Forgotten Password Management

1. Log in to the server where you installed the identity applications.
2. Run the RBPM configuration utility. For more information, see "Running the Identity Applications Configuration Utility" on page 339.
3. In the utility, navigate to **Authentication > Password Management**.
4. For **Password Management Provider**, specify **User Application (Legacy)**.
5. For **Forgotten Password**, specify **Internal**.
6. Navigate to **SSO Clients > Self Service Password Reset**.
7. For **OSP redirect URL**, the setting should be empty.
8. Save your changes and close the utility.

Reassigning Permissions for the Password Management Pages

The settings for the identity applications default to SSPR during installation. You must assign or reassign the permissions for the users, groups, or containers that you want to access the shared pages for managing passwords. When you assign users `View` permission for a container page or shared page, the users can access the page and see it in a list of available pages.

1. Ensure that Identity Manager is using the legacy provider. For more information, see "Configuring the Legacy Provider for Forgotten Password Management" on page 335.
2. Log in to the User Application as the application administrator. For example, log in as `uaadmin`.
3. Navigate to **Administration > Page Admin**.
4. In the **Shared Pages** panel, navigate to **Password Management**.
5. Select the page for which you want to specify permissions. For example, Change Password or Password Challenge Response.
6. In the right panel, click **Assign Permission**.
7. In **View**, select the users, groups, or containers that you want to assign to the page.
8. (Optional) To ensure that only an application administrator can access the specified page, select **View Permission Set to Admin Only**.
9. Click **Save**.
10. Perform Step 5 through Step 9 for each page that you want to configure.
11. Select the **Home** icon to return to the Dashboard.
12. Navigate to **Applications**, then select ⚙.
13. On the **Manage Applications** page, replace the link to SSPR with the link for UserApp PwdMgt.

    For more information, see "Updating SSPR Links in the Dashboard for a Distributed or Clustered Environment" on page 338 and the *Help for the Identity Applications*.
14. Log out, and then restart Tomcat.

Using an External System for Forgotten Password Management

To use an external system, you must specify the location of a WAR file containing Forgot Password functionality. This process includes the following activities:

- "Specifying an External Forgotten Password Management WAR File" on page 336
- "Testing the External Forgot Password Configuration" on page 337
- "Configuring SSL Communication between Application Servers" on page 337

Specifying an External Forgotten Password Management WAR File

If you did not specify this values during installation and want to modify the settings, you can use either the RBPM Configuration utility or make the changes in the User Application as an administrator.

1. (Conditional) To modify the settings in the RBPM Configuration utility, complete the following steps:
   - **1a** Log in to the server where you installed the identity applications.
   - **1b** Run the RBPM configuration utility. For more information, see "Running the Identity Applications Configuration Utility" on page 339.

1c In the utility, navigate to **Authentication > Password Management**.

1d For **Password Management Provider**, specify **User Application (Legacy)**.

2 (Conditional) To modify the settings in the User Application, complete the following steps:

2a Log in as the User Application Administrator.

2b Navigate to **Administration > Application Configuration > Password Module Setup > Login**.

3 For **Forgotten Password**, specify **External**.

4 For **Forgot Password Link**, specify the link shown when the user clicks **Forgot password** on the login page. When the user clicks this link, the application directs the user to the external password management system. For example:

```
http://localhost:8180/ExternalPwd/jsps/pwdmgt/ForgotPassword.jsp
```

5 For **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. For example:

```
http://localhost/IDMProv
```

6 For **Forgot Password Web Service URL**, specify the URL for the web service that the external forward password WAR uses to call back to the identity applications. Use the following format:

```
https://idmhost:sslport/idm/pwdmgt/service
```

The return link must use SSL to ensure secure web service communication to the identity applications. For more information, see "Configuring SSL Communication between Application Servers" on page 337.

7 Manually copy `ExternalPwd.war` to the remote application server deploy directory that runs the external password WAR functionality.

Testing the External Forgot Password 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`.
- On the User Application login page, click the link for **Forgot password**.

Configuring SSL Communication between Application Servers

If you use an external password management system, you must configure SSL communication between the Tomcat instances on which you deploy the identity applications and the External Forgotten Password Management WAR file. For more information, refer to the Tomcat documentation.

Updating SSPR Links in the Dashboard for a Distributed or Clustered Environment

The installation process assumes that you deploy SSPR on the same application server as the identity applications and Identity Reporting. By default, the built-in links on the **Applications** page in the Dashboard use a relative URL format that points to SSPR on the local system. For example, `/sspr/private/changepassword`. If you install the applications in a distributed or clustered environment, you must update the URLs for the SSPR links.

For more information, see the *Help for the Identity Applications*.

1. Log in as an administrator to the Dashboard. For example, log in as `uaadmin`.
2. Click **Edit**.
3. In the Edit Home Items page, hover on the item that you want to update, and then click the edit icon. For example, select **Change My Password**.
4. For **Link**, specify the absolute URL. For example, `http://10.10.10.48:8180/sspr/changepassword`.
5. Click **Save**.
6. Repeat for each SSPR link that you want to update.
7. Upon completion, click **I'm done**.
8. Log out, and then log in as a regular user to test the changes.

40 Configuring the Settings for the Identity Applications

The Identity Applications Configuration utility helps you manage the settings for the User Application drivers and the identity applications. The installation program for the identity applications invokes a version of this utility so that you can more quickly configure the applications. You can also modify most of these settings after installation.

The file to run the Configuration utility is located by default in an installation subdirectory for the identity applications:

- **Linux**: `configupdate.sh` script
- **Windows**: `configupdate.bat` file

NOTE: In a cluster, the configuration settings must be identical for all members of the cluster.

This section explains the settings in the configuration utility. The settings are organized by tabs. If you install Identity Reporting, the process adds parameters for Reporting to the utility.

- "Running the Identity Applications Configuration Utility" on page 339
- "User Application Parameters" on page 340
- "Authentication Parameters" on page 349
- "SSO Clients Parameters" on page 354
- "Reporting Parameters" on page 361

Running the Identity Applications Configuration Utility

1. On Linux, using a text editor, open the `configupdate.sh` file, located by default in the installation directory for the User Application: `/opt/netiq/idm/apps/UserApplication`.
2. In `configupdate.sh.properties`, 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, use one of the following methods to run the configuration utility:
   - **Linux**: `./configupdate.sh`
   - **Windows**: `configupdate.bat`

   NOTE: You might need to wait a few minutes for the utility to start up.

User Application Parameters

When configuring the identity applications, this tab defines the values that the applications use when communicating with the Identity Vault. Some settings are required for completing the installation process.

By default, the tab displays the basic options. To see all settings, click **Show Advanced Options**. This tab includes the following groups of settings:

- "Identity Vault Settings" on page 340
- "Identity Vault DNs" on page 341
- "Identity Vault User Identity" on page 343
- "Identity Vault User Groups" on page 344
- "Identity Vault Certificates" on page 345
- "Email Server Configuration" on page 345
- "Trusted Key Store" on page 347
- "NetIQ Sentinel Digital Signature Certificate & Key" on page 347
- "Miscellaneous" on page 348
- "Container Object" on page 349

Identity Vault Settings

This section defines the settings that enable the identity applications to access the user identities and roles in the Identity Vault. Some settings are required for completing the installation process.

Identity Vault Server

Required

Specifies the hostname or IP address for your LDAP server. For example: `myLDAPhost`.

LDAP port

Specifies the port on which the Identity Vault listens for LDAP requests in clear text. The default value is 389.

For more information about using LDAP, see "Using LDAP to Communicate with the Identity Vault" on page 80.

LDAP secure port

Specifies the port on which the Identity Vault listens for LDAP requests using Secure Sockets Layer (SSL) protocol. The default value is 636.

If a service already loaded on the server (before you install eDirectory) uses the default port, you must specify a different port. For more information about using LDAP, see "Using LDAP to Communicate with the Identity Vault" on page 80.

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 identity applications use 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.

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 RBPM uses TLS/SSL protocol for all communication related to the logged-in user's account. This setting allows other operations that do not require TLS/SSL to operate without the protocol.

NOTE: This option might have adverse performance implications.

Identity Vault DNs

This section defines the distinguished names for containers and user accounts that enable communication between the identity applications and other Identity Manager components. Some settings are required for completing the installation process.

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 Container DN

Required

When showing the advanced options, the utility displays this parameter under Identity Vault User Identity.

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 in to the identity applications.
- If you have started Tomcat hosting the identity applications, 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.

Group Container DN

Required

When showing the advanced options, the utility displays this parameter under Identity Vault User Groups.

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 Tomcat hosting the identity applications, you cannot change this setting with the `configupdate.sh` or `configupdate.bat` files.

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 Tomcat 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, 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, 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, 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 identity applications, use the **Administration > Administrator Assignments** page in the User Application.
- During a configuration update, 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 identity applications, use the **Administration > Administrator Assignments** page in the User Application.
- During a configuration update, 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 identity applications, 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 identity applications, 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 identity applications, 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.

Identity Vault User Identity

This section defines the values that enable the identity applications to communicate with a user container in the Identity Vault. Some settings are required for completing the installation process.

The utility displays these settings only when you select **Show Advanced Options**.

User Container DN

Required

When not showing the advanced options, the utility displays this parameter under Identity Vault DNs.

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 in to the identity applications.
- If you have started Tomcat hosting the identity applications, 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 Search 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.

Identity Vault User Groups

This section defines the values that enable the identity applications to communicate with a group container in the Identity Vault. Some settings are required for completing the installation process.

The utility displays these settings only when you select **Show Advanced Options**.

Group Container DN

Required

When not showing the advanced options, the utility displays this parameter under Identity Vault DNs.

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 Tomcat hosting the identity applications, 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.

You must also specify a value for **Dynamic Group Object Class**.

Dynamic Group Object Class

Applies only when you select **Use Dynamic Groups***.*

Specifies the object class of the LDAP dynamic group. Usually the class is `dynamicGroup`.

Identity Vault Certificates

This section defines the path and password for the JRE keystore. Some settings are required for completing the installation process.

Keystore Path

Required

Specifies the full path to your keystore (`cacerts`) file of the JRE that Tomcat 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 installation program for the identity applications 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`.

Email Server Configuration

This section defines the values that enable email notifications, which you can use for email-based approvals. For more information, see "Manage Approvals by Email" in the *Help for the Identity Applications*.

Notification Template Host

Specifies the name or IP address of Tomcat that hosts the identity applications. 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 Tomcat that hosts the identity applications.

This values 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 Tomcat that hosts the identity applications.

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 identity applications use to send email notifications.

SMTP Server Name

Specifies the IP address or DNS name of the SMTP email host that the identity applications use for provisioning emails. Do not use `localhost`.

Server requires authentication

Specifies whether you want the server to require authentication.

You must also specify the credentials for the email server.

User name

Applies only when you enable **Server requires authentication***.*

Specifies the name of a login account for the email server.

Password

Applies only when you enable **Server requires authentication***.*

Specifies the password of an login account for the mail server.

Use SMTP TLS

Specifies whether you want to secure the contents of email messages during transmission between the mail servers.

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`.

Sign email

Specifies whether you want to add a digital signature to outgoing messages.

If you enable this option, you must also specify settings for the keystore and signature key.

Keystore Path

Applies only when you enable **Sign email***.*

Specifies the full path to the keystore (`cacerts`) file that you want to use for digitally signing an email. You can manually enter the path or browse to the `cacerts` file.

For example, `/opt/netiq/idm/apps/jre/lib/security/cacerts`.

Keystore Password

Applies only when you enable **Sign email***.*

Specifies the password for the keystore file. For example, `changeit`.

Alias of signature key

Applies only when you enable **Sign email***.*

Specifies the alias of the signing key in the keystore. For example, `idmapptest`.

Signature key password

Applies only when you enable **Sign email***.*

Specifies the password that protects the file containing the signature key. For example, `changeit`.

Trusted Key Store

This section defines the values for the trusted keystore for the identity applications. The utility displays these settings only when you select **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 identity applications get 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 identity applications 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.

Trusted Store Type

Specifies whether the trusted store path uses a Java keystore (JKS) or PKCS12 for digital signing.

NetIQ Sentinel Digital Signature Certificate & Key

This section defines the values that allows Identity Manager to communicate with Sentinel for auditing events. The utility displays these settings only when you select **Show Advanced Options**.

NetIQ Sentinel Digital Signature Certificate

Lists the custom public key certificate that you want the OAuth server to use to authenticate audit messages sent to Sentinel.

NetIQ Sentinel Digital Signature Private Key

Specifies the path to the custom private key file that you want the OAuth server to use to authenticate audit messages sent to Sentinel.

Miscellaneous

The utility displays these settings only when you select **Show Advanced Options**.

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.

Identity Vault Indexes

During installation, specifies whether you want the installation program to create indexes on the manager, ismanager, and srvprvUUID attributes. After installation, you can modify the settings to point to a new location of the indexes. The following considerations apply to this setting:

- Without indexes on these attributes, identity applications users can experience impeded performance of the identity applications, particularly in a cluster environment.
- You can create these indexes manually by using iManager after you install the identity applications. For more information, see "Configuring the Identity Vault for the Identity Applications" on page 329.
- For best performance, you should create the index during installation.
- The indexes must be in Online mode before you make the identity applications available to users.
- To create or delete an index, you must also specify a value for **Server DN**.

Server DN

Applies only when you want to create or delete an Identity Vault index.

Specifies the eDirectory server where you want the indexes to be created or removed.

You can specify only one server at a time. To configure indexes on multiple eDirectory servers, you must run the RBPM Configuration utility multiple times.

Reinitialize RBPM Security

Specifies whether you want to reset RBPM security when the installation process completes. You must also redeploy the identity applications.

IDMReport URL

Specifies the URL of the Identity Manager Reporting Module. For example, `http://hostname:port/IDMRPT`.

Custom Themes Context Name

Specifies the name of the customized theme that you want to use for displaying the identity applications in the browser.

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`.

Change RBPM Context Name

Specifies whether you want to change the context name for RBPM.

You must also specify the new name and DN of the Roles and Resource driver.

RBPM Context Name

Applies only when you select **Change RBPM Context Name***.*

Specifies the new context name for RBPM.

Role Driver DN

Applies only when you select **Change RBPM Context Name***.*

Specifies the DN of the Roles and Resource driver.

Container Object

These parameters apply only during installation.

This section helps you to define the values for container objects or create new container objects.

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.

Authentication Parameters

When configuring the identity applications, this tab defines the values that Tomcat uses to direct users to the identity application and password management pages.

By default, the tab displays the basic options. To see all settings, click **Show Advanced Options**. This tab includes the following groups of settings:

- "Authentication Server" on page 350
- "Authentication Configuration" on page 350
- "Authentication Method" on page 351
- "Password Management" on page 352
- "Novell Audit Digital Signature Certificate and Key" on page 353

Authentication Server

This section defines settings for the identity applications to connect to the authentication server.

OAuth server host identifier

Required

Specifies the relative URL of the authentication server that issues tokens to OSP. For example, 192.168.0.1.

OAuth server TCP port

Specifies the port for the authentication server.

OAuth server is using TLS/SSL

Specifies whether the authentication server uses TLS/SSL protocol for communication.

Optional TLS/SSL keystore file

Applies only when you select **OAuth server is using TLS/SSL** *and the utility is showing the advanced options.*

Optional TLS/SSL keystore password

Applies only when you select **OAuth server is using TLS/SSL** *and the utility is showing the advanced options.*

Specifies the password used to load the keystore file for the TLS/SSL authentication server.

NOTE: If you do not specify the keystore path and password, and the trust certificate for the authentication server is not in the JRE trust store (cacerts), the identity applications fail to connect to the authentication service that uses TLS/SSL protocol.

Authentication Configuration

This section defines settings for the authentication server.

OAuth server's authentication endpoint

Required

Specifies the URL through which OSP or the authentication server can an obtain a token for authentication.

OAuth server 's token endpoint

Required

Specifies the URL through which OSP can validate an obtained token.

OAuth server 's token endpoint

Required

Specifies the URL through which OSP ends the session with the authentication server.

LDAP DN of Admins Container

Required

Specifies the distinguished name of the container in the Identity Vault that contains any administrator User objects that OSP must authenticate. For example, `ou=sa,o=data`.

OAuth keystore file

Required

Specifies the path to the Java JKS keystore file you want to use for authentication. The keystore file must contain at least one public/private key pair.

OAuth keystore file password

Required

Specifies the password used to load the OAuth keystore file.

Key alias of key for use by OAuth

Required

Specifies the name of the public/private key pair in the OSP keystore file that you want to use to symmetric key generation.

Key password key for use by OAuth

Required

Specifies the password for the private key used by the authentication server.

URL to custom CSS file for login screen

Specifies the URL of a CSS stylesheet that you want to use to customize the appearance of the login page for the identity applications.

Duplicate resolution naming attribute

Specifies the name of the LDAP attribute used to differentiate between multiple eDirectory User objects with the same `cn` value. The default value is `mail`.

Restrict authentication sources to contexts

Specifies whether searches in the user and administrator containers in the Identity Vault are restricted to only User objects in those containers or searches should also include subcontainers.

Session Timeout (minutes)

Specifies the number of minutes of inactivity in a session before the server times out the user's session. The default value is 20 minutes.

Validity duration for access token

Specifies the number of seconds an OSP access token remains valid. The default value is 60 seconds.

Validity duration for refresh token

Specifies the number of seconds an OSP refresh token remains valid. The refresh token is used internally by OSP. The default value is 48 hours.

Authentication Method

This section defines the values that enable OSP to authenticate users who log in to the browser-based components of Identity Manager.

For more information about OSP, see "Using Single Sign-on Access in Identity Manager" on page 37 and Part XI, "Installing the Password Management Component," on page 263.

Method

Specifies the type of authentication that you want Identity Manager to use when a user logs on.

- **Name and Password**: OSP verifies authentication with the identity vault.
- **Kerberos**: OSP accepts authentication from both a Kerberos ticket server and the identity vault. You must also specify a value for **Mapping attribute name**.
- **SAML**: OSP accepts authentication from both a SAML identity provider and the identity vault. You must also specify values for **Mapping attribute name** and **Metadata URL**.

Mapping attribute name

Applies only when you specify **Kerberos** *or* **SAML***.*

Specifies the name of the attribute that maps to the Kerberos ticket server or SAML representations at the identity provider.

Metadata URL

Applies only when you specify **SAML***.*

Specifies the URL that OSP uses to redirect the authentication request to SAML.

Password Management

This section defines the values that enable users to modify their passwords as a self-service operation.

Password Management Provider

Specifies the type of password management system that you want to use.

- **SSPR**: Uses the integrated SSPR method.

  For your convenience, NetIQ provides SSPR with the installation media. For more information about SSPR, see "Using Self-Service Password Management in Identity Manager" on page 35 and Part XI, "Installing the Password Management Component," on page 263.
- **User Application (Legacy)**: Uses the password management program that Identity Manager traditionally has used. This option also allows you to use an external password management program.

Forgotten Password

This check box parameter applies only when you want to use SSPR.

Specifies whether you want users to recover a forgotten password without contacting a help desk.

You must also configure the challenge-response policies for the Forgotten Password feature. For more information, see the *NetIQ Self Service Password Reset Administration Guide*.

Forgotten Password

This menu list applies only when you select **User Application (Legacy)***.*

Specifies whether you want to use the password management system integrated with the User Application or an external system.

- **Internal**: Use the default internal Password Management functionality, `./jsps/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.
- **External**: Use an e external Forgot Password WAR to call back the User Application through a web service. You must also specify the settings for the external system.

Forgotten Password Link

Applies only when you want to use an external password management system.

Specifies the URL that points to the Forgot Password functionality page. Specify a `ForgotPassword.jsp` file in an external or internal password management WAR.

Forgotten Password Return Link

Applies only when you want to use an external password management system.

Specifies the URL for the **Forgot Password Return Link** that the user can click after performing a forgot password operation.

Forgotten Password Web Service URL

Applies only when you want to use an external password management system.

Specifies the URL that the External Forgot Password WAR will use to call back to the User Application to perform core forgot password functionalities. Use the following format:

```
https://<idmhost>:<sslport>/<idm>/
pwdmgt/service
```

Novell Audit Digital Signature Certificate and Key

This section defines the values that allows Identity Manager to communicate with Sentinel for auditing events.

NetIQ Sentinel Digital Signature Certificate

Specifies a custom public key certificate that you want the OSP server to use to authenticate audit messages sent to the audit system.

For information about configuring certificates for Novell Audit, see "Managing Certificates" in the *Novell Audit Administration Guide*.

NetIQ Sentinel Digital Signature Private Key

Specifies the path to the custom private key file that you want the OSP server to use to authenticate audit messages sent to the audit system.

SSO Clients Parameters

When configuring the identity applications, this tab defines the values for managing single sign-on access to the applications.

By default, the tab displays the basic options. To see all settings, click **Show Advanced Options**. This tab includes the following groups of settings:

- "Landing" on page 354
- "Dashboard" on page 355
- "IDM Dashboard" on page 357
- "RBPM" on page 357
- "Reporting" on page 358
- "DCS Driver" on page 359
- "Catalog Administrator" on page 359
- "Self Service Password Reset" on page 360

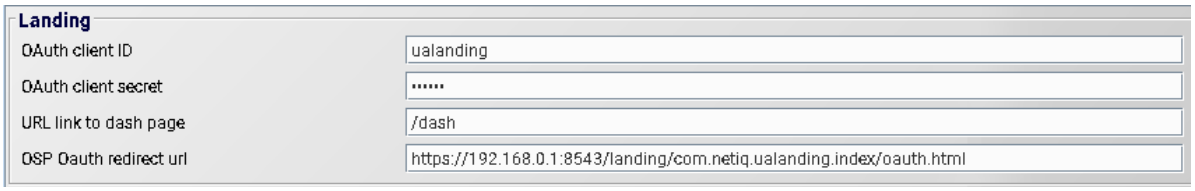
For more information about configuring single sign-on access, see Part XV, "Configuring Single Sign-on Access in Identity Manager," on page 417.

Landing

This section defines the values for the URL that users need to access the landing page for the identity applications. Usually, this URL directs users to Identity Manager Home.

NOTE: Starting with Identity Manager v4.6, the Identity Manager Dashboard replaces Identity Manager Home and Provisioning Dashboard. Until the latter two are deprecated, they continue to be installed with the identity applications.

Figure 40-1 *Landing*



OAuth client ID

Required

Specifies the name that you want to use to identify the single sign-on client for the Dashboard to the authentication server. The default value is `ualanding`.

OAuth client secret

Required

Specifies the password for the single sign-on client for Identity Manager Home.

URL link to dash page

Required

Specifies the relative URL to use to access Identity Manager Home. The default value is `/dash`.

OSP OAuth redirect url

Required

Specifies the absolute URL to which the authentication server redirects a browser client when authentication is complete.

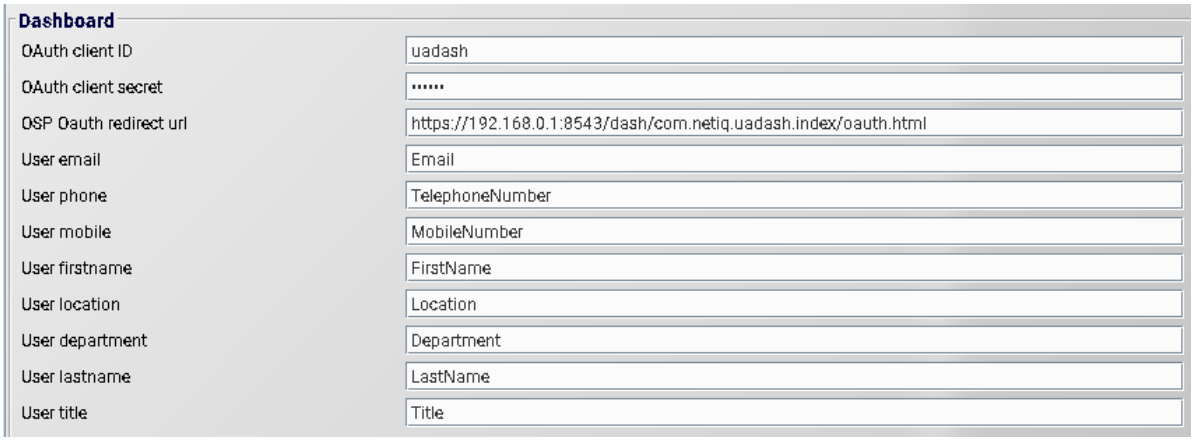
Use the following format: `protocol://server:port/path`. For example, `http://192.168.0.1:8543/dash/com.netiq.test`.

Dashboard

This section defines the values for the URL that users need to access the landing page for the identity applications. Usually, this URL directs users to the Provisioning Dashboard.

NOTE: Starting with Identity Manager v4.6, the Identity Manager Dashboard replaces Identity Manager Home and Provisioning Dashboard. Until the latter two are deprecated, they continue to be installed with the identity applications.

Figure 40-2 *Dashboard*



OAuth client ID

Required

Specifies the name that you want to use to identify the single sign-on client for Identity Manager Provisioning Dashboard to the authentication server. The default value is `uadash`.

OAuth client secret

Required

Specifies the password for the single sign-on client for Identity Manager Provisioning Dashboard.

OAuth redirect url

Required

Specifies the absolute URL to which the authentication server redirects a browser client when authentication is complete.

Use the following format: `protocol://server:port/path`. For example, `http://192.168.0.1:8543/dash/com.netiq.udash.index/oauth.html`.

User email

Required

Specifies the value that the Roles Based Provisioning Module uses to identity a user's email attribute in the user information REST API results.

The value must match the Entities configured using Designer. The default value is `Email`.

User phone

Required

Specifies the value that the Roles Based Provisioning Module uses to identity a user's phone number attribute in the user information REST API results.

The value must match the Entities configured using Designer. The default value is `TelephoneNumber`.

User mobile

Required

Specifies the value that the Roles Based Provisioning Module uses to identity a user's mobile phone number attribute in the user information REST API results.

The value must match the Entities configured using Designer. The default value is `MobileNumber`.

User firstname

Required

Specifies the value that the Roles Based Provisioning Module uses to identity a user's first name attribute in the user information REST API results.

The value must match the Entities configured using Designer. The default value is `FirstName`.

User location

Required

Specifies the value that the Roles Based Provisioning Module uses to identity a user's location attribute in the user information REST API results.

The value must match the Entities configured using Designer. The default value is `Location`.

User department

Required

Specifies the value that the Roles Based Provisioning Module uses to identity a user's department attribute in the user information REST API results.

The value must match the Entities configured using Designer. The default value is `Department`.

User lastname

Required

Specifies the value that the Roles Based Provisioning Module uses to identify a user's last name attribute in the user information REST API results.

The value must match the Entities configured using Designer. The default value is `LastName`.

User title

Required

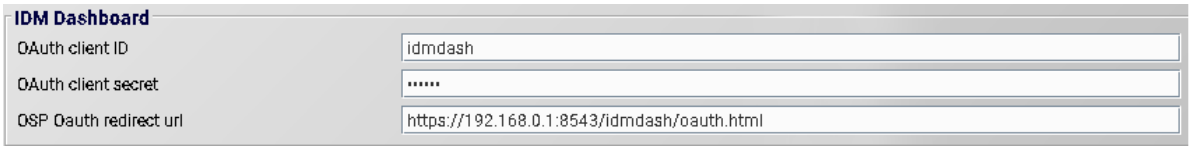
Specifies the value that the Roles Based Provisioning Module uses to identity a user's job title attribute in the user information REST API results.

The value must match the Entities configured using Designer. The default value is `Title`.

IDM Dashboard

This section defines the values for the URL that users need to access the Identity Manager Dashboard, which is the primary login location for the identity applications.

Figure 40-3 *IDM Dashboard*



OAuth client ID

Required

Specifies the name that you want to use to identify the single sign-on client for the Dashboard to the authentication server. The default value is `idmdash`.

OAuth client secret

Required

Specifies the password for the single sign-on client for the Dashboard.

OSP OAuth redirect url

Required

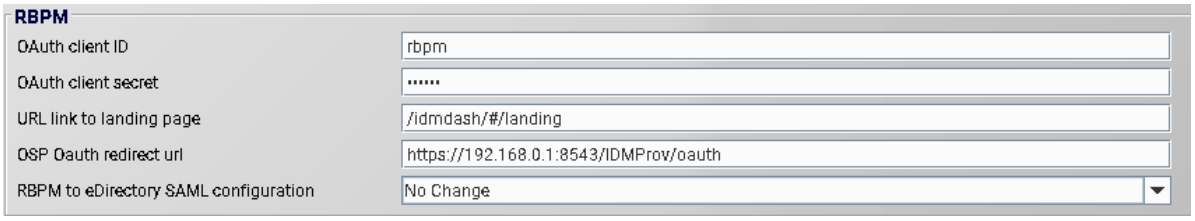
Specifies the absolute URL to which the authentication server redirects a browser client when authentication is complete.

Use the following format: `protocol://server:port/path`. For example, `http://192.168.0.1:8543/idmdash/oauth.html`.

RBPM

This section defines the values for the URL that users need to access the User Application.

Figure 40-4 *RBPM*



OAuth client ID

Required

Specifies the name that you want to use to identify the single sign-on client for the User Application to the authentication server. The default value is `rbpm`.

OAuth client secret

Required

Specifies the password for the single sign-on client for the User Application.

URL link to landing page

Required

Specifies the relative URL to use to access the Dashboard from the User Application. The default value is `/landing`.

OAuth redirect url

Required

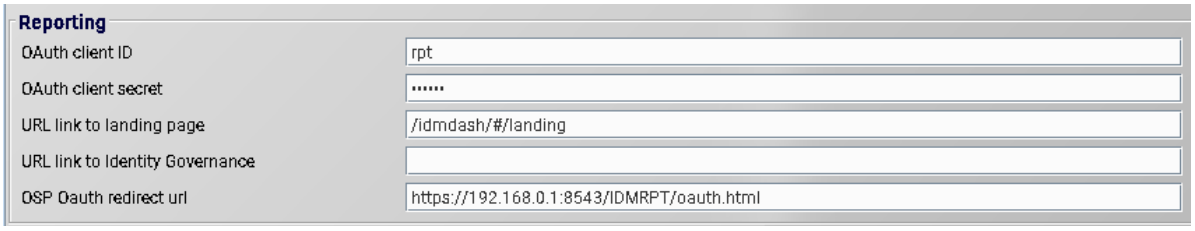
Specifies the absolute URL to which the authentication server redirects a browser client when authentication is complete.

Use the following format: `protocol://server:port/path`. For example, `http://192.168.0.1:8543/IDMProv/oauth`.

Reporting

This section defines the values for the URL that users need to access Identity Reporting. The utility display these values only if you add Identity Reporting to your Identity Manager solution.

Figure 40-5 *Reporting*



OAuth client ID

Required

Specifies the name that you want to use to identify the single sign-on client for the Identity Reporting to the authentication server. The default value is `rpt`.

OAuth client secret

Required

Specifies the password for the single sign-on client for Identity Reporting.

URL link to landing page

Required

Specifies the relative URL to use to access the Dashboard from Identity Reporting. The default value is `/dashboard`.

If you installed Identity Reporting and the identity applications in separate servers, then specify an absolute URL. Use the following format: `protocol://server:port/path`. For example, `http://192.168.0.1:8543/IDMRPT/oauth`.

OAuth redirect url

Required

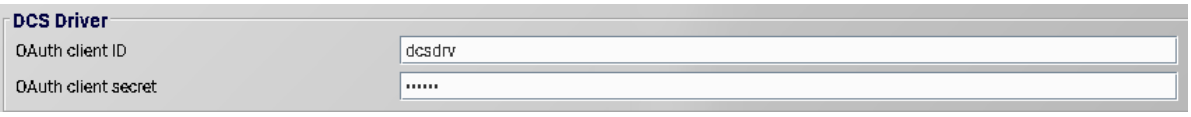
Specifies the absolute URL to which the authentication server redirects a browser client when authentication is complete.

Use the following format: `protocol://server:port/path`. For example, `http://10.10.10.48:8180/IDMRPT/oauth`.

DCS Driver

This section defines the values for managing the Data Collection Services driver. For more information about the driver, see Chapter 44, “Managing the Drivers for Reporting,” on page 385.

Figure 40-6



OAuth client ID

Specifies the name that you want to use to identify the single sign-on client for the Data Collection Service driver to the authentication server. The default value for this parameter is `dcsdrv`.

OAuth client secret

Specifies the password for the single sign-on client for the Data Collection Service driver.

Catalog Administrator

This section defines the values for the URL that users need to access Catalog Administrator.

Figure 40-7

OAuth client ID

Required

Specifies the name that you want to use to identify the single sign-on client for Catalog Administrator to the authentication server. The default value is `rra`.

OAuth client secret

Required

Specifies the password for the single sign-on client for Catalog Administrator.

URL link to landing page

Required

Specifies the relative URL to use to access the Dashboard from Catalog Administrator. The default value is `/dashboard`.

OAuth redirect url

Required

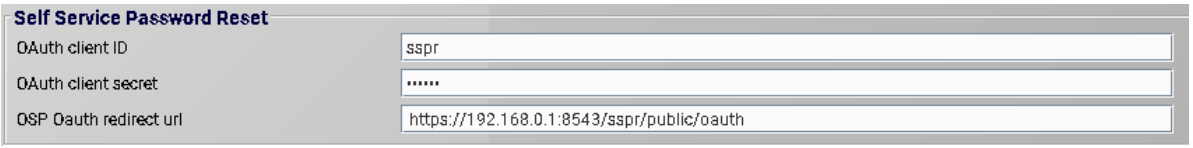
Specifies the absolute URL to which the authentication server redirects a browser client when authentication is complete.

Use the following format: `protocol://server:port/path`. For example, `http://192.168.0.1:8543/com.netiq.rra.index/oauth.html`.

Self Service Password Reset

This section defines the values for the identity applications to communicate with SSPR.

Figure 40-8



OAuth client ID

Required

Specifies the name that you want to use to identify the single sign-on client for SSPR to the authentication server. The default value is `sspr`.

OAuth client secret

Required

Specifies the password for the single sign-on client for SSPR.

OAuth redirect URL

Required

Specifies the absolute URL to which the client will redirect when actions such as password changes or challenge questions have been completed in SSPR. For example, forward to the Dashboard.

Use the following format: `protocol://server:port/path`. For example, `http://192.168.0.1/sspr/public/oauth`.

Reporting Parameters

When configuring the identity applications, this tab defines the values for managing Identity Reporting. The utility adds this tab when you install Identity Reporting.

By default, the tab displays the basic options. To see all settings, click **Show Advanced Options**. This tab includes the following groups of settings:

- "Email Delivery Configuration" on page 361
- "Report Retention Values" on page 361
- "Modify Locale" on page 362
- "Role Configuration" on page 362

Email Delivery Configuration

This section defines the values for sending notifications.

SMTP Server Host

Specifies the DNS name or IP address of the email server than you want Identity Reporting to use when sending notification. Do not use `localhost`.

SMTP Server Port

Specifies the port number for the SMTP server.

SMTP Use SSL

Specifies whether you want to use TLS/SSL protocol for communication with the email server.

Server Needs Authentication

Specifies whether you want to use authentication for communications with the email server.

SMTP User Name

Specifies the email address that you want to use for authentication.

You must specify a value. If the server does not require authentication, you can specify an invalid address.

SMTP User Password

Applies only when you specify that the server requires authentication.

Specifies the password for the SMTP user account.

Default Email Address

Specifies the email address that you want Identity Reporting to use as the origination for email notifications.

Report Retention Values

This section defines the values for storing completed reports.

Report Unit, Report Lifetime

Specifies the amount of time that Identity Reporting keeps completed reports before deleting them. For example, to specify six months, enter `6` and then select **Month**.

Location of Reports

Specifies a path where you want to store the report definitions. For example, `/opt/netiq/IdentityReporting`.

Modify Locale

This section defines the values for the language that you want Identity Reporting to use. Identity Reporting uses the specific locales in searches. For more information, see the *Administrator Guide to NetIQ Identity Reporting*.

Role Configuration

This section defines the values for the authentication sources that Identity Reporting uses to generate reports.

Add Authentication Source

Specifies the type of authentication source that you want to add for reporting. Authentication sources can be

- **Default**
- **LDAP Directory**
- **File**

XIII Installing Identity Reporting

This section guides you through the process of installing the required components for running reports. The installation process includes all components required for the application:

- NetIQ Identity Reporting
- Identity Manager Managed System Gateway Driver (MSGW driver)
- Identity Manager Driver for Data Collection Service (DCS driver)

The installation files are located in the `products/Reporting` 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/netiq/idm/apps/IDMReporting`
- **Windows**: `C:\NetIQ\idm\apps\IDMReporting`

For your convenience, the Identity Manager installation kit includes Sentinel Log Management for IGA (Sentinel) to use as a built-in auditing service. For more information, see "Installing and Managing Sentinel Log Management for Identity Governance and Administration" on page 115.

NetIQ recommends that you review the installation process before beginning. For more information, see Chapter 41, "Planning to Install Identity Reporting," on page 365.

41 Planning to Install Identity Reporting

This section provides guidance for preparing to install the components for Identity Reporting. You can use Sentinel to audit events.

- "Checklist for Installing Identity Reporting" on page 365
- "Understanding the Installation Process for the Identity Reporting Components" on page 366
- "Prerequisites for Installing the Identity Reporting Components" on page 367
- "System Requirements for Identity Reporting" on page 368

Checklist for Installing Identity Reporting

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

	Checklist Items
❑	1. Learn about the interaction among Identity Manager components. For more information, see "Identity Reporting" on page 29.
❑	2. Decide which servers you want to use for your Identity Manager components. For more information, see "Recommended Installation Scenarios and Server Setup" on page 44.
❑	3. Review the considerations for installing Identity Reporting. For more information, see "Prerequisites for Installing the Identity Reporting Components" on page 367.
❑	4. Review the hardware and software requirements for the computers that will host Identity Reporting. For more information, see "System Requirements for Identity Reporting" on page 368.
❑	5. (Conditional) For computers running a SLES 12 SP1 or later operating system, ensure that you have installed the appropriate set of libraries for a guided installation. For more information, see "Installing Identity Manager on SLES 12 SP1 or Later Servers" on page 55.
❑	6. (Conditional) For computers running an RHEL 6.x or RHEL 7.x operating system, ensure that you have installed the appropriate set of libraries. For more information, see "Installing Identity Manager on RHEL 6.x or 7.x Servers" on page 55.
❑	7. Ensure that you have installed the identity applications. For more information, see Chapter 33, "Planning to Install the Identity Applications," on page 279.
❑	8. Install Sentinel. For more information, see Section 14, "Installing SLM for IGA," on page 127
❑	9. Ensure that the server where you want to install Identity Reporting has an application server, such as Tomcat. For more information, see Chapter 28, "Installing PostgreSQL and Tomcat," on page 247.
❑	10. (Conditional) To use the Apache Log4j service to record events in Tomcat, ensure that you have the appropriate files. For more information, see "Using the Apache Log4j Service to Log Sign-on" on page 254.

	Checklist Items
❑	11. Install Identity Reporting: ◆ For a guided installation, see "Using the Guided Process to Install Identity Reporting" on page 371. ◆ To install reporting silently, see "Installing Identity Reporting Silently" on page 378.
❑	12. Complete the Identity Reporting set up. For more information, see Chapter 43, "Configuring Identity Reporting," on page 383.
❑	13. Configure the Managed System Gateway and Data Collection Service drivers. For more information, see "Configuring Drivers for Identity Reporting" on page 385.
❑	14. Deploy and start the drivers. For more information, see "Deploying and Starting Drivers for Identity Reporting" on page 391.
❑	15. Configure the environment for the drivers. For more information, see "Configuring the Runtime Environment" on page 395.
❑	16. Configure Identity Manager and eDirectory to send data to the drivers. For more information, see "Setting Auditing Flags for the Drivers" on page 404.

Understanding the Installation Process for the Identity Reporting Components

You can install Sentinel, Identity Reporting and the Reporting drivers on the same server. However, due to the workload, NetIQ recommends installing Sentinel and Reporting on separate servers. For more information, see "Recommended Installation Scenarios and Server Setup" on page 44.

In case of a fresh installation, the installation program creates tables in 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.

If you have migrated your data, for example, SIEM, from EAS to PostgreSQL database, then the installation program will connect to the existing database.

The installation program for Identity Reporting 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 Tomcat
- Deploys the core WAR file, which contains the core REST services needed for reporting
- Deploys the API WAR file, which contains the documentation of REST services needed for reporting
- Configures the authentication services for Identity Reporting
- Configures the email delivery system for Identity Reporting
- Configures the core reporting services for Identity Reporting
- Creates the user accounts for Identity Reporting (**idmrptsrv** and **idmrptuser**)
- Creates the user accounts for interacting with Sentinel (**appuser** and **rptuser**)

Prerequisites for Installing the Identity Reporting Components

NetIQ recommends that you review the following prerequisites and considerations before starting the installation process.

- "Prerequisites for Identity Reporting" on page 367

Prerequisites for Identity Reporting

When installing Identity Reporting, consider the following prerequisites and considerations:

- Requires a supported and configured version of the following Identity Manager components:
  - Identity applications, including the User Application driver
  - Sentinel installed on a separate Linux computer.
  - Driver for Data Collection Service
  - Driver for the Managed System Gateway service

  For more information about required versions and patches for these components, see the latest Release Notes. For more information about installing the drivers, see Chapter 44, "Managing the Drivers for Reporting," on page 385.
- Ensure that the Identity Vault includes the SecretStore module, and that the module is configured. For more information, see "Adding SecretStore to the Identity Vault Schema" on page 109.
- Do not install Identity Reporting on a server in a clustered environment.
- (Conditional) To run reports against an Oracle 12c database, you must install the appropriate JDBC file. For more information, see "Running Reports on an Oracle Database" on page 383.
- (Conditional) You can use your own Tomcat installation program instead of the one provided in the Identity Manager installation kit. However, to use the Apache Log4j service with your version of Tomcat, ensure that you have the appropriate files installed. For more information, see "Using the Apache Log4j Service to Log Sign-on" on page 254.
- Assign the Report Administrator role to any users that you want to access reporting functionality.
- Ensure that all servers in your Identity Manager environment are set to the same time. 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.
- The installation process modifies `JAVA_OPTs` or `CATALINA_OPTS` entries for JRE mapping in the `setenv.sh` file for Tomcat.

  By default, the convenience installer for Tomcat places the `setenv.sh` file in the `/opt/netiq/idm/apps/tomcat/bin/` directory. The installer also configures the JRE location in the file.
- (Optional) You can configure Identity Reporting to work with NetIQ Access Manager 4.0 using SAML 2.0 authentication. For more information, see Chapter 49, "Using SAML Authentication with NetIQ Access Manager for Single Sign-on," on page 423.

Identifying Audit Events for Identity Reporting

This section provides information on how to identify different audit events required for Identity Manager reports and custom reports. You can unzip all report sources and run the following script to identify the audit events:

```
find . -name *.jrxml -print0 |xargs -0 grep -H "'000[B3]" | perl -ne '($file) = /
^\.\/(.*?)\//;@a = /000[3B]..../g; foreach $a (@a) { print "$file;$a\n"}' |sort -u
```

The following section provides information on how to identify and select various audit events for identity Manager reports and custom reports:

Event Name	Audit Flag
Authentication and Password Change	**Selecting Audit Flag using SSPR:** Launch **SSPR Configuration Editor** > **Audit Configuration** > Select from the following audit flags: ◆ Authenticate ◆ Change Password ◆ Unlock Password ◆ Recover Password ◆ Intruder Attempt ◆ Intruder Lock ◆ Intruder Lock User **Selecting Audit Flag using iManager:** Go to **iManager Roles and Tasks** > **eDirectory Auditing** > > **Audit Configuration** > **Novell Audit** > Select from the following audit flags: ◆ Change Password ◆ Verify Password ◆ Login ◆ Logout
All other reporting events	Go to **NetIQ Identity Manager UserApp** > **Administration** > **Logging** > **Enable audit service**

System Requirements for Identity Reporting

This section provides the minimum requirements for the server(s) where you want to install the Identity Reporting components. For more information about whether to install the components on the same server, see “Recommended Installation Scenarios and Server Setup” on page 44.

Also, ensure that you review the prerequisites and considerations for installation, particularly those related to the operating system.

Category	Requirement
Processor	Pentium* III 600MHz processor

Category	Requirement
Disk space	1 GB **NOTE:** Enough space for the content of supporting applications, such as the database and application server logs.
Memory	512 MB (4 GB recommended)
Operating system (certified)	One of the following 64-bit operating systems: ◆ Open Enterprise Server 2015 SP1 ◆ Open Enterprise Server 11 SP3 ◆ Red Hat Enterprise Linux 7.2 ◆ Red Hat Enterprise Linux 7.1 ◆ Red Hat Enterprise Linux 7.0 ◆ SUSE Linux Enterprise Server 12 SP1 ◆ SUSE Linux Enterprise Server 11 SP4 ◆ Windows Server 2012 R2 NetIQ recommends that you apply the latest operating system patches according to the manufacturer's automated update facility before you install Identity Manager. **NOTE:** *Certified* means that the operating system has been fully tested and is supported.
Operating system (supported)	Latest versions of service packs for the certified operating systems **NOTE:** *Supported* means that the operating system has not yet been tested but is expected to work
Virtualization system	◆ Hyper-V Server 2012 R2 ◆ VMWare ESX 5.5 and later ◆ Windows Server 2012 R2 Virtualization with Hyper-V (supported) NetIQ supports Identity Manager on enterprise-class virtualization systems that provide official support for the operating systems where NetIQ products are running. As long as the vendors of the virtualization systems officially support these operating systems, NetIQ supports the entire Identity Manager stack on them.
Database	The reporting database runs on the following platform, at a minimum: ◆ PostgreSQL 9.6.1 (for SLES 12 SP1, RHEL 7.x, and Win2K12 platforms) ◆ PostgreSQL 9.4.10 (for SLES 11 SP4) You can run reports against the following databases, at a minimum: ◆ Oracle 12c ◆ PostgreSQL 9.6.1 (for SLES 12 SP1, RHEL 7.x, and Win2K12 platforms) ◆ PostgreSQL 9.4.10 (for SLES 11 SP4)
Application server	Apache Tomcat 8.5.x

Category	Requirement
Java	Java Development Kit (JDK) or Java Runtime Environment (JRE) version 1.8.0_112 or later from Sun (Oracle)
Web browser	Any of the following browsers, at a minimum: **Desktop** ◆ Apple Safari 7.0.1 ◆ Apple Safari 5.1.7 for Windows ◆ Google Chrome 51 ◆ Microsoft Internet Explorer 11 ◆ Mozilla Firefox 47 **iPad** ◆ Apple Safari 7 ◆ Google Chrome 51 **NOTE:** The browser must have cookies enabled. If cookies are disabled, the product does not work.
Audit	Sentinel Log Management for IGA

42 Installing Identity Reporting

This section describes the process for installing Identity Reporting.

- "Using the Guided Process to Install Identity Reporting" on page 371
- "Installing Identity Reporting Silently" on page 378
- "Manually Generating the Database Schema" on page 379
- "Connecting to a Remote PostgreSQL Database" on page 380

Using the Guided Process to Install Identity Reporting

The following procedure describes how to install Identity Reporting using an installation wizard, either in GUI format or from the console. To perform a silent, unattended installation, see "Installing Identity Reporting Silently" on page 378.

To prepare for the installation, review the prerequisites and system requirements listed in "System Requirements for Identity Reporting" on page 368. Also see the Release Notes accompanying the release.

1. Log in to the computer where you want to install Identity Reporting.
2. Stop Tomcat.
3. (Conditional) If you have the `.iso` image file for the Identity Manager installation package, navigate to the directory containing the installation files for Identity Reporting, located by default in the `products/Reporting/` directory.
4. (Conditional) If you downloaded Identity Reporting installation files from the NetIQ Downloads website, complete the following steps:
   - **4a** Navigate to the `.tgz` file for the downloaded image.
   - **4b** Extract the contents of the file to a folder on the local computer.
5. From the directory that contains the installation files, complete one of the following actions:
   - **Linux (console)**: Enter `./rpt-install-linux.bin -i console`
   - **Linux (GUI)**: Enter `./rpt-install-linux.bin`
   - **Windows**: Run `rpt-install.exe`
6. In the installation program, specify the language that you want to use for installation, and then click **OK**.
7. Review the Introduction text and click **Next**.
8. Accept the license agreement and click **Next**.
9. Complete the guided process, using the following parameters:
   - **Installation Folder**

     Specifies the path to a directory where the installation program creates the application files, including installation log files, helper scripts, and configuration scripts.
   - **Reporting Setup**

     Represents the environment and its settings to which you want to add Identity Reporting. For **Identity Manager**, specify the following values:

Identity Vault Server

Specifies the hostname to the eDirectory server.

Secure LDAP Port

Specifies the port you want to use to establish an LDAP connection to the eDirectory server over SSL. The default port is 636.

Provisioning Home

Specifies the Identity Manager provisioning home location. This can be the full application server URL or a relative path for the URL.

- **Application Server Details**

Represents Tomcat that you want to run Identity Reporting. The application server must already be installed.

Secondary

Specifies whether the current install is on a secondary node of a cluster.

Tomcat root folder

Specifies a path to the Tomcat instance. For example, `/opt/netiq/idm/apps/tomcat`.

Java JRE Base folder

Specifies the Java JRE base folder location.

The path contains the config update utility file and is used to launch this utility after Identity Reporting is installed.

- **Application Address**

Represents the settings for the server that hosts Identity Reporting.

Protocol

Specifies whether you want to use *http* or *https*. To use SSL for communication, specify `https`.

Host name

Specifies the DNS name or IP address of Tomcat. Do not use `localhost`.

Port

Specifies the port that you want Tomcat to use for communication with the Identity Reporting application.

Connect to an external authentication server

Specifies whether a different instance of Tomcat hosts the authentication server (OSP). The authentication server contains the list of users who can log in to Identity Reporting.

If you select this setting, specify values for the authentication server's **Protocol**, **Host name**, and **Port**.

- **Authentication Server Details**

Specifies the password for the Identity Reporting Service.

Identity Manager uses this password to connect to the OSP client on the authentication server.

- **Database Details**

Represents the settings for the reporting database, including whether you want the installation process to create the database or generate an SQL file for creating the database later.

Database name

Specify the database name as per your requirement:

- In case of a new installation, specify the name of your Reporting database. For example, `idmrptdb` or `SIEM`.
- If you are migrating from EAS, specify the name for the EAS database, for example, `SIEM`.

Database host

Specify the database host as per your requirement:

- In case of a new installation, specify the DNS name or IP address of the server where the database has to be created.
- If you are migrating from EAS, specify the DNS name or IP address of the server that hosts your `SIEM` database.

Database type

Select the database that you want to use.

If you select **Oracle**, specify the following details:

- **JDBC driver jar**

  Specifies the path to the jar file for the Oracle JDBC driver. For example, `opt\oracl\ojdbc7.jar`.

  For more information, see "Running Reports on an Oracle Database" on page 383.

- **JDBC driver classname**

  Specifies the class of the JDBC driver.

- **JDBC driver type**

  Specifies the type of JDBC driver.

If you select **PostgresSQL**, click **Next**.

Share password

Enables you to specify a single password for all reporting users when they connect to the database.

Specify password for each user

Enables you to specify a unique password for each reporting user to the database. You need to specify a password for `idm_rpt_data_password`, `idm_rpt_cfg_password`, and `idmrptuserpassword`.

Database port

Specifies the port to connect to the database.The default port is 5432.

Configure database now or at startup

Indicates that you have the login settings for the database so the installation program can create the database immediately or during reporting startup. You must also specify the following values:

- **DBA userid**

  Specifies the name of the administrative account for the SIEM database server. For example, *postgres.*

- **DBA password**

  Specifies the password for the administrative account for the database.

- **Test Database Connection:** Indicates whether you want the installation program to test the values specified for the database.

  The installation program attempts the connection when you click **Next** or press **Enter**.

  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 "Manually Generating the Database Schema" on page 379.

Generate SQL for later

Instructs the installation program to generate a SQL file that your database administrator will use to create the database after your complete the installation process.

- **Default Language**

  Specifies the language that you want Identity Reporting to use in searches.

- **Identity Vault Credentials**

  Represents the settings that Identity Reporting uses to connect to the Identity Vault.

Identity Vault Administrator

Specifies the distinguished name for the LDAP Administrator. For example, `cn=admin`. This user must already exist in the Identity Vault.

Identity Vault Administrator Password

Specifies the password for the Identity Vault administrator.

Keystore Path

Specifies the full path to your keystore (`cacerts`) file of the JRE that Tomcat uses to run.

Keystore Password

Specifies the password for the keystore file.

Report Admin Role Container DN

Specify the DN for the container that stores the Report Administrator role.

Report Admin User DN

Specifies an existing user account in the Identity Vault that has the rights to perform administrative tasks for Identity Reporting.

- **User Application driver**

  Represents the name of your application driver, driver set, and driver set container.

User Application Driver

Specifies the name of the User Application driver.

Driver set name

Specifies the name of the driver set.

Driver set container

Specifies the name of the driver set container.

- **Email Delivery**

  Represents the settings for the SMTP server that sends report notifications. To modify these settings after installation, use the RBPM Configuration utility.

Default email address

Specifies the email address that you want Identity Reporting to use as the origination for email notifications.

SMTP server

Specifies the IP address or DNS name of the SMTP email host that Identity Reporting uses for notifications. Do not use `localhost`.

SMTP server port

Specifies the port number for the SMTP server. The default port is 465.

Use SSL for SMTP

Specifies whether you want to use SSL protocol for communication with the SMTP server.

Require server authentication

Specifies whether you want to use authentication for communication with the SMTP server. You must also specify the following values:

- ***SMTP user name***

  Specifies the name of an login account for the SMTP server.

- ***SMTP password***

  Specifies the password of a login account for the SMTP server.

- **Report Details**

Represents the settings for report definitions and completed reports.

Keep finished reports for

Specifies the amount of time that Identity Reporting will retain completed reports before deleting them.

For example, to specify six months, enter `6` and then select **Month**.

Location of report definitions

Specifies a path where you want to store the report definitions.

For example, `/opt/netiq/IdentityReporting`.

- **Novell Identity Audit**

Represents the settings for sending log events to an auditing server.

For your convenience, NetiQ includes Sentinel Log Management for IGA.

Enable auditing for Identity Reporting

Specifies whether you want to send log events to an auditing server.

- ***Audit server***

  Applies only when you select **Enable auditing for Identity Reporting**.

  Specify the host name of the auditing server, that is, the IP where Sentinel is hosted.

- ***Audit log cache folder***

  Applies only when you select **Enable auditing for Identity Reporting**.

  Specify the location of the cache directory that you want to use for auditing. For example, `/opt/novell/Identity Reporting`.

NOTE: Ensure that the logevent file has valid paths for the cache directory and `nauditpa.jar` file. If these settings are not defined correctly, Identity Reporting will not start.

- **NAudit Certificates**

  Specifies whether you want to push NAudit events from Identity Reporting to the auditing server.

  Specify existing certificate / Generate a certificate

  Applies only when you select Enable auditing for Identity Reporting.

  Indicates whether you want to use an existing certificate for the NAudit server or create a new one.

  Enter Public key

  Applies only when you want to use an existing certificate.

  Specify the custom public key certificate that the NAudit service will use to authenticate audit messages.

  Enter RSA Key

  Applies only when you want to use an existing certificate.

  Specify the path to the custom private key file that the NAudit service will use to authenticate audit messages.

10 In the Pre-Installation Summary window, click **Install**.

Configuring Create_rpt_roles_and_schemas.sql Schema against Oracle Database

1 Install the Oracle database on a connected sever.

2 Create an Oracle System ID (SID) for Identity Reporting.

3 Log in to the Oracle SQL developer tool or Oracle database as database admin.

4 Connect to the database instance created in Step 2.

5 To create `Create_rpt_roles_and_schemas` procedure, copy the following script to SQL Developer where you run it against the connected Database:

```
CREATE OR REPLACE PROCEDURE create_rpt_roles_and_schemas(
        idm_rpt_data_password character varying,
        idm_rpt_cfg_password character varying,
        idmrptuser_password character varying)
AUTHID CURRENT_USER
AS
        cnt number;
BEGIN
        /* Create user IDM_RPT_DATA if it does not exist already */
       select count(*) into cnt from ALL_USERS WHERE USERNAME = 'IDM_RPT_DATA';
        IF cnt = 0 THEN
                execute immediate 'CREATE USER idm_rpt_data IDENTIFIED BY ' ||
idm_rpt_data_password;
                 DBMS_OUTPUT.put_line('Created user idm_rpt_data');
        END IF;
        /* Grant rights to the idm_rpt_data user */
        execute immediate 'GRANT CREATE SESSION, CREATE TABLE, CREATE VIEW,
CREATE PROCEDURE, CREATE SEQUENCE, CREATE TRIGGER, UNLIMITED TABLESPACE to
idm_rpt_data';
```

```
        DBMS_OUTPUT.put_line('Granted rights to user idm_rpt_data');

        /* Create user IDM_RPT_CFG if it does not exist */
        select count(*) into cnt from ALL_USERS WHERE USERNAME = 'IDM_RPT_CFG';
        IF cnt = 0 THEN
                execute immediate 'CREATE USER idm_rpt_cfg IDENTIFIED BY ' ||
idm_rpt_cfg_password;
                DBMS_OUTPUT.put_line('Created user idm_rpt_cfg');
        END IF;
        /* Grant rights to the idm_rpt_cfg user */
        execute immediate 'GRANT CREATE SESSION, CREATE TABLE, CREATE VIEW,
CREATE PROCEDURE, CREATE SEQUENCE, CREATE TRIGGER, UNLIMITED TABLESPACE to
idm_rpt_cfg';
        DBMS_OUTPUT.put_line('Granted rights to user idm_rpt_cfg');
        /* Create user IDMRPTUSER if it does not exist */
        select count(*) into cnt from ALL_USERS WHERE USERNAME = 'IDMRPTUSER';
        IF cnt = 0 THEN
                execute immediate 'CREATE USER idmrptuser IDENTIFIED BY ' ||
idmrptuser_password;
                DBMS_OUTPUT.put_line('Created user idmrptuser');
        END IF;
        /* Grant rights to the idmrptuser user */
        execute immediate 'GRANT CREATE SESSION to idmrptuser';
        DBMS_OUTPUT.put_line('Granted rights to user idmrptuser');
END;
```

6 To create IDM_RPT_DATA, IDM_RPT_CFG, and IDMRPTUSER roles, execute the following command:

```
begin
CREATE_RPT_ROLES_AND_SCHEMAS('<Set pwd for IDM_RPT_DATA>', '<Set pwd for
IDM_RPT_CFG>', '<Set pwd for IDMRPTUSER>');
end;
```

7 Start and complete the Identity Manager Reporting installation.

NOTE: In the Database Details parameter, select Generate SQL for later option.

---

8 Stop Tomcat.

For example:`/etc/init.d/idmapps_tomcat_init stop`

9 Navigate to /opt/netiq/idm/apps/IdentityReporting/sql/ and verify that the following files are available:

- DbUpdate-01-run-as-idm_rpt_cfg.sql
- DbUpdate-02-run-as-idm_rpt_cfg.sql
- DbUpdate-03-run-as-idm_rpt_data.sql
- DbUpdate-04-run-as-idm_rpt_data.sql
- DbUpdate-05-run-as-idm_rpt_cfg.sql
- DbUpdate-06-run-as-idm_rpt_cfg.sql

10 Log in to the Oracle SQL Developer tool or Oracle database as IDM_RPT_CFG user and execute the following commands:

- DbUpdate-01-run-as-idm_rpt_cfg.sql
- DbUpdate-02-run-as-idm_rpt_cfg.sql (Add a separator ‘/’ after the line 183 and then run the SQL command)

11 Log in to the Oracle SQL Developer tool or Oracle database as IDM_RPT_DATA user and execute the following commands:
   - DbUpdate-03-run-as-idm_rpt_data.sql
   - DbUpdate-04-run-as-idm_rpt_data.sql
12 Log in to the Oracle SQL Developer tool or Oracle database as IDM_RPT_CFG user and execute the following commands:
   - DbUpdate-05-run-as-idm_rpt_cfg.sql
   - DbUpdate-06-run-as-idm_rpt_cfg.sql
13 Start Tomcat.

   For example:`/etc/init.d/ idmapps_tomcat_init start`

Installing Identity Reporting 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 Guided Process to Install Identity Reporting" on page 371.

To prepare for the installation, review the prerequisites and system requirements listed in "System Requirements for Identity Reporting" on page 368. 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_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 To specify the installation parameters, complete the following steps:

   2a Ensure that the `.properties` file is located in the same directory as the execution file for installation.

For your convenience, NetIQ provides two `.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

2b In a text editor, open the `.properties` file.

2c Specify the parameter values. For a description of the parameters, see Step 9 on page 371.

NOTE: The `.properties` file for installing Standard Edition includes only the parameters required for that version.

2d Save and close the file.

3 To launch the installation process, enter one of the following commands:

- **Linux**: `./rpt-install-linux.bin -i silent -f` *`path_to_properties_file`*
- **Windows**: `./rpt-install.exe -i silent -f` *`path_to_properties_file`*

NOTE: If the `.properties` file resides in a different directory from the installation 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.

Manually Generating the Database Schema

You can recreate the database tables after installation without having to reinstall. This section helps you create the database schema.

1 Stop Tomcat.

For example:

```
/etc/init.d/idmapps_tomcat_init stop
```

2 (Conditional) Delete the existing database

3 (Conditional) Create a new database with the same name as the one that you deleted in Step 2

4 (Conditional) Clear the database checksums

4a Log in to your database as `idm_rpt_cfg`.

4b Execute the following command for PostgresSQL:

```
  DO
$do$
 BEGIN
  IF EXISTS
   (select table_name from information_schema.tables where table_schema =
'public' and table_name = 'databasechangelog')
  THEN
   update databasechangelog set md5sum = null;
  END IF;
END $do$
```

or

Execute the following command for Oracle:

```
  BEGIN
 FOR i IN
  (select null from ALL_TABLES where OWNER = user and TABLE_NAME =
'DATABASECHANGELOG')
 LOOP
  EXECUTE IMMEDIATE 'update DATABASECHANGELOG set MD5SUM = NULL';
 END LOOP;
END;
```

4c Log in to your database as `idm_rpt_data`.

4d Repeat the commands issued in Step 4b as the `idm_rpt_data` user.

5 Define the JAVA_HOME variable. For example:

```
export JAVA_HOME=/opt/netiq/idm/apps/jre
```

6 Re-initialize the database using the installed script:

6a Regenerate the database tables by executing the following command:

```
/opt/netiq/idm/apps/IdentityReporting/bin/db-init.sh -cfg_password *** -
data_password ***
```

6b Generate the SQL files by executing the following command:

```
/opt/netiq/idm/apps/IdentityReporting/bin/db-init.sh -cfg_password *** -
data_password *** -sql >
/opt/netiq/idm/apps/IdentityReporting/sql/output.sql
```

You use SQL files to regenerate the database tables.

7 Start Tomcat. For example:

```
/etc/init.d/idmapps_tomcat_init start
```

Connecting to a Remote PostgreSQL Database

If your PostgreSQL database is installed on a separate server, you need to change the default settings in the `postgresql.conf` and `pg_hba.conf` files in the remote database.

1 Change the listening address in the `postgresql.conf` file.

By default, PostgreSQL allows to listen for the localhost connection. It does not allow a remote TCP/IP connection. To allow a remoteTCP/IP connection, add the following entry to the `/opt/netiq/idm/postgres/data/postgresql.conf` file:

```
listen_addresses = '*'
```

If you have multiple interfaces on the server, you can specify a specific interface to be listened.

2 Add a client authentication entry to the `pg_hba.conf` file.

By default, PostgreSQL accepts connections only from the `localhost`. It refuses remote connections. This is controlled by applying an access control rule that allows a user to log in from an IP address after providing a valid password (the md5 keyword). To accept a remote connection, add the following entry to the `/opt/netiq/idm/postgres/data/pg_hba.conf` file.

```
host all all 0.0.0.0/0 md5
```

For example, 192.168.104.24/26 trust

This works only for IPv4 addresses. For IPv6 addresses, add the following entry:

```
host all all ::0/0 md5
```

If you want to allow connection from multiple client computers on a specific network, specify the network address in the CIDR-address format in this entry.

The pg_hba.conf file supports the following client authentication formats.

- local database user authentication-method [authentication-option]
- host database user CIDR-address authentication-method [authentication-option]
- hostssl database user CIDR-address authentication-method [authentication-option]
- hostnossl database user CIDR-address authentication-method [authentication-option]

Instead of CIDR-address format, you can specify the IP address and the network mask in separate fields using the following format:

- host database user IP-address IP-mask authentication-method [authentication-option]
- hostssl database user IP-address IP-mask authentication-method [authentication-option]
- hostnossl database user IP-address IP-mask authentication-method [authentication-option]

3 Test the remote connection.

3a Restart the remote PostgreSQL server.

3b Log in to the server remotely using the username and password.

43 Configuring Identity Reporting

After installing Identity Reporting, you can still modify many of the installation properties. To make changes, run the configuration update utility depending on your platform. Run `configupdate.sh` on Linux or run `configupdate.bat` on Windows.

If you change any setting for Identity Reporting with the configuration tool, you must restart Tomcat for the changes to take effect. However, you do not need to restart the server after making changes in the web user interface for Identity Reporting.

- "Running Reports on an Oracle Database" on page 383
- "Deploying REST APIs for Identity Reporting" on page 383

Running Reports on an Oracle Database

Identity Reporting provides the ability to run reports against remote Oracle databases. However, you must add an Oracle JDBC file to the library for your application server.

1. Download the `ojdbc7.jar` file from the Oracle website.
2. Copy the file to the appropriate location for your application server:
   - **Tomcat**: The `common/lib` directory in the *`tomcat_lib`*.

For more information about supported Oracle databases, see "System Requirements for Identity Reporting" on page 368.

Deploying REST APIs for Identity Reporting

Identity Reporting incorporates several REST APIs that enable different features within the reporting functionality. These REST API uses the OAuth2 protocol for authentication.

On Tomcat, the `rptdoc war` is automatically deployed when Identity Reporting is installed.

While working in a staging or production environment, manually delete the `rptdoc war` files and folders from your environment on Tomcat.

44 Managing the Drivers for Reporting

Identity Reporting 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. This process includes the following activities:

- "Configuring Drivers for Identity Reporting" on page 385
- "Deploying and Starting Drivers for Identity Reporting" on page 391
- "Configuring the Runtime Environment" on page 395
- "Setting Auditing Flags for the Drivers" on page 404

Configuring Drivers for Identity Reporting

This section helps you install and configure the Managed System Gateway and Data Collection Service drivers for Identity Reporting.

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 38, "Creating and Deploying the Drivers for the Identity Applications," on page 323.

- "Installing the Driver Packages for Identity Reporting" on page 385
- "Configuring the Managed System Gateway Driver" on page 386
- "Configuring the Driver for Data Collection Service" on page 387
- "Configuring Identity Reporting to Collect Data from the Identity Applications" on page 390

Installing the Driver Packages for Identity Reporting

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 Identity Reporting 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**.

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**.
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 Identity Reporting 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 Identity Reporting to function correctly.

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**.

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 Identity Reporting 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.

You must specify an IP address. Do not specify an address of localhost for the Identity Vault Registration.

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.

In environments where the driver receives large numbers of events, NetIQ recommends setting the number of batches per file to no more than 5. If you set this parameter to a value greater than 5, the driver cannot process events efficiently.

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 Identity Reporting.

Port

Specifies the port number that Identity Reporting uses for REST connections.

Protocol

Specifies the protocol for accessing Identity Reporting. 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 Identity Reporting.

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 Identity Reporting).

20f (Conditional) To collect data from the identity applications, specify the values for **SSO Service Support**. For more information, see "Configuring Identity Reporting to Collect Data from the Identity Applications" on page 390.

20g Click **Apply**.

21 To configure DNs, 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**.

Configuring Identity Reporting to Collect Data from the Identity Applications

For Identity Reporting to collect data from the identity applications, you must configure the DCS driver to support the single sign-on process.

1. Open your project in Designer.
2. In the **Outline** view, right-click the Data Collection Service driver, then click **Properties**.
3. Click **Driver Configuration > Driver Parameters**.
4. Click **Show connection parameters > show**.
5. Click **SSO Service Support > Yes**.
6. Specify the parameters for single sign-on functionality:

   SSO Service Address

   Required

   Specifies the relative URL of the authentication server that issues tokens to OSP. For example, `10.10.10.48`.

   This value must match the value that you specified in the RBPM configuration utility for **OSP server host identifier**. For more information, see "Authentication Server" on page 350.

   SSO Service Port

   Required

   Specifies the port for the authentication server. The default value is 8180.

   This value must match the value that you specified in the RBPM configuration utility for **OSP server TCP port**. For more information, see "Authentication Server" on page 350.

   SSO Service Client ID

   Required

   Specifies the name that you want to use to identify the single sign-on client for the DCS driver to the authentication server. The default value is `dcsdrv`.

   This value must match the value that you specified in the RBPM configuration utility for **OSP client ID**. For more information, see "Reporting" on page 358.

   SSO Service Client Secret

   Required

   Specifies the password for the single sign-on client for the DCS driver.

   This value must match the value that you specified in the RBPM configuration utility for **OSP client secret**. For more information, see "Reporting" on page 358.

   Protocol

   Specifies whether the service client uses the `http` (non-secure) or `https` (secure) protocol when communicating with the authentication server.
7. Click **Apply**, then click **OK**.
8. (Conditional) If you changed these settings after deploying the driver, you must deploy and restart the driver. For more information, see "Deploying and Starting Drivers for Identity Reporting" on page 391.
9. Repeat this procedure for each DCS driver in your environment.

Deploying and Starting Drivers for Identity Reporting

Identity Reporting requires the following drivers:

- Identity Manager Managed System Gateway Driver
- Identity Manager Driver for Data Collection Service

This process includes the following activities:

- "Deploying the Drivers" on page 391
- "Verifying that the Managed Systems are Working" on page 391
- "Starting the Drivers for Identity Reporting" on page 394

For more information about installing and configuring these drivers, see "Configuring Drivers for Identity Reporting" on page 385.

Deploying the Drivers

You must deploy the two drivers for Identity Reporting.

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.

Verifying that the Managed Systems are Working

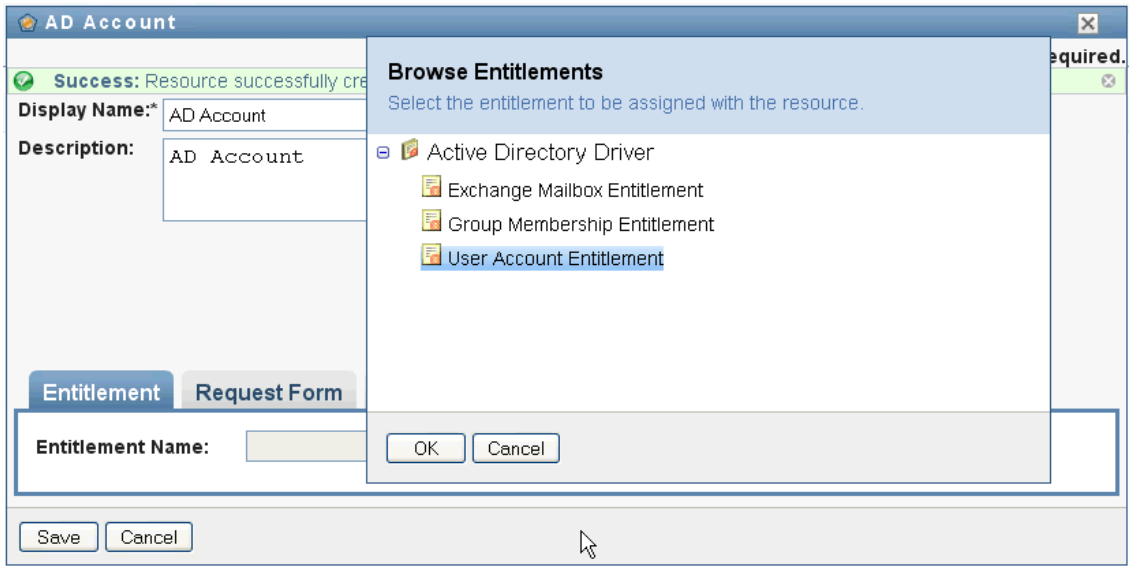
Before you start the Managed System Gateway Driver and the Data Collection Service Driver, you should confirm that the underlying managed systems are properly configured. This process helps you isolate problems with your environment that do not relate to the configuration of the reporting drivers.

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 *NetIQ Identity Manager Driver for Active Directory Implementation Guide*.

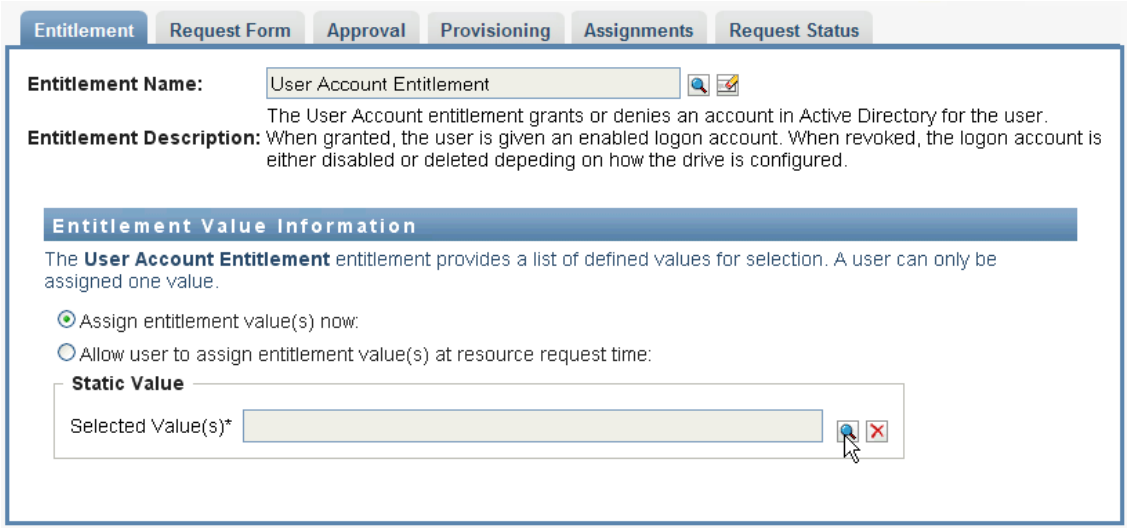
The following steps demonstrate one way to confirm that Active Directory is properly configured:

1. Ensure that the User Application and Identity Reporting 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 in 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**.



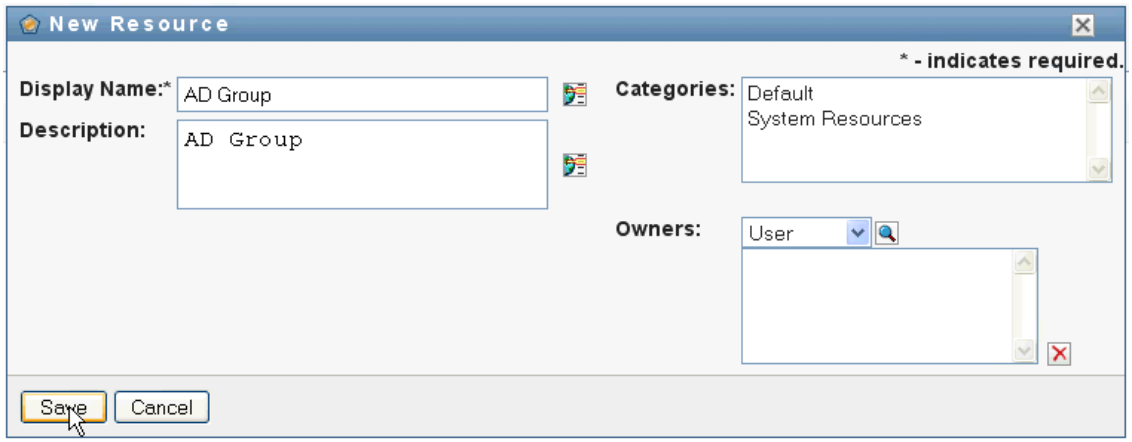
The User Application can retrieve the entitlement from the driver.

6 Because this particular resource pertains to accounts, configure the resource to assign an account value.



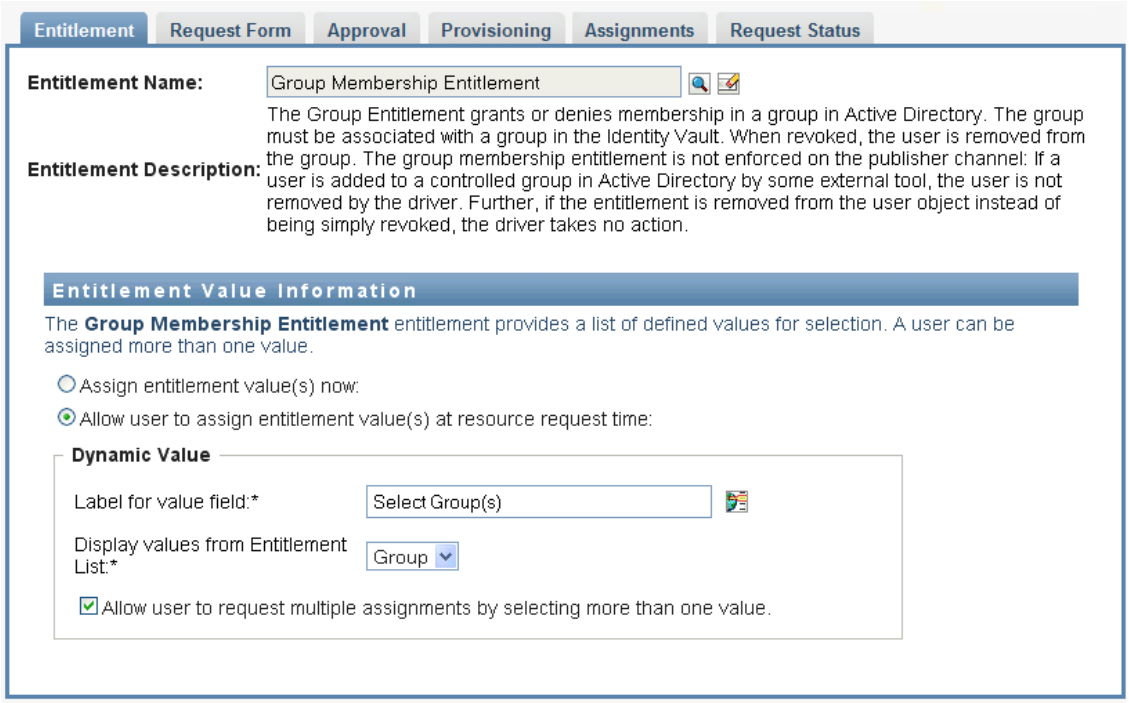
7 Select the account value, and then click **Add**.

8 Create another resource that assigns groups.

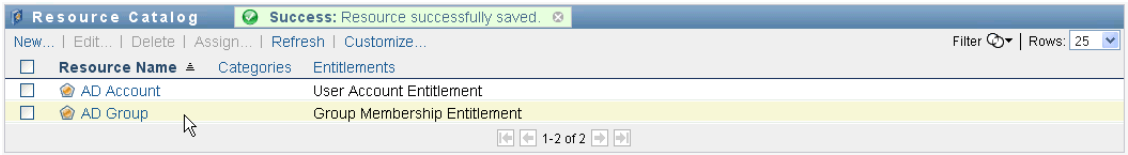


9 Bind the resource to an entitlement that is suitable for groups. For this particular resource, map to the **Group Membership Entitlement**.

10 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.



11 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.

Starting the Drivers for Identity Reporting

This section provides instructions for starting the Managed System Gateway Driver and the Data Collection Service Driver.

1. Open iManager.
2. Right-click the Managed System Gateway Driver, and then click **Start driver**.
3. Right-click the Data Collection Service Driver, and then click **Start driver**.
4. 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 in to Identity Reporting 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.

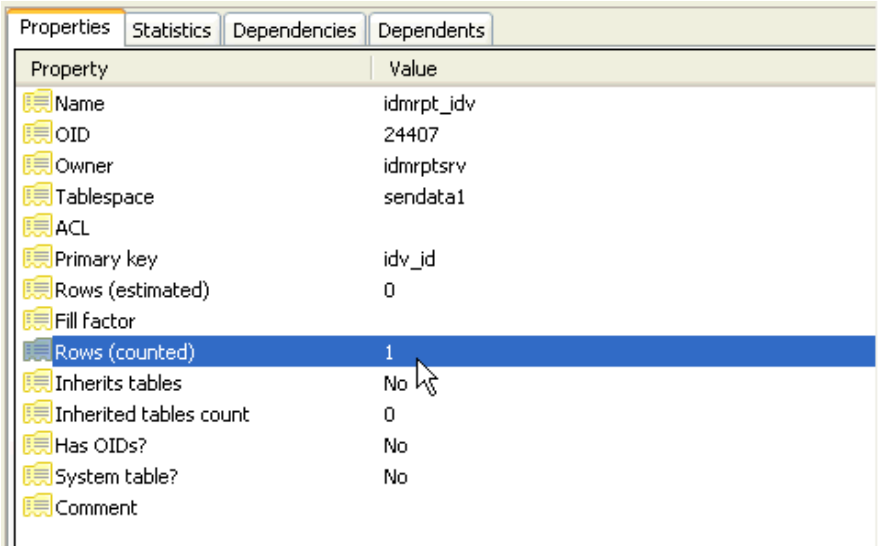
   At this point, you can look at the contents of the Identity Information Warehouse to learn more about the rich data that is stored about the Identity Vault, as well as the managed systems in your enterprise.
10. To see the data in the Identity Information Warehouse, use a database administration tool 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

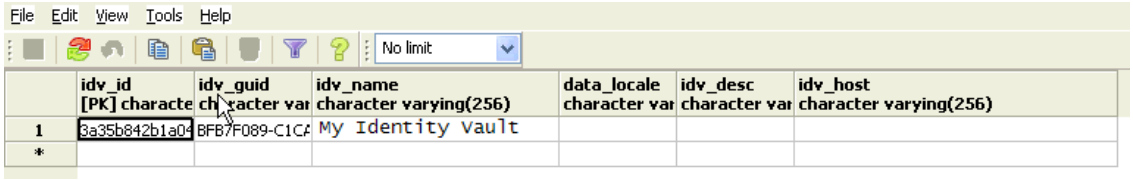
    Contains reporting configuration data, such as report definitions and schedules. The installation program for Identity Reporting adds this schema to the database.

    idm_rpt_data

    Contains information collected by the Managed System Gateway Driver and the Data Collection Service Driver. The installation program for Identity Reporting adds this schema to the 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:



13 Verify that the data for this table shows the name of the Identity Vault:



If you see the new row in this table, the driver registration process was successful.

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.

This process includes the following activities:

- "Configuring the Data Collection Services Driver to Collect Data from the Identity Applications" on page 396
- "Migrating the Data Collection Service Driver" on page 397
- "Adding Support for Custom Attributes and Objects" on page 399
- "Adding Support for Multiple Driver Sets" on page 401
- "Configuring the Drivers to Run in Remote Mode with SSL" on page 403

If you have problems with one or more of the drivers that are difficult to understand, see Troubleshooting the Drivers in the *Administrator Guide to NetIQ Identity Reporting*.

Configuring the Data Collection Services Driver to Collect Data from the Identity Applications

For the identity applications to function properly with Identity Reporting, you must configure the DCS driver to support the OAuth protocol.

NOTE

- You only need to install and configure the DCS driver if you use Identity Reporting in your environment.
- If you have multiple DCS drivers configured in your environment, you must complete the following steps for each driver.

1. Log in to Designer.
2. Open your project in Designer.
3. (Conditional) If your project does not already include a Data Collection Service driver, import the driver into your project. For more information, see Chapter 38, "Creating and Deploying the Drivers for the Identity Applications," on page 323.
4. (Conditional) If you have not already upgraded your DCS driver to the supported patch version, complete the following steps:
   - **4a** Download the latest DCS driver patch file.
   - **4b** Extract the patch file to a location on your server.
   - **4c** 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
     ```

   - **4d** Restart eDirectory.
   - **4e** 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 "Prerequisites for Installing the Identity Reporting Components" on page 367.
   - **4f** Redeploy and restart the DCS driver in Designer.
5. In the **Outline** view, right-click the DCS driver, then select **Properties**.
6. Click **Driver Configuration**.
7. Click the **Driver Parameters** tab.
8. Click **Show connection parameters**, then select **show**.
9. Click **SSO Service Support**, then select **Yes**.
10. Specify the IP address and port for the Reporting Module.
11. Specify a password for the SSO Service Client. The default password is `driver`.
12. Click **Apply**, then click **OK**.
13. In the **Modeler** view, right-click the DCS driver, then select **Driver > Deploy**.
14. Click **Deploy**.
15. If prompted to restart the DCS driver, click **Yes**.
16. Click **OK**.

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 in to the iManager.

2 In the **Overview** panel for the Data Collection Service Driver, select **Migrate From Identity Vault**.

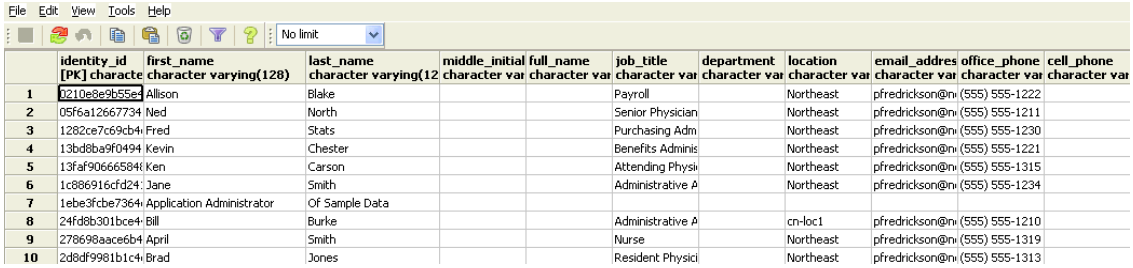
3 Select the organizations that contain relevant data, and click **Start**.

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.

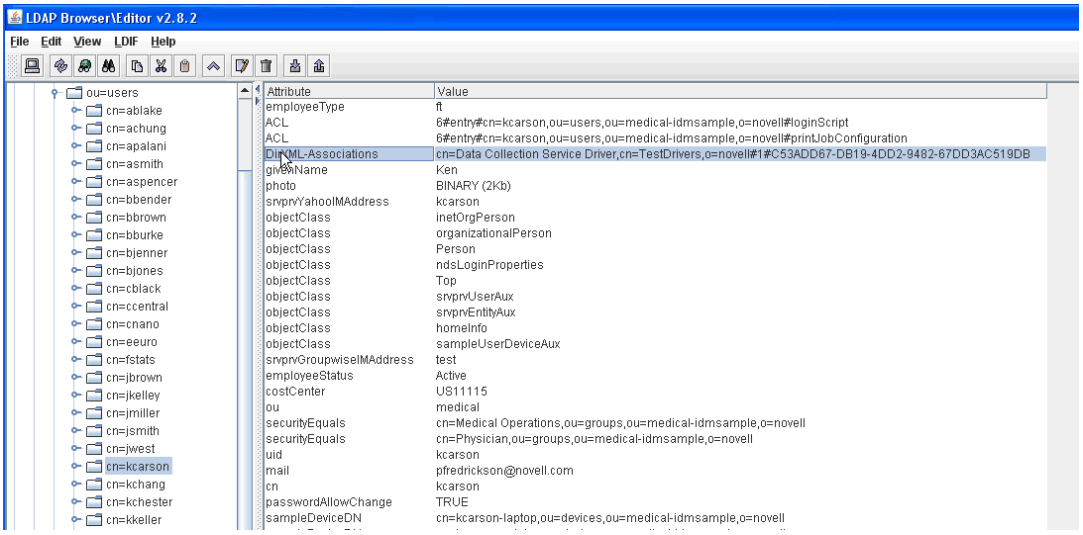
5 In the **idmrpt_identity** and **idmrpt_acct** tables, which provide information about the identities and accounts in the Identity Vault, ensure they contain the following type of information:



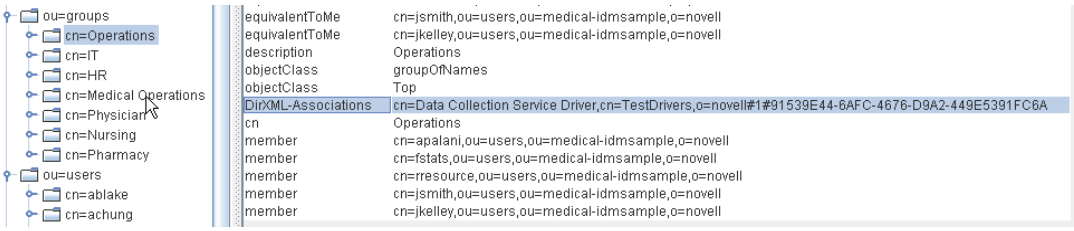
	identity_id [PK] characte	first_name character varying(128)	last_name character varying(12	middle_initial character var	full_name character var	job_title character var	department character var	location character var	email_addres character var	office_phone character var	cell_phone character var
1	0210e8e9b55e4	Allison	Blake			Payroll		Northeast	pfredrickson@n	(555) 555-1222	
2	05f6a12667734	Ned	North			Senior Physician		Northeast	pfredrickson@n	(555) 555-1211	
3	1282ce7c69cb4	Fred	Stats			Purchasing Adm		Northeast	pfredrickson@n	(555) 555-1230	
4	13bd8ba9f0494	Kevin	Chester			Benefits Adminis		Northeast	pfredrickson@n	(555) 555-1221	
5	13faf90666584	Ken	Carson			Attending Physi		Northeast	pfredrickson@n	(555) 555-1315	
6	1c886916cfd24	Jane	Smith			Administrative A		Northeast	pfredrickson@n	(555) 555-1234	
7	1ebe3fcbe7364	Application Administrator	Of Sample Data								
8	24fd8b301bce4	Bill	Burke			Administrative A		cn-loc1	pfredrickson@n	(555) 555-1210	
9	278698aace6b4	April	Smith			Nurse		Northeast	pfredrickson@n	(555) 555-1319	
10	2d8df9981b1c4	Brad	Jones			Resident Physici		Northeast	pfredrickson@n	(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_gro boolean	dynamic_rule character var	nested_group boolean	idmrpt_valid_from timestamp without tin	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 Resourc	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 Operati	Medical Operati	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.

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 399
- "Including a Name and Description in the Database" on page 400
- "Adding Extended Attributes to Known Object Types" on page 400

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.

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.

  If you use the integrated installation process to add a second server to the tree, the server receives only a copy of the root and its own driverset partition. If you also use the Data Collection Service Driver as primary on this secondary server, the driver cannot see object changes that it needs to report. To configure the Data Collection Service Driver on this server, see “Configuring the Driver for Data Collection Service” on page 387.

- **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.

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 **NetIQ 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 **NetIQ Certificate Access > Server Certificates**.
   - **2b** Select the certificate created in Step 1 on page 403 and click **Export**.
   - **2c** In the **Certificates** menu, select the name of your certificate.
   - **2d** Ensure that **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 403 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 403.

5e Save and restart the driver.

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.

- "Setting Audit Flags in Identity Manager" on page 404
- "Setting Audit Flags in eDirectory" on page 405

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	◆ Metadirectory Engine Warnings
Status Events	◆ Success **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. ◆ Error ◆ Fatal

Category	Recommended Flags
Operation Events	◆ 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	◆ Password Reset ◆ User Agent Request ◆ Password Sync
Credential Provisioning Events	◆ Set SSO Credentials ◆ Clear SSO Credentials ◆ Set SSO Passphrase

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	◆ Do Not Send Replicated Events
Meta	◆ (*Select all flags)*

Category	Recommended Flags
Objects	◆ 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	◆ *(Select all flags)*
Agent	◆ DS Reloaded ◆ Local Agent Opened ◆ Local Agent Closed ◆ NLM Loaded
Miscellaneous	◆ Generate CA Keys ◆ Recertified Public Key

Category	Recommended Flags
LDAP	◆ 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

XIV Installing Analyzer for Identity Manager

This section guides you through the process of installing Analyzer for Identity Manager. 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.

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:\NetIQ\Analyzer`

NetIQ recommends that you review the installation process before beginning. For more information, see "Checklist for Installing Analyzer" on page 411.

45 Planning to Install Analyzer

This section provides guidance for preparing to install Analyzer for Identity Manager. NetIQ recommends that you review the installation process before beginning.

- "Checklist for Installing Analyzer" on page 411
- "Prerequisites for Installing Analyzer" on page 411
- "System Requirements for Installing Analyzer" on page 412

Checklist for Installing Analyzer

Before beginning the installation process, NetIQ recommends that you review the following steps:

	Checklist Items
❑	1. Learn about the interaction among Identity Manager components. For more information, see Chapter 1, "Overview of the Components of Identity Manager," on page 23.
❑	2. Decide which servers you want to use for your Identity Manager components. For more information, see "Recommended Installation Scenarios and Server Setup" on page 44.
❑	3. (Conditional) For computers running a SLES 12 SP1 or later operating system, ensure that you have installed the appropriate set of libraries for a guided installation. For more information, see "Installing Identity Manager on SLES 12 SP1 or Later Servers" on page 55.
❑	4. Ensure that your environment meets the considerations and requirements for hosting Analyzer. For more information, see the following sections: ◆ "Prerequisites for Installing Analyzer" on page 411 ◆ "System Requirements for Installing Analyzer" on page 412
❑	5. To install Analyzer, see the following sections: ◆ To use the installation wizard, see "Using the Wizard to Install Analyzer" on page 413. ◆ For a silent installation, see "Installing Analyzer Silently" on page 414
❑	6. (Optional) To automatically receive and display audit events from Analyzer, install the XDAS client. For more information, see "Installing an Audit Client for Analyzer" on page 415.
❑	7. To activate Analyzer, see "Activating Analyzer" on page 455.
❑	8. (Optional) To upgrade Analyzer, see "Upgrading Analyzer" on page 499.

Prerequisites for Installing Analyzer

Before installing Analyzer, ensure that you install an appropriate package that contains the `/usr/lib/libpng12.so.0` library.

System Requirements for Installing Analyzer

This section provides the minimum requirements for the servers where you want to install Analyzer. Ensure that you review the prerequisites and considerations for installation, particularly those related to the operating system.

Category	Requirement
Processor	1 GHz
Memory	512 MB (4 GB recommended)
Video resolution	1024*768 (1280*1025 recommended)
Operating system (certified)	One of the following 64-bit operating systems: ◆ openSUSE 13.2 ◆ SUSE Linux Enterprise Server 12 SP1 ◆ SUSE Linux Enterprise Server 11 SP4 ◆ Windows Server 2012 R2 ◆ Windows Server 2012 ◆ Windows Server 2008 One of the following 32-bit operating systems: ◆ openSUSE 13.2 NetIQ recommends that you apply the latest operating system patches according to the manufacturer's automated update facility before you install Identity Manager. **NOTE:** *Certified* means that the operating system has been fully tested and is supported.
Operating system (supported)	Latest versions of service packs for the certified operating systems **NOTE:** *Supported* means that the operating system has not yet been tested but is expected to work
Virtualization system	◆ Hyper-V Server 2012 R2 ◆ VMWare ESX 5.0 and later NetIQ supports Identity Manager on enterprise-class virtualization systems that provide official support for the operating systems where NetIQ products are running. As long as the vendors of the virtualization systems officially support these operating systems, NetIQ supports the entire Identity Manager stack on them.
Additional software	◆ 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)

46 Installing Analyzer

This section guides you through the process of installing Analyzer and configuring your environment for Analyzer.

- "Using the Wizard to Install Analyzer" on page 413
- "Installing Analyzer Silently" on page 414
- "Adding XULrunner to Analyzer.ini on Linux Platforms" on page 414
- "Installing an Audit Client for Analyzer" on page 415

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 "Installing Analyzer Silently" on page 414.

To prepare for the installation, review the prerequisites and system requirements listed in "Checklist for Installing Analyzer" on page 411.

1. Log in 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 "Adding XULrunner to Analyzer.ini on Linux Platforms" on page 414.
9. (Optional) To configure role-based services for Analyzer on the Windows computer, open the link to the `gettingstarted.html` website, located by default in the `C:\Program Files (x86)\NetIQ\Tomcat\webapp\nps\help\en\install` directory.

   You use iManager to configure the role-based services.
10. To activate Analyzer, see "Activating Analyzer" on page 455.

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)\NetIQ\Analyzer` directory.

1. Log in 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 NetIQ Downloads website, 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 `analzerInstaller.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 "Adding XULrunner to Analyzer.ini on Linux Platforms" on page 414.
7. To activate Analyzer, see "Activating Analyzer" on page 455.

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:\NetIQ\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.

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 *NetIQ Analyzer 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).

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.

XV Configuring Single Sign-on Access in Identity Manager

By default, Identity Manager uses OSP for single sign-on access in Identity Manager. When you install Identity Reporting and the identity applications, you specify the basic settings for user authentication. However, you can also configure the OSP authentication server to accept authentication from the Kerberos ticket server or SAML IDP. For example, you can use SAML to support authentication from NetIQ Access Manager. For more information about OSP, see "Using Single Sign-on Access in Identity Manager" on page 37.

47 Preparing for Single Sign-on Access

By default, Identity Manager uses OSP for single sign-on access in Identity Manager. When you install Identity Reporting and the identity applications, you specify the basic settings for user authentication. However, you can also configure the OSP authentication server to accept authentication from the Kerberos ticket server or SAML IDP. For example, you can use SAML to support authentication from NetIQ Access Manager.

NetIQ recommends that you complete the steps in the following checklist.

	Checklist Items
❑	1. Understand how Identity Manager uses OSP for single sign-on access. For more information, see "Using Single Sign-on Access in Identity Manager" on page 37.
❑	2. Install OSP. For more information, see Part XI, "Installing the Password Management Component," on page 263.
❑	3. Install the identity applications. For more information, see Part XII, "Installing the Identity Applications," on page 277.
❑	4. (Optional) Install Identity Reporting. For more information, see Part XIII, "Installing Identity Reporting," on page 363.
❑	5. Configure the identity applications for single sign-on access using OSP. For more information, see Chapter 48, "Using One SSO Provider for Single Sign-on Access in Identity Manager," on page 421.
❑	6. Install the authentication system that you want to use with Identity Manager. For example, Access Manager or Kerberos.
❑	7. (Conditional) Configure Access Manager and OSP. For more information, see Chapter 49, "Using SAML Authentication with NetIQ Access Manager for Single Sign-on," on page 423.
❑	8. Verify the single sign-on settings. For more information, see Chapter 51, "Verifying Single Sign-on Access for the Identity Applications," on page 433.

48 Using One SSO Provider for Single Sign-on Access in Identity Manager

To provide single sign-on access to the identity applications, you must configure the settings in the RBPM Configuration utility. You should already have the certificates and keys necessary for single sign-on from installing OSP.

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.

Preparing eDirectory for Single Sign-on Access

You must configure the Identity Vault, as part of your eDirectory installation, to support single sign-on access for the identity applications and Identity Reporting.

Perform the steps in "Configuring the Identity Vault for the Identity Applications" on page 329. If you previously extended the eDirectory schema to include the SAML schema and installed the required NMAS methods, you do not need to perform those steps a second time. Instead, skip to the subsection about creating the Trusted Root Container.

Modifying the Basic Settings for Single Sign-on Access

When you install the identity applications, you generally configure the basic settings for single sign-on access. This section helps you ensure that the settings work for your environment.

1. Run the RBPM Configuration utility. For more information, see "Running the Identity Applications Configuration Utility" on page 339.
2. To modify the authentication settings, complete the following steps:
   - **2a** Click **Authentication**.
   - **2b** (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 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 when you installed OSP. For more information, see Chapter 32, "Installing Password Management for Identity Manager," on page 267.
     - 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.
   - **2c** For **LDAP DN of Admins Container**, click the **Browse** button, then select the container within the Identity Vault that contains your identity applications administrator.

2d Specify the OAuth keystore file that you created when you installed OSP. For more information, see Chapter 32, “Installing Password Management for Identity Manager,” on page 267.

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`.

3 To modify the single sign-on settings, complete the following steps:

3a Click **SSO Clients**.

3b (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 the 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 when you installed OSP. For more information, see Chapter 32, “Installing Password Management for Identity Manager,” on page 267.
- 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.

3c (Conditional) If you use non-default ports, update the port numbers for the following Identity Manager components:

- Catalog Administrator
- Identity Manager Dashboard
- Identity Reporting
- User Application

4 Click **OK** to save your changes, then close the configuration utility.

5 Start Tomcat.

Configuring Self Service Password Reset to Trust OSP

In order for single sign-on to work properly, you must configure a trust relationship with certificates between the OSP and Self Service Password Rest (SSPR). You must export a certificate from the keystore file of the OSP which is `osp.jks`.

After you export the certificate, you must import the certificate in to the keystore file for SSPR. The default path keystore file for SSPR is:

- **Linux/UNIX:** `/[Java_Home]/lib/security/cacerts`
- **Windows:** `C:\[Java_Home]\lib\security\cacerts`

For more information about setting a secure channel, see “Setting Up a Secure Channel Between the Application Server and the LDAP Server ” in the “Self Service Password Reset Administration Guide”.

49 Using SAML Authentication with NetIQ Access Manager for Single Sign-on

This section helps you configure both NetIQ Access Manager and OSP to support single sign-on access in Identity Manager using SAML 2.0 authentication. Before beginning, review the following assumptions for these instructions:

- You have installed a new, supported version of Access Manager.
- You have installed a new version of Identity Manager.
- Both installations use DNS names for the host name configuration.
- Both installations use SSL protocol for communication.
- You have to set up a cluster environment for Access Manager that uses the Identity Vault as the LDAP User Store. For more information, see *NetIQ Access Manager Administration Guide*.

Understanding Third-Party Authentication and Single Sign-On

You can configure Identity Manager to work with NetIQ Access Manager using SAML 2.0 authentication. This capability enables you to use a technology that is not password-based to log in to the identity applications through Access Manager. For example, users can log in through a user (client) certificate, such as from a smart card.

Access Manager interacts with OSP to map the user to a DN in the Identity Vault. When a user logs in to the identity applications through Access Manager, Access Manager can inject a SAML assertion (with the user's DN as the identifier) into an HTTP header and forward the request to the identity applications. The identity applications use the SAML assertion to establish the LDAP connection with the Identity Vault.

Accessory portlets that allow single sign-on authentication based on passwords do not support single sign-on when SAML assertions are used for identity application authentication.

Creating and Installing SSL Certificates

To ensure authentication, Access Manager and OSP must share the trusted root of their SSL certificates. This section helps you create a new certificate for Access Manager then ensure that the trust stores have the correct certificates.

- "Creating an SSL Certificate for Access Manager" on page 424
- "Installing the Access Manager Certificate in the Identity Manager Trust Store" on page 424
- "Installing the SSL Server Certificate in the Access Manager Trust Store" on page 425

Creating an SSL Certificate for Access Manager

Access Manager cannot use its default SSL certificate, `test-connector`, to communicate with Identity Manager. Instead, you must create a certificate that includes the host name in the certificate subject field and assign it to Access Manager.

For more information, see "Security and Certificate Management" in the *NetIQ Access Manager Administration Console Guide*.

1. Open the Administration Console of Access Manager.
2. Click **Security > Certificates**.
3. Click **New**.
4. Specify a name for the new certificate. For example, *`hostname`*`_ssl`.
5. Click the edit button on the right side of the window.
6. For **Common name**, specify the DNS name of the server that hosts Access Manager, then click **OK**.
7. For **Months valid**, specify a value up to 99.
8. For **Key size**, specify `2048`.
9. Select the newly-created certificate, then click **Actions > Add certificate to Keystores...**.
10. Click the edit button on the right side of **Keystores**.
11. Select **SSL connector**, and then click **OK**.
12. Click **OK**.
13. Install the new certificate in the OSP trust store. For more information, see "Installing the Access Manager Certificate in the Identity Manager Trust Store" on page 424.

Installing the Access Manager Certificate in the Identity Manager Trust Store

The OSP trust store must include the security certificate for Access Manager.

1. To export the new SSL certificate, complete the following actions:
   - Under **Security** > **Trusted Roots** in the Administration Console of Access Manager, export the root certificate of the SSL certificate. Name the root certificate **configCA**.
   - Export the SSL server certificate.

     For more information, see "Managing Trusted Roots and Trust Stores" in the *NetIQ Access Manager Administration Console Guide*.
2. Copy the exported certificate to the server where OSP is running.
3. Use the keytool available with Java to import the file into the cacerts keystore of the JRE.

   For example, `/opt/netiq/idm/apps/jre/bin/keytool -importcert -trustcacerts -alias <NAM-cert> -keystore /opt/netiq/idm/apps/jre/lib/security/cacerts -storepass <password>  -file custom_location/<exported_file>`
4. Install the OSP certificate in the Access Manager trust store.

   For more information, see "Installing the SSL Server Certificate in the Access Manager Trust Store" on page 425.

Installing the SSL Server Certificate in the Access Manager Trust Store

The Access Manager trust store must include the security certificate for OSP. For more information, see "Managing Trusted Roots and Trust Stores" in the *NetIQ Access Manager Administration Console Guide*.

Obtain the server certificate being used for SSL by the Tomcat instance running OSP.

1. Copy the SSL server certificate of the Tomcat instance that hosts OSP to the server where you installed Access Manager.
2. Open the Administration Console of Access Manager.
3. To import the certificate, click **Security > NIDP Trust Store.**
4. Click **Add**.
5. Select Trusted Root from **Add dialog** > **Import**.
6. Select the root certificate that you want to import and then click **OK**.
7. Ensure that OSP recognizes assertions of authentication from SAML.

   For more information, see "Creating an Attribute Set for SAML" on page 426.

Configuring Identity Manager to Trust Access Manager

Identity Manager needs the URL of the SAML metadata to redirect users for authentication requests. By default, Access Manager uses the following URL for storing the SAML metadata:

`https://server:port/nidp/saml2/metadata`

where *server*:*port* represent the Access Manager Identity Server.

1. (Optional) To view an `.xml` document for the SAML metadata, open the URL in a browser.

   If the URL does not produce the document, ensure that the link is correct.
2. On the OSP server, run the RBPM Configuration utility. For more information, see "Running the Identity Applications Configuration Utility" on page 339.
3. In the utility, select **Authentication**.
4. For **Authentication Method**, specify **SAML 2.0**.
5. For **Metadata URL**, specify the URL that OSP uses to redirect the authentication request to SAML metadata of Access Manager.

   For example, `https://server:port/nidp/saml2/metadata`
6. In the **Authentication Server** section, specify the DNS name of the server that hosts OSP in the **Oauth server host identifier** setting.
7. Click **OK** to save the changes.
8. Restart the Tomcat instance that hosts OSP.

Configuring Access Manager to Work with Identity Manager

To ensure that Access Manager recognizes Identity Manager as a trusted service provider, add the metadata text for OSP to the Identity Server and configure an attribute set. This process includes the following activities:

- "Copying the Metadata for Identity Manager" on page 426
- "Creating an Attribute Set for SAML" on page 426
- "Adding Identity Manager as a Trusted Service Provider" on page 427

Copying the Metadata for Identity Manager

Access Manager needs the metadata text for OSP. You should copy the contents of the metadata `.xml` file to a document that you can open on the Access Manager Identity Server.

1. In a browser, navigate to the URL for the OSP metadata. By default, Identity Manager uses the following URL:

   `https://server:port/osp/a/idm/auth/saml2/spmetadata`

   where *server*:*port* represent the Tomcat server that hosts OSP.
2. View the page source for the `spmetadata.xml` file.
3. Copy the contents of the file to a document that you can access in "Adding Identity Manager as a Trusted Service Provider" on page 427

Creating an Attribute Set for SAML

To ensure that SAML can perform an assertion exchange between Access Manager and OSP, create an attribute set in Access Manager. Attribute sets provide a common naming scheme for the exchange. OSP looks for an attribute value that identifies the subject of the assertion. By default, the attribute is `mail`.

For more information, see "Configuring Attribute Sets" in the *NetIQ Access Manager Administration Guide*.

1. Open the Administration Console for Access Manager.
2. Click **Devices > Identity Servers > Shared Settings > Attribute Sets > New**.
3. Specify a name for the attribute set. For example, `IDM SAML Attributes`.
4. Click **Next**, and then click **New**.
5. For **Local Attribute**, select **Ldap attribute: mail [LDAP Attribute Profile]**.
6. For **Remote Attribute**, specify `mail`.
7. Click **OK**, and then click **Finish**.

Adding Identity Manager as a Trusted Service Provider

Configure Access Manager to recognize Identity Manager as a trusted service provider. For more information, see "Creating a Trusted Service Provider for SAML 2.0" in the *NetIQ Access Manager Administration Guide*.

1. Open the Administration Console for Access Manager.
2. Click **Devices > Identity Servers > Edit > SAML 2.0**.
3. Click **New > Service Provider**.
4. For **Provider Type**, specify **General**.
5. For **Source**, specify **Metadata Text**.
6. In the **Text** field, paste the contents of the `spmetadata.xml` file that you copied in "Copying the Metadata for Identity Manager" on page 426.
7. Specify a name for the new OSP service provider.
8. Click **Next**, then click **Finish**.
9. On the **SAML 2.0** tab, select the OSP service provider that you created in Step 7.
10. Click **Attributes**.
11. Select the attribute set that you created in "Creating an Attribute Set for SAML" on page 426. For example, `IDM SAML Attributes`.
12. Move the attributes available for the OSP service provider set to the **Send with authentication** panel on the left side of the page.

    The attributes that you move to the **Send with authentication** panel are the attributes that you want to be obtained during authentication.
13. Click **OK** twice.
14. To update the Identity Server, click **Devices > Identity Servers > Update > Update All Configuration**.

Updating the Login Pages for Access Manager

The default login pages for Access Manager use HTML iFrame elements that conflict with the elements used for the identity applications. This section provides instructions for eliminating that conflict by creating a new login method and contract for Access Manager. The `.jsp` files referenced in this section are located by default in the `/opt/novell/nam/idp/webapps/nidp/jsp` directory.

For more information, see "Customizing the Identity Server Login Page" in the *NetIQ Access Manager Administration Guide*.

1. Modify the `top.jsp` file according to TID 7004020 and TID 7018468.
2. (Optional) For backup purposes, copy and rename the `login.jsp` file. For example, rename it to `idm_login.jsp`.
3. Open the Administration Console for Access Manager.
4. To create a new login method, complete the following steps:
   - **4a** Click **Devices > Identity Servers > Edit > Local > Methods**.
   - **4b** Click **New**, then specify the **Display Name** for the new method. For example, `IDM Name/Password`.
   - **4c** For **Class**, specify **Name/Password-Form**.
   - **4d** For **User Store**, specify Identity Vault as an LDAP user store.

4e In the **Properties** section, click **New**, then specify the following properties:

Name	Value
JSP	idm_login
MainJSP	true

4f Click **OK**.

5 To create a contract that uses the new login method, complete the following steps:

5a Click **Contracts > New**.

5b In the **Configuration** tab, specify the **Display Name** for the new contract. For example, `IDM Name/Password`.

5c For **URI**, specify `name/password/uri/idm`.

5d Under **Methods**, add the method that you created in Step 4. For example, `IDM Name/Password`.

5e In the **Authentication Card** tab, specify an **ID** for the card. For example, `IDM_NamePassword`.

5f Specify an image for the card.

5g Click **OK**.

6 To specify the default values for how the system processes the new authentication contract, complete the following steps:

6a On the **Local** tab, click **Defaults**.

6b For User Store, specify Identity Vault as an LDAP user store.

6c For **Authentication Contract**, specify the contract that you created in Step 5. For example, `IDM Name/Password-Form`.

6d Click **OK**.

7 To update the Identity Server, click **Devices > Identity Servers > Update > Update All Configuration**.

50 Using Kerberos for Single Sign-On

You can use Kerberos as an authentication method for the identity applications that allows single sign-on (SSO). This also allows users to use Integrated Windows Authentication to log in to the applications. This section provides instructions for configuring Active Directory to use Kerberos for connecting to the identity applications:

- "Configuring the Kerberos User Account in Active Directory" on page 429
- "Configuring the Identity Applications Server" on page 430
- "Configure the End-User Browsers to Use Integrated Windows Authentication" on page 432

Configuring the Kerberos User Account in Active Directory

Use the Active Directory administration tools to configure Active DIrectory for Kerberos authentication. You need to create a new Active Directory user account for the identity applications and identity reporting. The user account name must use the DNS name of the server that hosts the identity applications and identity reporting.

NOTE: For domain or realm references, use uppercase format. For example `@MYCOMPANY.COM`.

---

1. As an Administrator in Active Directory, use the Microsoft Management Console (MMC) to create a new user account with the DNS name of the server that hosts the identity applications.

   For example, if the DNS name of the identity applications server is `rbpm.mycompany.com`, use the following information to create the user:

   First name: rbpm

   User login name: HTTP/rbpm.mycompany.com

   Pre-windows logon name: rbpm

   Set password: Specify the appropriate password. For example: `Passw0rd`.

   Password never expires: Select this option.

   User must change password at next logon: Do not select this option.

2. Associate the new user with the Service Principal Name (SPN).

   2a In the Active Directory server, open a cmd shell.

   2b At the command prompt, enter the following:

   ```
   setspn -A HTTP/DNS_Identity_Applications_server@WINDOWS-DOMAIN userID
   ```

   For example:

   ```
   setspn -A HTTP/rbpm.mycompany.com@MYCOMPANY.COM rbpm
   ```

   2c Verify setspn by entering `setspn -L userID`.

3. To generate the `keytab` file, use the `ktpass` utility:

   3a At the command line prompt, enter the following:

```
ktpass /out filename.keytab /princ servicePrincipalName /mapuser
userPrincipalName /mapop set /pass password /crypto ALL /ptype
KRB5_NT_PRINCIPAL
```

For example:

```
ktpass /out rbpm.keytab /princ HTTP/rbpm.mycompany.com@MYCOMPANY.COM /mapuser
rbpm  /mapop set /pass Passw0rd /crypto All /ptype KRB5_NT_PRINCIPAL
```

IMPORTANT: For domain or realm references, use uppercase format. For example, `@MYCOMPANY.COM`.

3b Copy the `rbpm.keytab` file to your identity applications server.

4 An an Administrator in Active Directory, create an end user account with the MCC to prepare for SSO.

The end user account name has to match some attribute value of an eDirectory user in order to support single sign-on. Create the user with some name such as `cnano`, remember the password, and ensure that **User must change password at next logon** is not selected.

5 (Optional) Repeat these steps for Identity Reporting if you installed the reporting component on a separate server.

6 Configure the server for the identity applications to accept the Kerberos configuration. For more information, see "Configuring the Identity Applications Server" on page 430.

Configuring the Identity Applications Server

You must configure your identity applications server to use the Kerberos keytab file and the user account that you have created in Active Directory. Ensure that you complete "Configuring the Kerberos User Account in Active Directory" on page 429 before proceeding.

NOTE: For domain or realm references, use uppercase format. For example `@MYCOMPANY.COM`.

---

1 To define your operating system settings for the Kerberos configuration, complete the following steps:

1a Open the `krb5` file in a text editor on the server that hosts the identity applications.

Linux: `/etc/krb5.conf`

Windows: `C:\Windows\krb5.ini`

Unix: `/etc/krb5/krb5.conf`

1b Add the following information to the `krb5` file:

```
[libdefaults]
    default_realm = WINDOWS-DOMAIN
    kdc_timesync = 0
    forwardable = true
    proxiable = false
[realms]
    WINDOWS-DOMAIN = {
         kdc = FQDN Active Directory Server
         admin_server = FQDN Active  Directory Server
    }
[domain_realm]
    .your.domain = WINDOWS-DOMAIN
    your.domain = WINDOWS-DOMAIN
```

For example:

```
[libdefaults]
    default_realm = MYCOMPANY.COM
    kdc_timesync = 0
    forwardable = true
    proxiable = false
[realms]
    MYCOMPANY.COM = {
         kdc = myadserver.mycompany.com
         admin_server = myadserver.mycompany.com
    }
[domain_realm]
    .mycompany.com = MYCOMPANY.COM
    mycompany.com = MYCOMPANY.COM
```

1c Save the changes and close the `krb5` file.

2 (Conditional) To define the Kerberos configuration information for Tomcat, complete the following steps:

2a Create a sample `Kerberos_login.config` file on the Tomcat application server with the following content:

NOTE: The novlua user needs permissions to create the `Kerberos_login.config` file.

```
com.sun.security.jgss.krb5.accept {
    com.sun.security.auth.module.Krb5LoginModule required
    debug="true"
    refreshKrb5Config="true"
    useTicketCache="true"
    ticketCache="/opt/netiq/idm/apps/tomcat/kerberos/spnegoTicket.cache"
    doNotPrompt="true"
    principal="HTTP/DNS_Identity_Applications_server@WINDOWS-DOMAIN"
    useKeyTab="true"
        keyTab="/absolute_path/filename.keytab"
    storeKey="true";
    };
```

An example on a Windows server is as follows:

```
keyTab="c:\\NetIQ\\IdentityManager\\apps\\tomcat\kerberos\\rbpm.keytab"
```

2b In the file, specify values for `principal` and `keyTab`. For example:

```
principal="HTTP/rbpm.mycompany.com@MYCOMPANY.COM"
keyTab="/home/usr/rbpm.keytab"
```

- The value for `principal` must match the same value that you specified for Kerberos. For more information, see Step 3 on page 429.
- Provide the absolute path of the `keytab` file on your identity applications server. The file does not have to reside in the default directory for the identity applications.

2c Refer to the `Kerberos_login.config` file in JVM `java.security` file with the following line:

```
login.config.url.1=file:/opt/netiq/idm/apps/tomcat/kerberos/
Kerberos_login.config
```

The path listed is the default installation location for a Linux server.

An example of the `java.security` file on a Windows server is as follows:

```
login.config.url.1=file:c:/NetIQ/IdentityManager/apps/tomcat/kerberos/
Kerberos_login.config
```

3 To specify the Authentication method in the RBPM Configuration utility, complete the following steps:

   3a Open the `Configupdate` utility.

   3b Click the **Authentication** tab.

   3c Scroll down to the **Authentication Method** section.

   3d In the **Method** field, select **Kerberos**.

   3e In the **Mapping attribute name** field, specify `cn`.

NOTE: For more information about the RBPM Configuration utility, see Chapter 40, "Configuring the Settings for the Identity Applications," on page 339.

4 (Optional) Repeat these steps for Identity Reporting if you installed the reporting component on a separate server.

5 Configure the browsers that end-users use to access the identity applications. For more information, see "Configure the End-User Browsers to Use Integrated Windows Authentication" on page 432.

Configure the End-User Browsers to Use Integrated Windows Authentication

The browsers that your end-users use to access the identity applications and identity reporting also need to be configured for Integrated Windows Authentication. This section provides instructions for configuring an end-user computer to support single sign-on access using Integrated Windows Authentication.

NOTE: You must perform this procedure for each end-user computer where you want to provide single sign-on access to the identity applications and identity reporting.

1 Log in to the computer where users will need single sign-on access.

2 Open the Internet options control panel.

3 Click **Security**.

4 Click **Trusted Sites** > **Sites**.

5 Add the DNS name of the identity applications server.

   For example: `rbpm.mycompany.com`

6 Click **Add**, then click **Close**.

7 Click **Custom level...**.

8 Under **User Authentication**, select **Automatic logon with current user name and password**.

9 Click **OK**.

10 In Internet Options, click **Advanced**.

11 Under Security, select **Enable Integrated Windows Authentication**.

12 Repeat this procedure for each end-user computer where you want to provide single sign-on access to the identity applications and identity reporting.

51 Verifying Single Sign-on Access for the Identity Applications

After you install the identity applications and configure the settings for single sign-on, you should verify that you can log in to the individual applications and switch among them without logging out. By default, the applications use the following suffix in the URL link:

- Catalog Administrator: `/rra`
- Identity Manager Dashboard: `/idmdash`
- User Application: `/IDMProv`
- Identity Reporting: `/IDMRPT`

To customize the suffix, use the RBPM Configuration utility. For more information, see Chapter 40, “Configuring the Settings for the Identity Applications,” on page 339.

To verify single sign-on functionality:

1. In a new browser window on your identity applications server, enter the URL for the Dashboard:

   `https://server:port/idmdash`

   Do not log in to the Dashboard.
2. In your browser, navigate to the User Application:

   `https://server:port/IDM-context`
3. Verify that the User Application displays the same login page as shown in Step 1.
4. Log in to the User Application.
5. In the top right corner, click the **Home** icon and verify that you can access the Dashboard without logging on again.

52 Using SSL for Secure Communication

The identity applications and Identity Reporting use HTML forms for authentication. As a result, the login process might expose user credentials. NetIQ recommends that you enable SSL protocol to protect sensitive information. SSL protocol ensures that communications handled between Identity Manager components are secured.

You should have certificates to configure Tomcat server to communicate using SSL, you can obtain certificates in two ways:

- External trusted Certificate Authority (CA) issued certificate
- Self-signed certificate

Checklist for Ensuring SSL Connections

To ensure secure connections among the identity applications, Identity Reporting, SSPR, and OSP, NetIQ recommends that you perform the steps in the following checklist:

	Checklist Items
❑	1. Use keystore to store the authentication certificates. For more information, see "Creating a Keystore and Certificate Signing Request" on page 435.
❑	2. (Conditional) You can use self signed certificate or external CA issued certificate in your environment. For more information, see "Enabling SSL with a Self-signed Certificate" on page 438. For production environment, it is recommended to use external CA issued certificate.
❑	3. (Conditional) In a production environment, import a signed certificate. For more information, see "Enabling SSL with a External CA Signed Certificate" on page 437.
❑	4. Configure the authentication server, identity applications, and Identity Reporting to support SSL communication. For more information, see "Updating the SSL Settings for the Application Server" on page 444 and "Updating the SSL Settings in the Configuration Utility" on page 445.

Creating a Keystore and Certificate Signing Request

A keystore is a Java file that contains encryption keys and optionally, security certificates. To create a keystore, you can use the Java Keytool utility included in the JRE. You create the `.jks` file, generate a certificate into the keystore. Each certificate is associated with a unique alias. You place the keystore in the `conf` directory for your application server that supports the identity applications and Identity Reporting.

1. In a command prompt, navigate to the `conf` directory for your application server installation where you have deployed the identity applications. For example, `opt/netiq/idm/apps/tomcat/conf`.

   The `tomcat/conf` path is the default for the identity applications installed on Tomcat. The path can vary, depending on how you installed the application and Tomcat.

2. Set the environment path for creating the keystore using the following command:

```
cd /opt/netiq/idm/apps/tomcat/conf
export PATH=/opt/netiq/idm/jre/bin:$PATH
```

3 Create the keystore using the following command:

```
keytool -genkey -alias keystore_name -keyalg RSA -keystore
keystore_name.keystore -validity 3650 -keysize 2048
```

For example:

```
keytool -genkey -alias IDMkey -keyalg RSA -keystore IDMkey.keystore -validity
3650 -keysize 2048
```

4 At the prompt, specify the parameter values according to the following considerations:

- For first and last name, specify the fully qualified name of the server. For example:

  `MyTomcatServer.NetIQ.com`

- Use correct spelling. If you spell any words incorrectly, you will see errors when you generate your signed certificate from the signing authority.

5 (Optional) Create a simple text file to save a copy of the information that you provide for the parameter values.

Saving this information helps ensure that you supply the same information when you apply to the signing authority and when you import your certificate.

6 Copy the keystore file to the `tomcat/conf` directory for each application server instance where you have deployed Identity Manager components and SSPR.

7 To generate the CA certificate request, complete the following steps:

7a In the `conf` directory, create a simple text file named `your_request.csr`. For example, `IDMcertrequest.csr`.

7b Run the following command:

```
keytool -certreq -v -alias keystore_name -file your_request.csr -keypass
keystore_password -keystore your.keystore -storepass your_password
```

For example,

```
keytool -certreq -v -alias IDMkey.keystore -file IDMcertrequest.csr -
keypass IDMkeypass -keystore IDMkey.keystore -storepass IDMpass
```

When you run the command, the Keytool utility populates the .csr file with the appropriate data for requesting a certificate.

8 (Conditional) To obtain a signed certificate, submit the .csr file to a valid Certificate Authority.

9 Copy the certificate in the configuration directory of your application server.

For example, `opt/netiq/idm/apps/tomcat/conf`.

10 Stop Tomcat.

After creating a keystore and generating CA certificate request. Follow the below procedures to Import certificates into the keystore:

- For external CA signed certificate, see “Enabling SSL with a External CA Signed Certificate” on page 437.
- For self-signed certificate, see “Enabling SSL with a Self-signed Certificate” on page 438.

Enabling SSL with a External CA Signed Certificate

For a production environment, use a signed certificate issued by a valid Certificate Authority. This section explains how to import a signed certificate into the default Tomcat application server for the identity applications.

This procedure assumes that you have a signed certificate from a valid Certificate Authority. For more information, see "Creating a Keystore and Certificate Signing Request" on page 435.

To use a signed certificate and SSL:

1. Copy the certificate in the configuration directory of your application server. For example, `opt/netiq/idm/apps/tomcat/conf`.
2. To convert the root certificate to DER format, complete the following steps:
   - **2a** Double-click on your certificate stored in the `conf` directory.
   - **2b** In the Certificate dialog, click **Certificate Path**.
   - **2c** Select the root certificate that you received from the signing authority.
   - **2d** Click **View Certificate**.
   - **2e** Click **Details > copy to file**.
   - **2f** In the Export Certificate Wizard, click **next**.
   - **2g** Select **DER encoded binary for X.509 (.CER)** and then click **next**.
   - **2h** Create a new file to store the newly formatted certificate and store it in the `conf` directory for your application server.

     For example, `opt/netiq/idm/apps/tomcat/conf`.
   - **2i** Click **Finish**.
3. To import the converted certificate, complete the following steps:
   - **3a** In a command prompt, navigate to the `conf` directory for your application server.
   - **3b** Enter the following command:

     ```
     keytool -import -trustcacerts -alias root -keystore your.keystore -file
     yourRootCA.der
     ```

     For example:

     ```
     keytool -import -trustcacerts -alias root -keystore IDMkey.keystore -file
     IDMTESTREE.der
     ```

     NOTE: You must specify **root** as your alias.

     After importing the certificate, the server displays **Certificate was added to keystore**.
   - **3c** Verify that the signed certificate is imported correctly into the `conf` directory using the following command:

     ```
     keytool -list -v -alias root -keystore your.keystore
     ```

     For example:

     ```
     keytool -list -v -alias root -keystore IDMkey.keystore
     ```

     The server lists your certificates.
4. NetIQ recommends you to import the signed certificates to Java cacerts location also. For example:

```
keytool -import -trustcacerts -alias root -keystore /opt/netiq/idm/jre/lib/
security/cacerts -file IDMTESTREE.der
```

5 Update the SSL settings for the application server, see "Updating the SSL Settings for the Application Server" on page 444.

6 Update the SSL settings in the Configuration utility. For more information, see "Updating the SSL Settings in the Configuration Utility" on page 445.

7 Update the SSL settings for Self Service Password Reset. For more information, see "Updating the SSL Settings for Self Service Password Reset" on page 446

8 Restart Tomcat.

Enabling SSL with a Self-signed Certificate

If you want to use a self-signed certificate in your test environment, since this type of certificate is easier to obtain than a signed certificate from a valid authority.

- "Exporting the Certificate Authority" on page 438
- "Generating the Self-signed Certificate" on page 439

Exporting the Certificate Authority

You can use iManager to export the Certificate Authority (CA) from your eDirectory server to generate your self-signed certificate.

1 Log in to iManager with the eDirectory administrator's username and password.

2 Click **Administration > Modify Object**.

3 In the Security container, browse to the CA object called *`TreeName`* `CA.Security`. For example, `IDMTESTTREE CA.Security`.

4 Click **OK**.

5 Click **Certificates > Self-Signed Certificate**.

6 Select the self-signed certificate that you want to use.

Example: **Self Signed Certificate RSA**

6a Check **Self Signed Certificate RSA**.

6b Click **Validate**.

7 Click **Export**.

8 Clear **Export private key**.

9 Click **Export format > DER**.

10 Click **Next**.

11 Click **Save the exported certificate**.

12 Click **Save File**.

iManager saves the file as *`TreeName`* `cert.der`. For example, `IDMTESTREE cert.der`.

13 Click **Close**.

14 Copy the certificate in the configuration directory of your application server (`cert.der`).

For example, `opt/netiq/idm/apps/tomcat/conf`.

15 To import the root certificate, complete the following steps:

15a In a command prompt, navigate to the conf directory for your application server using following command:

```
keytool -import -trustcacerts -alias root -keystore <keystore
file>.keystore -file exported_certificate_filename.der
```

Example:

```
keytool -import -trustcacerts -alias root -keystore IDMkey.keystore -file
cert.der
```

NOTE: You must specify **root** as your alias.

After importing the certificate, the server displays **Certificate was added to keystore**.

15b NetIQ recommends you to import root certificate to Java cacerts location also.

For example:

```
keytool -import -trustcacerts -alias root -keystore /opt/netiq/idm/jre/lib/
security/cacerts -file cert.der
```

15c Verify the signed certificate is imported correctly in the `conf` directory using following command:

```
keytool -list -v -alias root -keystore your.jks
```

For example,

```
keytool -list -v -alias root -keystore IDMkey.jks
```

The server lists the certificates.

Generating the Self-signed Certificate

Before generating the self-signed certificate, ensure that you have a keystore and certificate request file. For more information see, "Creating a Keystore and Certificate Signing Request" on page 435

1 Log in to iManager.

2 Navigate to **Certificate Server > Issue Certificate**.

3 Browse to the `.csr` file created in Step 7 in the "Creating a Keystore and Certificate Signing Request" on page 435.

Example: `IDMcertrequest.csr`

4 Click **Next** twice.

5 For the certificate type, click **Unspecified**.

6 Click **Next** twice.

iManager saves the file as `csr_request_name.der`. Example: `IDMcertrequest.der`

7 Copy the certificate in the configuration directory of your application server (`IDMcertrequest.der`).

For example, `opt/netiq/idm/apps/tomcat/conf`.

8 To import the generated self-signed certificate, complete the following steps:

8a In a command prompt, navigate to the conf directory for your application server using following command:

```
keytool -import -alias keystore_name -keystore <keystore_file> -file
<signed_certificate_filename>.der
```

Example:

```
keytool -import -alias IDMkey -keystore IDMkey.keystore -file
IDMcertrequest.der
```

NOTE: You must specify the keystore name as your alias.

After importing the certificate, the server displays **Certificate was added to keystore**.

8b NetIQ recommends you to import self-signed certificate to Java cacerts location also.

For example:

```
keytool -import -alias IDMkey -keystore /opt/netiq/idm/jre/lib/security/
cacerts -file IDMcertrequest.der
```

8c Verify the signed certificate is imported correctly in the `conf` directory using the following command:

```
keytool -list -v -alias keystore_name -keystore your.jks
```

For example,

```
keytool -list -v -alias IDMkey -keystore IDMkey.jks
```

The server lists the certificates.

9 Update the SSL settings for the Application server. For more information, see "Updating the SSL Settings for the Application Server" on page 444.

10 Update the SSL settings in the Configuration utility. For more information, see "Updating the SSL Settings in the Configuration Utility" on page 445.

11 Update the SSL settings for Self Service Password Reset. For more information, see "Updating the SSL Settings for Self Service Password Reset" on page 446

12 Restart Tomcat.

Enabling SSL Between Sentinel and Identity Manager Components

You can create and export a self-signed server certificate to ensure secure communication between Sentinel and Identity Manager components. Use a signed certificate issued by a valid Certificate Authority.

- "Enabling SSL between Sentinel and Identity Manager Engine/Remote Loader" on page 440
- "Enabling SSL between Sentinel and User Application" on page 442

Enabling SSL between Sentinel and Identity Manager Engine/Remote Loader

1 To create a new certificate, complete the following steps:

1a Log in to iManager.

1b Click **NetIQ 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 `.pfx` format, 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. For example, `certificate.pfx`.

3 Extract the private key from the exported certificate to `dxipkey.pem` file using the following command.

```
openssl pkcs12 -in certificate.pfx -nocerts -out dxipkey.pem –nodes
```

4 Extract the certificate to `dxicert.pem` file.

```
openssl pkcs12 -in certificate.pfx -nokeys -out dxicert.pem
```

5 To export the CA certificate of the eDirectory server created in Step 1 to Base64 format, complete the following steps:

5a In iManager, navigate to **Roles and Tasks** > **NetIQ Certificate Access** > **User Certificates**.

5b Browse and select the created certificate.

5c Click **Export**.

5d Select the **CA Certificate** as **OU=organizationCA.O=TREENAME** from the drop-down menu.

5e Select the **Export Format** as **BASE64** from the drop-down menu.

5f Click **Next** and save the certificate. For example, `cacert.b64`.

6 Import the CA certificate to a keystore using the following command:

```
keytool -import -alias <alias name> -file <b64 file> -keystore <keystore file>
–noprompt
```

For example,

```
keytool -import -alias trustedroot -file cacert.b64 -keystore idmKeystore.ks –
noprompt
```

7 To import the certificate into the trust store of Audit Connector, complete the following steps:

7a Log in to the Sentinel Main interface as an administrator.

7b In the main ESM display, locate the Audit Server.

7c Right-click the **Audit Server**, then click **Edit**.

7d In the Security tab, select **Strict**.

NOTE: By default, it is configured to use **Open** (insecure) mode to allow initial connectivity. However, when you are using it in a production environment, ensure that you set the mode to **Strict**.

7e Click **Import** and navigate to the certificate you created in Step 6. For example, `idmkeystore.ks`.

7f Click **Open** and then click **Save**.

7g Restart Audit Server.

8 Copy the private key and certificates created in Step 3 and Step 4 to the following locations based on your components:

Component	Linux Path	Windows Path
Identity Manager Engine	`/var/opt/novell/eDirectory/data/dib`	`C:\NetIQ\IdentityManager\NDS\DIBFiles`

Remote Loader	`/var/opt/novell/dirxml/rdxml`	Remote Loader Installation Directory:
		`C:\NetIQ\IdentityManager\RemoteLoader`
		OR
		`C:\NetIQ\IdentityManager\RemoteLoader\64bit`
		OR
		`C:\NetIQ\IdentityManager\RemoteLoader\32bit`

.NET Remote Loader		`C:\NetIQ\IdentityManager\RemoteLoader.NET`
FanOut Agent	`/opt/novell/dirxml/fanoutagent`	`C:\NetIQ\IdentityManager\FanoutAgent`

9 Restart Identity Manager services.

Enabling SSL between Sentinel and User Application

1 To create a new certificate, complete the following steps:
   - 1a Log in to iManager.
   - 1b Click **NetIQ Certificate Server** > **Create User Certificate**.
   - 1c Select the appropriate user.
   - 1d Specify a nickname for the user.
   - 1e In **Creation Method**, select **Custom**.
   - 1f Accept the rest of the certificate defaults.
   - 1g Click **Next**.
   - 1h In **Custom Extensions**, Select **New DER Encoded Extensions**.
   - 1i Browse to `/products/RBPM/ext.der` custom extension.
   - 1j (Optional) Specify the e-mail address.
   - 1k Review the certificate parameters and click **Finish**.
2 To export the user certificate, complete the following steps:
   - 2a Click **NetIQ Certificate Access > User Certificates**.
   - 2b Select the user certificate that is imported in Step 1.
   - 2c Select the valid user certificate and click **Export**.
   - 2d Specify a password.
   - 2e Save the user certificate as a PKCS12. For example, `certificate.pfx`.
3 Extract the private key from the exported certificate to `key.pem` file using the following command.

```
openssl pkcs12 -in certificate.pfx -nocerts -out key.pem –nodes
```

4 Extract the certificate to `cert.pem` file.

```
openssl pkcs12 -in certificate.pfx -nokeys -out cert.pem
```

5 Stop User Applications.

6 Add the private key and certificate in `configupdate.sh`.

   6a Open `configupdate.sh`.

   6b Click **Show Advanced Options**.

   6c In the **NetIQ Sentinel Digital Signature Certificate** field, copy the `cert.pem`.

   6d In the **NetIQ Sentinel Digital Signature Private Key** field, navigate to the location where you have extracted the private key (`key.pem`) and import the key.

   6e Save the changes in `configupdate.sh`.

7 Restart User Applications.

8 To export the CA certificate of the eDirectory server created in Step 1 to Base64 format, complete the following steps:

   8a In iManager, navigate to **Roles and Tasks** > **NetIQ Certificate Access** > **User Certificates**.

   8b Select the created certificate.

   8c Click **Export** and clear the Export private key check box.

   8d Select the **Export Format** as **BASE64** from the drop-down menu.

   8e Click **Next** and save the certificate. For example, `cacert.b64`.

9 Import the CA certificate to a keystore using the following command:

```
keytool -import -alias <alias name> -file cacert.b64 -keystore <keystore file>
–noprompt
```

For example,

```
keytool -import -alias trustedroot -file cacert.b64 -keystore idmKeystore.ks –
noprompt
```

10 To import the certificate into the trust store of Audit Connector, complete the following steps:

   10a Log in to the Sentinel Main interface as an administrator.

   10b In the main ESM display, locate the Audit Server.

   10c Right-click the **Audit Server**, then click **Edit**.

   10d In the **Security** tab, select **Strict**.

   > **NOTE:** By default, it is configured to use **Open** (insecure) mode to allow initial connectivity. However, when you are using it in a production environment, ensure that you set the mode to **Strict**.

   10e Click **Import** and navigate to the certificate you created in Step 9. For example, `idmKeystore.ks`.

   10f Click **Open** and then click **Save**.

   10g Restart Audit Server.

11 Restart User Applications.

Updating the SSL Settings for the Application Server

The application server that hosts the identity applications and Identity Reporting needs to be configured to support SSL communication. This section provides instructions for updating a Tomcat application server, which is the default application server.

1 Stop Tomcat, if it is running.

For example, `/etc/init.d/idmapps_tomcat_init stop`.

2 Configure SSL port for the Tomcat server.

For example, connector port for SSL is `8543`. Edit the `server.xml` file which is located in the `/opt/netiq/idm/apps/tomcat/conf` directory.

```
<Connector port="8543" protocol="HTTP/1.1"
maxThreads="150" SSLEnabled="true" scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS"
keystoreFile="path_to_keystore_file"
keystorePass="keystore_password" />
```

where:

keystoreFile

Specifies the path to the `userapp.keystore` file, located by default in the `/netiq/idm/apps/tomcat/conf/userapp.keystore` directory.

keystorePass

Specifies the password for the `userapp.keystore` file.

Also, update the `redirectPort` attribute to `8543` and save `server.xml`.

3 Navigate to the `conf` directory for Tomcat, located by default at `opt/netiq/idm/apps/tomcat/conf`.

4 Ensure that you have a keystore file in the `/conf` directory. For example, `idmapps.keystore`.

If you create the keystore file after performing this procedure, ensure that you use the same file name that you provide in this procedure. For more information, see "Creating a Keystore and Certificate Signing Request" on page 435.

5 In a text editor, open the `server.xml` file in the `conf` directory.

6 Add the following content to the `server.xml` file:

```
<Connector port="port_number" protocol="HTTP/1.1" maxThreads="150"
SSLEnabled="true" scheme="https" secure="true" clientAuth="false"
sslProtocol="TLS" keystoreFile="path_to_file/filename.keystore"
keystorePass="password"/>
```

For example:

```
<Connector port="8543" protocol="HTTP/1.1" maxThreads="150" SSLEnabled="true"
scheme="https" secure="true" clientAuth="false" sslProtocol="TLS"
keystoreFile="/opt/netiq/idm/apps/tomcat/conf/idmapps.keystore"
keystorePass="encrypted_password"/>
```

NetIQ recommends that you specify an encrypted password in keystorePass instead of providing cleartext passwords. For more information about the usage of cleartext and encrypted passwords in SSL communication, see Securing Tomcat.

7 Start Tomcat.

For example, `/ect/init.d/idmapps_tomcat_init start`.

Updating the SSL Settings in the Configuration Utility

When you install the identity applications and Identity Reporting, you should specify *https* for the communication method. For example, *"Protocol" on page 308*. However, after installation, you can use the RBPM Configuration utility to ensure that the applications communicate with SSL. For more information about these parameters, see Chapter 40, "Configuring the Settings for the Identity Applications," on page 339.

1 Stop Tomcat, if it is running.

   For example, `/etc/init.d/idmapps_tomcat_init stop`.

2 Navigate to the RBPM Configuration utility, by default, it is located in the installation directory for the identity applications. For example, `/opt/netiq/idm/apps/UserApplication`.

3 At the command prompt, use one of the following methods to run the configuration utility:

   - **Linux**: `./configupdate.sh`
   - **Windows**: `configupdate.bat`

   NOTE: You might need to wait a few minutes for the utility to start up.

4 (Conditional) if you configure SSL in configupdate.sh, then navigate to Authentication tab and replace all the references mentioned in the SSO Clients tab.

   `https://<IP address>:<SSL Port number>`

   For example,

   `https://192.168.0.1:8543`

5 Click **Authentication**, and then modify the following settings:

   OAuth server TCP port

   Specifies the port for the authentication server.

   For example: `8543`

   OAuth server is using TLS/SSL

   Specifies that you want the authentication server to use TLS/SSL protocol for communication.

   Optional TLS/SSL keystore file

   Specifies the path and filename of the Java JKS keystore file that contains the authentication server trust certificate. This parameter applies when the authentication server uses TLS/SSL protocol, and the trust certificate for the authentication server is not in the JRE trust store (`cacerts`).

   Optional TLS/SSL keystore password

   Specifies the password used to load the keystore file for the TLS/SSL authentication server.

   OAuth keystore file

   Specifies the path to the Java JKS keystore file you want to use for authentication. The keystore file must contain at least one public/private key pair.

   OAuth keystore file password

   Specifies the password used to load the OAuth keystore file.

   Key alias of key for use by OAuth

   Specifies the name of the public/private key pair in the OSP keystore file that you want to use to symmetric key generation.

Key password key for use by OAuth

Specifies the password for the private key used by the authentication server.

6 Click **SSO Clients**.

7 Update all of the URL settings, such as **URL link to landing page** and **OAuth redirect URL**.

These settings specify the absolute URL to which the authentication server directs a browser client when authentication is complete.

Use the following format: `https://DNS_name:sslport/path`. For example, `https://nqserver.testsite:8543/landing/com.netiq.test`.

8 Save the changes in the configuration utility.

9 Start Tomcat.

For example, `/ect/init.d/idmapps_tomcat_init start`.

Updating the SSL Settings for Self Service Password Reset

To modify the SSL settings for SSPR, you must be logged in to the application.

1 In a browser, enter the `https` URL that you specified in the Configuration utility for the Landing page. For example, `https://myserver.host:8543/landing`.

2 Log in using administrator credentials for the identity applications.

The application displays a warning that you need to change the Redirect Whitelist URL.

3 To change the Redirect Whitelist URL, follow the instructions on the page.

4 Navigate to **Settings > OAuth SSO**.

5 For all three URLs, specify the `https` protocol and port.

6 Navigate to **Settings > Application**.

7 For all three URLs, specify the `https` protocol and port.

8 Click **Save**, and then click **OK**.

9 Verify that all URLs for the identity applications now use the `https` protocol.

Troubleshooting Tip

After updating the SSL settings for SSPR, if you are not able to access the SSPR landing page. Follow the below steps to update necessary URLs in the `SSPRConfiguration.xml` file.

1 Navigate to the `SSPRConfiguration.xml` file in the below path:

```
cd/opt/netiq/idm/apps/sspr/sspr_data
```

2 Update all the URLs with appropriate IP address and Port numbers.

```
https://<IP address>:<SSL Port number>
```

Example:

```
https://192.168.0.1:8543
```

53 Post-Installation Tasks

After Identity Manager installs, you should configure the drivers you installed to meet the policies and requirements defined by your business processes. You also need to configure Sentinel Log Management for IGA to gather audit events. Post-installation tasks typically include the following items:

- "Configuring a Connected System" on page 447
- "Creating and Configuring a Driver Set" on page 447
- "Creating a Driver" on page 450
- "Defining Policies" on page 450
- "Managing Driver Activities" on page 450
- "Configuring Sentinel Log Management for IGA" on page 451
- "Activating Identity Manager" on page 453

Configuring a Connected System

Identity Manager enables applications, directories, and databases to share information. For driver-specific configuration instructions, see the Identity Manager Driver Documentation.

Creating and Configuring a Driver Set

A driver set is a container that holds Identity Manager drivers. Only one driver set can be active on a server at a time. You can use the Designer tool to create a driver set.

To support password synchronization to the Identity Vault, Identity Manager requires that driver sets have a password policy. You can use the Default Universal Password Policy package in Identity Manager or create a password policy based on your existing organizational requirement. However, the password policy must include the `DirMXL-PasswordPolicy` object. If the policy object does not exist in the Identity Vault, you can create the object.

- "Creating Driver Set" on page 447
- "Assigning the Default Password Policy to Driver Sets" on page 448
- "Creating the Password Policy Object in the Identity Vault" on page 448
- "Creating a Custom Password Policy" on page 449
- "Creating the Default Notification Collection Object in the Identity Vault" on page 449

Creating Driver Set

Designer for Identity Manager provides many settings to create and configure a driver set. These settings allow you to specify Global Configurations Values, driver set packages, driver set named passwords, log levels, trace levels, and Java Environment Parameters. For more information, see "Configuring Driver Sets" in the *NetIQ Designer for Identity Manager Administration Guide*.

Assigning the Default Password Policy to Driver Sets

You must assign the DirMXL-PasswordPolicy object to each driver set in the Identity Vault. The Identity Manager Default Universal Password Policy package includes this policy object. The default policy installs and assigns a universal password policy to control how the Identity Manager engine automatically generates random passwords for drivers.

Alternatively, to use a custom password policy, you must create the password policy object and the policy. For more information, see "Creating the Password Policy Object in the Identity Vault" on page 448 and "Creating a Custom Password Policy" on page 449.

1. Open your project in Designer.
2. In the Outline pane, expand your project.
3. Expand **Package Catalog > Common** to verify whether the Default Universal Password Policy package exists.
4. (Conditional) If the password policy package is not already listed in Designer, complete the following steps:
   - **4a** Right-click **Package Catalog**.
   - **4b** Select **Import Package**.
   - **4c** Select **Identity Manager Default Universal Password Policy**, and then click **OK**.

     To ensure that the table displays all available packages, you might need to deselect **Show Base Packages Only**.
5. Select each driver set and assign the password policy.

Creating the Password Policy Object in the Identity Vault

If the `DirMXL-PasswordPolicy` object does not exist in the Identity Vault, you can use Designer or the ldapmodify utility to create the object. For more information about how to do this in Designer, see "Configuring Driver Sets" in *NetIQ Designer for Identity Manager Administration Guide*. To use the ldapmodify utility, use the following procedure:

1. In a text editor, create an LDAP Data Interchange Format (LDIF) file with the following attributes:

```
dn: cn=DirXML-PasswordPolicy,cn=Password Policies,cn=Security
changetype: add
nsimPwdRuleEnforcement: FALSE
nspmSpecialAsLastCharacter: TRUE
nspmSpecialAsFirstCharacter: TRUE
nspmSpecialCharactersAllowed: TRUE
nspmNumericAsLastCharacter: TRUE
nspmNumericAsFirstCharacter: TRUE
nspmNumericCharactersAllowed: TRUE
nspmMaximumLength: 64
nspmConfigurationOptions: 596
passwordUniqueRequired: FALSE
passwordMinimumLength: 1
passwordAllowChange: TRUE
objectClass: nspmPasswordPolicy

dn: cn=DirXML-PasswordPolicy,cn=Password Policies,cn=Security
changetype: modify
add: nsimAssignments
nsimAssignments: <driverset LDAP dn>
```

NOTE: Copying the content as is might insert some hidden special characters in the file. If you receive a `ldif_record() = 17` error message when you add these attributes to the Identity Vault, insert an extra space between the two DNs.

2 To add the DirMXL-PasswordPolicy object in the Identity Vault, import the attributes from the file by performing one of the following actions:

Linux:

From the directory containing the ldapmodify utility, enter the following command:

```
ldapmodify -x -c -h hostname_or_IP_address -p 389 -D
"cn=admin,ou=sa,o=system" -w password -f path_to_ldif_file
```

For example:

```
ldapmodify -x -ZZ -c -h server1.test.com -p 389 -D
"cn=admin,ou=sa,o=system" -w test123 -f /root/dirxmlpasswordpolicy.ldif
```

The ldapmodify utility is located by default in the `/etc/opt/novell/eDirectory/conf` directory.

Windows:

Run `ldapmodify.exe` from the `install/utilities` directory of the Identity Manager installation kit.

Creating a Custom Password Policy

Rather than using the default password policy in Identity Manager, you can create a new policy based on your organizational requirements. You can assign a password policy to the entire tree structure, a partition root container, a container, or a specific user. To simplify management, NetIQ recommends that you assign password policies as high in the tree as possible. For more information, see Creating Password Policies in the *Password Management 3.3.2 Administration Guide*.

NOTE: You must also assign the DirXML-PasswordPolicy object to the driver sets. For more information, see "Creating the Password Policy Object in the Identity Vault" on page 448.

Creating the Default Notification Collection Object in the Identity Vault

The Default Notification Collection is an Identity Vault object that contains a set of e-mail notification templates and an SMTP server that is used when sending e-mails generated from the templates. If the Default Notification Collection object does not exist in the Identity Vault, use Designer to create the object.

1 Open your project in Designer.
2 In the Outline pane, expand your project.
3 Right-click the Identity Vault, then click Identity Vault **Properties**.
4 Click **Packages**, then click the **Add Packages** icon.
5 Select all the notification templates packages, and then click **OK**.
6 Click **Apply** to install the packages with the **Install** operation.
7 Deploy the notification templates to the Identity Vault.

Creating a Driver

To create drivers, use the package management feature provided in Designer. For each Identity Manager driver you plan to use, create a driver object and import a driver configuration. The driver object contains configuration parameters and policies for that driver. As part of creating a driver object, install the driver packages and then modify the driver configuration to suit your environment.

The driver packages contain a default set of policies. These policies are intended to give you a good start as you implement your data sharing model. Most of the time, you will set up a driver using the shipping default configuration, and then modify the driver configuration according to the requirements of your environment. After you create and configure the driver, deploy it to the Identity Vault and start it. In general, the driver creation process involves the following actions:

1. Importing the Driver Packages
2. Installing the Driver Packages
3. Configuring the Driver Object
4. Deploying the Driver Object
5. Starting the Driver Object

For additional and driver-specific information, refer to the relevant driver implementation guide from the Identity Manager Drivers Web site.

Defining Policies

Policies enable you to customize the flow of information into and out of the Identity Vault, for a particular environment. For example, one company might use the inetorgperson as the main user class, and another company might use User. To handle this, a policy is created that tells the Identity Manager engine what a user is called in each system. Whenever operations affecting users are passed between connected systems, Identity Manager applies the policy that makes this change.

Policies also create new objects, update attribute values, make schema transformations, define matching criteria, maintain Identity Manager associations, and many other things.

NetIQ recommends that you use Designer to define policies for drivers to meet your business needs. For a detailed guide to Policies, see *NetIQ Identity Manager - Using Designer to Create Policies* guide and *NetIQ Identity Manager Understanding Policies Guide*. For information about the document type definitions (DTD) that Identity Manager uses, see Identity Manager DTD Reference. These resources contain:

- A detailed description of each available policy.
- An in-depth Policy Builder user guide and reference, including examples and syntax for each condition, action, noun, and verb.
- A discussion on creating policies using XSLT style sheets.

Managing Driver Activities

To perform administration and configuration functions of Identity Manager drivers, use Designer or iManager. These functions are described in detail in *NetIQ Identity Manager Driver Administration Guide*.

Configuring Sentinel Log Management for IGA

You can monitor and manage the connection between Sentinel Log Management for IGA (Sentinel) and the event sources that provide data to Sentinel, such as Identity Reporting and OSP. The Event Source Management (Live View) in Sentinel helps you accomplish this.

- "Checking for Sentinel Events" on page 451
- "Configuring the Collector Instances in Sentinel" on page 451
- "Configuring Event Data Retention" on page 451
- "Configuring Disk Space Usage for Sentinel" on page 452
- "Configuring Raw Data Retention Policy in Sentinel" on page 452
- "Configuring the Sentinel Link Connection" on page 452

Checking for Sentinel Events

1. Log in to the Sentinel Main interface as an administrator.

   `https://<IP_Address/DNS_Sentinel_server:8443>/sentinel/views/main.html`

2. In the toolbar, click **Applications** > **Launch Control Center**.

   or

   In the toolbar, click **Collection** > **Advanced** > **Launch Control Center**.

3. Log in to Sentinel Control Center.
4. In the toolbar, click **Event Source Management** > **Live View**.

Configuring the Collector Instances in Sentinel

In the Event Source Management view, manually configure the following collectors:

NetIQ iManager and NetIQ One SSO Provider (OSP)

See Step 7 of the **Quickstart Collector Configuration** section in the Sentinel Plug-ins website. The process for configuring both collectors are the same.

NetIQ Self Service Password Reset

See the **Manual Event Source Configuration** section in the Sentinel Plug-ins website.

Configuring Event Data Retention

Event Data Retention controls the duration for which Sentinel keeps different types of event data in the system before deletion.

1. Log in to the Sentinel Web interface as a administrator.
2. Click **Storage** > **Events**.
3. In the **Data Retention** section, select **Default Data Retention** and then click **Edit**.
4. Specify the following information to edit the event data retention:

   Policy name: Specifies the name for the data retention.

   Keep at least: Specify the duration for which the events will be persisted in the Sentinel system. The default value is 7 days.

The value must be a valid positive integer and must be greater than or equal to the Keep at least value.

Keep at most: Specify the duration for which the events will be persisted in the Sentinel system. The default value is 21 days.

The value must be a valid positive integer and must be greater than or equal to the **Keep at least** value.

5 Click **Save**.

Configuring Disk Space Usage for Sentinel

1 Log in to the Sentinel Main interface as an administrator.

2 Click **Storage** > **Events**.

3 In the **Disk Space Usage** section, specify the following values in the **Primary storage utilization** field:

- **Start deleting data from primary storage when __% full:** Specify the threshold at which the event data deletion process should start.
- **Stop when __% full:** Specify the threshold below which the disk space cleanup process should stop. The amount of freed disk space should be sufficient to store an additional full days' worth of event data.

Configuring Raw Data Retention Policy in Sentinel

The Raw Data Retention policy determines the duration for which Sentinel keeps the raw data in the system before deletion. The is turned off by default. When you enable the policy, ensure that you set the value for raw data retention as per your requirement. Setting a higher value for raw data retention would consume more disk space.

You can modify the **Keep at most** and **Keep at Least** values, which determine the maximum and minimum number of days to keep the raw data file in the system. All the files exceeding the retention time are removed permanently from the data storage.

1 Log in to the Sentinel Main interface as an administrator.

2 Click **Storage** > **Events**.

3 In the **Data Retention** section, select **Raw Data Retention** and then click **Edit**.

4 **Keep at least:** Specify the duration for which the raw data will be persisted in the Sentinel system.

The value must be a valid positive integer and must be greater than or equal to the **Keep at least** value.

Keep at most: Specify the duration for which the raw data will be persisted in the Sentinel system.

The value must be a valid positive integer and must be greater than or equal to the **Keep at least** value.

Configuring the Sentinel Link Connection

You can forward events from NetIQ Sentinel to Sentinel Log Management for IGA. In a Sentinel Link Solution setup, the Sentinel system that forwards the events is called the sender and the Sentinel system that receives the events is called the receiver. You can simultaneously link multiple Sentinel

systems to a single receiver system. To configure a Sentinel link, you need to configure at least two systems: the sender machine and the receiver machine. For more information on configuring Sentinel Link, see the *Sentinel Link Overview Guide*.

Activating Identity Manager

Some Identity Manager components activate automatically the first time that you log in. Other components require a procedure for activation.

- "Installing a Product Activation Credential" on page 453
- "Reviewing Product Activations for Identity Manager and Drivers" on page 454
- "Activating Identity Manager Drivers" on page 454
- "Activating Specific Identity Manager Components" on page 455

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 in 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, specify the saved location.
10. (Conditional) If you copied the contents of the Product Activation Credential file, paste the contents into the text area.
11. Click **Next**.
12. Click **Finish**.

NOTE: Identity Manager does not show the correct Identity Manager Edition after applying the Bundle Edition activation.

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 in 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.

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
ID Provider	Bidirectional Driver for eDirectory
Managed System Gateway	eDirectory
Role and Resource Service	GroupWise 2014
User Application	LDAP
	Lotus Notes

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 "Installing a Product Activation Credential" on page 453. For more information about the drivers, see the Identity Manager Drivers documentation website.

Activating Specific Identity Manager Components

This section provides information about activating specific components for Identity Manager.

- "Activating Designer and Catalog Administrator" on page 455
- "Activating Analyzer" on page 455
- "Activating Sentinel Log Management for IGA" on page 455

Activating Designer and Catalog Administrator

When you activate the Identity Manager engine or the Identity Manager drivers, you also activate Designer and Catalog Administrator.

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 box.

---

1. Launch Analyzer.
2. In the **Analyzer Activation** window, you can add a new license or access customer center for license.
3. (Conditional) To add a new license:
   - **3a** Click **Add a new license**.
   - **3b** In the **License** window, type the activation code that you downloaded from the NetIQ Customer Care Portal, and then click **OK**.
4. (Conditional) To access customer center for license:
   - **4a** Click **Access Customer Center for license**.
   - **4b** Click **Visit the NetIQ Customer Center** from the **Micro Focus Customer Center** page.
   - **4c** Browse to and select the Analyzer license.
   - **4d** Copy the activation code and then close the Customer Care Portal.
   - **4e** In the **License** window, type the activation code 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.

Activating Sentinel Log Management for IGA

You can add a license key when installing Sentinel. This section provides information about adding the license key after the Sentinel installation.

If you are using an evaluation license key that is installed by default, you must activate Sentinel before the evaluation key expires to avoid any interruption in the Sentinel functionality. For information about how to purchase the license, see the Identity Manager Product Web site.

You can add a license key either by using the Sentinel Main interface or through the command line.

- "Adding a License Key By Using the Sentinel Main Interface" on page 456
- "Adding a License Key through the Command Line" on page 456

Adding a License Key By Using the Sentinel Main Interface

1. Log in to the Sentinel Main interface as an administrator.
2. Click **About > Licenses**.
3. In the Licenses section, click **Add License**.
4. Specify the license key in the **Key** field.

   After you specify the license, the following information is displayed in the Preview section:

   - **Features:** The features that are available with the license.
   - **Hostname:** This field is for internal NetIQ use only.
   - **Serial:** This field is for internal NetIQ use only.
   - **EPS:** Event rate built into the license key. Beyond this rate, Sentinel generates warnings but will continue to collect data.
   - **Expires:** Expiry date of the license. You must specify a valid license key before the expiry date to prevent an interruption in functionality.
5. Click **Save**.

Adding a License Key through the Command Line

If you are using the Sentinel traditional installation, you can add the license through the command line by using the `softwarekey.sh` script.

1. Log in to the Sentinel server as root.
2. Change to the `/opt/novell/sentinel/bin` directory.
3. Enter the following command to change to the novell user:

   ```
   su novell
   ```
4. Specify the following command to run the `softwarekey.sh` script.

   ```
   ./softwarekey.sh
   ```
5. Enter **1** to insert the license key.
6. Specify the license key, then press **Enter**.

XVI Upgrading Identity Manager

This section provides information for upgrading Identity Manager components. To migrate existing data to a new server, see Part XVII, “Migrating Identity Manager Data to a New Installation,” on page 513. For more information about the difference between upgrade and migration, see “Understanding Upgrade and Migration” on page 461.

54 Preparing to Upgrade 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.

- "Checklist for Upgrading Identity Manager" on page 459
- "Understanding Upgrade and Migration" on page 461
- "Upgrade Order" on page 463
- "Supported Upgrade Paths" on page 463
- "Backing Up the Current Configuration" on page 465

Checklist for Upgrading Identity Manager

To perform the upgrade, NetIQ recommends that you complete the steps in the following checklist.

	Checklist Items
❑	1. Review the differences between an upgrade and a migration. For more information, see "Understanding Upgrade and Migration" on page 461.
❑	2. Upgrade to Identity Manager 4.5. You cannot upgrade or migrate to version 4.6 from versions before 4.5. For more information, see the NetIQ Identity Manager 4.5 Setup Guide.
❑	3. Ensure that you have the latest installation kit to upgrade Identity Manager.
❑	4. Learn about the interaction among Identity Manager components. For more information, see Part I, "Introduction," on page 21.
❑	5. Ensure that your computers meet the hardware and software prerequisites for a newer version of Identity Manager. For more information, see Chapter 6, "Considerations and Prerequisites for Installation," on page 53 and the Release Notes for the version to which you want to upgrade.
❑	6. Back up the current project, driver configuration, and databases. For more information, see "Backing Up the Current Configuration" on page 465.
❑	7. Upgrade Designer to the latest version. For more information, see "Upgrading Designer" on page 469.
❑	8. 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 205 ◆ **Upgrade**: "Upgrading iManager" on page 470

	Checklist Items
❑	9. On the server running Identity Manager, upgrade eDirectory to the latest version and patch. If you are upgrading eDirectory 9.0 or later in an environment where a 64-bit Remote Loader is already upgraded, the eDirectory installation fails and the Remote Loader stops working. To ensure that the Remote Loader works properly, perform the following steps before upgrading eDirectory: 1. Stop the Remote Loader and its instances. 2. Uninstall `novell-DXMLopensslx` RPM. 3. Install eDirectory 9.0 or later version. Upgrading eDirectory stops ndsd, which in turn stops all drivers. For more information, see the *NetIQ eDirectory Installation Guide* and NetIQ Identity Manager 4.6 Release Notes.
❑	10. Update the iManager plug-ins to match the version of iManager. For more information, see "Updating iManager Plug-ins after an Upgrade or Re-installation" on page 475.
❑	11. Stop the drivers that are associated with the server where you installed the Identity Manager engine (Metadirectory). For more information, see "Stopping the Drivers" on page 139.
❑	12. Upgrade the Identity Manager engine. For more information, see "Upgrading the Identity Manager Engine" on page 476. **NOTE:** If you are migrating the Identity Manager engine to a new server, you can use the same the eDirectory replicas that are on the current Identity Manager server. For more information, see "Migrating the Identity Manager Engine to a New Server" on page 520.
❑	13. (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 "Upgrading the Remote Loader" on page 475.
❑	14. (Conditional) If you are using packages, upgrade the packages on the existing drivers to get new policies. For more information, see "Upgrading the Identity Manager Drivers" on page 499. 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.
❑	15. Perform a migration from EAS to Sentinel Log Management for IGA (SLM for IGA). For more information, see "Migrating from Event Auditing Service to Sentinel Log Management for IGA" on page 489.
❑	16. Upgrade or install Tomcat and PostgreSQL. For more information, see Part IX, "Installing PostgreSQL and Tomcat for Identity Manager," on page 241.
❑	17. (Conditional) If OSP is not installed, install OSP. For more information, see Part X, "Installing the Single Sign-on Component," on page 251.
❑	18. (Conditional) If SSPR is not installed, install SSPR. For more information, see Part XI, "Installing the Password Management Component," on page 263. **NOTE:** Install SSPR if you are currently using the legacy provider for password management. For more information, see "Understanding the Legacy Password Management Provider" on page 36.
❑	19. Upgrade the User Application, Identity Manager Dashboard, OSP, SSPR, and Catalog Administrator using upgrade program. For more information, see "Upgrading Identity Applications and Supporting Components" on page 477. Alternatively, you can upgrade these components manually. For more information, see Part XVII, "Migrating Identity Manager Data to a New Installation," on page 513.

	Checklist Items
❑	20. Upgrade Identity Reporting and associated drivers. For more information, see "Upgrading Identity Reporting" on page 489.
❑	21. Start the drivers associated with the Identity Applications and the Identity Manager engine. For more information, see "Starting the Drivers" on page 140.
❑	22. (Conditional) If you migrated the Identity Manager engine or the identity applications to a new server, add the new server to the driver set. For more information, see "Adding New Servers to the Driver Set" on page 501.
❑	23. (Conditional) If you have custom policies and rules, restore your customized settings. For more information, see "Restoring Custom Policies and Rules to the Driver" on page 502.
❑	24. Activate your upgraded Identity Manager solution. For more information, see "Activating Identity Manager" on page 453.

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.

During the product evaluation period or after activating Advanced Edition, you might want to **switch** to Standard Edition if you do not want Advanced Edition functionality in your environment. Identity Manager allows you to switch from Advanced Edition to Standard Edition by following a simple procedure.

Upgrade

In general, you can upgrade Identity Manager 4.5 Standard and Advanced Editions.

- **Identity Manager 4.5 Standard Edition:** If you currently have Identity Manager 4.5 Standard Edition, you can directly upgrade it to Identity Manager 4.6 Standard Edition. For more information, see Quick Start Guide for Installing and *Upgrading NetIQ Identity Manager 4.6 Standard Edition*.

  To upgrade Identity Manager 4.5 Standard Edition to Identity Manager 4.6 Advanced Edition, choose one of the following approaches to complete the upgrade:

  - Upgrade Identity Manager 4.5 Standard Edition to Identity Manager 4.6 Standard Edition and then upgrade to Identity Manager 4.6 Advanced Edition. For more information, see *Upgrading NetIQ Identity Manager 4.6 Standard Edition*.
  - Upgrade Identity Manager 4.5 Standard Edition to Identity Manager 4.5 Advanced Edition and then upgrade to Identity Manager 4.6 Advanced Edition. For more information, see *Upgrading NetIQ Identity Manager 4.6 Standard Edition*.

- **Identity Manager 4.5 Advanced Edition:** If you currently have Identity Manager 4.5 Advanced Edition, you can directly upgrade it to Identity Manager 4.6 Advanced Edition. For more information, see "Checklist for Upgrading Identity Manager" on page 459.

Migration

In some cases you cannot perform an upgrade. Instead, you must perform a **migration**. For example:

- **Unsupported OS:** If you previously installed Identity Manager on a server running an operating system that is no longer supported, you must perform a migration instead of an upgrade.

  The following table provides information on the operating systems that support in-place upgrade or migration.

Operating System	Action Required
SLES 11 SP4	In-Place Upgrade
SLES 12 SP1	In-Place Upgrade
RHEL 6.5	Migration
RHEL 7.2	In-Place Upgrade
Windows 2012 R2	In-Place Upgrade
Windows 2012	In-Place Upgrade
Windows 2008	Migration

- **Identity Manager 4.0.2:** If you currently have Identity Manager 4.0.2 with or without RBPM, you cannot perform a direct upgrade. You must complete the following actions:
  - Upgrade to Identity Manager 4.5 Advanced Edition
  - Upgrade to Identity Manager 4.6 Advanced Edition
  - Migrate your roles-based data (identity applications). For more information, see Upgrading the Identity Applications.

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 4.6 engine can run Identity Manager 4.5 drivers without problems. However, you must upgrade the Roles and Resources driver immediately after upgrading the Identity Manager engine.

IMPORTANT: If you enable features for drivers that are supported only on Identity Manager 4.6 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 4.6 or later.

Switch From Advanced Edition to Standard Edition

Identity Manager allows you to switch from Advanced Edition to Standard Edition during the product evaluation period or after activating Advanced Edition.

IMPORTANT: If you have already applied Advanced Edition activation, you need not move to Standard Edition as all Standard Edition functionality is available in Advanced Edition. You must switch to Standard Edition only if you do not want any Advanced Edition functionality in your environment and want to scale down your Identity Manager deployment. For more information, see “Switching from Advanced Edition to Standard Edition” on page 505.

Upgrade Order

You must upgrade the Identity Manager components in the following sequence:

1. Designer
2. iManager
3. Sentinel Log Management for IGA (you need to perform a migration from EAS to Sentinel Log Management for IGA)
4. Identity Vault
5. Identity Manager Engine/Remote Loader
6. iManager Plug-Ins
7. Tomcat and PostgreSQL Components
8. Single Sign-on (One SSO Provider)
9. Self Service Password Reset
10. Identity Applications (for Advanced Edition)
11. Identity Reporting
12. Analyzer

For information about the latest supported upgrade paths, see the Release Notes for your version from the Identity Manager 4.6 Documentation web site.

Supported Upgrade Paths

Identity Manager 4.6 includes support for NetIQ eDirectory 8.8.8 SP 9 Hotfix 2 and NetIQ eDirectory 9.0.2 Hotfix 2. This allows for different upgrade paths to Identity Manager 4.6. You can directly upgrade from Identity Manager 4.5.4 or later with eDirectory 8.8.8 SP8 or eDirectory 9.0.1 as depicted in the following table:

Base Version	Upgraded Version
Identity Manager 4.5.5 with eDirectory 9.0.2	Identity Manager 4.6 with eDirectory 9.0.2
Identity Manager 4.5.5 with eDirectory 9.0.1	Identity Manager 4.6 with eDirectory 9.0.2
Identity Manager 4.5.5 with eDirectory 8.8.8 SP9	Identity Manager 4.6 with eDirectory 8.8.8 SP9
	Identity Manager 4.6 with eDirectory 9.0.2
Identity Manager 4.5.5 with eDirectory 8.8.8 SP8	Identity Manager 4.6 with eDirectory 8.8.8 SP9
	Identity Manager 4.6 with eDirectory 9.0.2
Identity Manager 4.5.4 or later with eDirectory 9.0.1	Identity Manager 4.6 with eDirectory 9.0.2
Identity Manager 4.5.4 with eDirectory 8.8.8 SP8	Identity Manager 4.6 with eDirectory 8.8.8 SP9
	Identity Manager 4.6 with eDirectory 9.0.2

To upgrade from versions lower than Identity Manager 4.5.4, see Upgrading from Versions Lower Than 4.5.4.

Before starting the upgrade, NetIQ recommends that you review the information from the release notes for your current version:

- NetIQ Identity Manager 4.5 Service Pack 5 Release Notes
- NetIQ Identity Manager 4.5 Service Pack 4 Release Notes

Upgrading from Versions Lower Than 4.5.4

NetIQ does not support a direct upgrade to Identity Manager 4.6 from Identity Manager 4.5, 4.5.1, 4.5.2, or 4.5.3. To upgrade from any of these versions, you must first upgrade to version 4.5.4. For example, if you are running Identity Manager 4.5.3 with eDirectory 8.8.8.x (where x is less than 9), first upgrade to eDirectory 8.8.8.9 or 9.0.1 and Identity Manager to 4.5.4 and then upgrade to Identity Manager 4.6 as depicted in the following table:

Base Version	Intermediate Version	Upgraded Version
Identity Manager 4.5.x (where x is less than SP4) with eDirectory 8.8.8.x (where x is less than SP9)	Identity Manager 4.5.4 with eDirectory 9.0.1	Identity Manager 4.6 with eDirectory 9.0.2
	Identity Manager 4.5.4 with eDirectory 8.8.8 SP8	Identity Manager 4.6 with eDirectory 8.8.8 SP9

Before starting the upgrade, NetIQ recommends that you review the information from the release notes for your current version:

- NetIQ Identity Manager 4.5 Service Pack 4 Release Notes
- NetIQ Identity Manager 4.5 Service Pack 3 Release Notes
- NetIQ Identity Manager 4.5 Service Pack 2 Release Notes
- NetIQ Identity Manager 4.5 Service Pack 1 Release Notes
- NetIQ Identity Manager 4.5 Release Notes

Upgrading from Identity Manager 4.0.2

You cannot perform a direct upgrade or migration to version 4.6 from versions before 4.5. This upgrade/migration involves two steps: upgrade to Identity Manager 4.5 and then upgrade to 4.6 version. For more information, see *NetIQ Identity Manager 4.5 Setup Guide*.

Before starting the upgrade, NetIQ recommends that you review the information from one of the following release notes:

- NetIQ Identity Manager 4.5 Advanced Edition Release Notes
- NetIQ Identity Manager 4.5 Standard Edition Release Notes

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 to back up the User Application. All User Application configuration is stored in the User Application driver. You can create the backup in the following ways:

- "Exporting the Designer Project" on page 465
- "Exporting the Configuration of the Drivers" on page 466

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 465
- "Creating a New Project from the Identity Vault" on page 465

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 *NetIQ Designer for Identity Manager 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 *NetIQ Designer for Identity Manager 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.
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 following values for connecting to the Identity Vault:

- **Host Name**, which represents the IP address or DNS name of the Identity Vault server
- **User name**, which represents the DN of the user used to authenticate to the Identity Vault
- **Password**, which represents 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.

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 466
- "Using iManager to Create an Export of the Driver" on page 466

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 *NetIQ Designer for Identity Manager Administration Guide*.

2 In the Modeler, right-click the line of the driver that 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.

55 Upgrading Identity Manager Components

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 upgrading iManager. This section also provides steps that you might need to take after performing an upgrade.

- "Upgrading Designer" on page 469
- "Upgrading iManager" on page 470
- "Upgrading the Remote Loader" on page 475
- "Upgrading the Identity Manager Engine" on page 476
- "Upgrading Identity Applications and Supporting Components" on page 477
- "Upgrading Identity Reporting" on page 489
- "Upgrading Analyzer" on page 499
- "Upgrading the Identity Manager Drivers" on page 499
- "Adding New Servers to the Driver Set" on page 501
- "Restoring Custom Policies and Rules to the Driver" on page 502

Upgrading Designer

1. Log in 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 *NetIQ Designer for Identity Manager Administration Guide*.
3. Launch the Designer installation program from Identity Manager media:
   - **Linux:** `products/Designer/install`

     To execute the binary file, enter `./install`.
   - **Windows:** `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 Release Notes, 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 *NetIQ Designer for Identity Manager Administration Guide*.

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 have previously modified them.

If you are on eDirectory 8.8.8 Patch 9, upgrade your iManager version to 2.7.7 Patch 9. If you are on eDirectory 9.0.2, upgrade your iManager version to 3.0.2 Patch1. iManager 3.0.2 Patch 1 installation files are located in the `<iso_extracted_directory>/products/iManager/installs/linux` directory and iManager 2.7.7 Patch 9 installation files are located in the `<iso_extracted_directory>/products/iManager277/installs/linux` directory.

The upgrade process includes the following activities:

- "Upgrading iManager on Linux" on page 470
- "Upgrading iManager on Windows" on page 472
- "Upgrading iManager Silently" on page 473
- "Updating Role-Based Services" on page 473
- "Re-installing or Migrating Plug-ins for Plug-in Studio" on page 474
- "Updating iManager Plug-ins after an Upgrade or Re-installation" on page 475

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.
- For iManager, see "Considerations for Installing iManager on a Linux Platform" on page 210.
- For iManager Workstation, see "Considerations for Installing iManager Workstation on Linux Clients" on page 212.

NOTE: The upgrade process uses the HTTP port and SSL port values that were configured in the previous version of iManager.

To upgrade iManager Server on Linux:

1. Log in 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 NetIQ Downloads website, 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_version_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 "Configuring iManager for IPv6 Addresses after Installation" on page 231.
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 in. For more information, see "Accessing iManager" in the *NetIQ iManager 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.

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.
- For iManager, see "Considerations for Installing iManager on a Linux Platform" on page 210.
- For iManager Workstation, see "Considerations for Installing iManager Workstation on Linux Clients" on page 212.

NOTE: The upgrade process uses the HTTP port and SSL port values that were configured in the previous version of iManager.

To install iManager Server on Windows:

1. Log in 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 NetIQ Downloads website, 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 "Configuring iManager for IPv6 Addresses after Installation" on page 231.
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 in. For more information, see "Accessing iManager" in the *NetIQ iManager 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.

Upgrading iManager Silently

To perform a standard silent install on a Linux or Windows server, use the default installation values.

1. At the NetIQ Downloads website, 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**: `./iManagerInstall`*`platform`*`.bin -i silent`
   - **Windows**: `iManagerInstall.exe -i silent`

Updating Role-Based Services

The first time that you use iManager to log in 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 "Understanding Installation for iManager Plug-ins" on page 209.
- 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 in 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.

Re-installing or Migrating Plug-ins for Plug-in Studio

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 in 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.

Updating iManager Plug-ins after an Upgrade or Re-installation

When you upgrade or re-install your iManager, the installation process does not update the existing plug-ins. Ensure that the plug-ins match the correct iManager version. For more information, see "Understanding Installation for iManager Plug-ins" on page 209.

1. Open iManager.
2. Navigate to **Configure > Plug-in Installation > Available Novell Plug-in Modules**.
3. Update the plug-ins.

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:\...\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 "Stopping the Drivers" on page 139.
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. (Conditional) Stop the lcache process using Windows Task Manager.
5. (Conditional) To run a silent installation on a Windows server, ensure that the `silent.properties` file includes the path to the directory that contains the installed Remote Loader files. For example:

   ```
   X64_CONNECTED_SYSTEM_LOCATION=c:\novell\remoteloader\64bit
   ```

   The installation program does not detect the default path for the previous installation.
6. Run the installation program for the Remote Loader.

   The installation process updates the files and binaries to the current version. For more information, see Part V, "Installing the Identity Manager Engine, Drivers, and Plug-ins," on page 131.
7. After the installation finishes, verify that your configuration files contain your environment's information.
8. (Conditional) If there is a problem with the configuration file, copy the backup file that you created in Step 1. Otherwise, continue with Step 9 on page 475.
9. 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**.

Upgrading the Identity Manager Engine

After you upgrade the Remote Loader and the Roles Based Services, you can upgrade the Identity Manager Engine. The upgrade process updates the driver shim files that are stored in the file system on the host computer. The upgrade program does not detect the updated versions of Identity Manager Engine or Remote Loader on your system. It allows you to reinstall these components.

NOTE: When you upgrade Identity Manager engine or separately update a SAML method, iMonitor displays both present and not present status flags for SAML methods. You can ignore the not present status flag because eDirectory correctly uses the updated method. When the engine is upgraded, the upgrade process restarts eDirectory that internally takes care of using the updated SAML method. If you separately update a SAML method, manually restart the eDirectory server to use the updated SAML method.

Performing a Guided Upgrade

1. Verify that the drivers are stopped. For more information, see "Stopping the Drivers" on page 139.
2. Launch the installation program for Identity Manager engine:
   - **Linux:** `IDM`*`version`*`_Lin/products/IDM/install.bin`
   - **Windows:** `IDM`*`version`*`_Win:\products\IDM\Windows\setup\idm_install.exe`
3. Select the language that you want to use for the installation.
4. Read and accept the license agreement.
5. To update the Identity Manager engine and driver shim files, select the following options:
   - **Identity Manager Server**
   - **iManager Plug-ins for Identity Manager**
   - **Drivers**
6. Specify a user and the user password with administrative rights to eDirectory in LDAP format.
7. Review the summary, then click **Install**.
8. Read the installation summary, then click **Done**.

Performing a Silent Upgrade

To run a silent upgrade of the Identity Manager components, you must create a properties file with the parameters necessary to complete the upgrade. The installation kit provides a sample `silent.properties` file in the `IDM`*`version`*`\products\IDM\`*`platform`*`\setup` directory.

To perform a silent upgrade:

1. Copy the sample `silent.properties` file to the directory where you want to run the upgrade.
2. Edit the `silent.properties` file. For more information, see "Performing a Silent Installation" on page 146.
3. Ensure that the `silent.properties` file includes the following parameters:
   - `EDIR_USER_NAME`
   - `EDIR_USER_PASSWORD`
   - `EDIR_NDS_CONF`

- `EDIR_IP_ADDRESS`
- `EDIR_NCP_PORT`
- `METADIRECTORY_SERVER_SELECTED = True`

4 To start the upgrade process, enter one of the following commands from the directory containing the installation and `silent.properties` files:
   - **Linux**: `./install.bin -i silent -f silent.properties`
   - **Windows**: `idm_install.exe -i silent -f silent.properties`

Upgrading Identity Applications and Supporting Components

This section provides information about upgrading Identity Applications and supporting software, which includes updating the following components:

- Identity Manager User Application
- One SSO Provider (OSP)
- Self-Service Password Reset (SSPR)
- Tomcat, JDK, and ActiveMQ

NetIQ provides an upgrade program to upgrade these components. This program is located in the `products/RBPM/` directory in the Identity Manager installation package. Navigate to the directory that contains following upgrade files:

- **Linux**: `RBPM_upgrade.bin`
- **Windows**: `RBPM_upgrade.exe`

You can run the upgrade program only in GUI and in the silent mode. Console mode is not supported.

The upgrade program updates the components to the following versions:

- Tomcat – `8.5.9`
- ActiveMQ – `5.14`
- Java – `1.80_112`
- One SSO Provider – `6.1.3`
- Self-Service Password Reset – `4.1.0.0`

This section provides information about the following topics:

- “Understanding the Upgrade Program” on page 478
- “Prerequisites and Considerations for Upgrade” on page 478
- “Upgrading the PostgreSQL Database” on page 479
- “Changing the Custom Context Name for User Application” on page 483
- “System Requirements” on page 483
- “Using the Guided Process to Upgrade” on page 483
- “Silently Upgrading the Identity Manager Applications” on page 485
- “Post-Upgrade Tasks” on page 486

Understanding the Upgrade Program

The upgrade process reads the configuration values from the existing components. This information includes `ism-configuration.properties`, `server.xml`, `SSPRConfiguration`, and other configuration files. The upgrade process uses these configuration files and internally invokes the upgrade program. The process also creates a backup of the current installation.

Prerequisites and Considerations for Upgrade

Before performing an upgrade, review the following considerations:

- **Identity Manager is upgraded to version 4.5.5:** You cannot upgrade or migrate to version 4.6 from versions lesser than 4.5.5. For more information about how to upgrade to Identity Manager 4.5, see Upgrading Identity Manager in the NetIQ Identity Manager Setup Guide.
- **System Requirements:** The upgrade process requires at least 3 GB free disk space for storing the current configuration and the temporary files that are created during upgrade. Ensure that your server has sufficient space to store the back-up and additional free space available for upgrade.

  On a Linux server, if you have installed the identity applications in a separate partition other than the root partition, ensure that the partition has sufficient space to store the backup configuration. Also, ensure that `/tmp` directory has enough space for storing the logs and temporary files. If this directory does not have the required space, set `IATEMPDIR` environment variable to a directory on a partition that has sufficient free space. This will redirect the upgrade program to store the files in that directory.

  To set `IATEMPDIR` to a directory:

  1. Open a terminal and enter the following command:

     ```
     export IATEMPDIR=/opt/custom_tmp
     ```

     where `/opt/custom_tmp` is the path to the directory that has sufficient free disk space.
  2. Start the upgrade program from the command line.

  On a Windows server, the upgrade program stores the temporary files in a directory specified in the `%TEMP%` environment variable. If this directory does not have the required space, set TEMP and TMP environment variables to a directory on your file system that has sufficient free space. This will redirect the upgrade program to store the files in that directory.

  To set these environment variables to a different directory, complete the following steps before starting the upgrade:

  1. Open the command prompt and enter the following command:

     ```
     SET TMP=D:\custom_tmp
     SET TEMP=D:\custom_tmp
     ```

     where `D:\custom_tmp` is the path to the directory that has sufficient free disk space.
  2. Start the upgrade program from the command line.
- **Tomcat as an application server:** This version of Identity Manager supports only Tomcat as an application server.

  NOTE: Ensure you have installed Tomcat application server using the convenience installer during Identity Manager 4.5 installation. The upgrade process allows you to upgrade only Tomcat that has been installed using the convenience installer.

If you are running your identity applications on an application server other than Tomcat, migrate the application server to Tomcat. For more information, see "Migrating from Websphere or JBoss to Tomcat Web Application Server" on page 522.

- **Database platform is upgraded:** This program does not upgrade the database platform for the identity applications. Manually upgrade your current version of the database to a supported version. For upgrading the PostgreSQL database, see "Upgrading the PostgreSQL Database" on page 479.
- **Roles and Resource Service driver package is upgraded:** For more information, see Upgrading Installed Packages in the *NetIQ Designer for Identity Manager Administration Guide*.
- **User Application context name is set to the default name:** If you have configured User Application's context name other than default `IDMProv`, change the context name. For more information, see "Changing the Custom Context Name for User Application" on page 483.
- **Self Service Password Reset:** If you are upgrading from SSPR 4.0, ensure you have updated `CATALINA_OPTS` property and `-Dsspr.application.Path` is set to the folder where your SSPR configuration is stored.

  For example,

  Linux: `export CATALINA_OPTS="-Dsspr.applicationPath=/home/sspr_data`

  Windows: `set CATALINA_OPTS="-Dsspr.applicationPath=C:\sspr_data`

  Backup your SSPR LocalDB before upgrading. To export or download LocalDB, perform the following steps:

  1. Log in to SSPR portal as an administrator.
  2. In top-right corner of the page, click **Configuration Manager** from the drop-down menu.
  3. Click **LocalDB**.
  4. Click **Download LocalDB**.

Upgrading the PostgreSQL Database

IMPORTANT: The upgrade process may take time depending on the size of the database. Therefore, plan your upgrade accordingly.

---

1 Stop the PostgreSQL service that is running on your server.

2 Rename the `postgres` directory.

Linux: `/opt/netiq/idm/apps`

Windows: `C:\Netiq\IdentityManager\apps`

For example, rename `postgres` to `postgresql_9_3`.

3 Install PostgreSQL version supported on your operating system.

You must choose a location other than the current installation location of PostgreSQL.

3a Mount the `Identity_Applications_`*`version_platform`*`.iso` image file and navigate to the `products/RBPM/postgre_tomcat_install` directory containing the PostgreSQL installation files.

3b Install the PostgreSQL application.

- **Linux (GUI):** Run `./TomcatPostgreSQL.bin`
- **Linux (Console):** Run `./TomcatPostgreSQL.bin -i console`
- **Windows:** Run `TomcatPostgreSQL.exe`

Select only **PostgreSQL** option during installation.

NOTE: Do not provide any database details in **PostgreSQL details** page. Ensure that **Create database login account** and **Create empty database** are deselected.

4 Stop the newly installed PostgreSQL service.

- **Linux (SLES 12 SP1 or later and RHEL 7.x or later):** Run the `systemctl stop postgresql-9.6.service` command.
- **Linux (SLES 11 SP4 or later):** Run the `/etc/init.d/postgresql-9.x stop` command.
- **RHEL 6.x or Later:** Run the `/etc/init.d/postgresql-9.6 stop` command.
- **Windows:** Go to **Services**, search for PostgreSQL 9.6 service, and stop the service.

  NOTE: Appropriate user can perform stop operations after providing valid authentication.

5 Change the permissions for the newly installed PostgreSQL directory.

- **Linux:** Run the following command:

  ```
  chown -R postgres:postgres <postgres directory path>
  ```

  For example,

  ```
  chown -R postgres:postgres /opt/netiq/idm/apps/postgres
  ```

- **Windows:** Perform the following actions:

  To create a `postgres` user:

  1. Go to **Control Panel > User Accounts > User Accounts > Manage Accounts**.
  2. Click **Add a user account**.
  3. In the Add a User page, specify `postgres` as the user name and provide a password for the user.

  To provide permissions to `postgres` user to the existing and newly installed PostgreSQL directories:

  1. Right click the PostgreSQL directory and go to **Properties > Security > Edit**.
  2. Select **Full Control** for the user to provide complete permissions.
  3. Click **Apply**.

6 Access the PostgreSQL directory as `postgres` user.

- **Linux:** Perform the following actions:
  1. Switch to `postgres` user by using the following command:

     ```
     su - postgres
     ```

  2. Change the directory to `postgres/bin` directory.
  3. Export the installed PostgreSQL location using the following command:

     ```
     export PATH=/opt/netiq/idm/apps/postgres/bin:$PATH
     ```

  4. Export the PostgreSQL password using the following command:

     ```
     export PGPASSWORD=<enter the database password>
     ```

- **Windows:** Perform the following actions:
  1. Login to the server as `postgres` user.

     Before logging in, make sure that `postgres` can connect to the Windows server by verifying if a remote connection is allowed for this user.

  2. Open a command prompt and set `PGPASSWORD` by using the following command:

     ```
     set PGPASSWORD=<your pg password>
     ```

3. Change to the newly installed PostgreSQL directory.

   For example: `C:\Users\postgres>cd C:\NetIQ\IdentityManager\apps1\postgresql962\bin`.

7 Upgrade PostgreSQL from new PostgreSQL `bin` directory.

- **Linux:** Run the following command.

  ```
  pg_upgrade --old-datadir <old_postgres_location\data> --new-datadir
  <new_postgres_location\data> --old-bindir <old_postgres_location\bin> --
  new-bindir <new_postgres_location\bin>
  ```

  For example, `./pg_upgrade --old-datadir /opt/netiq/idm/apps/postgresql_9_3/data/ --new-datadir /opt/netiq/idm/apps/postgres/data/ --old-bindir /opt/netiq/idm/apps/postgresql_9_3/bin --new-bindir /opt/netiq/idm/apps/postgres/bin/`

  After a successful upgrade, it displays the message to run `analyze_new_cluster.sh` and `delete_old_cluster.sh`.

- **Windows:** Run the following command and click **Enter**:

  ```
  pg_upgrade.exe --old-datadir
  "C:\NetIQ\IdentityManager\apps1\postgres\data" --new-datadir
  "C:\NetIQ\IdentityManager\apps1\postgresql962\data" --old-bindir
  "C:\NetIQ\IdentityManager\apps1\postgres\bin" --new-bindir
  "C:\NetIQ\IdentityManager\apps1\postgresql962\bin"
  ```

  If the upgrade is successful on Linux, you will see messages similar to the below in the command prompt.

  ```
  Performing Consistency Checks
  -----------------------------
  Checking cluster versions                                   ok
  Checking database user is the install user                  ok
  Checking database connection settings                       ok
  Checking for prepared transactions                          ok
  Checking for reg* system OID user data types                ok
  Checking for contrib/isn with bigint-passing mismatch       ok
  Creating dump of global objects                             ok
  Creating dump of database schemas                           ok
  Checking for presence of required libraries                 ok
  Checking database user is the install user                  ok
  Checking for prepared transactions                          ok

  If pg_upgrade fails after this point, you must re-initdb the new cluster
  before continuing.

  Performing Upgrade
  ------------------
  Analyzing all rows in the new cluster                       ok
  Freezing all rows on the new cluster                        ok
  Deleting files from new pg_clog                             ok
  Copying old pg_clog to new server                           ok
  Setting next transaction ID and epoch for new cluster       ok
  Deleting files from new pg_multixact/offsets                ok
  Copying old pg_multixact/offsets to new server              ok
  Deleting files from new pg_multixact/members                ok
  Copying old pg_multixact/members to new server              ok
  Setting next multixact ID and offset for new cluster        ok
  Resetting WAL archives                                      ok
  Setting frozenxid and minmxid counters in new cluster       ok
  Restoring global objects in the new cluster                 ok
  ```

```
Restoring database schemas in the new cluster                 ok
Copying user relation files                                   ok
Setting next OID for new cluster                              ok
Sync data directory to disk                                   ok
Creating script to analyze new cluster                        ok
Creating script to delete old cluster                         ok

Upgrade Complete
----------------
Optimizer statistics are not transferred by pg_upgrade so,
once you start the new server, consider running:
    analyze_new_cluster.sh

Running this script will delete the old cluster's data files:
    delete_old_cluster.sh
```

You should see similar messages for Windows.

If the upgrade fails on Linux and reports `cannot write to log file pg_upgrade_internal.log` error message, run the upgrade command from a directory that is writable by `postgres` user. For example, `/tmp`.

8 Start the upgraded PostgreSQL database service.

- **Linux (SLES 12 SP1 or later or RHEL 7.x or later):** Run the `systemctl start postgresql-9.6.service` command.
- **Linux (SLES 11 SP4 or later):** Run the `/etc/init.d/postgresql-9.x start` command.
- **RHEL 6.x or Later:** Run the `/etc/init.d/postgresql-9.6 start` command.
- **Windows:** Go to **Services**, search for PostgreSQL 9.6 service, and start the service.

NOTE: Appropriate user can perform start operations after providing valid authentication.

9 Disable the old PostgreSQL service to ensure that the service does not automatically start.

10 (Optional) Delete the old data files from the `bin` directory of the newly installed PostgreSQL service.

- **Linux:** Perform the following actions:
  1. Switch to `postgres` user and run `analyze_new_cluster.sh`.

     ```
     su - postgres
     ```

  2. Navigate to `/opt/netiq/idm/apps/postgres/bin` and run the following scripts:
     - `./analyze_new_cluster.sh`
     - `./delete_old_cluster.sh`

     Ensure that scripts are executed without errors.
- **Windows:** Perform the following actions:
  1. Login as `postgres` user.
  2. Navigate to the bin directory and run `analyze_new_cluster.bat` and `delete_old_cluster.bat` files.

     For example: `C:\NetIQ\IdentityManager\apps1\postgresql961\bin`

NOTE: You must run this step only if you want to delete the old data files.

Changing the Custom Context Name for User Application

If you specified User Application's context name other than the default `IDMProv`, complete the following steps to change the context name to the default context name `IDMProv`:

NOTE: You can verify the context name in `portal.context` property of `ism-configuration.properties` file.

---

1. Stop the Tomcat service.

   ```
   /etc/init.d/idmapps_tomcat_init stop
   ```

2. Navigate to `webapps` folder and rename the folder which has non-default context name to `IDMProv`.

   Linux: `/opt/netiq/idm/apps/tomcat/webapps`

   Windows: `C:\Netiq\IdentityManager\apps\tomcat\webapps`

   For example, if the `portal.context` name in the `ism-configuration.properties` file is `IDMDev`, then change the folder name from `IDMDev` to `IDMProv`.

3. Run the Identity Applications upgrade program. See, "Using the Guided Process to Upgrade" on page 483 or "Silently Upgrading the Identity Manager Applications" on page 485.

4. After upgrading identity applications restore the `WAR` files to your original context name. For more information, see "Identity Applications" on page 487.

System Requirements

The upgrade process creates a back-up of the current configuration for the installed components. Ensure that your server has sufficient space to store the back-up and additional free space available for upgrade.

Using the Guided Process to Upgrade

This section describes the guided process for upgrading the identity applications components.

1. Log in as a `root` or administrative user to the server where you want to run upgrade process.
2. Mount the `Identity_Applications.iso` image file, navigate to the directory containing the upgrade executable, located by default in the `products/RBPM/` directory.
3. Launch the upgrade program. Execute one of the following files depending on your platform:
   - **Linux:** `RBPM_upgrade.bin`
   - **Windows:** `RBPM_upgrade.exe`
4. On the **Introduction** page, you can view Identity Manager components that you can upgrade, then click **Next**.
5. Read and accept the license agreement, then click **Next**.
6. Review the **Deployed Applications** page, then click **Next**.

   This page lists the currently installed components. It also lists the version and installation directories of Tomcat and JRE. If other applications are deployed on the server, the upgrade process displays a warning that those applications might not work properly after the upgrade.

   For example, Identity Reporting or user-defined war files. You must restore them manually from the back-up created by the upgrade process.

7 To proceed with the upgrade, click **Next**.

8 Complete the guided process, using the following parameters. This program autopopulates the values for existing components. Ensure that the correct values are specified for the parameters.

- **One SSO Provider**

  Represents the path to a directory where the upgrade program creates the application files for OSP. If the path is not correct, browse to the path where OSP is installed.

- **SSPR**

  Represents the path to a directory where the upgrade program creates the application files for SSPR. If the path is not correct, browse to the path where SSPR is installed.

- **User Application**

  Represents the path to a directory where the upgrade program creates the application files for the User Application. If the path is not correct, browse to the path where User Application is installed.

- **Database Connection**

  Represents the settings for connecting to the User Application database, Identity Applications also connects to this database. The upgrade program includes these details in the User Application configuration file.

  Database Platform

  Represents the platform of the User Application database.

  Database Host

  Specifies the name or IP address of the server that hosts the User Application.

  Database Port

  Specifies the port that the database server uses for communication with the User Application.

  Database Driver JAR

  Specifies jar file for the database platform.

  The database vendor provides the driver JAR file, which represents the jar for the database server. For example, for PostgreSQL, you might specify `postgresql-9.4-1212.jdbc42.jar`, by default in the `/opt/netiq/idm/apps/postgres` folder on Linux and `C:\netiq\idm\apps\postgres` on Windows. Similarly, specify the appropriate jar files for your database platform.

- **Database Credentials**

  Database Name

  Specifies the name of the database. By default, the database name is `idmuserappdb`.

  Database Username

  Specifies the name of an account that allows the User Application to access and modify data in the databases. By default, the database username is `idmadmin`.

  Database Password

  Specifies the password for the specified username.

- **Upgrade Database**

  Upgrade Database Now

  The upgrade program updates the schema for the database tables as part of the upgrade process.

Upgrade Database at Application Startup

The upgrade program leaves instructions to update the schema for the database tables when the User Application starts for the first time after the upgrade.

Write SQL to File

Generates a SQL script that the database administrator can run to update the databases. If you choose this option, you must also specify a name for **Schema File**. The setting is in the **SQL Output** File configuration.You might select this option if you do not have permissions to create or modify a database in your environment. For more information about generating the tables with the file, see "Manually Creating the Database Schema" on page 327.

- **Database Administrator**

  Represents the name and password for the database administrator.

  Database Username

  Specifies the account for a database administrator that can create database tables, views, and other artifacts.

  Password

  Specifies the password for the database administrator.

- **Backup Folder**

  Depending on where you installed the components, the process creates the backup directory in that location and appends a time stamp (indicating the time of backup) to the backed-up directory.

  For example,

  - Tomcat – `/opt/netiq/idm/apps/tomcat_backup_02262017_033634`
  - OSP and SSPR - `/opt/netiq/idm/apps/osp_sspr_backup_02262017_033634`
  - ActiveMQ - `/opt/netiq/idm/apps/activemq_backup_02262017_033634`
  - User Application - `/opt/netiq/idm/apps/UserApplication_backup_02262017_033634`

9 Review the **Pre-Upgrade Summary** page, then click **Install**.

  The upgrade process stops the Tomcat service and starts the upgrade, which might take some time to complete.

10 When the upgrade process completes, review the upgrade log files from `/tmp/rbpm_upgrade/` and you need to update few configurations manually, see "Post-Upgrade Tasks" on page 486.

Silently Upgrading the Identity Manager Applications

A silent (non-interactive) installation does not display a user interface.

1 Login as a root user or administrator where you want to upgrade Identity Manager applications.

2 Open a terminal session.

3 Specify the values for installation in the properties file.

  - **Linux**: `products/RBPM/RBPM_Upgrade_Linux.properties`
  - **Windows**: `products\RBPM\RBPM_Upgrade_Win.properties`

4 To launch the upgrade program for your platform, enter the following command:

  - **Linux**: `RBPM_Upgrade.bin -i silent -f RBPM_Upgrade_Linux.properties`
  - **Windows**: `RBPM_Upgrade.exe -i silent -f RBPM_Upgrade_Win.properties`

NOTE: If the `RBPM_Upgrade_Linux.properties` file is in a different directory from the installer script, you must specify the absolute path to the file. The script unpacks the necessary files to a temporary directory and then launches the silent installation.

Post-Upgrade Tasks

After completing the upgrade, you must restore the customized settings for Tomcat, SSPR, OSP, or Identity Applications, manually.

Perform the post-upgrade steps for the required components:

- "Java" on page 486
- "Tomcat" on page 486
- "Identity Applications" on page 487
- "One SSO Provider" on page 488
- "Self-Service Password Reset" on page 488

Java

Verify the certificates in newly upgrade JRE location: `jre/lib/security/cacerts` with your older JRE location. Manually import the missed certificates into your `cacerts`.

1. Import `java cacerts` using `keytool` command:

   ```
   keytool -import -trustcacerts -file Cerificate_Path -alias ALIAS_NAME -keystore
   cacerts
   ```

   NOTE: After upgrade, JRE is stored in the identity applications install location. For example: `/opt/netiq/idm/apps/jre`

2. Verify JRE home location.

   Linux: `tomcat/bin/setenv.sh`

   Windows: `tomcat/bin/setenv.bat`

3. Launch **Configuration Update** utility and verify the path of your `cacerts`.

Tomcat

1. (Conditional) To restore the customized files from the backup taken earlier by the upgrade process, perform the following tasks:
   - Restore customized https certificates. To restore these certificates, copy the Java Secure Socket Extension (JSSE) contents from the backed up `server.xml` to the new `server.xml` file in the `/tomcat/conf` directory.
   - Do not copy the configuration files from the backed-up Tomcat directory to the new Tomcat directory. Start with the default configuration of the new version and make changes as needed. For more information, see this Apache Website.

     Verify that new `server.xml` file has the following entries:

```
<Connector port="8543" protocol="HTTP/1.1"
       maxThreads="150" SSLEnabled="true" scheme="https" secure="true"
       clientAuth="false" sslProtocol="TLS"
       keystoreFile="path_to_keystore_file"
       keystorePass="keystore_password" />
```

or

```
<Connector port="8543"
protocol="org.apache.coyote.http11.Http11NioProtocol"
       maxThreads="150" SSLEnabled="true" scheme="https" secure="true"
       clientAuth="false" sslProtocol="TLS"
       keystoreFile="path_to_keystore_file"
       keystorePass="keystore_password" />
```

- If you have customized keystore files, include the correct path in the new `server.xml` file.

2 (Conditional) Navigate to the User Application and restore the customized settings manually by reading the backed-up configuration.

Identity Applications

Restore the customized identity applications configurations from the backup taken during the upgrade process.

Manually create the compound indexes for each attribute that you want to use to sort users in Identity Manager Dashboard, see "Creating Compound Indexes" on page 318.

If you have renamed the custom context folder name to `IDMProv` before running the upgrade program, you should change the context folder name to original context name using `configupdate` utility. For example, the original custom context name is `IDMDev` and it is renamed to `IDMProv`.

Complete the following steps to change the context name back to the original context name:

1 Navigate to the User Application directory located in `/opt/netiq/idm/apps/UserApplication`.

2 (Optional) To launch the configupdate utility in GUI mode, ensure that the `use_console` option is set to `false` in `configupdate.sh.properties` or `configupdate.bat.properties` file.

   This step is required because the upgrade utility changes the value of this option to `true`.

   Alternatively, launch the configupdate utility and pass an additional command line argument on Linux.

   ```
   ./configupdate.sh use_console=false
   ```

3 Launch the `configupdate` utility.

   Linux: `configupdate.sh`

   Windows: `configupdate.bat`

4 In **User Application** tab, click **Show Advanced Options** and perform the following steps:

   4a Check **Change RBPM Context Name** check box.

   4b Change the RBPM context name to the original context name.

   4c Browse and select the appropriate **Roles Driver DN** and click **OK**.

   4d Change the permission and ownership of the `WAR` file using the following command.

   ```
   chmod 755 <Original_Context_Name>.war; chown -R novlua:novlua
   <Original_Context_Name>.war
   ```

For example, if the original custom context name is `IDMDev`:

```
chmod 755 IDMDev.war; chown -R novlua:novlua IDMDev.war
```

5 (Conditional) If you have completed all the post-upgrade tasks, then start the Tomcat service for Identity Applications.

One SSO Provider

If OSP and User Applications are deployed on different servers, then update the SSO client parameter using Configuration Update Utility. For more information, see "IDM Dashboard" on page 357 in the "SSO Clients Parameters" on page 354.

By default, the `LogHost` entry located at `/etc/logevent.conf` file is set to `localhost`.

To modify the `LogHost` entry, manually restore the customized OSP configurations from the backup taken during the upgrade process.

Self-Service Password Reset

After upgrading SSPR, update SSO client parameter using Configuration Update Utility. For more information, see "Self Service Password Reset" on page 360 in the "SSO Clients Parameters" on page 354.

To update the SSPR configuration details, perform the following steps:

1 Log in to SSPR portal as an administrator.

2 Update the audit server details:

   2a Navigate to **Configuration Editor**, specify the configuration password.

   2b Select **Settings > Auditing > Audit Forwarding > Syslog Audit Server Certificates**.

   2c Import these certificates from the sever and click **Save**.

3 Import the **LocalDB** into SSPR:

   3a In top-right corner for the page, click **Configuration Manager** from the drop-down menu.

   3b Click **LocalDB**.

   3c Click **Import (Upload) LocalDB Archive File**.

4 Configure administrator permissions for SSPR, see "Post-Installation Tasks" on page 271

NOTE: If you are upgrading from SSPR 4.0 to SSPR 4.1, the customized location of SSPR configurations is changed to the default location of SSPR 4.1. You can find additional information about the configuration locations in the `setenv.sh` file. However, this change does not affect the behavior of the components.

For example, if the pre-upgrade of SSPR configuration is `-Dsspr.applicationPath='/home/sspr-data`, then after the upgrade, the path changes to `-Dsspr.applicationPath=/opt/netiq/idm/apps/osp_sspr/sspr/sspr_data` and restores all the associated configurations in this location.

To verify that the upgrade is successful, launch the upgraded components.

For example, launch Identity Manager Dashboard, click **About**. Check whether the application displays the new version, such as **4.6.0**.

Upgrading Identity Reporting

Identity Reporting includes two drivers. Also, you might need to migrate content from NetIQ Event Auditing Service to Sentinel Log Management for IGA. 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. Migrate to Sentinel Log Management for IGA
4. Upgrade Identity Reporting

Upgrading the Driver Packages for Identity Reporting

This section explains how to update the packages for the Managed System Gateway and Data Collection Service drivers to the latest version. You must perform this task before upgrading Identity Reporting.

1. In Designer, open your current project.
2. Right-click **Package Catalog > Import Package**.
3. Select the appropriate package. For example, **Manage System Gateway Base package 2.0.0.20120509205929**.
4. Click **OK**.
5. In the Developer View, right-click the driver and then click **Properties**.
6. Navigate to the **Packages** tab in the **Properties** page.
7. Click the **Add package (+)** symbol in the top right corner.
8. Select the package, and then click **OK**.
9. Complete the configuration process for the driver. For more information, see the following sections:
   - “Configuring the Managed System Gateway Driver” on page 386
   - “Configuring the Driver for Data Collection Service” on page 387
10. Repeat Step 2 through Step 9 to upgrade the package for the Data Collection Service Driver.
11. Ensure that the Managed System Gateway Driver and Data Collection Service Driver are connected to the upgraded Identity Manager.

Migrating from Event Auditing Service to Sentinel Log Management for IGA

This section provides information about migrating existing data from NetIQ Event Auditing Service (EAS) to Sentinel Log Management for IGA.

- “Preparing for Migration” on page 490
- “Migrating Data to the New PostgreSQL Database” on page 491
- “Setting up the Reporting Server” on page 493
- “Creating the Data Synchronization Policy” on page 494

Preparing for Migration

Before you start the migration, you need to prepare the SLM for IGA and EAS databases. This involves importing the required connector to receive events from SLM for IGA and upgrading all the Identity Manager components to 4.6.

Perform the following actions before migrating your EAS data to SLM for IGA.

1. Import the `NetIQ-Audit_2011.1r4-201701130600-release.cnz` connector into EAS.
2. Upgrade all the existing Identity Manager components from 4.5.4 to 4.6.
3. Ensure that you take a backup of the `logevent.conf` file.

   Linux: `/etc/logevent.conf`

   Windows: `C:\Windows\logevent.cfg`

   The `logevent.conf` file should contain EAS details.
4. Ensure that the following Identity Manager components are running:
   - eDirectory
   - Identity Manager Engine
   - iManager
   - Identity Applications (specifically OSP, SSPR, and RBPM)
5. Update the audit server details for SSPR:

   5a Log in to SSPR portal as an administrator.

   5b Navigate to **Configuration Editor** and specify the configuration password.

   5c Select **Settings > Auditing > Audit Forwarding.**

   5d Provide SLM for IGA details under **Syslog Audit Server**. For example, `tls,<sentinel IP>,1443`.

   5e Click **Clear** to clear the Syslog Audit Server certificates.

   5f Click **Import from server** to import certificates from the updated Syslog Audit Server.

   5g Save your changes.
6. Ensure that your EAS server is running until all the cached audit events from all Identity Manager components are sent to EAS.
7. Stop the following Identity Manager components:
   - eDirectory
   - Identity Manager Engine
   - iManager
   - Identity Applications (specifically OSP, SSPR, and RBPM)
8. Stop the Novell Audit `lcache` and `jcache` processes.

   ```
   kill -15 <PID of lcache>
   kill -15 <PID of jcache>
   ```
9. Follow the steps mentioned in Step 1 to Step 6 of Enabling SSL between Sentinel and User Application to create naudit certificates so that User Application can connect to SLM for IGA.
10. Modify the `LogHost` entry to point to SLM for IGA in the `logevent.conf` file.
11. Start the following Identity Manager components.
    - eDirectory
    - Identity Manager Engine

- iManager
- Identity Applications (specifically OSP, SSPR, and RBPM)

Migrating Data to the New PostgreSQL Database

This section provides information about migrating the SIEM data from the EAS database to a supported PostgreSQL database. For information about installing a PostgreSQL database, see Chapter 28, “Installing PostgreSQL and Tomcat,” on page 247.

You must create the required roles and table spaces to ensure there are no failures during migration.

Preparing the New PostgreSQL Database

1. Stop EAS to ensure that none of the events are sent to the EAS server.
2. Using iManager, stop the DCS driver:
   - **2a** Log in to iManager.
   - **2b** Stop the DCS driver.
   - **2c** Edit the driver properties to change the startup option to **Manual**.

     This step ensures that the driver does not start automatically.
3. Run the following SQL commands to create the required roles, table space, and database using `PGAdmin`.

   This step ensures there are no failures during migration.

   - **3a** Run the following commands to create the required roles:

```
CREATE ROLE esec_app
  NOSUPERUSER INHERIT NOCREATEDB NOCREATEROLE;

CREATE ROLE esec_user
  NOSUPERUSER INHERIT NOCREATEDB NOCREATEROLE;

CREATE ROLE admin LOGIN
  ENCRYPTED PASSWORD '<specify the password for admin>'
  NOSUPERUSER INHERIT NOCREATEDB NOCREATEROLE;
GRANT esec_user TO admin;

CREATE ROLE appuser LOGIN
  ENCRYPTED PASSWORD '<specify the password for appuser>'
  NOSUPERUSER INHERIT NOCREATEDB CREATEROLE;
GRANT esec_app TO appuser;

CREATE ROLE dbauser LOGIN
  ENCRYPTED PASSWORD '<specify the password for dbauser>'
  SUPERUSER INHERIT CREATEDB CREATEROLE;
```

```
CREATE ROLE idmrptsrv LOGIN
  ENCRYPTED PASSWORD '<specify the password for idmrptsrv>'
  NOSUPERUSER INHERIT NOCREATEDB NOCREATEROLE;
GRANT esec_user TO idmrptsrv;

CREATE ROLE idmrptuser LOGIN
  ENCRYPTED PASSWORD '<specify the password for idmrptuser>'
  NOSUPERUSER INHERIT NOCREATEDB NOCREATEROLE;

CREATE ROLE rptuser LOGIN
  ENCRYPTED PASSWORD '<specify the password for rptuser>'
  NOSUPERUSER INHERIT NOCREATEDB NOCREATEROLE;
GRANT esec_user TO rptuser;
```

3b Run the following command for creating table spaces:

```
 CREATE TABLESPACE sendata1
  OWNER dbauser
  LOCATION '<provide the location where table space has to be created>';
```

For example,

```
CREATE TABLESPACE sendata1
  OWNER dbauser
  LOCATION '</opt/netiq/idm/apps/postgres/data>';
```

3c Run the following command for creating a SIEM database:

```
CREATE DATABASE "SIEM"
  WITH OWNER = dbauser
       ENCODING = 'UTF8'
       TABLESPACE = sendata1
       CONNECTION LIMIT = -1;
```

Exporting Data from EAS

1. Stop EAS to ensure that none of the events are sent to the EAS server.
2. Using iManager, stop the DCS driver:
   - **2a** Log in to iManager.
   - **2b** Stop the DCS driver.
   - **2c** Edit the driver properties to change the startup option to **Manual**.

     This step ensures that the driver does not start automatically.
3. Export the data from EAS database to a file:
   - **3a** Log in to the EAS user account:

     ```
     # su - novleas
     ```
   - **3b** Specify a location where the EAS user has full access, for example, `/home/novleas`.
   - **3c** Navigate to the PostgreSQL installation directory and execute the following commands:

     For example,

     ```
     export PATH=/opt/novell/sentinel_eas/3rdparty/postgresql/bin/:$PATH
     ```

     ```
     export LD_LIBRARY_PATH=/opt/novell/sentinel_eas/3rdparty/postgresql/lib/
     :$LD_LIBRARY_PATH
     ```
   - **3d** Export the data to a `.sql` file using the following command:

     ```
     ./pg_dump -p <portnumber> -U <username> -d <dbname> -f <export location>
     ```

For example,

```
./pg_dump -p 15432 -U dbauser SIEM -f /home/novleas/SIEM.sql
```

Importing Data into the New PostgreSQL Database

1. Stop EAS to ensure that none of the events are sent to the EAS server.
2. Using iManager, stop the DCS driver:
   - **2a** Log in to iManager.
   - **2b** Stop the DCS driver.
   - **2c** Edit the driver properties to change the startup option to **Manual**.

     This step ensures that the driver does not start automatically.
3. Import the data to the new PostgreSQL database:
   - **3a** (Conditional) Create a `postgres` user.

     This is specific to Windows only. A user is automatically created on Linux.
   - **3b** Copy the file exported in Step 3d to a location to which the postgres user has full access. For example,
     - **Linux:** `/opt/netiq/idm/apps/postgres`
     - **Windows:** `C:\NetIQ\IdentityManager\apps\postgres`
   - **3c** Execute the following command to import data to the PostgreSQL database.

     ```
     psql -d <dbname> -U <username> -f <full path where the exported file is located>
     ```

     For example,
     - **Linux:** `psql -d SIEM -U postgres -f /opt/netiq/idm/apps/postgres/SIEM.sql`
     - **Windows:** `psql -d SIEM -U postgres –f C:\NetIQ\IdentityManager\apps\postgres\SIEM.sql`
4. Check for any migration log errors and resolve them.

NOTE: The Identity Manager 4.6 reports will not use the audit data that is migrated from EAS to SLM for IGA. Instead, these reports will use the audit data that is directly synchronized from SLM for IGA.

Setting up the Reporting Server

After importing the EAS data to the new PostgreSQL database, configure your Reporting database with the new PostgreSQL database.

This section assumes that you have installed Identity Reporting on the same server where you migrated the database server (SLM for IGA database). For more information about installing Identity Reporting, see "Using the Guided Process to Install Identity Reporting" on page 371.

1. In the `configupdate` utility, perform the following steps to configure the new reporting server details:
   - **1a** At the command prompt, use one of the following methods to run `configupdate` utility.

     Linux: `./configupdate.sh`

     Windows: `configupdate.bat`
   - **1b** Change the **OAuth Redirect URL** to point to the new Identity Reporting server and port details. For more information, see "Reporting" on page 358.

2 Edit the DCS driver configuration to include the new reporting server details using Designer or iManager.

3 Start the DCS driver.

Creating the Data Synchronization Policy

After the Reporting server is configured, enable SLM for IGA to forward the events to an external database. There are two ways through which you can create the data synchronization policy:

- "Using the JAR File" on page 494
- "Using the SLM for IGA Interface" on page 497

Using the JAR File

Identity Manager provides a utility that creates the data synchronization policy in SLM for IGA for forwarding events from SLM for IGA to an external database. The utility is located in the `IdentityReporting/Sentinel` folder.

Create the data synchronization policy using the following steps:

1 Navigate to the Data Synchronization utility directory and run the following command:

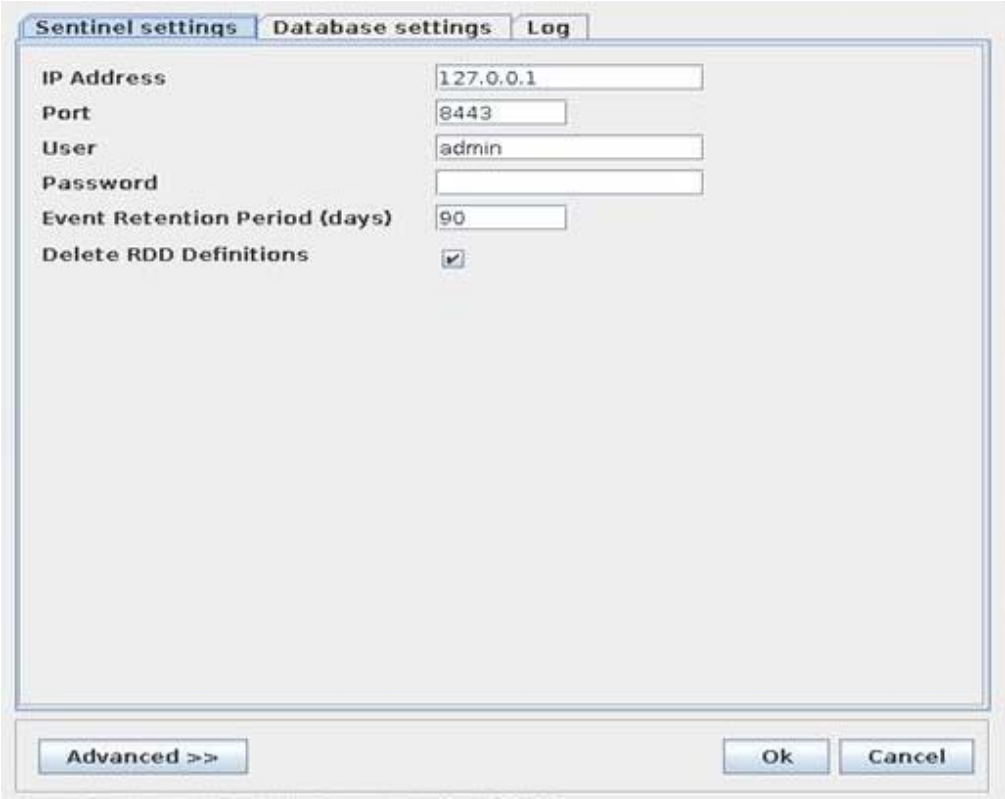
`<java path>/bin/java –jar sentineldatasync.jar`, where `<java path>` is the JRE installed location.

This opens the data synchronization utility.

NOTE: If Identity Reporting is running with an Oracle database, verify that the `ojdbc<version>.jar` is present in the `<java path>/lib/ext` directory, where `<java path>` is the JRE installed location

---

2 In the **Sentinel Settings** tab of the utility, specify the following details:



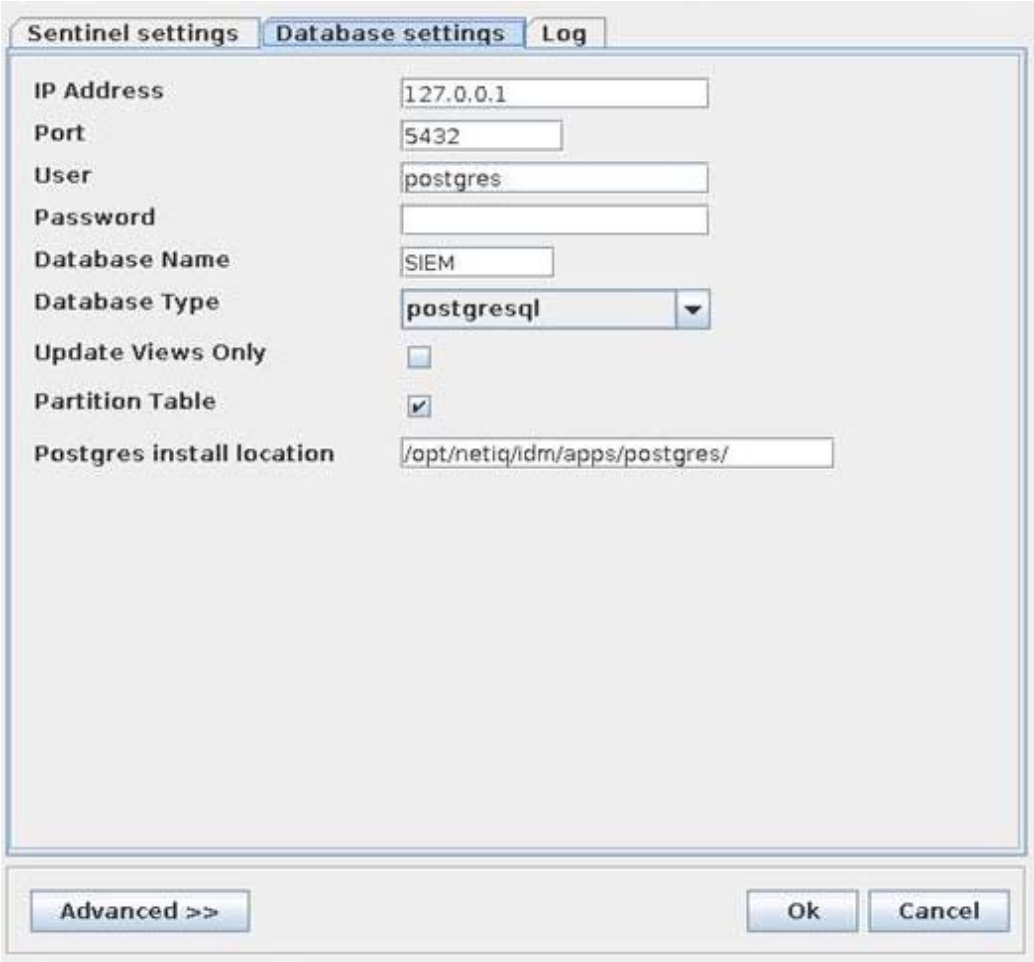
- **IP Address:** Specify the IP address of the computer where SLM for IGA is installed.
- **Port:** Specify the port for the SLM for IGA server. The default port is 8443.
- **Password:** Specify the password for the SLM for IGA user.
- **Event Retention Period:** Specify the duration for the events to persist in the database before they are deleted. The default is 90 days.
- **Delete RDD Definitions:** While creating the data synchronization policy on SLM for IGA, the default setting is to delete the default Sentinel policies. If you want to execute Sentinel reports, you need not delete the default Sentinel policies.

  IMPORTANT: Deselect this option if you are using Sentinel or Identity Tracking.

- **Advanced:** If you are using **Advanced** mode, you may edit the following parameter:
  - **Event Table Payload:** Contains a JSON document for creating the data synchronization table through REST APIs. The authentication information is substituted when a request is sent for creating the data synchronization table.
  - **Data Sync Policy Payload:** Contains a JSON document for creating the data synchronization table through REST APIs. The authentication information is substituted when a request is sent for creating the data synchronization table.

    NOTE: To add additional fields to the data synchronization policy, modify the JSON document in **Data Sync Policy Payload**. Ensure that the changes are present in both event table and the data synchronization policy. Otherwise, the policy creation fails.

3 In the **Database settings** tab, specify the following details. For example, if you select PostgresSQL as your database, the **Database settings** screen would look like the following:



- **IP Address:** Specify the IP address of the database.
- **Port:** Specify the port for the database.
- **Password:** Specify a password to connect to the database.
- **Database Name:** Specify a target database name where Reporting is installed.

  For example, if you are migrating from EAS, you can specify `SIEM` and if you are performing a new install of SLM for IGA, specify `idmrptdb`.
- **Database Type:** Select the database type from the drop-down list.
- **Update Views Only:** Select this option only if you encounter errors while updating the views. When this option is selected, the Data Synchronization utility updates the views and does not create the data synchronization policy in SLM for IGA.
- **Partition Table:** Partitioning the table improves the overall query performance and table management capability. The database stores the events received from Sentinel in separate partitions on a daily basis. You are recommended to leave this setting as is.
- **PostgreSQL Install Location:** This option is available only if you select `PostgresSQL` in the **Database Type** field. This option specifies the location where PostgreSQL is installed. For example, `/opt/netiq/idm/apps/postgres/`.

  If you are using PostgreSQL on a different server, you need to copy the `sentineldatasync.jar` to the server where PostgreSQL is installed.

- **Advanced:** If you are using **Advanced** mode, you may edit the following parameter:

  Partition SQL: This contains the SQL script for partitioning the table. The script is specific to the selected database.

4 In the **Logs** tab, specify the name of the log file.

  The log file is located in the same location as your Data Synchronization utility.

Using the SLM for IGA Interface

To ensure that SLM for IGA receives the events from the specified Identity Manager collectors, you can modify the filter for the data synchronization policy.

1 Log in to the SLM for IGA main interface as an administrator.

2 Click **Storage** > **Data Synchronization**.

3 Click **Edit** to configure the data synchronization policy.

4 Edit the required information:

  Criteria: Specify a valid Lucene query.

  The following query is an example of a criteria for receiving events only from Identity Manager components:

```
(pn:"NetIQ Identity Manager" OR pn:"NetIQ Self Service Password Reset" OR
pn:"NetIQ eDirectory" OR pn:"NetIQ NMAS" OR pn:"NetIQ iManager" OR pn:"NetIQ
One SSO Provider") AND (sev:[0 TO 5]) AND NOT
(evt:"CombinedRealTimeSummariesStatus" OR evt:"EnginePerformanceSummary" OR
evt:"EventThroughputUtilization" OR evt:"LostConnection")
```

  Policy Name: Specify a name for the data synchronization policy.

  Retention Period: Specify the duration for which the events will be persisted in the `sentinel_events` table of the Reporting database.

  Batch Size: Specify the number of events that can be sent to the external database in one batch.

  Sleep period: Specify the duration after which the data synchronization process checks for more events to process.

  Schedule: Select an appropriate option to synchronize the data to the external database.

  - **All the time:** If you select this option, the events are synchronized to the external database immediately after any event is modified.
  - **Custom:** This option allows you to configure specific time intervals to synchronize data.

    If you select **Custom**, provide the following information to set the custom synchronization time:

    - **Day of the Week:** Select the required day of the week or select **Everyday**.
    - **Start time:** Specify the time at which the data synchronization process should start.
    - **Duration:** Specify the synchronization period in minutes.

  If you do not see the data in the database tables immediately, you need to wait for the next synchronization cycle.

NOTE: If Identity Reporting is running with an Oracle database, log in to the query tool as the database administrator (`sysdba`) and assign the following permissions:

- `GRANT ALL ON IDM_RPT_DATA.SENTINEL_EVENTS TO IDM_RPT_DATA;`

- `GRANT SELECT ON IDM_RPT_DATA.SENTINEL_EVENTS TO PUBLIC;`
- `GRANT CREATE PUBLIC SYNONYM to IDM_RPT_CFG;`

Upgrading Identity Reporting

Before upgrading Identity Reporting, you must upgrade the identity applications and SLM for IGA. To upgrade Identity Reporting from version 4.0.2 or later, install the new version on top of the older version. For more information, see "Installing Identity Reporting" on page 371.

Changing the References to reportRunner in the Database

After upgrading Identity Reporting and before starting Tomcat for the first time, ensure that you update the references to reportRunner from the database.

1. Stop Tomcat.
2. Navigate to the Identity Reporting installation directory and rename the `reportContent` folder to `ORG-reportContent`.

   For example: `/opt/netiq/idm/apps/IdentityReporting`
3. Clean the temporary and work directories under the Tomcat folder.
4. Log in to the PostgreSQL database.

   4a Locate the reportRunner references in the following tables:

   - `idm_rpt_cfg.idmrpt_rpt_params`
   - `idm_rpt_cfg.idmrpt_definition`

   4b Issue the following delete statements:

   ```
   DELETE FROM idm_rpt_cfg.idmrpt_rpt_params WHERE
   rpt_def_id='com.novell.content.reportRunner';
   ```

   ```
   DELETE FROM idm_rpt_cfg.idmrpt_definition WHERE
   def_id='com.novell.content.reportRunner';
   ```
5. Start Tomcat.

   Check the logs to see if the reports are regenerated with the correct reportRunner.
6. Log into Identity Reporting and run the reports.

Verifying the Upgrade for Identity Reporting

1. Launch Identity Reporting.
2. Verify that old and new reports are being displayed in the tool.
3. Look at the **Calendar** to see whether your scheduled reports appear.
4. Ensure that the **Settings** page displays your previous settings for managed and unmanaged applications.
5. Verify that all other settings look correct.
6. Verify whether the application lists your completed reports.

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_4.6_patch1_20121128.zip`, from the NetIQ download website.
2. Extract the `.zip` file to the directory that contains the Analyzer installation files, such as the plug-ins, 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 **4.6 Update 1** and Build ID **20121128**.

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 *NetIQ Designer for Identity Manager 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 might 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:

- "Creating a New Driver" on page 499
- "Replacing Existing Content with Content from Packages" on page 500
- "Keeping the Current Content and Adding New Content with Packages" on page 500

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 website. The driver now functions as before, but with content from packages instead of from a driver configuration file.

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 "Exporting the Configuration of the Drivers" on page 466.

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 provides the auto-import facility for importing the latest packages. You do not need to manually import the driver packages into the package catalog.

   For more information, see "Importing Packages into the Package Catalog" in the *NetIQ Designer for Identity Manager 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 website.

4. Restore any custom policies and rules to the driver. For instructions, see "Restoring Custom Policies and Rules to the Driver" on page 502.

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 "Exporting the Configuration of the Drivers" on page 466.

   NOTE: Designer provides the auto-import facility for importing the latest packages. You do not need to manually import the driver packages into the package catalog.

   For more information, see "Importing Packages into the Package Catalog" in the *NetIQ Designer for Identity Manager Administration Guide*.

2. Install the packages on the driver.

   For instructions, see each driver guide at the Identity Manager Drivers documentation website.

3. Add the desired packages to the driver. These steps are specific for each driver.

   For more information, see the Identity Manager Drivers documentation website.

The driver contains the new functionality added by the packages.

Adding New Servers to the Driver Set

When you upgrade or migrate Identity Manager to new servers, you must update the driver set information. This section guides you through the process. You can use Designer or iManager to update the driver set.

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 "Copying the Server-specific Information in Designer" on page 519. 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 server, then click **OK**.

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.

- "Using Designer to Remove the Old Server from the Driver Set" on page 501
- "Using iManager to Remove the Old Server from the Driver Set" on page 501
- "Decommissioning the Old Server" on page 502

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 *NetIQ Designer for Identity Manager Administration Guide*.

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**.

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 *NetIQ eDirectory Administration Guide*.

2 Remove eDirectory from this server.

   For more information, see TID 10056593, "Removing a Server From an NDS Tree Permanently".

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.

- "Using Designer to Restore Custom Policies and Rules to the Driver" on page 502
- "Using iManager to Restore Custom Policies and Rules to the Driver" on page 503

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 "Starting the Drivers" on page 140. For more information on testing the driver, see "Testing Policies with the Policy Simulator" in *NetIQ Identity Manager - Using Designer to Create Policies*.

9 After you verify that the policies work, move the driver to the production environment.

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 "Starting the Drivers" on page 140. 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.

56 Switching from Advanced Edition to Standard Edition

You should switch to Standard Edition only if you do not want any Advanced Edition functionality in your environment and want to scale down your Identity Manager deployment.

1. (Conditional) If you have already applied the Advanced Edition activation, remove the activation.
2. (Conditional) To switch to the Standard Edition evaluation mode, perform the following actions:
   - **2a** Navigate to the Identity Vault `dib` directory.

     Linux: `/var/opt/novell/eDirectory/data/dib`

     Windows: `C:\Novell\NDS\DIBFiles`
   - **2b** Create a new file, name it `.idme`, and add 2 (numeric) to the file.
   - **2c** Restart eDirectory.
   - **2d** Continue with Step 4.
3. (Conditional) If you have already purchased a Standard Edition activation, apply the activation.
4. Stop Tomcat.
5. Remove the following WAR files and Webapps folder from the Tomcat `Webapps` directory:

   Linux: `/opt/netiq/idm/apps/tomcat/webapps`

   Windows: `C:\netiq\/idm\apps\tomcat\webapps`

   - `IDMProv*`
   - `IDMRPT*`
   - `dash*`
   - `idmdash*`
   - `landing*`
   - `rra*`
   - `rptdoc*`
6. Move the following existing folders to a backup directory:
   - `IDMReporting`
   - `UserApplication`
7. Copy the `ism-configuration.properties` file from `<install folder>/tomcat/conf` directory to a backup directory.
8. Install Identity Reporting from the Identity Manager 4.6 media.
9. Start `configupdate.sh` from the `<reporting install folder>/bin` directory and specify values for the following parameters:

   Reporting tab: Specify the settings in the following sections:

   - ID Vault
   - Identity Vault User Identity

- Report Administrators
  - **Report Admin Role Container DN**. For example, `ou=sa,o=data`
  - **Report Administrators**. For example, `cn=uaadmin,ou=sa,o=data`

Authentication tab: Specify the settings in the following sections:

- Authentication Server
  - **OAuth server host identifier**. For example, IP address or DNS name of the authentication server such as `192.99.17.22`
  - **OAuth server TCP port**
  - **OAuth server is using TLS/SSL**
- Authentication Configuration
  - **OAuth keystore file**. For example, `/opt/netiq/idm/apps/osp/osp.jks`
  - **Key alias of key for use by OAuth**
  - **Key password of key for use by OAuth**
  - **Session Timeout (minutes)**. For example, 60 minutes.

SSO Clients tab: Specify the settings in the following sections:

- Reporting
  - **URL link to landing page**. For example, `http://192.99.17.22:8180/IDMRPT`
- Self Service Password Reset
  - **OAuth client ID**. For example, *sspr*
  - OAuth client secret For example, *<sspr client secret>*
  - **OSP OAuth redirect url**. For example, `http://192.99.179.202:8180/sspr/public/oauth`

For more information about Configuration Utility, see "Running the Identity Applications Configuration Utility" on page 339.

10 Save the changes and exit the Configuration Utility.

11 Start Tomcat.

57 Applying a Software Update to Identity Manager Components

This section provides information about installing a software update (service pack or patch) for an Identity Manager component.

- "Applying a Service Pack to Identity Manager Engine and Remote Loader" on page 507
- "Applying a Patch for an Identity Manager Driver" on page 510

Applying a Service Pack to Identity Manager Engine and Remote Loader

The Identity Manager engine and Remote Loader service pack updates the Identity Manager server and the Remote Loader. You can install the service pack in the guided (GUI) and silent modes only. The service pack does not support console mode.

To view the log files for the installation, navigate to the following locations:

- **Linux**: `/tmp/logs/idmPatchInstall.log`
- **Windows**: `\%Temp%\logs`

NOTE: For Windows servers, the service pack creates a backup folder in the `\%UserProfile%\PatchInstallerBackUp<Date><Time>` directory.

- "Prerequisites for Installing the Service Pack" on page 507
- "Installing the Service Pack as a Root User in GUI Mode" on page 508
- "Installing the Service Pack as a Non-Root User in GUI Mode" on page 509
- "Silently Installing the Service Pack" on page 509

Prerequisites for Installing the Service Pack

Before installing the service pack, complete the following steps:

1. Stop the eDirectory daemon.

   If you do not stop eDirectory, the service pack installer attempts to stop it. If the program fails to stop eDirectory, it displays a warning message. Then you will need to manually stop eDirectory.
2. Stop the Remote Loader services.

   If the Remote Loader is in use, the service pack cannot update the Remote Loader.
3. (Conditional) For a non-`root` installation, set the Java path by completing one of the following actions:
   - Edit the `JAVA_NONROOT` variable in the `install.sh` file for the service pack.
   - Export the Java 1.8 path.
4. In a browser, navigate to the NetIQ downloads page (https://dl.netiq.com/index.jsp).

5 Under **Patches**, click **Search Patches**.

6 Specify **Identity Manager *nn* patch** in the search box

7 Download and unzip the contents of the file.

Installing the Service Pack as a Root User in GUI Mode

For a `root` installation, complete the following steps.

1 Ensure that you have completed the prerequisites for installing the service pack. For more information, see "Prerequisites for Installing the Service Pack" on page 507.

2 On the server where you want to run the service pack, log in as `root`.

3 Navigate to the `cd-image` directory where you unzipped the service pack files.

For more information, see "Prerequisites for Installing the Service Pack" on page 507.

4 Depending on your platform, run one of the following commands:

- **Linux** Execute the `./install.sh` command in a terminal window.
- **Windows** Launch the `install.bat` file.

5 Select the components that you want to install, then click **Install**.

6 (Conditional) To update the Remote Loader, complete the following actions:

6a Click **OK** for the warning message about stopping the Remote Loader.

Ensure that you have stopped the Remote Loader.

6b If the installer cannot detect a 32-bit or 64-bit Remote Loader installed on your computer, **Browse** to the path for the installed Remote Loader.

NOTE: By default, the service pack installer provides a **Browse** option for the Identity Manager server on Linux. It is not available on Windows by default.

---

7 Review the installation status of the selected components, then click **Done**.

8 (Conditional) **Linux**: To verify that the service pack has been successfully applied for the Identity Manager components that you selected in Step 5, complete the following steps:

8a Check the Identity Manager server trace to verify that your Identity Manager version is updated. The trace window shows the following output:

```
<product version="4.5.n.n">DirXML</product>
```

where *n* represents the version of the Identity Manager service pack.

8b To verify that Identity Manager RPMs are installed on your computer, run the command:

```
rpm -qa | grep nov | grep 4.5
```

9 (Conditional) **Windows**: To verify that the service pack has been successfully applied for the Identity Manager components that you selected in Step 5, complete the following steps:

9a Check the modification date for the files updated by the service pack installer.

9b Launch the Remote Loader.

9c Click **Properties**, then right-click `rlconsole.exe`.

9d Click **Properties > Details**.

9e Verify that the value in the file version is 4.5.*n.n* where *n* represents the version of the Identity Manager service pack.

Installing the Service Pack as a Non-Root User in GUI Mode

To run a non-`root` installation using the guided process, complete the following steps.

1. Ensure that you have completed the prerequisites for installing the service pack. For more information, see "Prerequisites for Installing the Service Pack" on page 507.
2. On the server where you want to run the service pack, log in as a non-`root` user.
3. Run the `install.sh` file.
4. Browse for the base location of eDirectory. For example, `/home/<user>/eDirectory`.
5. Click **Install**.

Silently Installing the Service Pack

To run a silent installation of the Identity Manager service pack installer, you must have a `patchUpgradeSilent.Properties` file. NetIQ provides a sample file located by default in the `cd-image` directory. This procedure can be used for a `root` or non-`root` installation.

1. Ensure that you have completed the prerequisites for installing the service pack. For more information, see "Prerequisites for Installing the Service Pack" on page 507.
2. Modify the contents of the `patchUpgradeSilent.Properties` file.

   The sample file contains the following information:

   ```
   #Silent Properties File IDMPatchInstaller
   #eDirectory and RemoteLoader services should be stopped before installation
   #Set this property to true/false for Engine Upgrade for root and non root
   install
   install_Engine=true
   #Set this property to true/false for Remote Loader32 Upgrade
   install_RL32=true
   #Set this property to true/false for Remote Loader64 Upgrade
   install_RL64=true
   #Set this property for Engine Upgrade for NON ROOT user
   #eg: If the engine location is /home/eDirectoryNonRoot/eDirectory/opt/novell/
   eDirectory select till eDirectory(parent directory of /opt)
   engine_Location=/home/eDirectoryNonRoot/eDirectory/
   #Set this property for Remote Loader 32-Bit Install location
   #Only for Windows
   RL32_Location=C:\\Novell\\IdentityManager\\RemoteLoader\\32bit
   #Set this property for Remote Loader 64-Bit Install location
   #Only for Windows
   RL64_Location=C:\\Novell\\IdentityManager\\RemoteLoader\\64bit
   ```

   NOTE: On Windows servers, the service pack installation uses the same installation path for the Identity Manager engine server that was specified when Identity Manager 4.5 was installed.

3. (Conditional) For a non-`root` installation, uncomment the `engine_Location` property to point to the exact location of the Identity Manager engine.

4 To launch the installation process, enter one of the following commands:

- **Linux**: `<service pack location>/install.sh -i silent -f <filename>`
- **Windows**: `<service pack location>\install.bat -i silent -f <filename>`

NOTE: If you run the non-`root` installation of Identity Manager as a `root` user, the installation program displays following warning:

```
NetIQ recommends that you apply only patches pertaining to the installed IDM
version. If you understand the risk and want to proceed, type yes else no.
```

Ignore the warning message, and enter **Yes** to proceed.

Applying a Patch for an Identity Manager Driver

This section contains information about installing a software update (commonly known as patch) for an Identity Manager driver.

- "Applying the Identity Manager Driver Patch as a Root User" on page 510
- "Applying the Identity Manager Driver Patch as a Non-Root User" on page 510

Applying the Identity Manager Driver Patch as a Root User

In a `root` installation, the driver patch installs the driver RPMs in the default locations in the `/opt/novell/eDirectory` path.

Applying the Identity Manager Driver Patch as a Non-Root User

1 Verify that `</local/home/bshidm/base/bshappl/edir>` directory exists and contains the file, `_db.000`.

   The `_db.000` file is created during a non-root installation of the Identity Manager engine. Absence of this file might indicate that Identity Manager is not properly installed. Reinstall Identity Manager to correctly place the file in the directory.

2 To set the `root` directory to `non-root` eDirectory location, enter the following command in the command prompt:

```
ROOTDIR=/local/home/bshidm/base/bshappl/edir
```

   This will set the environmental variables to the directory where eDirectory is installed as a `non-root` user.

3 Download the driver patch and untar or unzip the downloaded file.

4 To install the driver files, run the following script in a command prompt:

```
*************************************************************
#!/bin/sh
#set -x
#© 2017 NetIQ Corporation and its affiliates. All Rights Reserved

clear

echo "======================================================================"
echo " Installing packages... "
echo "======================================================================"

if [ "$1" == "" ] ; then
        exit
fi

pkgfile=$1
ROOTDIR="/local/home/bshidm/base/bshappl/edir"
RPMDB=$ROOTDIR/rpm

if [ ! -d "$RPMDB" ] ; then
        mkdir $RPMDB
fi
        # create rpm database if it doesn't exist
        if [ ! -f $RPMDB/__db.000 ]
        then
#                mkdir -p $RPMDB
                rpm  --dbpath "$RPMDB" --initdb
        fi


RPM_FLAGS="--dbpath $RPMDB -Uvh --relocate=/etc=$ROOTDIR/etc --relocate=/
opt=$ROOTDIR/opt --relocate=/opt/novell/eDirectory/lib64=$ROOTDIR/opt/novell/
eDirectory/lib64 --relocate=/var=$ROOTDIR/var --badreloc --nodeps --
replacefiles --force"

rpm  $RPM_FLAGS $pkgfile
```

XVI Migrating Identity Manager Data to a New Installation

This section provides information on migrating existing data in Identity Manager components to a new installation. Most migration tasks apply to the Identity Applications. To upgrade Identity Manager components, see Part XVI, “Upgrading Identity Manager,” on page 457. For more information about the difference between upgrade and migration, see “Understanding Upgrade and Migration” on page 461.

58 Preparing to Migrate Identity Manager

This section provides information to help you prepare for migrating your Identity Manager solution to the new installation.

Checklist for Performing a Migration

To perform a migration, NetIQ recommends that you complete the steps in the following checklist.

	Checklist Items
❑	1. Determine whether you should perform an upgrade or a migration. For more information, see "Understanding Upgrade and Migration" on page 461.
❑	2. Ensure that you have the latest installation kit to migrate your Identity Manager data.
❑	3. Learn about the interaction among Identity Manager components. For more information, see Part I, "Introduction," on page 21.
❑	4. Ensure that your computers meet the hardware and software prerequisites for a newer version of Identity Manager. For more information, see Chapter 6, "Considerations and Prerequisites for Installation," on page 53 and the Release Notes for the version to which you want to upgrade.
❑	5. Upgrade eDirectory to the latest supported version for the Identity Vault. For more information, see "Prerequisites and Considerations for Installing the Identity Vault" on page 62.
❑	6. Add the eDirectory replicas that are on the current Identity Manager server to the new server. For more information, see "Migrating the Identity Manager Engine to a New Server" on page 520.
❑	7. Install Identity Manager on the new server. For more information, see "Planning to Install Identity Manager" on page 39.
❑	8. (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 "Upgrading the Remote Loader" on page 475.
❑	9. (Conditional) If you are running the User Application on your old server, update the component and its drivers. For more information, see "Checklist for Migrating Identity Manager" on page 517.
❑	10. Add the new server to the driver set. For more information, see "Adding the New Server to the Driver Set" on page 501.
❑	11. Change the server-specific information for each driver. For more information, see "Copying the Server-specific Information in Designer" on page 519.
❑	12. (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 "Copying Server-specific Information for the Driver Set" on page 519
❑	13. Update your drivers to the package format. For more information, see "Upgrading the Identity Manager Drivers" on page 499.

	Checklist Items
❑	14. (Conditional) If you have custom policies and rules, restore your customize settings. For more information, see "Restoring Custom Policies and Rules to the Driver" on page 502.
❑	15. Remove the old server from the driver set. For more information, see "Removing the Old Server from the Driver Set" on page 501.
❑	16. Activate your upgraded Identity Manager solution. For more information, see "Activating Identity Manager" on page 453.

Stopping and Starting Identity Manager Drivers during 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. For more information, see the following sections:

- "Stopping the Drivers" on page 139
- "Starting the Drivers" on page 140

59 Migrating Identity Manager to a New Server

This section provides information for migrating from the User Application to the identity applications on a new server. You might also need to perform a migration when you cannot upgrade an existing installation. This section includes the following activities:

- "Checklist for Migrating Identity Manager" on page 517
- "Preparing Your Designer Project for Migration" on page 518
- "Copying Server-specific Information for the Driver Set" on page 519
- "Migrating the Identity Manager Engine to a New Server" on page 520
- "Migrating the User Application Driver" on page 521
- "Migrating from Websphere or JBoss to Tomcat Web Application Server" on page 522
- "Upgrading the Identity Applications" on page 523
- "Completing the Migration of the Identity Applications" on page 524

Checklist for Migrating Identity Manager

NetIQ recommends that you complete the steps in the following checklist.

	Checklist Items
❑	1. Back up the directories and databases of your Identity Manager solution.
❑	2. Ensure that you have installed the latest versions of the Identity Manager components, except for the identity applications. For more information, see "Recommended Server Setup" on page 46 and the latest release notes for the components. **NOTE:** To continue using your current User Application database, specify **Existing Database** in the installation program. For more information, see Part XII, "Installing the Identity Applications," on page 277.
❑	3. Run a health check of the Identity Vault to ensure that the schema extends properly. Use TID 3564075 to complete the health check.
❑	4. Import your existing User Application drivers into Designer.
❑	5. Archive the Designer project. It represents the pre-migration state of the drivers. For more information, see "Preparing Your Designer Project for Migration" on page 518.
❑	6. (Conditional) To migrate the Identity Manager engine to a new server, copy the eDirectory replicas to the new server. For more information, see "Migrating the Identity Manager Engine to a New Server" on page 520.
❑	7. Create a new Designer project in the latest version of Designer, then import the User Application driver to prepare for migration.

	Checklist Items
❑	8. Migrate the User Application driver. For more information, see "Migrating the User Application Driver" on page 521.
❑	9. Create a new Role and Resource Service driver. You cannot migrate an existing Role and Resource Service driver. For more information, see "Creating the Role and Resource Service Driver" on page 324.
❑	10. Deploy the two drivers to the Identity Vault. For more information, see "Deploying the Drivers for the User Application" on page 325.
❑	11. Upgrade the Identity Applications. For more information, see "Upgrading Identity Applications and Supporting Components" on page 477.
❑	12. (Conditional) To upgrade an Oracle database with an SQL file created by the installation process, prepare the Oracle environment. For more information, see "Preparing an Oracle Database for the SQL File" on page 524.
❑	13. Ensure that your browsers do not contain content from the previous versions of Identity Manager. For more information, see "Flushing the Browser Cache" on page 525.
❑	14. (Conditional) Reinstate your custom settings for the SharedPagePortlet. For more information, see "Updating the Maximum Timeout Setting for the SharedPagePortlet" on page 525.
❑	15. Ensure that the search option for groups does not display information until the user provides filter parameters. For more information, see "Disabling the Automatic Query Setting for Groups" on page 525.

Preparing Your Designer Project for Migration

Before you migrate the driver, you need to perform some setup steps to prepare the Designer project for migration.

NOTE: If you do not have an existing Designer project to migrate, create a new project by using **File > Import > Project (From Identity Vault)**.

1. Launch Designer.
2. (Conditional) If you have an existing Designer project that contains the User Application that you want to migrate, back up the project:
   - **2a** Right-click the name of the project in Project view, then select **Copy Project**.
   - **2b** Specify a name for the project, then click **OK**.
3. To update the schema for your existing project, complete the following steps:
   - **3a** In the Modeler view, select the Identity Vault.
   - **3b** Select **Live > Schema > Import**.
4. (Optional) To verify that the version number for Identity Manager is correct in your project, complete the following steps:
   - **4a** In the Modeler view, select the Identity Vault and then click **Properties**.
   - **4b** In the left navigation menu, select **Server List**.
   - **4c** Select a server and then click **Edit**.

     The **Identity Manager version** field should show the latest version.

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.

- "Copying the Server-specific Information in Designer" on page 519
- "Changing the Server-specific Information in iManager" on page 520
- "Changing the Server-specific Information for the User Application" on page 520

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 *NetIQ Designer for Identity Manager Administration Guide*.

8 Start the drivers.

For more information, see "Starting the Drivers" on page 140.

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.

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 Chapter 40, "Configuring the Settings for the Identity Applications," on page 339.

Migrating the Identity Manager Engine to a New Server

When migrating the Identity Manager engine to a new server, you can keep the eDirectory replicas that you currently use on the old server.

1 Install a supported version of eDirectory on the new server.
2 Copy the eDirectory replicas that are on the current Identity Manager server to the new server.

   For more information, see "Administering Replicas" in the *NetIQ eDirectory Administration Guide*.

3 Install the Identity Manager engine on the new server.

For more information, see Part V, “Installing the Identity Manager Engine, Drivers, and Plug-ins,” on page 131.

Migrating the User Application Driver

When upgrading to a new version of Identity Manager or migrating to a different server, you might need to import a new base package for the User Application driver, or upgrade the existing package. For example, **User Application Base Version 2.2.0.20120516011608**.

When you begin working with an Identity Manager project, Designer automatically prompts you to import new packages into the project. You can also manually import the package at that time.

Importing a New Base Package

1 Open your project in Designer.

2 Right-click **Package Catalog > Import Package**, then select the appropriate package.

3 (Conditional) If the Import Package dialog does not list the User Application Base package, complete the following steps:

   3a Click the Browse button.

   3b Navigate to `designer_root/packages/eclipse/plugins/NOVLUABASE_version_of_latest_package.jar`.

   3c Click **OK**.

4 Click **OK**.

Upgrading an Existing Base Package

1 Open your project in Designer.

2 Right-click the User Application Driver.

3 Click **Driver > Properties > Packages**.

   If the base package can be upgraded, the application displays a check mark in the **Upgrades** column.

4 Click **Select Operation** for the package that indicates there is an upgrade available.

5 From the drop-down list, click **Upgrade**.

6 Select the version to which you want to upgrade. Then click **OK**.

7 Click **Apply**.

8 Fill in the fields with appropriate information to upgrade the package. Then click **Next**.

9 Read the summary of the installation. Then click **Finish**.

10 Close the Package Management page.

11 Deselect **Show only applicable package versions**.

Deploying the Migrated Driver

The driver migration is not complete until you deploy the User Application driver to the Identity Vault. After the migration, the project is in a state in which only the entire migrated configuration can be deployed. You cannot import any definitions into the migrated configuration. After the entire migration configuration has been deployed, this restriction is lifted, and you can deploy individual objects and import definitions.

1. Open the project in Designer and run the Project Checker on the migrated objects.

   For more information, see "Validating Provisioning Objects" in the *NetIQ Identity Manager - Administrator's Guide to Designing the Identity Applications*. If validation errors exist for the configuration, you are informed of the errors. These errors must be corrected before you can deploy the driver.
2. In the **Outline** view, right-click the User Application driver.
3. Select **Deploy**.
4. Repeat this process for each User Application driver in the driver set.

Migrating from Websphere or JBoss to Tomcat Web Application Server

Before upgrading to Identity Manager 4.6 or later version, you must migrate existing JBoss or Websphere to Tomcat Application Server.

This section helps you migrate the Identity Applications from your existing web application servers such as Websphere or JBoss to Tomcat application server. This process requires you to install Identity Applications on Tomcat and configure the settings using configuration update utility.

To migrate from Websphere or JBoss to Tomcat, perform the following steps:

1. Stop the Websphere or JBoss server.
2. (Conditional) If Tomcat is not installed then install Tomcat and JRE using convenience installer.
   - **Linux**: `products/RBPM/postgre_tomcat_install/TomcatPostgreSQL.bin`
   - **Windows**: `products\RBPM\postgre_tomcat_install\TomcatPostgreSQL.exe`

   NOTE: Use Tomcat application server that is bundled along with IDM 4.5 `.iso`.
3. (Conditional) If you use existing JRE file, installer prompts you to overwrite certain files. Click **Yes to all**.
4. Install the Identity Applications using convenience installer located at:

   `products/RBPM/user_app_install/IdmUserApp.bin`

   4a Select **Tomcat** as web application server.

   4b Select the **Existing Database** option and provide the host credentials. The default **user ID** is `idmadmin`.

   4c Specify the installation path of Tomcat and JRE.

   4d (Conditional) On cluster environment, Specify the same **Engine ID** that is mentioned during JBoss/Websphere installation.

   NOTE: If you have single instance running on your application server, leave the **Engine ID** field blank unless you have specified during JBoss or Websphere installation.

4e (Conditional) To import the master key value on your cluster environment, select **Yes** and specify the master key value. You can find the master key value from your previous configurations of JBoss or Websphere application servers.

4f In the **Configure IDM** page, select **Configure Later** and click **Next**.

4g Review the **Pre-Installation Summary** page and click **Install**.

5 Open the **Configuration Update** utility:

```
/opt/netiq/idm/apps/UserApplication
```

For more information about specifying values for the settings, see Chapter 40, "Configuring the Settings for the Identity Applications," on page 339.

6 Click **Save**.

7 (Conditional) Upgrade to the latest Identity Manager 4.5 service pack.

NOTE: If you want to upgrade to Identity Manager 4.6, you need not upgrade to the latest Identity Manager service pack.

---

8 Start the Tomcat Application server and verify that Identity Applications are deployed correctly.

After migration is complete, upgrade the Identity applications. For more information, see "Upgrading Identity Applications and Supporting Components" on page 477.

Upgrading the Identity Applications

When you run the Upgrade program for the identity applications, ensure that you incorporate the following considerations:

- Use the same database that you used for the previous User Application. That is, the installation from which you are migrating. In the installation program, specify **Existing Database** for the database type.
- (Conditional) If your existing database runs on Oracle and you instruct the installation program to write a SQL file to update the schema, you must perform additional steps. For more information, see "Preparing an Oracle Database for the SQL File" on page 524.
- You can specify a different name for the User Application context.
- Specify an installation location that is different from the one for the previous installation.
- Point to a supported version of Tomcat.
- Do not use case-insensitive collation for your database. Case-insensitive collation is not supported. If you use case-insensitive collation, you might encounter duplicate key errors during migration. If a duplicate key error is encountered, check the collation and correct it, then re-install the identity applications.
- Understand the differences in the providers for managing passwords. SSPR is the default provider. To use Identity Manager's legacy provider or an external provider, you must update the configuration of the identity applications after the upgrade. For more information, see "Using Self-Service Password Management in Identity Manager" on page 35.

For more information about upgrading the Identity Applications, see "Upgrading Identity Applications and Supporting Components" on page 477.

Completing the Migration of the Identity Applications

After upgrading or migrating the identity applications, complete the migration process.

Preparing an Oracle Database for the SQL File

During the installation process, you might have chosen to write a SQL file to update the identity applications database. If your database runs on an Oracle platform, you must perform some steps before you can run the SQL file.

1. In the database, run the following SQL statements:

```
ALTER TABLE DATABASECHANGELOG ADD ORDEREXECUTED INT;
UPDATE DATABASECHANGELOG SET ORDEREXECUTED = -1;
ALTER TABLE DATABASECHANGELOG MODIFY ORDEREXECUTED INT NOT NULL;
ALTER TABLE DATABASECHANGELOG ADD EXECTYPE VARCHAR(10);
UPDATE DATABASECHANGELOG SET EXECTYPE = 'EXECUTED';
ALTER TABLE DATABASECHANGELOG MODIFY EXECTYPE VARCHAR(10) NOT NULL;
```

2. Run the following `updateSQL` command:

```
/opt/novell/idm/jre/bin/java -Xms256m -Xmx256m  -Dwar.context.name=IDMProv
-jar /opt/novell/idm/liquibase.jar
--databaseClass=com.novell.soa.persist.liquibase.OracleUnicodeDatabase
--driver=oracle.jdbc.driver.OracleDriver
--classpath=/root/ojdbc6.jar:/opt/novell/idm/tomcat/server/IDMProv/deploy/
IDMProv.war
--changeLogFile=DatabaseChangeLog.xml
--url="jdbcURL" --logLevel=debug
--logFile=/opt/novell/idm/db.out --contexts="prov,updatedb" --username=xxxx
--password=xxxx updateSQL  > /opt/novell/idm/db.sql
```

3. In a text editor, open the SQL file, by default in the `/installation_path/userapp/sql` directory.
4. Insert a backslash (/) after the definition of the function `CONCAT_BLOB`. For example

```
  -- Changeset icfg-data-load.xml::700::IDMRBPM
CREATE OR REPLACE FUNCTION CONCAT_BLOB(A IN BLOB, B IN BLOB) RETURN BLOB AS
                C BLOB;
            BEGIN
                DBMS_LOB.CREATETEMPORARY(C, TRUE);
                DBMS_LOB.APPEND(C, A);
                DBMS_LOB.APPEND(C, B);
                RETURN c;
            END;
/
```

5. Execute the SQL file.

   For more information about running the SQL file, see "Manually Creating the Database Schema" on page 327.

NOTE: Do not use SQL*Plus to execute the SQL file. The line lengths in the file exceed 4000 characters.

Flushing the Browser Cache

Before you log in to the identity applications, you should flush the cache on the browser. If you do not flush the cache, you might experience some runtime errors.

Using the Legacy Provider or an External Provider for Managing Passwords

By default, Identity Manager uses SSPR for password management. However, to use your existing password policies, you might want to use Identity Manager's internal legacy provider. Alternatively, you can use an external provider. For more information about configuring Identity Manager for these providers, see one of the following sections:

- "Using the Legacy Provider for Forgotten Password Management" on page 335
- "Using an External System for Forgotten Password Management" on page 336

Updating the Maximum Timeout Setting for the SharedPagePortlet

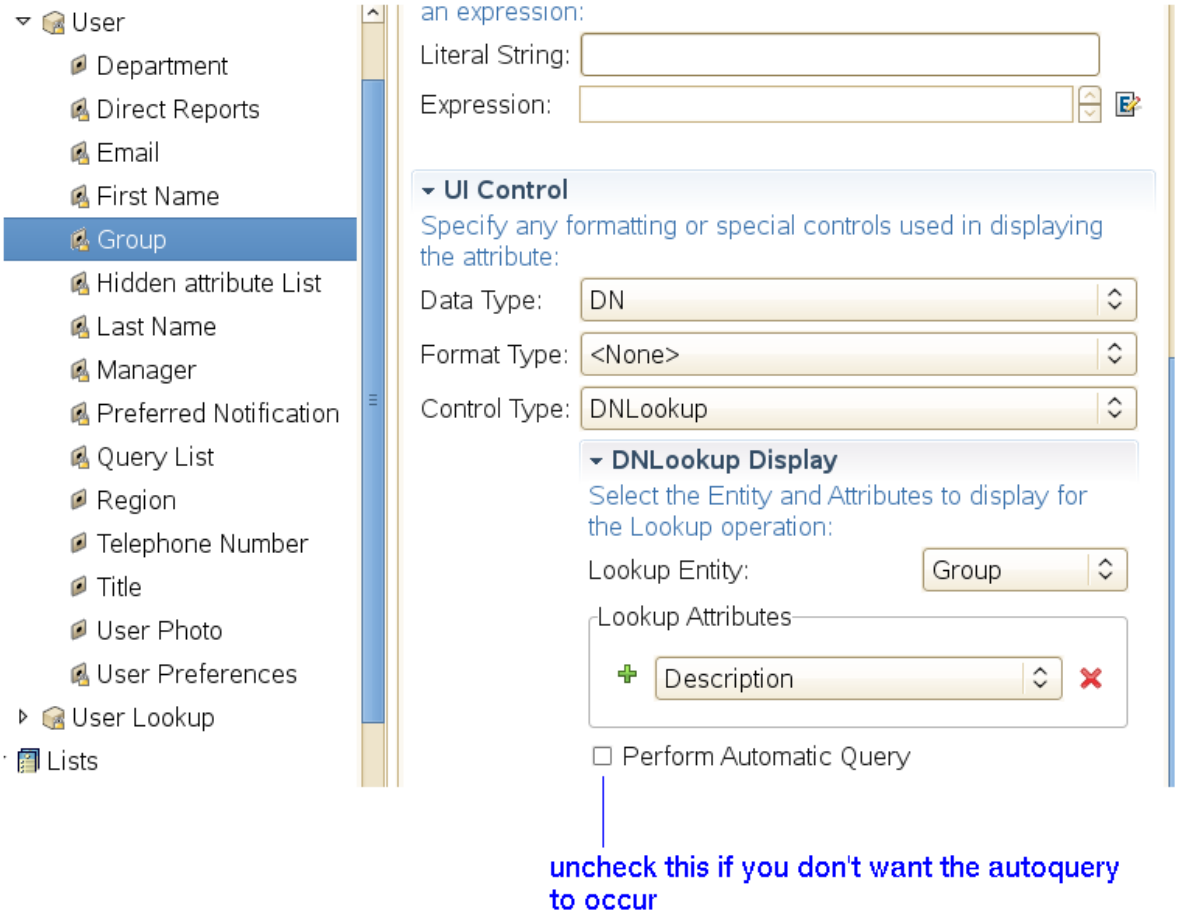
If you have customized any of the default settings or preferences for the SharedPagePortlet, then it has been saved to your database and this setting will get overwritten. As a result, navigating to the Identity Self-Service tab might not always highlight the correct Shared Page. To be sure that you do not have this problem, complete the following steps:

1. Log in as a User Application Administrator.
2. Navigate to **Administration > Portlet Administration**.
3. Expand **Shared Page Navigation**.
4. In the portlet tree on the left, click **Shared Page Navigation**.
5. On the right side of the page, click **Settings**.
6. Ensure that **Maximum Timeout** is set to 0.
7. Click **Save Settings**.

Disabling the Automatic Query Setting for Groups

By default, the DNLookup Display for the Group entity in the Directory Abstraction Layer is enabled. This means that whenever the object selector is opened for a group assignment, all the groups are displayed by default without the need to search them. You should change this setting, since the window to search for groups should be displayed without any results until the user provides input for search.

You can change this setting in Designer by unchecking **Perform Automatic Query**, as shown below:



uncheck this if you don't want the autoquery to occur

60 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.

NOTE: You must stop all services such as Tomcat, PostgreSQL, and ActiveMQ before uninstalling the Identity Manager components.

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" in the *NetIQ eDirectory Administration Guide*.

2. Log in 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.

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 "Removing Objects from the Identity Vault" on page 527.

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
```

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 in 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`*`/etc/opt/novell/eDirectory/conf/idm-uninstall`.
3. To execute the uninstallation script, enter the following command:

   ```
   ./Uninstall_Identity_Manager
   ```

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 2012 R2, click **Programs and Features**. Right-click **Identity Manager**, then click **Uninstall**.

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.

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.

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 in 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
   ```

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.

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 "Uninstalling the Identity Manager Engine" on page 527.

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.

Uninstalling the User Application on Linux/UNIX

You must uninstall the User Application and its database from Tomcat. This procedure explains how to remove the User Application and its database from Tomcat 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 Tomcat or PostgreSQL. For example, the uninstallation folder is typically `/opt/netiq/idm/apps/UserApplication`. This folder also contains the folders for Tomcat and PostgreSQL.

---

1. Log in to the server where you installed the User Application.
2. To uninstall the User Application, complete the following steps:
   - **2a** Navigate to the `Uninstall_UserApp` script, located by default in the `/opt/netiq/idm/apps/UserApplication/RemoveUserApp` directory.
   - **2b** Execute the following command:

     ```
     ./Uninstall_UserApp
     ```
3. To uninstall the database, execute the following command:

   ```
   ./Uninstall_TomcatPostgreSQL
   ```

Uninstalling the User Application on Windows

You must uninstall the User Application and its database from Tomcat. This procedure explains how to remove the User Application and its database from Tomcat 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 Tomcat or PostgreSQL. For example, the installation folder is typically `C:\NetIQ\IdentityManager\apps\UserApplication`. This folder also contains the folders for Tomcat and PostgreSQL.

---

1. Log in 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 2012 R2, click **Programs and Features**.
3. Right-click **Identity Manager User Application**, then click **Uninstall**.

Uninstalling the Identity Reporting

You must uninstall the Identity Reporting components in the following order:

1. Delete the drivers. For more information, see "Deleting the Reporting Drivers" on page 531.
2. Delete Identity Reporting. For more information, see "Uninstalling Identity Reporting" on page 531.
3. Delete Sentinel. For more information, see "Uninstalling Sentinel" on page 531.

NOTE: To conserve disk space, the installation programs for Identity Reporting 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.

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.

Uninstalling Identity Reporting

Before deleting Identity Reporting, ensure you have deleted the Data Collection and Managed System Gateway drivers. For more information, see "Deleting the Reporting Drivers" on page 531.

IMPORTANT: Before running the Identity Reporting uninstallation program, ensure you copied your generated reports from the Reporting installation directory to another location on your computer because the uninstallation process removes all the files and folders from the directory where Reporting was installed. For example, the Reporting installation folder `C:\NetIQ\IdentityManager\apps\IDMReporting` or `/opt/netiq/idm/apps/IDMReporting`.

To uninstall Identity Reporting, complete the following action for your operating system:

Linux and UNIX

Navigate to the `Uninstall_Identity Reporting` script, located by default in the `/opt/netiq/idm/apps/IDMReporting/` directory.

To execute the script, enter `./Uninstall_IdentityReporting`.

Windows

Use the Control Panel utility for adding and removing programs. For example, on Windows Server 2012 R2, click **Programs and Features**. Right-click **Identity Reporting**, then click **Uninstall**.

Uninstalling Sentinel

1. Log in to the Sentinel server.
2. Navigate to the directory containing the uninstallation script:

`/opt/novell/sentinel/setup/`

3 Execute the following command:

```
./uninstall-sentinel
```

4 When prompted to reconfirm that you want to proceed with the uninstall, press y.

The script first stops the service and then removes it completely.

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" in the *NetIQ eDirectory 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" in the *NetIQ eDirectory 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" in the *NetIQ eDirectory 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 2012 R2, click **Programs and Features**. Right-click **NetIQ 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" in the *NetIQ eDirectory Administration Guide*.

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**.

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/tomcat8/`
- `/etc/opt/novell/tomcat8/`

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.

Uninstalling iManager on Linux

The process for uninstalling iManager does not uninstall NICI. You can uninstall NICI separately, if required.

IMPORTANT: If eDirectory is installed on the same server as iManager, NICI is required to continue to run eDirectory.

---

1. Log in 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`

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 NICI 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 NICI. eDirectory requires NICI 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.

Uninstalling iManager Workstation

To uninstall iManager Workstation, delete the directory where you extracted the files.

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**.

61 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.

- "Troubleshooting the User Application and RBPM Installation" on page 535
- "Troubleshooting Uninstallation" on page 536
- "Troubleshooting Login" on page 537
- "Troubleshooting SSPR Page Request Error" on page 537
- "Troubleshooting an Issue When server.xml file Is Not Updated with a Non-Default Port Specified During Identity Reporting Installation" on page 537

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

You want to modify one or more of the following the User Application configuration settings created during installation:
◆ Identity Vault connections and certificates
◆ E-mail settings
◆ Identity Manager Engine User Identity and User Groups
◆ Access Manager or iChain settings
	Run the configuration utility independent of the installer.
	Linux: Run the following command from the installation directory (by default, `/opt/netiq/idm/apps/UserApplication/`):
	`configupdate.sh`
	Windows: Run the following command from the installation directory (by default, `C:\NetIQ\IdentityManager\apps\UserApplication\`):
	`configupdate.bat`

Starting Tomcat causes the following exception: `port 8180 already in use`	Shut down any instances of Tomcat (or other server software) that might already be running. If you reconfigure Tomcat to use a port other than 8180, edit the `config` settings for the User Application driver.
When Tomcat starts, the application reports it cannot find trusted certificates.	Ensure that you start Tomcat by using the JDK specified during the installation of the User Application.
Cannot log in to the portal admin page.	Ensure that the User Application Administrator account exists. This account is not the same as your iManager administrator account.

Issue	Suggested Actions
Cannot create new users even with administrator account.	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).
Starting application server throws keystore errors.	Your application server is not using the JDK specified during the installation of the User Application. Use the `keytool` command to import the certificate file: `keytool -import -trustcacerts -alias aliasName -file certFile -keystore ..\lib\security\cacerts -storepass changeit` ◆ Replace *aliasName* with a unique name of your choice for this certificate. ◆ Replace *certFile* with the full path and name of your certificate file. ◆ The default keystore password is `changeit` (if you have a different password, specify it).

Email notification not sent.	Run the `configupdate` utility to check whether you supplied values for the following User Application configuration parameters: **Email From** and **Email Host**.
	
	Linux: Run the following command from the installation directory (by default, `/opt/netiq/idm/apps/UserApplication/`):
	
	`configupdate.sh`
	
	Windows: Run the following command from the installation directory (by default, `C:\NetIQ\IdentityManager\apps\UserApplication\`):
	
	`configupdate.bat`

Troubleshooting Uninstallation

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
Uninstallation process reports as incomplete but the log file shows no failures.	The process failed to delete the `netiq` directory that contains the installation files by default. You can delete the directory if you have removed all NetIQ software from your computer.

Troubleshooting Login

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
User is unable to login in large scale environment (>2 million objects)	Add an index for `mail(Internet Mail Address)` attribute with the rule set as `Value` in both eDirectory master and replica servers.
When you sign out from Identity Applications page, SSPR shows an error `5053 ERROR_APP_UNAVALIABLE`.	Ignore this error. It does not cause any functionality loss.

Troubleshooting SSPR Page Request Error

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.

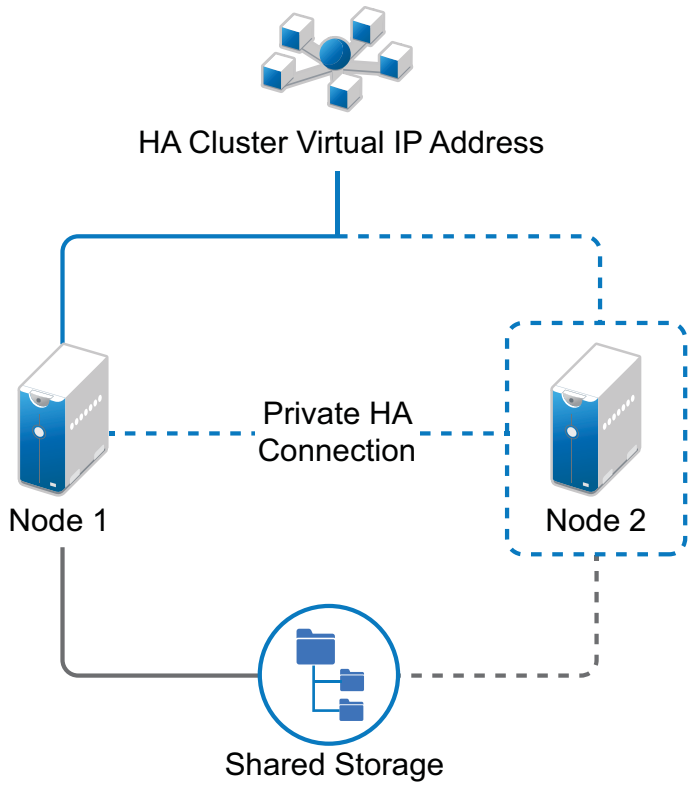
Issue	Suggested Actions
SSPR Reports Out of Order Page Request Error This issue occurs when you click the **Back** button while in an SSPR page. SSPR displays an incorrect sequence message in the SSPR error log similar to the following: `ERROR, password.pwm.servlet.TopServlet, 5035 ERROR_INCORRECT_REQUEST_SEQUENCE (expectedPageID=3, submittedPageID=4, url=<some sspr url>`	Disable the Back button detection from **SSPR Configuration Manager > Settings > Security > Web Security**. **NOTE:** Changing this setting has no effect on end users.

Troubleshooting an Issue When server.xml file Is Not Updated with a Non-Default Port Specified During Identity Reporting Installation

Issue	Suggested Actions
If you specify a different port for the Oracle database (for example,1523) than the default port (1521) when installing Identity Reporting, the new port is not written to the connection URL string in the `server.xml` file. The `sever.xml` file contains entries similar to this: `<Resource auth="Container" driverClassName="oracle.jdbc.OracleDriver" factory="com.netiq.tomcat.jdbc.pool.CustomBasicDataSourceFactory" initialSize="10" maxIdle="10" maxTotal="50" maxWaitMillis="30000" minIdle="10" name="shared/IDMRPTDataSource" password="/PiJIywBYaZA1MvOKlh5uQ==:ohTS0Kj6+PKzeEwYDkpu0A==:LhYVfBbtVivhX9IukfmuiQ==" testOnBorrow="true" type="javax.sql.DataSource" url="jdbc:oracle:thin:@192.168.32.235:1521/orcl" username="idm_rpt_data" validationInterval="120000" validationQuery="SELECT 1 from DUAL"/>` `<Resource auth="Container" driverClassName="oracle.jdbc.OracleDriver" factory="com.netiq.tomcat.jdbc.pool.CustomBasicDataSourceFactory" initialSize="10" maxIdle="10" maxTotal="50" maxWaitMillis="30000" minIdle="10" name="shared/IDMRPTCfgUpdateSource" password="SxthAeVNFznTIsmlI/Zgzw==:IpRocpIeUAETDqEc4pWArQ==:kStd+CafPm/qI9RIaGfnFA==" testOnBorrow="true" type="javax.sql.DataSource" url="jdbc:oracle:thin:@192.168.32.235:1521/orcl" username="idm_rpt_cfg" validationInterval="120000" validationQuery="SELECT 1 from DUAL"/>` `<Resource auth="Container" driverClassName="oracle.jdbc.OracleDriver" factory="com.netiq.tomcat.jdbc.pool.CustomBasicDataSourceFactory" initialSize="10" maxIdle="10" maxTotal="50" maxWaitMillis="30000" minIdle="10" name="shared/IDMRPTCfgDataSource" password="3NkqNV+halUUkP9W3A2O6A==:j4YLuRc5JShrUWurg2wQmA==:7stEUCrG7EVkSIayRU3J2A==" testOnBorrow="true" type="javax.sql.DataSource" url="jdbc:oracle:thin:@192.168.32.235:1521/orcl" username="idmrptuser" validationInterval="120000" validationQuery="SELECT 1 from DUAL"/>` `</GlobalNamingResources>`	Manually change the port in the `server.xml` file.

A Sample Identity Manager Cluster Deployment Solution on SLES

The appendix provides instructions on how to configure Identity Vault (eDirectory) and Identity Manager in an active-passive high availability (HA) mode, which allows Identity Manager to fail over to a redundant cluster node in case of hardware or software failure. The following figure represents an active-passive HA architecture:



NOTE: eDirectory does not support load balancing by using multiple cluster nodes.

For a production-level Linux 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).

This following sections provide step-by-step instructions for configuring eDirectory and Identity Manager on high availability clusters on a supported SUSE Linux Enterprise Server (SLES) cluster environment with shared storage.

- "Sample Cluster Deployment on SLES 12 SP1" on page 540
- "Sample Cluster Deployment on SLES 12 SP2" on page 549

Sample Cluster Deployment on SLES 12 SP1

Prerequisites

- Two servers running SLES 12 SP1 64-bit for nodes
- One server running SLES 12 SP1 64-bit for iSCSI Server
- SLES12 SP1 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.

Installation Procedure

This section explains the procedure to install and configure the following to set up the cluster environment. For more information about configuring the SLES High Availability Extension, download the **Guides** from **Previous Releases** > **SUSE Linux Enterprise High Availability Extension 12 SP1** on the SUSE Linux Enterprise High Availability Extension page.

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 12 SP1.

During the SLES 12 SP1 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 **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.

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.

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**.

Installing the HA Extension

To install the HA extension:

1. Go to the NetIQ Downloads website.
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.

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 Configuring the iSCSI initiator on all Nodes.

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]
```

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 in 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**.

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.

Configuring the DLM and O2CB Resources

To configure the DLM and O2CB resources on Node1:

1. Start shell and log in 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**.

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-149455400000000000000000030000002506000000f000000` as the SBD STONITH device, use `sbd -d /dev/disk/by-id/scsi 149455400000000000000000030000002506000000f000000 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:

   ```
   sbd -d /dev/sdb1 create
   ```

2. Run the `sbd -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

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
```

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.

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.

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.

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 in 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`

Mounting an OCFS2 Volume

To mount an OCFS2 volume on Node 1:

1. Start a shell and log in 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:

   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**.

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="clusteripoperations" 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
```

Installing and Configuring eDirectory and Identity Manager on Cluster Nodes

1. To install eDirectory on cluster nodes:

Install eDirectory a supported version of eDirectory. For step-by-step instructions to configure eDirectory on HA clusters, see "Deploying eDirectory on High Availability Clusters" in the *eDirectory 9.0 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 Identity Manager engine 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.

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
```

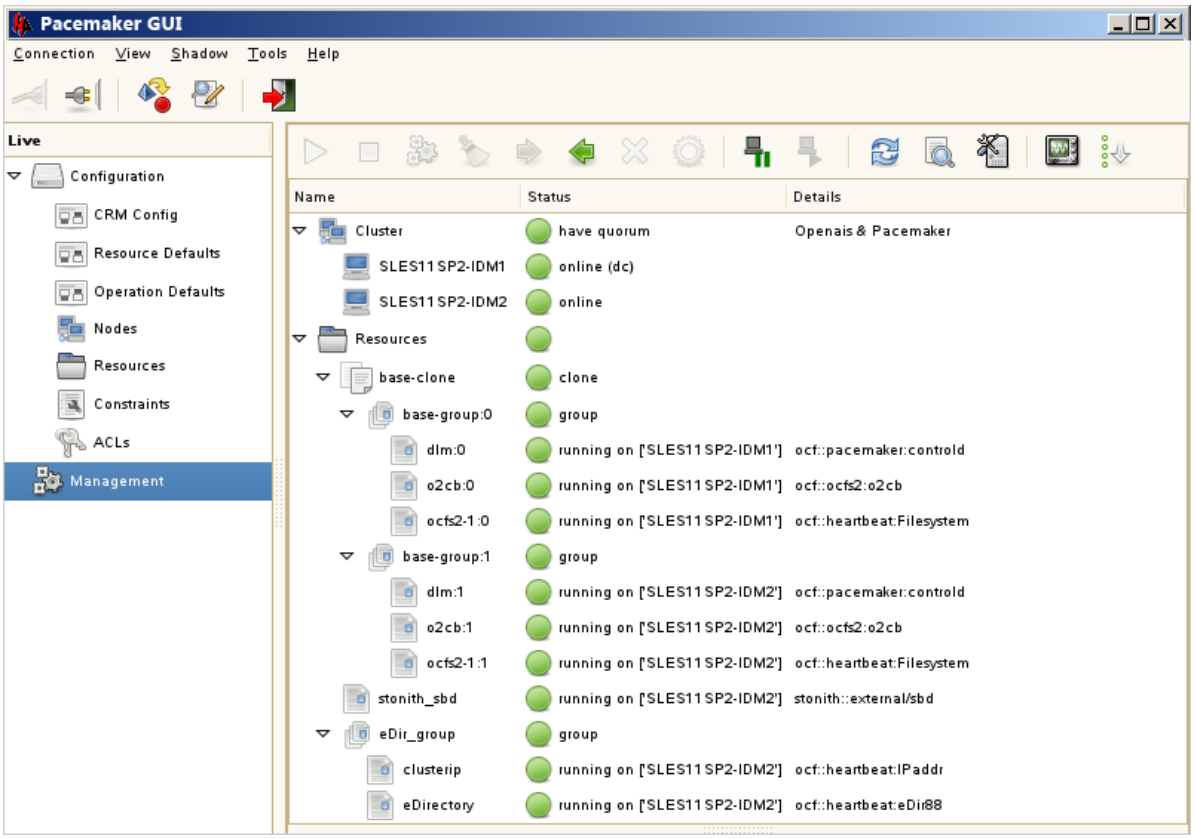
In the vi editor, modify the group, then add the text "eDirectory" after clusterip, as follows to save your changes:

```
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.



Sample Cluster Deployment on SLES 12 SP2

Prerequisites

- Two servers running SLES 12 SP2 64-bit for nodes
- One server running SLES 12 SP2 64-bit for iSCSI Server
- SLES12 SP1 64-bit HA extension ISO image file
- Six static IPs:
  - Two static IP addresses for each node.
  - 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.

Installation Procedure

This section explains the procedure to install and configure the following to set up the cluster environment. For more information about configuring the SLES High Availability Extension, see the SUSE Linux Enterprise High Availability Extension guide.

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 12 SP2.

During the SLES 12 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 **Do not mount the partition**.
5. Specify the partition size.
6. Type the `yast2 iscsi-server` or `yast2 iscsi-lio-server` command in terminal.
7. Click the **Service** tab, then select **When Booting** in the **Service Start** option.
8. In the **Targets** tab, click **Add** to enter the partition path (as created during the SLES installation).
9. In the **Modify iSCSI Target Initiator Setup** page, specify iSCSI client initiator host names for the target server and then click **Next**.

   For example, *iqn.sles12sp2node1.com* and *iqn.sles12sp2node2.com*.
10. Click **Finish**.
11. Run the `cat /proc/net/iet/volume` command in the terminal to verify if the iSCSI target is installed

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 the **Service Start** option.
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.

Partitioning the Shared Storage

Create two shared storage partitions: one for SBD and the other for Cluster File System.

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**.

Installing the HA Extension

To install the HA extension:

1 Go to the SUSE Downloads website.

SUSE Linux Enterprise High Availability Extension (SLE HA) is available for download for each available platform as two ISO images. Media 1 contains the binary packages and Media 2 contains the source code.

NOTE: Select and install the appropriate HA extension ISO file based on your system architecture.

---

2 Download the Media 1 ISO file on each server.

3 Open **YaST Control Center** dialog box, click **Add-on products > Add**.

4 Click **Browse** and select the DVD or local ISO image, then click **Next**.

5 In the **Patterns** tab, select **High Availability** under **Primary Functions**.

Ensure that all the components under high availability are installed.

6 Click **Accept**.

Setting up Softdog 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.

1. Enable the softdog watchdog:

   ```
   echo softdog > /etc/modules-load.d/watchdog.conf
   ```

   ```
   systemctl restart systemd-modules-load
   ```

2. Test if the softdog module is loaded correctly:

   ```
   lsmod | grep dog
   ```

Configuring the HA Cluster

This example assumes that you are configuring two nodes in a cluster.

Setting up the first node:

1. Log in as root to the physical or virtual machine you want to use as cluster node.
2. Run the following command:

   ```
   ha-cluster-init
   ```

   The command checks for NTP configuration and a hardware watchdog service. It generates the public and private SSH keys used for SSH access and Csync2 synchronization and starts the respective services.
3. Configure the cluster communication layer:
   - **3a** Enter a network address to bind to.
   - **3b** Enter a multicast address. The script proposes a random address that you can use as default.
   - **3c** Enter a multicast port. By default, the port is 5405.
4. Set up SBD as the node fencing mechanism:
   - **4a** Press *y* to use SBD.
   - **4b** Enter a persistent path to the partition of your block device that you want to use for SBD. The path must be consistent for both the nodes in the cluster.
5. Configure a virtual IP address for cluster administration:
   - **5a** Press *y* to configure a virtual IP address.
   - **5b** Enter an unused IP address that you want to use as administration IP for SUSE Hawk GUI. For example, *192.168.1.3*.

     Instead of logging in to an individual cluster node, you can connect to the virtual IP address.

Once the first node is up and running, add the second cluster node using the `ha-cluster-join` command.

Setting up the second node:

1. Log in as root to the physical or virtual machine through which you want to connect to the cluster.
2. Run the following command:

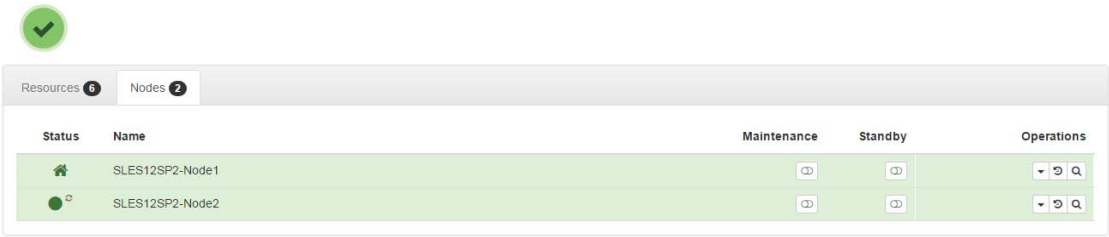
   ```
   ha-cluster-join
   ```

If NTP is not configured, a message appears. The command checks for a hardware watchdog device and notifies if it is not present.

3 Enter the IP address of the first node.

4 Enter the root password of the first node.

5 Log in to SUSE Hawk GUI and then click **Status** > **Nodes**. For example, `https://192.168.1.3:7630/cib/live`.



Installing and Configuring eDirectory and Identity Manager on Cluster Nodes

1 Install eDirectory on cluster nodes:

Install a supported version of eDirectory. For step-by-step instructions to configure eDirectory on a HA cluster, see "Deploying eDirectory on High Availability Clusters" in the *eDirectory 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 Identity Manager engine 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.

Configuring the eDirectory Resource

1 Log in to SUSE Hawk GUI.

2 Click **Add Resource** and create a new group.

2a Click ⊕ next to the **Group**.

2b Specify a group ID. For example, *Group-1*.

Ensure that the following child resources are selected when you create a group:

- *stonith-sbd*
- *admin_addr (Cluster IP address)*

3 In the **Meta Attributes** tab, set the **target-role** field to *Started* and **is-managed** field to *Yes*.

4 Click **Edit Configuration** and then click ✎ next to the group you created in Step 2.

5 In the **Children** field, add the following child resources:

- *shared-storage*
- *eDirectory-resource*

For example, the resources should be added in the following order within the group:

- *stonith-sbd*
- *admin_addr (Cluster IP address)*
- *shared-storage*
- *eDirectory-resource*

You can change the resource names if necessary. Every resource has a set of parameters that you need to define. For information about examples for shared-storage and eDirectory resources, see Primitives for eDirectory and Shared Storage Child Resources.

Primitives for eDirectory and Shared Storage Child Resources

The *stonith-sbd* and admin_addr resources are configured by HA Cluster commands by default when initializing the cluster node.

Table A-1 *Example for shared-storage*

Resource ID	Name of the shared storage resource
Class	ocf
Provider	heartbeat
Type	Filesystem
device	/dev/sdc1
directory	/shared
fstype	xfs
operations	◆ start (60, 0) ◆ stop (60, 0) ◆ monitor (40, 20)
is-managed	Yes
resource-stickiness	100
target-role	Started

Table A-2 Example for eDirectory-resource

Resource ID	Name of the eDirectory resource
Class	systemd
Type	ndsdtmpl-shared-conf-nds.conf@-shared-conf-env
operations	◆ start (100, 0) ◆ stop (100, 0) ◆ monitor (100, 60)
target-role	Started
is-managed	Yes
resource-stickiness	100
failure-timeout	125
migration-threshold	0

Change the location constraint score to 0.

1. Log in to SUSE Hawk GUI.
2. Click **Edit Configuration**.
3. In the **Constraints** tab, click ✎ next to the node 1 of your cluster.
4. In the **Simple** tab, set the score to *0*.
5. Click **Apply**.

Ensure that you set the score to *0* for all the nodes in your cluster.

NOTE: When you migrate the resources from one node to another from the SUSE Hawk GUI using the **Status** > **Resources** > **Migrate** option, the location constraint score will change to *Infinity* or *-Infintity*. This will give preference to only one of the nodes in the cluster and will result in delays in eDirectory operations.

B Sample Identity Manager Cluster Deployment Solution on Windows

This appendix provides step-by-step instructions on how to configure Identity Manager into a cluster environment on Windows 2012 R2 platform.

- "Prerequisites" on page 557
- "Configuring NetIQ Identity Manager on eDirectory Cluster" on page 557
- "Clustering Remote Loader" on page 558

Prerequisites

eDirectory 8.8.8 SP9 or 9.0.2 or later services are running in a cluster environment on Windows 2012 R2. For detailed information about setting up an eDirectory cluster, see Clustering eDirectory Services on Windows in the *NetIQ eDirectory Installation Guide*.

NOTE: eDirectory does not support load balancing by using multiple cluster nodes. eDirectory clustering is only meant for achieving failover capability.

Configuring NetIQ Identity Manager on eDirectory Cluster

This section assumes that you have already set up an eDirectory cluster.

Use the following procedure to configure Identity Manager in an eDirectory cluster environment.

1. In **Cluster Manager**, set the eDirectory clustered roles priority to **No Auto Start** on the primary node.
2. Stop the secondary node.
3. Install Identity Manager engine on the primary node by selecting the **Metadirectory Server** option in the Identity Manager installation wizard.

   IMPORTANT: Ensure that you are installing Identity Manager engine on a local storage.

   ---

4. Identity Manager installation wizard stops the eDirectory cluster role during installation. When this role is stopped, the status of this role may appear as failed. After installation, start the eDirectory cluster role from **Cluster Manager**.
5. Set the required priority for the eDirectory clustered role and make the secondary node active.
6. Install the Identity Manager engine on a secondary node using the `DCLUSTER_INSTALL` command.

   For example, `./idm_install.exe -DCLUSTER_INSTALL="true"`

Clustering Remote Loader

1. Install the Remote Loader on the primary and secondary cluster nodes.

   NOTE: For both primary and secondary node, ensure that Remote Loader is installed on the same shared storage path.

2. (Conditional) If you are using secured communications with the Remote Loader, store all the SSL certificates in a shared storage.
3. Before creating the Remote Loader cluster role, open the Remote Loader console and select **Remote Loader as a Windows Service**.
4. In **Cluster Manager > Roles**, create a new Remote Loader cluster role.

   Specify the following information for the role:

   Role Type: Generic Service

   Select Service: Remote Loader instance registered as a Windows service.

   Name: Cluster Role Name

   Address: Specify a unique IP address

   Select Storage: Shared Cluster Storage

   Replicate Registry Settings:

   1. `HKEY_LOCAL_MACHINE\SOFTWARE\Novell\RLConsole`
   2. `HKEY_LOCAL_MACHINE\SOFTWARE\Novell\DirXML Remote Loader\Command port 8000`

      Specify the registry path for the Remote Loader instance which you want to cluster.
   3. `HKEY_LOCAL_MACHINE\SOFTWARE\Novell\PassSync`

   NOTE

   - By default, each cluster role accepts only one Windows service. Therefore, specify a command port and a corresponding registry path unique to each Remote Loader instance.
   - Active Directory driver's password filter is not supported on a Windows cluster.

C Sample Identity Applications Cluster Deployment Solution on Tomcat Application Server

The appendix provides instructions on how to configure the identity applications into a cluster environment on an Apache Tomcat application server with an example deployment.

Clustering allows you to run the identity applications on several parallel servers (cluster nodes) to achieve high availability. To build a cluster, you need to group several Tomcat instances (nodes) together. The load is distributed across different servers, and even if any of the servers fail, the identity applications are accessible through other cluster nodes. For failover, you can create a cluster of the identity applications and configure them to act as a single server. However, this configuration does not include Identity Reporting.

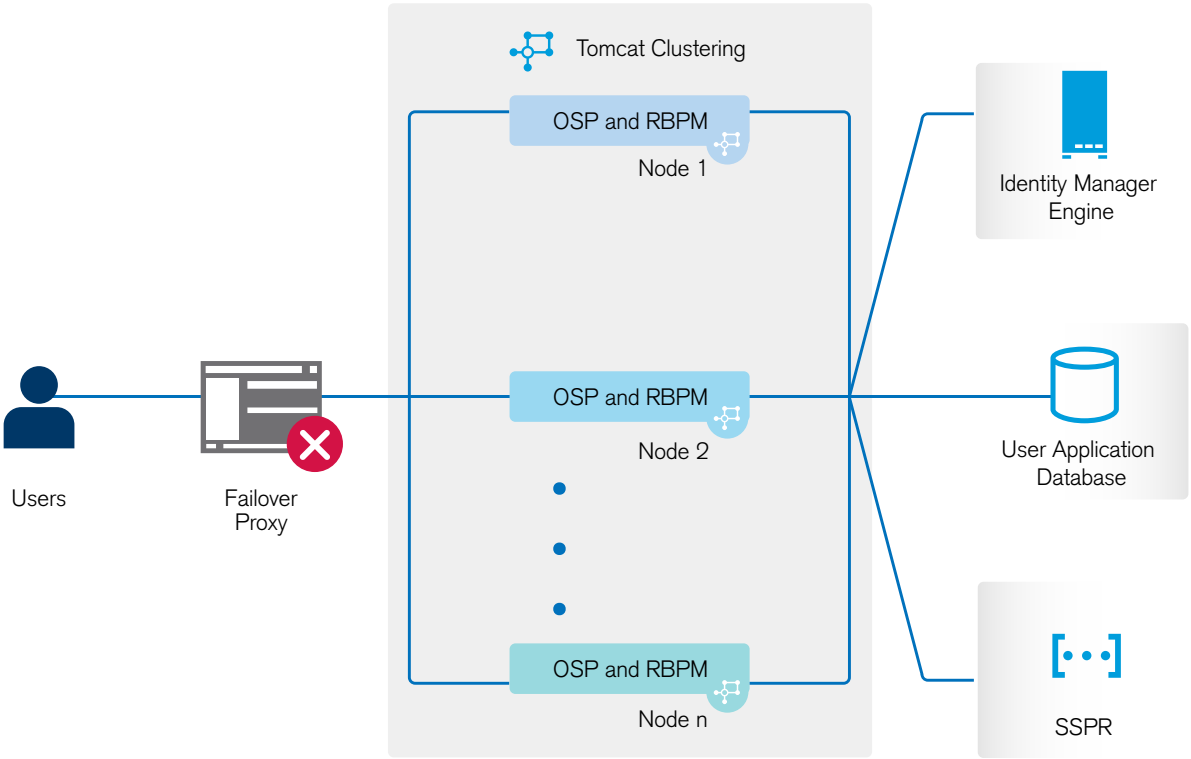
It is recommended to use a load balancer software that processes all user requests and dispatches them to the server nodes in the cluster. The load balancer is typically part of the cluster. It understands the cluster configuration as well as failover policies. You can select a solution that best suits you.

Figure C-1 shows a sample deployment with a two-node cluster with the following assumptions:

- All the communication is routed through the load balancer.
- Components such as Identity Manager engine and the User Application are installed on separate servers. This is a recommended approach for a production-level deployment.
- You are familiar with the installation procedures for eDirectory, Identity Manager engine, identity applications, Tomcat application server, and databases for the User Application.
- OSP (One Single-Sign On Provider) and User Application are installed on the same cluster node. However, you can install OSP on a different server in a production environment. In this case, you need to perform some configuration changes mentioned in "Installation Procedure" on page 561.
- SSPR (Single Sign-On Password Reset) is installed on a separate computer. For a production-level deployment, this is the recommended approach.
- PostgreSQL is used as a database for the User Application. However, you can use any of the supported databases, such as Oracle, SQL Server, or PostgreSQL.
- All the User Application nodes communicate to the same instance of eDirectory and the User Application database. Based on your requirement, you can increase the number of User Application instances.

NOTE: Be aware that eDirectory does not support load balancing by using multiple cluster nodes. eDirectory clustering is only meant for achieving failover capability.

Figure C-1 *Sample cluster deployment solution*



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.

To help you understand the step-by-step configuration, this sample deployment is referred throughout the subsequent sections of the document.

Prerequisites

- Two servers running SUSE Linux Enterprise Server (SLES) 12 SP1 64-bit, SLES 11 SP4 64-bit, or RedHat Enterprise Linux (RHEL) 6.8 64-bit for nodes installed with all the dependent libraries. For more information, see section on RHEL.
- Identity Manager 4.6 components installed.
- All the nodes have the same application server clocks. The easiest way to ensure this is to configure the nodes to use the same network time server for time synchronization using NTP.
- The cluster nodes reside in the same subnet.
- A failover proxy or a load balancing solution is installed on a separate computer.

Installation Procedure

This section provides step-by-step instructions of installing a new instance of the identity applications on Tomcat and then configuring it for clustering.

1. Install the Identity Manager 4.6 engine. For step-by-step instructions, see Chapter 7, “Planning to Install the Identity Vault,” on page 61. For a production-level deployment, it is recommended to install Identity Manager engine on a separate server.
2. Install PostgreSQL by using the convenience installer.

   Identity Manager supports PostgreSQL 9.4.10 on SLES 11 SP4 and PostgreSQL 9.6.1 on other supported platforms.

   For step-by-step instructions, see Chapter 28, “Installing PostgreSQL and Tomcat,” on page 247. For a production-level deployment, it is recommended to install PostgreSQL on a separate server.
3. Create and deploy the following drivers for the Identity Applications:
   - User Application driver
   - Roles and Resource Service driver

   For step-by-step instructions, see Chapter 38, “Creating and Deploying the Drivers for the Identity Applications,” on page 323.
4. On Node1, install the following Identity Manager components:
   a. Tomcat

      Install Tomcat by using the convenience installer and select only Tomcat during the installation process. For step-by-step instructions, see Chapter 28, “Installing PostgreSQL and Tomcat,” on page 247.

   b. OSP

      For more information about installing OSP, see Chapter 32, “Installing Password Management for Identity Manager,” on page 267.

      During the installation process, provide the IP address and port number of the Identity Manager engine (eDirectory) server in the Authentication details page.

   c. User Application

      During the installation process, configure the following settings:

      i. Select **Tomcat** as the application server.

      ii. Select **PostgreSQL** as the database platform.

      > **NOTE:** You can use any of the Identity Manager 4.6 supported databases.

      iii. Provide the required database details in the subsequent pages.

      iv. Copy the database driver file, `postgresql-9.4.1212jdbc42.jar` file from the PostgreSQL server to all the User application nodes in the cluster.

      > **NOTE:** If you are using other supported databases, such as Oracle or SQL Server, ensure that you copy the respective driver jar files from the server where the database is installed to all the User Application nodes in the cluster. For more information, see Chapter 35, “Configuring the Database for the Identity Applications,” on page 295.

      v. Browse and select the copied database driver jar file.

      vi. In the New Database or Existing Database details page, select the **New Database** option.

vii. In the Identity Manager Configuration page, provide a unique name in the **Workflow Engine ID** field. For example, you can use the unique name as Engine1 for Node1.

viii. To create a new master key, select **No** in the Security – Master Key page.

The identity applications encrypt sensitive data using a master key. As this is the first instance of the identity applications in a cluster; therefore, you must instruct the installation program to create a new master key by selecting **No**. In a cluster, the User Application clustering requires every instance of the User Application to use the same master key. To ensure that the same master key is used, import the existing key by selecting **Yes** while configuring these instances.

NOTE: For detailed instructions and more information to install the User Application, see Chapter 37, "Installing the Identity Applications," on page 303.

---

5. On Node2, perform the following actions:

a. Install Tomcat by using the convenience installer (select only Tomcat during the installation process).

For step-by-step instructions, see Chapter 28, "Installing PostgreSQL and Tomcat," on page 247.

b. Install OSP.

For more information on installing OSP, seeChapter 32, "Installing Password Management for Identity Manager," on page 267.

During the installation process, provide the IP address and port number of the Identity Manager engine (eDirectory) server in the Authentication details page.

c. Install the User Application.

During the installation process, configure the following settings:

i. Select **Tomcat** as the application server.

ii. Select **PostgreSQL** as the database platform.

NOTE: You can use any supported database.

---

iii. Provide the required database details in the subsequent pages of the installation procedure.

iv. Copy `postgresql-9.4.1212jdbc42.jar` database driver jar file from the PostgreSQL server to Node2.

NOTE: If you are using any other Identity Manager 4.5.1 supported databases, such as Oracle or SQL Server, ensure that you copy the respective driver jar files from the server where the database is installed to all the User application nodes in the cluster. For more information, seeChapter 35, "Configuring the Database for the Identity Applications," on page 295.

---

v. Browse and select the copied database driver jar file.

vi. In the New Database or Existing Database details page, select the **Existing Database** option.

vii. In the Identity Manager Configuration page, provide a unique name in the **Workflow Engine ID** field. For example, you can use the unique name as Engine2 for Node2.

viii. To create a new Master key in the Security – Master Key page, select **Yes**.

The User Application clustering requires every instance of the User Application to use the same master key. To ensure that the same master key is used, import the existing key by selecting **Yes**. This key is created when you installed the first instance of the User Application in Node1.

You can obtain the master key from the ism-configuration properties file located in `/TOMCAT_INSTALLED_HOME/conf/` on Node1. The parameter that contains the master key is `com.novell.idm.masterkey`.

ix. Click **Install** to complete the installation.

NOTE: For detailed information about installing the User Application, see Chapter 37, "Installing the Identity Applications," on page 303.

---

6. Install SSPR on a separate computer.

   Before installing, make a note of the following settings and specify them during installation process:

   a. Install **Tomcat**. For installation instructions, see Step 4a.

   b. Install **SSPR**.

      During the SSPR installation, perform the following actions:

      i. In the Application Server connection page, select **Connect to external authentication server** and provide the DNS name of the server where the load balancer is installed.

      ii. In the Authentication details page, provide the **IP address** and the **port** of the Identity Manager engine server. The password for the CA certificates is 'changeit'.

   c. After completing the SSPR installation, start Tomcat and launch SSPR (`http://<IP>:<port>/sspr/private/config/ConfigEditor`) and log in. Click **Configuration Editor** > **Settings** > **Security** > **Redirect Whitelist**.

      i. Click **Add value** and specify the following URL:

         OSP: `http://<dns of the failover>:<port>/osp`

      ii. Save the changes.

      iii. In the SSPR Configuration page, click **Settings** > **OAuth SSO** and modify the OSP links by replacing the IP addresses with the DNS name of the server where the load balancer software is installed.

      iv. Click **Settings** > **Application** and update the forward and logout URLs by replacing the IP addresses with the DNS name of the server where the load balancer software is installed.

   d. To update the SSPR information on Node1, launch the Configuration utility located at `/opt/netiq/idm/apps/UserApplication/configupdate.sh`.

      In the window that opens, click **SSO clients** > **Self Service Password Reset** and enter values for **Client ID**, **Password**, and **OSP Auth redirect URL** parameters.

NOTE: Verify that the values for these parameters are updated in Node2.

---

7. Perform the following configuration tasks on the cluster nodes:

   a. Restart Tomcat on all the cluster nodes.

   b. To update the Forgot Password link with the SSPR IP address, log in to the User Application on Node1 and click **Administration** > **Forgot Password**.

      For more information on SSPR configuration, see "Configuring Forgotten Password Management" on page 333.

c. To change the Change my password link, see "Updating SSPR Links in the Dashboard for a Distributed or Clustered Environment" on page 338.

d. Verify that the Forgot Password link and Change my password links are updated with the SSPR IP address on Node2.

NOTE: If the Change Password and Forgot Password links are already updated with the SSPR IP address, no changes are required.

---

8. In Node1, stop Tomcat and generate a new `osp.jks` file by specifying the DNS name of the load balancer server by using the following command:

   ```
   /opt/netiq/idm/jre/bin/keytool -genkey -keyalg RSA -keysize 2048 -keystore osp.jks -storepass <password> -keypass <password> -alias osp -validity 1800 -dname "cn=<loadbalancer IP/DNS>"
   ```

   For example: `/opt/netiq/idm/jre/bin/keytool -genkey -keyalg RSA -keysize 2048 -keystore osp.jks -storepass changeit -keypass changeit -alias osp -validity 1800 -dname "cn=mydnsname"`

NOTE: Ensure that the key password is the same as the one provided during OSP installation. Alternatively, this can also be changed using Configuration Update utility including the keystore password.

---

9. (Conditional) To verify if the `osp.jks` file is updated with the changes, run the following command:

   ```
   /opt/netiq/idm/jre/bin/keytool -list -v -keystore osp.jks -storepass changeit
   ```

10. Take backup of the original `osp.jks` file located at `/opt/netiq/idm/apps/osp_sspr/osp/` and copy the new `osp.jks` file to this location. The new `osp.jks` file was created in Step 8.

11. Copy the new `osp.jks` file located at `/opt/netiq/idm/apps/osp_sspr/osp/` from Node1 to other User Application nodes in the cluster.

12. Launch the Configuration utility in Node1 and change all of the URL settings, such as URL link to landing page and OAuth redirect URL to the load balancer DNS name under the SSO Client tab.

    a. Save the changes in the Configuration utility.

    b. To reflect this change in all other nodes of the cluster, copy the ism-configuration properties file located in `/TOMCAT_INSTALLED_HOME/conf` from Node1 to other User Application nodes in the cluster.

NOTE: You copied the `ism.properties` file from Node1 to the other nodes in the cluster. If you specified custom installation paths during the User Application installation, ensure that referential paths are corrected by using Configuration update utility in the cluster nodes.

In this scenario, both OSP and User Application are installed on the same server; therefore, the same DNS name is used for redirect URLs.

If OSP and User Application are installed on separate servers, change the OSP URLs to a different DNS name pointing to the load balancer. Do this for all the servers where OSP is installed. Doing this ensures that all OSP requests are dispatched through load balancer to the OSP cluster DNS name. This involves having a separate cluster for OSP nodes.

---

13. Perform the following actions in the `setenv.sh` file located at `/TOMCAT_INSTALLED_HOME/bin/` directory:
    a. To ensure that the mcast_addr binding is successful, JGroups requires that the `preferIPv4Stack property` be set to **true**. To do so, add the JVM property "-Djava.net.preferIPv4Stack=true" in the `setenv.sh` file in all nodes.
    b. Add `-Dcom.novell.afw.wf.Engine-id=`*`"Engine1"`* in the `setenv.sh` file on Node1. Similarly, add a unique engine name for each node of the cluster. For example, for Node2, you can add the engine name as *`Engine2`*.
14. Enable clustering in the User Application.
    a. Start Tomcat on Node1.

       Do not start any other servers.
    b. Log in to the User Application as a User Application administrator.
    c. Click the **Administration** tab.

       The User Application displays the Application Configuration portal.
    d. Click **Caching**.

       The User Application displays the Caching Management page.
    e. Select **True** for the **Cluster Enabled** property.
    f. Click **Save**.
    g. Restart Tomcat.

NOTE: If you have selected Enable Local settings, repeat this procedure for each server in the cluster.

The User Application cluster uses JGroups for cache synchronization across nodes using default UDP. In case you want to change this protocol to use TCP, see Portal Configuration Tasks in NetIQ Analyzer for Identity Manager Administration Guide.

---

15. Enable the permission index for clustering.
    a. Log in to iManager on Node1 and navigate to **View Objects**.
    b. Under **System**, navigate to the driver set containing the User Application driver.
    c. Select **AppConfig** > **AppDefs > > Configuration**
    d. Select the XMLData attribute and set the `com.netiq.idm.cis.clustered` property to **true**.

       For example:

       ```
       <property>
       <key>com.netiq.idm.cis.clustered</key>
       <value>true</value>
       </property>
       ```
    e. Click **OK**.
16. Enable Tomcat cluster.

    Open the Tomcat `server.xml` file from `/TOMCAT_INSTALLED_HOME/conf/` and uncomment this line in this file on all the cluster nodes:

    ```
    <Cluster className="org.apache.catalina.ha.tcp.SimpleTcpCluster"/>
    ```

    For advanced Tomcat clustering configuration, follow the steps from https://tomcat.apache.org/tomcat-8.5-doc/cluster-howto.html.
17. Restart Tomcat on all the nodes.

18. Configure the User Application Driver for clustering.

    In a cluster, the User Application driver must be configured to use the DNS name of the load balancer for the cluster. You configure the User Application driver using iManager.

    a. Log in to iManager that manages your Identity Manager engine.
    b. Click the **Identity Manager node** in the iManager navigation frame.
    c. Click **Identity Manager Overview.**
    d. Use the search page to display the Identity Manager Overview for the driver set that contains your User Application driver and Roles and Resource Service Driver.
    e. Click the round status indicator in the upper right corner of the driver icon:

       A menu is displayed that lists commands for starting and stopping the driver, and editing driver properties.
    f. Select **Edit Properties**.
    g. In the Driver Parameters section, change **Host** to the host name or IP address of the dispatcher.
    h. Click **OK**.
    i. Restart the driver.
19. To change the URL of Roles and Resource Service Driver, repeat steps from 18a to 18f and click **Driver Configuration** and update the **User application URL** with the load balancer DNS name.
20. Ensure session stickiness is enabled for the cluster created in the load balancer software for the User Application nodes.
21. Configure client settings on Identity Manager dashboard. For more information, see Configuring Client Settings Mode in the NetIQ Identity Manager - Administrator's Guide to the Identity Applications.

Most loadbalancers provide a healthcheck feature for determining whether an HTTP server is up and listening. The User Application contains a URL that can be used for configuring HTTP healthchecks on your loadbalancer. The URL is:

```
http://<NodeIP>:port/IDMProv/jsps/healthcheck.jsp
```