

# **User Application: User Guide**

## **Identity Manager Roles Based Provisioning**

### **Module 4.0.2**

October 2013

## Legal Notices

Novell, Inc. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc. makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. See the [Novell International Trade Services Web page \(http://www.novell.com/info/exports/\)](http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Copyright © 2013 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

Novell, Inc.  
1800 South Novell Place  
Provo, UT 84606  
U.S.A.  
[www.novell.com](http://www.novell.com)

*Online Documentation:* To access the latest online documentation for this and other Novell products, see [the Novell Documentation Web page \(http://www.netiq.com/documentation\)](http://www.netiq.com/documentation).

## Novell Trademarks

For Novell trademarks, see [the Novell Trademark and Service Mark list \(http://www.novell.com/company/legal/trademarks/tmlist.html\)](http://www.novell.com/company/legal/trademarks/tmlist.html).

## Third-Party Materials

All third-party trademarks are the property of their respective owners.

---

# Contents

|   |           |
|---|-----------|
| <b>About This Guide</b>                                 | <b>11</b> |
| <b>Part I Welcome to Identity Manager</b>               | <b>13</b> |
| <b>1 Getting Started</b>                                | <b>15</b> |
| 1.1 Identity Manager and You                            | 15        |
| 1.1.1 Introducing the Identity Manager User Application | 15        |
| 1.1.2 The Big Picture                                   | 17        |
| 1.1.3 Typical Uses                                      | 17        |
| 1.2 Accessing the Identity Manager User Application     | 19        |
| 1.2.1 Your User Application Might Look Different        | 20        |
| 1.3 Logging In  | 20        |
| 1.3.1 If You Forget Your Password                       | 21        |
| 1.3.2 If You Have Trouble Logging In                    | 22        |
| 1.3.3 If You're Prompted for Additional Information     | 22        |
| 1.4 Exploring the User Application                      | 22        |
| 1.4.1 Getting Help                                      | 23        |
| 1.4.2 Preferred Locale                                  | 24        |
| 1.4.3 Logging Out                                       | 24        |
| 1.4.4 Common User Actions                               | 24        |
| 1.5 What's Next   | 29        |
| <b>Part II Using the Identity Self-Service Tab</b>      | <b>31</b> |
| <b>2 Introducing the Identity Self-Service Tab</b>      | <b>33</b> |
| 2.1 About the Identity Self-Service Tab                 | 33        |
| 2.2 Accessing the Identity Self-Service Tab             | 33        |
| 2.3 Exploring the Tab's Features                        | 34        |
| 2.4 Identity Self-Service Actions You Can Perform       | 35        |
| <b>3 Using the Organization Chart</b>                   | <b>39</b> |
| 3.1 About the Organization Chart                        | 39        |
| 3.2 Navigating the Chart                                | 42        |
| 3.2.1 Navigating to the Next Higher Level               | 42        |
| 3.2.2 Resetting the Root of the Relationship            | 43        |
| 3.2.3 Switching the Default Relationship                | 44        |
| 3.2.4 Expanding or Collapsing the Default Chart         | 44        |
| 3.2.5 Choosing a Relationship to Expand or Collapse     | 45        |
| 3.2.6 Looking Up a User in Organization Chart           | 47        |
| 3.3 Displaying Detailed Information                     | 48        |
| 3.4 Sending E-Mail from a Relationship Chart            | 49        |
| 3.4.1 E-Mailing Information About a User in a Chart     | 49        |
| 3.4.2 Sending New E-Mail to a User in the Chart         | 50        |
| 3.4.3 Sending E-Mail to a Manager's Team                | 51        |

|          |  |           |
|----------|--|-----------|
| <b>4</b> | <b>Using the Associations Report</b>                   | <b>53</b> |
| 4.1      | About the Associations Report . . . . .                | 53        |
| 4.2      | Displaying Associations . . . . .                      | 54        |
| <b>5</b> | <b>Using My Profile</b>                                | <b>57</b> |
| 5.1      | About My Profile . . . . .                             | 57        |
| 5.2      | Editing Your Information . . . . .                     | 58        |
| 5.2.1    | Hiding Information . . . . .                           | 59        |
| 5.2.2    | Using the Editing Buttons . . . . .                    | 59        |
| 5.3      | E-Mailing Your Information . . . . .                   | 63        |
| 5.4      | Displaying Your Organization Chart . . . . .           | 64        |
| 5.5      | Linking to Other Users or Groups . . . . .             | 65        |
| 5.6      | Choosing a Preferred Language . . . . .                | 69        |
| 5.6.1    | Defining a Preferred Language in the Browser . . . . . | 70        |
| <b>6</b> | <b>Using Directory Search</b>                          | <b>71</b> |
| 6.1      | About Directory Search . . . . .                       | 71        |
| 6.2      | Performing Basic Searches . . . . .                    | 74        |
| 6.3      | Performing Advanced Searches . . . . .                 | 74        |
| 6.3.1    | Selecting an Expression . . . . .                      | 77        |
| 6.3.2    | Specifying a Value for Your Comparison . . . . .       | 79        |
| 6.4      | Working with Search Results . . . . .                  | 83        |
| 6.4.1    | About Search Results . . . . .                         | 84        |
| 6.4.2    | Using the Search List . . . . .                        | 85        |
| 6.4.3    | Other Actions You Can Perform . . . . .                | 87        |
| 6.5      | Using Saved Searches . . . . .                         | 89        |
| 6.5.1    | To List Saved Searches . . . . .                       | 89        |
| 6.5.2    | To Run a Saved Search . . . . .                        | 89        |
| 6.5.3    | To Edit a Saved Search . . . . .                       | 89        |
| 6.5.4    | To Delete a Saved Search . . . . .                     | 90        |
| <b>7</b> | <b>Performing Password Management</b>                  | <b>91</b> |
| 7.1      | About Password Management . . . . .                    | 91        |
| 7.2      | Password Challenge Response . . . . .                  | 92        |
| 7.3      | Password Hint Change . . . . .                         | 92        |
| 7.4      | Change Password . . . . .                              | 93        |
| 7.5      | Password Policy Status . . . . .                       | 95        |
| 7.6      | Password Sync Status . . . . .                         | 95        |
| <b>8</b> | <b>Creating Users or Groups</b>                        | <b>97</b> |
| 8.1      | About Creating Users or Groups . . . . .               | 97        |
| 8.2      | Creating a User . . . . .                              | 97        |
| 8.3      | Creating a Group . . . . .                             | 99        |
| 8.4      | Using the Editing Buttons . . . . .                    | 101       |
| 8.4.1    | To Look Up a Container . . . . .                       | 101       |
| 8.4.2    | To Look Up a User . . . . .                            | 103       |
| 8.4.3    | To Use the History List . . . . .                      | 104       |

**Part III Using the Work Dashboard Tab 107**

**9 Introducing the Work Dashboard Tab 109**

- 9.1 About the Work Dashboard Tab . . . . . 109
- 9.2 Accessing the Work Dashboard Tab . . . . . 109
- 9.3 Exploring the Tab's Features . . . . . 110
- 9.4 Work Dashboard Actions You Can Perform . . . . . 112
- 9.5 Understanding the Icons on the Work Dashboard . . . . . 113
- 9.6 Security Permissions for the Work Dashboard . . . . . 115
  - 9.6.1 User Self-Service . . . . . 116
  - 9.6.2 Domain Administrator in Manage Mode . . . . . 117
  - 9.6.3 Domain Manager in Manage Mode . . . . . 120
  - 9.6.4 Team Manager in Manage Mode . . . . . 122

**10 Managing Your Work 125**

- 10.1 Working with Tasks . . . . . 125
  - 10.1.1 Viewing the Task List . . . . . 126
  - 10.1.2 Viewing the Summary for a Task . . . . . 128
  - 10.1.3 Selecting a Task . . . . . 128
  - 10.1.4 Claiming a Task . . . . . 132
  - 10.1.5 Reassigning a Task . . . . . 136
  - 10.1.6 Releasing a Task . . . . . 136
  - 10.1.7 Filtering the Task List . . . . . 137
  - 10.1.8 Customizing the Task Columns . . . . . 138
  - 10.1.9 Controlling Whether the Task List is Expanded by Default . . . . . 139
  - 10.1.10 Controlling the Display of Task Details . . . . . 140
  - 10.1.11 Setting the Claim Action for Open Tasks . . . . . 141
  - 10.1.12 Sorting the Task List . . . . . 142
  - 10.1.13 Refreshing the Task List . . . . . 143
  - 10.1.14 Controlling the Number of Items Displayed on a Page . . . . . 143
  - 10.1.15 Viewing the Comments for a Task . . . . . 143
- 10.2 Working with Resources . . . . . 143
  - 10.2.1 Viewing Your Resource Assignments . . . . . 144
  - 10.2.2 Requesting a Resource Assignment . . . . . 146
  - 10.2.3 Refreshing the Resource Assignment List . . . . . 147
  - 10.2.4 Removing a Resource Assignment . . . . . 147
  - 10.2.5 Customizing the Resource Assignment List Display . . . . . 148
  - 10.2.6 Printing the List of Resource Assignments . . . . . 149
- 10.3 Working with Roles . . . . . 151
  - 10.3.1 Viewing Your Role Assignments . . . . . 152
  - 10.3.2 Requesting a Role . . . . . 154
  - 10.3.3 Refreshing the Role Assignment List . . . . . 155
  - 10.3.4 Removing a Role Assignment . . . . . 155
  - 10.3.5 Customizing the Role Assignment List Display . . . . . 155
  - 10.3.6 Printing the List of Role Assignments . . . . . 156
- 10.4 Viewing Your Request Status . . . . . 159
  - 10.4.1 Viewing the Request List . . . . . 160
  - 10.4.2 Viewing the Summary for a Request . . . . . 165
  - 10.4.3 Filtering the Request List . . . . . 165
  - 10.4.4 Customizing the Request Status Columns . . . . . 167
  - 10.4.5 Controlling the Number of Items Displayed on a Page . . . . . 168
  - 10.4.6 Controlling the Display of Request Status Details . . . . . 168
  - 10.4.7 Sorting the Request List . . . . . 169
  - 10.4.8 Refreshing the Request List . . . . . 169
  - 10.4.9 Viewing the Comments for a Request . . . . . 169
  - 10.4.10 Viewing the Details for a Request . . . . . 170

|                |   |            |
|----------------|---|------------|
| 10.4.11        | Retracting a Request . . . . .  | 170        |
| <b>11</b>      | <b>Managing Work for Users, Groups, Containers, Roles, and Teams</b>  | <b>173</b> |
| 11.1           | Selecting a User, Group, Container, Role, or Team . . . . .           | 173        |
| 11.2           | Changing to a Different Managed Entity . . . . .                      | 176        |
| 11.3           | Minimizing the Screen Space Used by The User Profile Section. . . . . | 176        |
| 11.4           | Exiting Manage Mode . . . . .   | 177        |
| <b>12</b>      | <b>Controlling Your Settings</b>                                      | <b>179</b> |
| 12.1           | About the Settings Menu . . . . .                                     | 179        |
| 12.1.1         | About Proxies and Delegates . . . . .                                 | 179        |
| 12.1.2         | Sample Usage Scenarios . . . . .                                      | 180        |
| 12.1.3         | User Access to the Settings Menu. . . . .                             | 180        |
| 12.2           | Acting as a Proxy . . . . .   | 183        |
| 12.3           | Specifying Your Availability . . . . .                                | 184        |
| 12.3.1         | Setting Your Availability Status . . . . .                            | 184        |
| 12.3.2         | Creating or Editing an Availability Setting . . . . .                 | 186        |
| 12.3.3         | Deleting an Availability Setting . . . . .                            | 189        |
| 12.4           | Viewing and Editing Your Proxy Assignments . . . . .                  | 190        |
| 12.4.1         | Displaying Your Proxy Settings . . . . .                              | 190        |
| 12.4.2         | Creating or Editing Proxy Assignments . . . . .                       | 190        |
| 12.4.3         | Deleting Proxy Assignments . . . . .                                  | 191        |
| 12.5           | Viewing and Editing Your Delegate Assignments . . . . .               | 192        |
| 12.5.1         | Displaying Your Delegate Settings . . . . .                           | 192        |
| 12.5.2         | Creating or Editing Delegate Assignments . . . . .                    | 193        |
| 12.5.3         | Deleting a Delegate Assignment . . . . .                              | 195        |
| 12.6           | Viewing and Editing Your Team Proxy Assignments. . . . .              | 195        |
| 12.7           | Viewing and Editing Your Team Delegate Assignments . . . . .          | 199        |
| 12.8           | Specifying Your Team's Availability . . . . .                         | 203        |
| 12.9           | Making a Team Process Request . . . . .                               | 206        |
| <b>13</b>      | <b>Making a Process Request</b>                                       | <b>209</b> |
| 13.1           | About Process Requests . . . . .                                      | 209        |
| 13.2           | Making a Process Request . . . . .                                    | 210        |
| 13.3           | Deep Linking to a Request. . . . .                                    | 213        |
| <b>14</b>      | <b>Launching the Identity Reporting Module</b>                        | <b>215</b> |
| 14.1           | About the Identity Reporting Module . . . . .                         | 215        |
| 14.2           | Accessing the Reporting Module . . . . .                              | 215        |
| <b>Part IV</b> | <b>Using the Roles and Resources Tab</b>                              | <b>217</b> |
| <b>15</b>      | <b>Introducing Roles and Resources</b>                                | <b>219</b> |
| 15.1           | About the Roles and Resources Tab . . . . .                           | 219        |
| 15.1.1         | About Roles . . . . .   | 220        |
| 15.1.2         | About Resources . . . . .   | 225        |
| 15.2           | Accessing the Roles and Resources Tab . . . . .                       | 227        |
| 15.3           | Exploring the Tab's Features . . . . .                                | 227        |
| 15.4           | Roles and Resources Actions You Can Perform . . . . .                 | 228        |
| 15.5           | Understanding the Icons Used on the Roles and Resources Tab . . . . . | 229        |

|           |   |            |
|-----------|---|------------|
| <b>16</b> | <b>Managing Roles in the User Application</b>                     | <b>233</b> |
| 16.1      | Browsing the Role Catalog . . . . .                               | 233        |
| 16.1.1    | Viewing Roles . . . . .   | 233        |
| 16.1.2    | Creating New Roles . . . . .                                      | 235        |
| 16.1.3    | Editing an Existing Role . . . . .                                | 244        |
| 16.1.4    | Deleting Roles . . . . .  | 245        |
| 16.1.5    | Assigning Roles . . . . .   | 246        |
| 16.1.6    | Refreshing the Role List . . . . .                                | 249        |
| 16.1.7    | Customizing the Role List Display . . . . .                       | 249        |
| <br>      |   |            |
| <b>17</b> | <b>Managing Resources in the User Application</b>                 | <b>251</b> |
| 17.1      | Browsing the Resource Catalog . . . . .                           | 251        |
| 17.1.1    | Viewing Resources . . . . .                                       | 251        |
| 17.1.2    | Creating New Resources . . . . .                                  | 253        |
| 17.1.3    | Editing an Existing Resource . . . . .                            | 266        |
| 17.1.4    | Deleting Resources . . . . .                                      | 267        |
| 17.1.5    | Assigning Resources . . . . .                                     | 267        |
| 17.1.6    | Refreshing the Resource List . . . . .                            | 269        |
| 17.1.7    | Customizing the Resource List Display . . . . .                   | 269        |
| <br>      |   |            |
| <b>18</b> | <b>Managing Separation of Duties in the User Application</b>      | <b>271</b> |
| 18.1      | Browsing the SoD Catalog . . . . .                                | 271        |
| 18.1.1    | Viewing Separation of Duties Constraints . . . . .                | 271        |
| 18.1.2    | Creating New Separation of Duties Constraints . . . . .           | 273        |
| 18.1.3    | Editing an Existing Separation of Duties Constraint . . . . .     | 274        |
| 18.1.4    | Deleting Separation of Duties Constraints . . . . .               | 274        |
| 18.1.5    | Refreshing the Separation of Duties Constraint List . . . . .     | 274        |
| <br>      |   |            |
| <b>19</b> | <b>Creating and Viewing Reports</b>                               | <b>275</b> |
| 19.1      | About the Role Reporting Actions . . . . .                        | 275        |
| 19.2      | Role Reports . . . . .  | 275        |
| 19.2.1    | The Role List Report . . . . .                                    | 275        |
| 19.2.2    | The Role Assignment Report . . . . .                              | 277        |
| 19.3      | SoD Reports . . . . .   | 279        |
| 19.3.1    | SoD Constraint Report . . . . .                                   | 279        |
| 19.3.2    | SoD Violations and Exceptions Report . . . . .                    | 280        |
| 19.4      | User Reports . . . . .  | 281        |
| 19.4.1    | User Roles Report . . . . .                                       | 281        |
| 19.4.2    | User Entitlements Report . . . . .                                | 283        |
| <br>      |   |            |
| <b>20</b> | <b>Configuring the Role and Resource Settings</b>                 | <b>287</b> |
| 20.1      | About the Configure Roles and Resources Settings Action . . . . . | 287        |
| 20.2      | Configuring the Roles Settings . . . . .                          | 288        |
| 20.3      | Configuring the Resources Settings . . . . .                      | 288        |
| 20.4      | Configuring the Entitlement Query Settings . . . . .              | 289        |
| 20.5      | Configuring the Separation of Duties Settings . . . . .           | 289        |
| 20.6      | Configuring the Report Settings . . . . .                         | 290        |

**Part V Using the Compliance Tab 291**

**21 Introducing the Compliance Tab 293**

- 21.1 About the Compliance Tab . . . . . 293
  - 21.1.1 About Compliance and Attestation . . . . . 294
- 21.2 Accessing the Tab . . . . . 296
- 21.3 Exploring the Tab's Features . . . . . 296
- 21.4 Compliance Actions You Can Perform . . . . . 297
- 21.5 Understanding the Attestation Requests Legend . . . . . 298
- 21.6 Common Compliance Actions . . . . . 300
  - 21.6.1 Specifying the Label and Description for a Request . . . . . 300
  - 21.6.2 Defining the Attesters . . . . . 300
  - 21.6.3 Specifying the Deadline . . . . . 301
  - 21.6.4 Defining the Attestation Form . . . . . 302
  - 21.6.5 Submitting an Attestation Request . . . . . 303
  - 21.6.6 Saving Request Details . . . . . 304
  - 21.6.7 Using a Saved Request . . . . . 305

**22 Making Attestation Requests 307**

- 22.1 About the Attestation Requests Actions . . . . . 307
- 22.2 Requesting User Profile Attestation Processes . . . . . 307
- 22.3 Requesting SoD Violation Attestation Processes . . . . . 309
- 22.4 Requesting Role Assignment Attestation Processes . . . . . 311
- 22.5 Requesting User Assignment Attestation Process . . . . . 313
- 22.6 Checking the Status of Your Attestation Requests . . . . . 315

**Part VI Appendixes 323**

**A Using the Identity Manager Approvals App 325**

- A.1 Product Requirements . . . . . 325
- A.2 Installing the Approvals App . . . . . 326
- A.3 Configuring the Approvals App . . . . . 326
  - A.3.1 Requesting Mobile Access Through the User Application . . . . . 326
  - A.3.2 Using a Configuration Link or QR Code . . . . . 327
  - A.3.3 Manually Configuring the Approvals App . . . . . 327
- A.4 Overview of the Approvals App . . . . . 329
  - A.4.1 Tasks View . . . . . 330
  - A.4.2 Details View . . . . . 330
  - A.4.3 Bulk Mode . . . . . 330
  - A.4.4 Completed Tasks View . . . . . 331
  - A.4.5 Login Settings View . . . . . 331
  - A.4.6 Advanced Settings View . . . . . 331
- A.5 Changing the Approvals App Display Language . . . . . 331







---

# About This Guide

This book describes the user interface of the Novell Identity Manager User Application and how you can use the features it offers, including:

- ◆ Identity self-service (for user information, passwords, and directories)
- ◆ Work dashboard (for making role, resource, and provisioning requests and managing the approval tasks relating to these requests)
- ◆ Roles and resources (for managing roles and resources)
- ◆ Compliance (for regulatory compliance and attestation)

## Audience

The information in this book is for end users of the Identity Manager user interface.

## Prerequisites

This guide assumes that you are using the default configuration of the Identity Manager user interface. However, it's possible that your version of the user interface has been customized to look or operate differently.

Before you get started, you should check with your system administrator for details on any customizations you might encounter.

## Organization

Here's a summary of what you'll find in this book:

---

| Part   | Description   |
|--|---|
| <a href="#">Part I, "Welcome to Identity Manager," on page 13</a>          | Introduction to the Identity Manager user interface and how to begin using it   |
| <a href="#">Part II, "Using the Identity Self-Service Tab," on page 31</a> | How to use the <i>Identity Self-Service</i> tab of the Identity Manager user interface to display and work with identity information, including: <ul style="list-style-type: none"><li>◆ Organization charts</li><li>◆ Profiles (your identity details)</li><li>◆ Directory searches</li><li>◆ Passwords</li><li>◆ User accounts (and more)</li></ul> |

---

| Part  | Description   |
|---|---|
| Part III, "Using the Work Dashboard Tab," on page 107     | <p>How to use the <i>Work Dashboard</i> tab of the Identity Manager user interface to:</p> <ul style="list-style-type: none"> <li>◆ Manage task notifications</li> <li>◆ Manage role assignments</li> <li>◆ Manage resource assignments</li> <li>◆ View request status for role, resource, and process requests</li> </ul>  |
| Part IV, "Using the Roles and Resources Tab," on page 217 | <p>How to use the <i>Roles and Resources</i> tab of the Identity Manager user interface to:</p> <ul style="list-style-type: none"> <li>◆ Make role requests for yourself or other users within your organization</li> <li>◆ Create roles and role relationships within the roles hierarchy</li> <li>◆ Create separation of duties (SoD) constraints to manage potential conflicts between role assignments</li> <li>◆ Look at reports that provide details about the current state of the Role Catalog and the roles currently assigned to users, groups, and containers</li> </ul> |
| Part V, "Using the Compliance Tab," on page 291           | <p>How to use the <i>Compliance</i> tab of the Identity Manager user interface to:</p> <ul style="list-style-type: none"> <li>◆ Make requests for user profile attestation processes</li> <li>◆ Make requests for separation of duties (SoD) attestation processes</li> <li>◆ Make requests for role assignment attestation processes</li> <li>◆ Make requests for user assignment attestation processes</li> </ul>   |
| Part VI, "Appendixes," on page 323                        | <p>How to use the NetIQ Identity Manager Approvals app to remotely approve or deny requests made in the User Application</p>  |

## Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation, or go to [www.novell.com/documentation/feedback.html](http://www.novell.com/documentation/feedback.html) and enter your comments there.

## Documentation Updates

For the most recent version of the *IDM User Application: User Guide*, visit the [Identity Manager Web site \(http://www.netiq.com/documentation/idm402/index.html\)](http://www.netiq.com/documentation/idm402/index.html).

---

# Welcome to Identity Manager

Read this part first to learn about the Identity Manager User Application and how to begin using it.

- ◆ [Chapter 1, “Getting Started,” on page 15](#)



---

# 1 Getting Started

This section tells you how to begin using the Identity Manager User Application. Topics include:

- ◆ [Section 1.1, “Identity Manager and You,” on page 15](#)
- ◆ [Section 1.2, “Accessing the Identity Manager User Application,” on page 19](#)
- ◆ [Section 1.3, “Logging In,” on page 20](#)
- ◆ [Section 1.4, “Exploring the User Application,” on page 22](#)
- ◆ [Section 1.5, “What’s Next,” on page 29](#)

## 1.1 Identity Manager and You

Novell Identity Manager is a system software product that your organization uses to securely manage the access needs of its user community. If you’re a member of that user community, you benefit from Identity Manager in a number of ways. For example, Identity Manager enables your organization to:

- ◆ Give users access to the information (such as group org charts, department white pages, or employee lookup), as well as roles and resources (such as equipment or accounts on internal systems) that they need, right from day one
- ◆ Synchronize multiple passwords into a single login for all your systems
- ◆ Modify or revoke access rights instantly when necessary (such as when someone transfers to a different group or leaves the organization)
- ◆ Support compliance with government regulations

To bring these benefits directly to you and your team, the Identity Manager User Application provides a user interface that you can use from your Web browser.

### 1.1.1 Introducing the Identity Manager User Application

The Identity Manager User Application is your view into the information, roles, resources, and capabilities of Identity Manager. Your system administrator determines the details of what you can see and do in the Identity Manager User Application. Typically, this includes:

- ◆ Identity self-service, which enables you to:
  - ◆ Display organization charts
  - ◆ Report applications associated with a user if you are an administrator. (Requires the Roles Based Provisioning Module for Identity Manager.)
  - ◆ Edit the information in your profile
  - ◆ Search a directory
  - ◆ Change your password, password challenge response, and password hint

- ◆ Review your password policy status and password synchronization status
- ◆ Create accounts for new users or groups (if you are authorized)
- ◆ Roles, which enable you to:
  - ◆ Request role assignments and manage the approval process for role assignment requests
  - ◆ Check the status of your role requests
  - ◆ Define roles and role relationships
  - ◆ Define separation of duties (SoD) constraints and manage the approval process in situations where a user requests an override to a constraint
  - ◆ Browse the Role Catalog
  - ◆ Look at detailed reports that list the roles and separation of duties constraints defined in the catalog, as well as the current state of role assignments, separation of duties exceptions, and user entitlements

---

**NOTE:** The ability to define custom roles is only available with Identity Manager 4.0.2 Advanced Edition. Standard Edition only supports the use of system roles.

---

- ◆ Resources, which enable you to:
  - ◆ Request resource assignments and manage the approval process for resource assignment requests
  - ◆ Check the status of your resource requests
  - ◆ Browse the Resource Catalog

---

**NOTE:** Resources require Identity Manager 4.0.2 Advanced Edition. Standard Edition does not support this feature.

---

- ◆ Workflow processes, which enable you to:
  - ◆ Request custom workflow processes
  - ◆ Check the approval of your role, resource, and process requests
  - ◆ Work on tasks assigned to you for approving other requests
  - ◆ Perform process requests and approvals as a proxy or delegate for someone else
  - ◆ Assign someone else to be your proxy or delegate (if you are authorized)
  - ◆ Manage all of these request and approval features for your team (if you are authorized)

---

**NOTE:** Workflow processes require Identity Manager 4.0.2 Advanced Edition. Standard Edition does not support this feature.

---

- ◆ Compliance, which enables you to:
  - ◆ Request user profile attestation processes
  - ◆ Request separation of duties (SoD) attestation processes
  - ◆ Request role assignment attestation processes
  - ◆ Request user assignment attestation processes

---

**NOTE:** Compliance requires Identity Manager 4.0.2 Advanced Edition. Standard Edition does not support this feature.

---

---

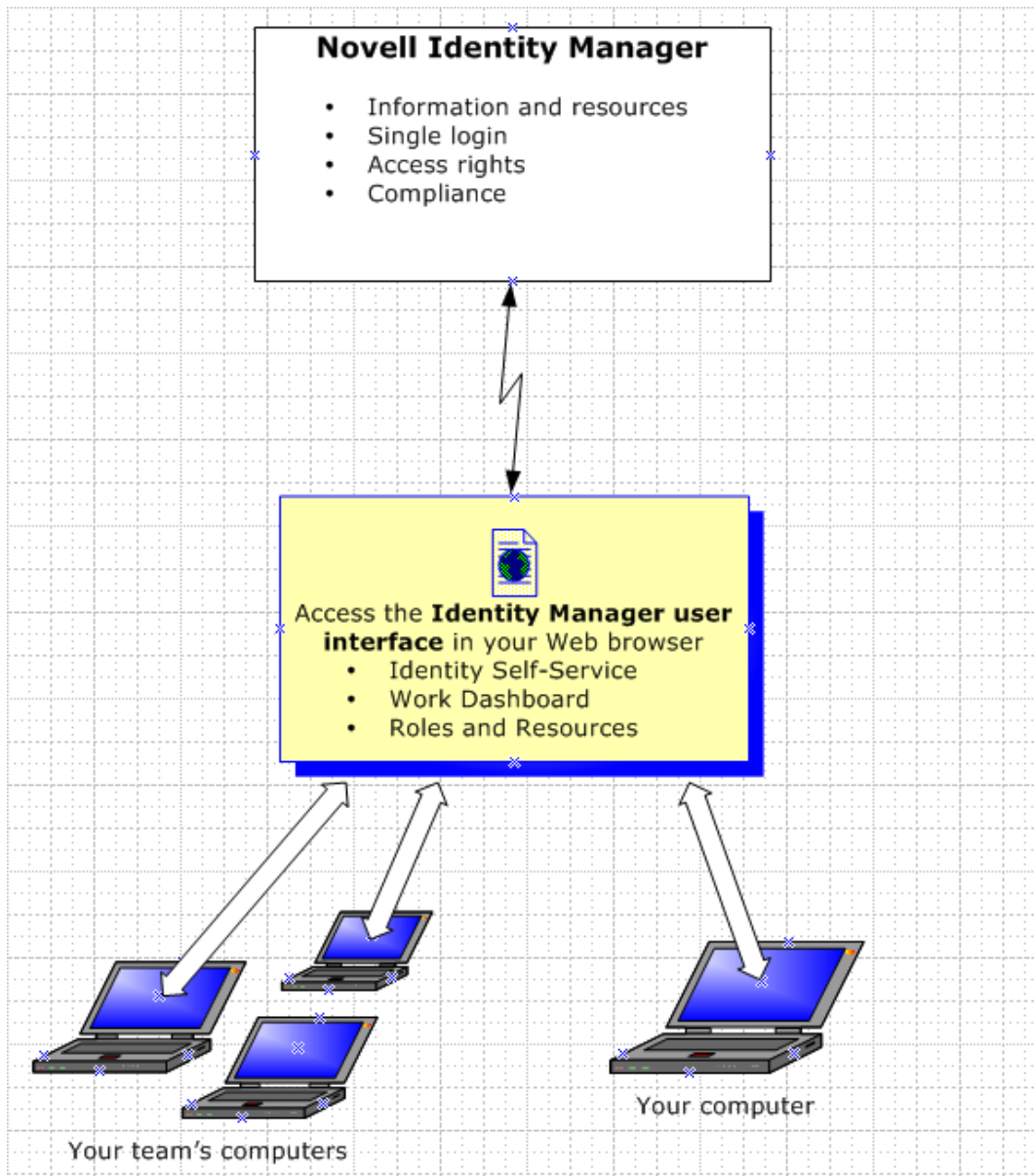
**IMPORTANT:** The User Application is an application and not a framework. The areas within the User Application that are supported to be modified are outlined within the product documentation. Modifications to areas not outlined within the product documentation are not supported.

---



## 1.1.2 The Big Picture

**Figure 1-1** The IDM User Application Provides the User Interface to Identity Manager



## 1.1.3 Typical Uses

Here are some examples of how people typically use the Identity Manager User Application within an organization.

### Working with Identity Self-Service

- ◆ Ella (an end user) recovers her forgotten password through the identity self-service features when logging in.

- ♦ Erik (an end user) performs a search for all employees who speak German at his location.
- ♦ Eduardo (an end user) browses the organization chart, finds Ella, and clicks the e-mail icon to send a message to her.

## Working with Roles and Resources

- ♦ Maxine (a Role Manager) creates the Nurse and Doctor business roles and the Administer Drugs and Write Prescriptions IT roles. Maxine creates several resources that are needed for these roles, and associates the resources with the roles.
- ♦ Maxine (a Role Manager) defines a relationship between the Nurse and Administer Drugs roles, specifying that the Nurse role contains the Administer Drugs role. Max also defines a relationship between the Write Prescriptions and Doctor roles, specifying that the Doctor role contains the Write Prescriptions role.
- ♦ Chester (a Security Officer) defines a separation of duties constraint that specifies that a potential conflict exists between the Doctor and Nurse roles. This means that ordinarily the same user should be not assigned to both roles at the same time. In some circumstances, an individual who requests a role assignment may want to override this constraint. To define a separation of duties exception, the individual who requests the assignment must provide a justification.
- ♦ Ernest (an end user) browses a list of roles available to him, and requests assignment to the Nurse role.
- ♦ Amelia (an approver) receives notification of an approval request via e-mail (which contains an URL). She clicks the link, is presented with an approval form, and approves it.
- ♦ Arnold (a Role Manager) requests that Ernest be assigned to the Doctor role. He is notified that a potential conflict exists between the Doctor role and Nurse role, to which Ernest has already been assigned. He provides a justification for making an exception to the separation of duties constraint.
- ♦ Edward (a separation of duties approver) receives notification of a separation of duties conflict via e-mail. He approves Arnold's request to override the separation of duties constraint.
- ♦ Amelia (an approver) receives notification of an approval request for the Doctor role via e-mail. She approves the Arnold's request to assign Ernest to the Doctor role.
- ♦ Bill (a Role Auditor) looks at the SoD Violations and Exceptions Report and sees that Ernest has been assigned to both the Doctor and Nurse roles. In addition, he sees that Ernest has been assigned the resources associated with these roles.

## Working with Process Requests

- ♦ Ernie (an end user) browses a list of resources available to him, and requests access to the Siebel\* system.
- ♦ Amy (an approver) receives notification of an approval request via e-mail (which contains an URL). She clicks the link, is presented with an approval form, and approves it.
- ♦ Ernie checks on the status of his previous request for Siebel access (which has now gone to a second person for approval). He sees that it is still in progress.
- ♦ Amy is going on vacation, so she indicates that she is temporarily unavailable. No new approval tasks are assigned to her while she is unavailable.
- ♦ Amy opens her approval task list, sees that there are too many for her to respond to in a timely manner, and reassigns several to co-workers.
- ♦ Pat (an administrative assistant, acting as a proxy user for Amy) opens Amy's task list and performs an approval task for her.

- ♦ Max (a manager) views the task lists of people in his department. He knows that Amy is on vacation, so he reassigns tasks to others in his department.
- ♦ Max initiates a request for a database account for someone in his department who reports directly to him.
- ♦ Max assigns Dan to be an authorized delegate for Amy.
- ♦ Dan (now a delegated approver) receives Amy's tasks when she is unavailable.
- ♦ Max engages an unpaid intern, who should not be entered into the HR system. The system administrator creates the user record for this intern and requests that he be given access to Notes, Active Directory\*, and Oracle\*.

## Working with Compliance

- ♦ Maxine (a Role Manager) creates the Nurse and Doctor business roles and the Administer Drugs and Write Prescriptions IT roles.
- ♦ Maxine (a Role Manager) defines a relationship between the Nurse and Administer Drugs roles, specifying that the Nurse role contains the Administer Drugs role. Max also defines a relationship between the Write Prescriptions and Doctor roles, specifying that the Doctor role contains the Write Prescriptions role.
- ♦ Chester (a Security Officer) defines a separation of duties constraint that specifies that a potential conflict exists between the Doctor and Nurse roles. This means that ordinarily the same user should be not assigned to both roles at the same time. In some circumstances, an individual who requests a role assignment may want to override this constraint. To define a separation of duties exception, the individual who requests the assignment must provide a justification.
- ♦ Arnold (a Role Manager) requests that Ernest be assigned to the Doctor role. He is notified that a potential conflict exists between the Doctor role and Nurse role, to which Ernest has already been assigned. He provides a justification for making an exception to the separation of duties constraint.
- ♦ Philip (a Compliance Module Administrator) initiates a role assignment attestation process for the Nurse role.
- ♦ Fiona (an attester) receives notification of the attestation task via e-mail (which contains an URL). She clicks the link and is presented with an attestation form. She provides an affirmative answer to the attestation question, thereby giving her consent that the information is correct.
- ♦ Philip (a Compliance Module Administrator) initiates a new request for a user profile attestation process for users in the Human Resources group.
- ♦ Each user in the Human Resources group receives notification of the attestation task via e-mail (which contains an URL). Each user clicks the link and is presented with an attestation form. The form gives the user an opportunity to review the values for various user profile attributes. After reviewing the information, each user answers the attestation question.

## 1.2 Accessing the Identity Manager User Application

When you're ready to start using the Identity Manager User Application, all you need on your computer is a Web browser. Identity Manager supports the most popular browser versions; see your system administrator for a list of supported browsers or for help installing one.

Because it works in a browser, the Identity Manager User Application is as easy to access as any Web page.

---

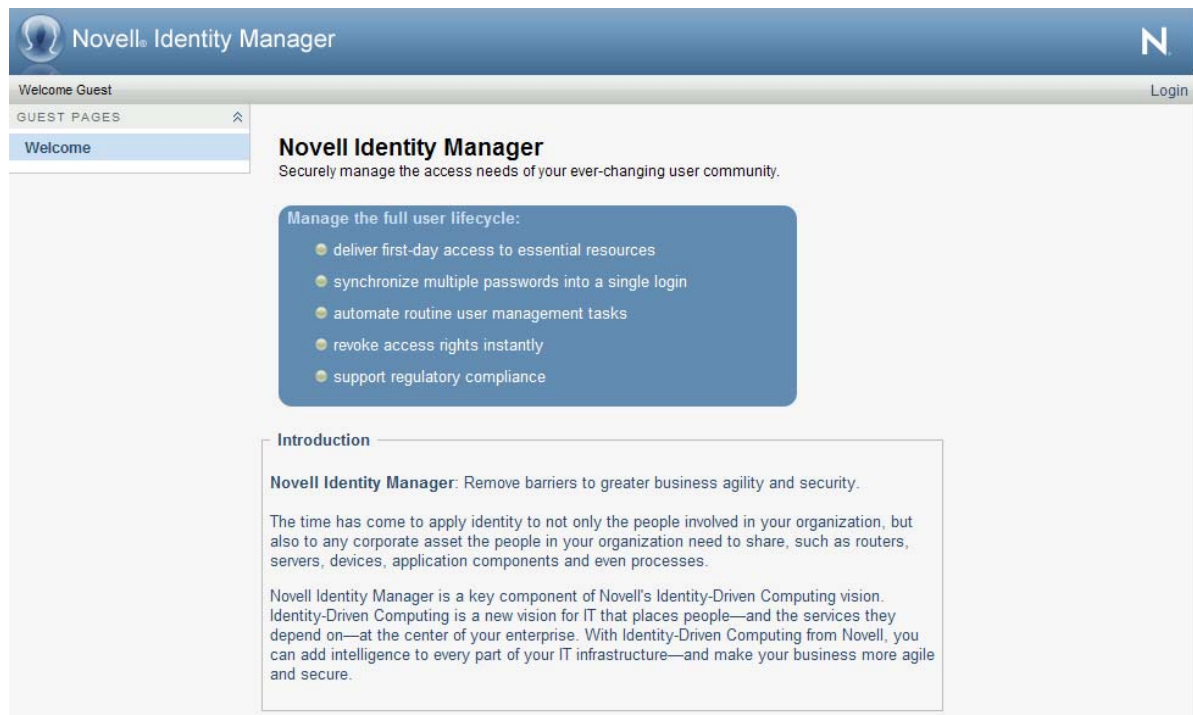
**NOTE:** To use the Identity Manager User Application, enable cookies (at least *Medium* privacy level in Internet Explorer) and JavaScript\* in your Web browser. If you are running Internet Explorer, you should also select the *Every time I visit the webpage* option under *Tools > Internet Options > General, Browsing History > Settings > Check for newer versions of stored pages*. If you do not have this option selected, some of the buttons may not be displayed properly.

---

To access the Identity Manager User Application, open a Web browser and go to the address (URL) for the Identity Manager User Application, as supplied by your system administrator. For example: `http://myappserver:8080/IDMProv`.

By default, this takes you to the Welcome Guest page of the User Application:

**Figure 1-2** The Welcome Guest Page of the User Application



From here, you can log in to the User Application to get access to its features.

## 1.2.1 Your User Application Might Look Different

If you see a different first page when accessing the Identity Manager User Application, it's typically because the application has been customized for your organization. As you work, you might find that other features of the User Application have also been customized.

If this is the case, you should check with your system administrator to learn how your customized User Application differs from the default configuration described in this guide.

## 1.3 Logging In

You must be an authorized user to log in to the Identity Manager User Application from the guest welcome page. If you need help getting a username and password to supply for the login, see your system administrator.

To log in to the Identity Manager User Application:

- 1 From the Welcome Guest page, click the *Login* link (in the top right corner of the page).  
The User Application prompts you for a username and password:

The image shows the Novell Identity Manager login interface. It features a blue header with a circular logo containing a stylized human head profile. Below the logo, the text "Novell® Identity Manager" is displayed. Underneath, there are two input fields: "Username:" and "Password:". A link labeled "Forgot Password?" is positioned below the password field. At the bottom left, there is a red "N" logo, and at the bottom right, there is a "Login" button.

- 2 Type your username and password, then click *Login*.

### 1.3.1 If You Forget Your Password

If you can't remember the password to type, you might be able to use the *Forgot Password?* link for assistance. When you are prompted to log in, this link appears on the page by default. You can take advantage of it if your system administrator has set up an appropriate password policy for you.

To use the Forgot Password feature:

- 1 When you're prompted to log in, click the *Forgot Password?* link.  
You are then asked for your username:

The image shows the "IDM Forgot Password" form. It has a blue header with the text "IDM Forgot Password". Below the header, there is a message: "To help you log in, you must specify your username." Underneath this message is a "Username:" label followed by a text input field. Below the input field is a "Submit" button. At the bottom of the form, there is a link labeled "Return to Calling Page".

- 2 Type your username and click *Submit*.  
If Identity Manager responds that it can't find a password policy for you, see your system administrator for assistance.
- 3 Answer any challenge questions that display and click *Submit*. For example:

**IDM Forgot Password**

Please provide a response for each presented challenge.

**Question:** What is your mother's maiden name? **Response:** ●●●●●●●

**Question:** What's your favorite color? **Response:** ●●●●●●●

**Question:** What is your User ID? **Response:** ●●●●●●●

Submit

Answer the challenge questions to get assistance with your password. Depending on how the system administrator has set up your password policy, you could:

- ◆ See a hint about your password displayed on the page
- ◆ Receive an e-mail containing your password or a hint about it
- ◆ Be prompted to reset your password

## 1.3.2 If You Have Trouble Logging In

If you are unable to log in to the Identity Manager User Application, make sure that you're using the right username and typing the password correctly (spelling, uppercase or lowercase letters, etc.). If you still have trouble, consult your system administrator. It's helpful if you can provide details about the problem you are having (such as error messages).

## 1.3.3 If You're Prompted for Additional Information

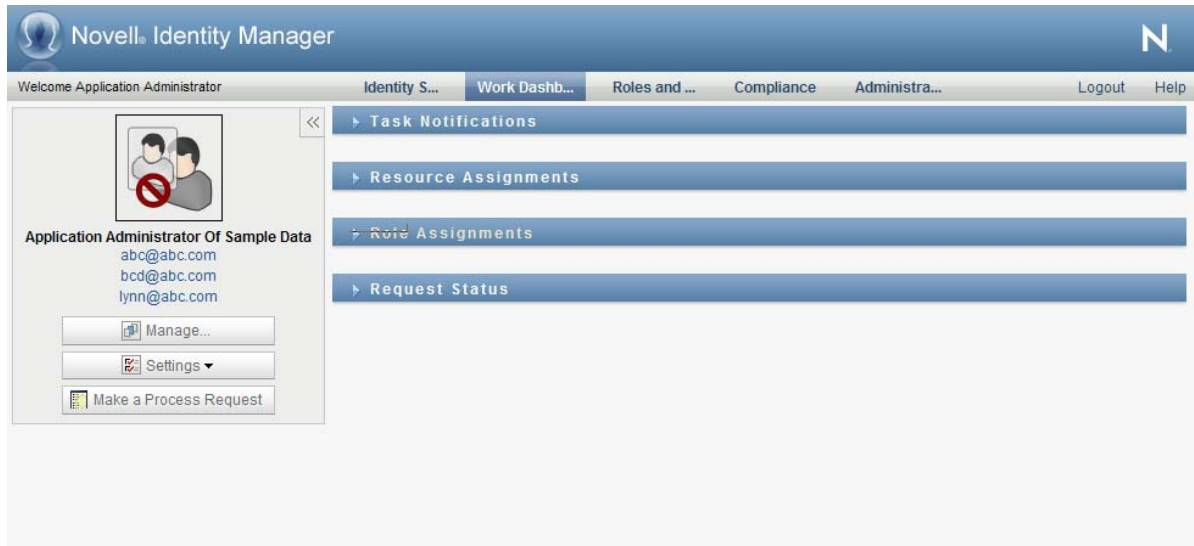
You might be prompted for other kinds of information as soon as you log in to the Identity Manager User Application. It all depends on how the system administrator has set up your password policy (if any). For example:

- ◆ If this is your first login, you might be prompted to define your challenge questions and responses, or your password hint
- ◆ If your password has expired, you might be prompted to reset it

## 1.4 Exploring the User Application

After you log in, the Identity Manager User Application displays the tab pages where you do your work:

**Figure 1-3** What You See When You Login



If you look along the top of the User Application, you'll see the main tabs:

- ◆ *Identity Self-Service* (which is open by default)  
To learn about this tab and how to work with it, see [Part II, "Using the Identity Self-Service Tab," on page 31](#).
- ◆ *Work Dashboard*  
To learn about this tab and how to work with it, see [Part III, "Using the Work Dashboard Tab," on page 107](#).
- ◆ *Role and Resources*  
To learn about this tab and how to work with it, see [Part IV, "Using the Roles and Resources Tab," on page 217](#).
- ◆ *Compliance*  
To learn about this tab and how to work with it, see [Part V, "Using the Compliance Tab," on page 291](#).

---

**NOTE:** What you see may vary depending on what security permissions you've been given.

---

To switch to a different tab, simply click the tab you want to use.

## 1.4.1 Getting Help

While working in the Identity Manager User Application, you can display online help to get documentation about the tab that you're currently using.

- 1 Go to the tab that you want to learn about (such as *Roles and Resources* or *Compliance*).
- 2 Click the *Help* link (in the top right corner of the page).

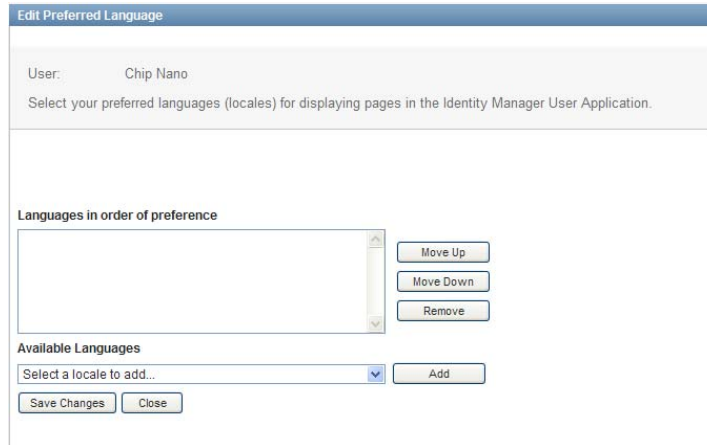
The help page for the current tab displays. The help page includes a link to more detailed information included in the documentation on the Novell Web site.

## 1.4.2 Preferred Locale

If your administrator has selected the *Enable Locale Check* option on the *Administration>Application Configuration>Password Module Setup>Login* screen, you receive a prompt to select your own preferred locale when you first log in.

- 1 When prompted, add a locale by opening the *Available Locales* list, selecting a locale, and clicking *Add*.

For more information, see [Section 5.6, “Choosing a Preferred Language,”](#) on page 69.



The screenshot shows a window titled "Edit Preferred Language". At the top, it displays "User: Chip Nano" and a subtitle "Select your preferred languages (locales) for displaying pages in the Identity Manager User Application." Below this is a section titled "Languages in order of preference" which contains an empty list box. To the right of the list box are three buttons: "Move Up", "Move Down", and "Remove". Below the list box is a section titled "Available Languages" which contains a dropdown menu with the text "Select a locale to add..." and an "Add" button. At the bottom of the window are two buttons: "Save Changes" and "Close".

## 1.4.3 Logging Out

When you're finished working in the Identity Manager User Application and want to end your session, you can log out.

- 1 Click the *Logout* link (in the top right corner of the page).


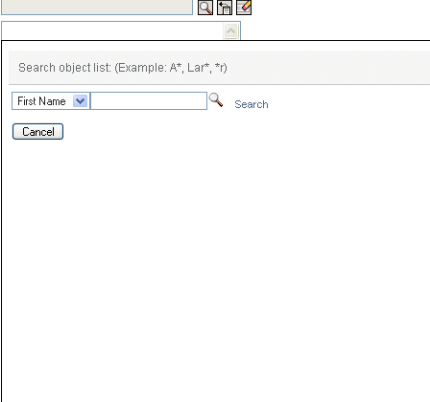

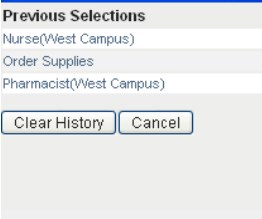

## 1.4.4 Common User Actions







The User Application provides a consistent user interface with common user interactions for accessing and displaying data. This section describes several of the common user interface elements and includes instructions for:

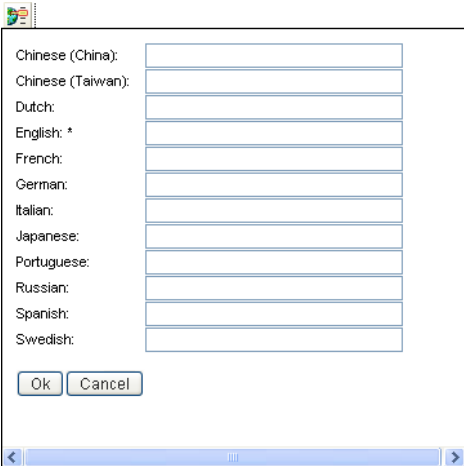
- ♦ [“Using the Object Selector Button for Searching”](#) on page 26
- ♦ [“Filtering Data”](#) on page 27
- ♦ [“Using the Lookahead Feature”](#) on page 28



**Table 1-1** Common Buttons

| Button  | Description   |
|---|---|
|    | <p><b>Object Selector</b> Provides access to a Search dialog box or popin. You can enter search criteria for different types of objects based on your location within the User Application. For example, in the Identity Self-Service tab, you can search for users and groups while in the Roles tab, you can search for users, groups, and roles.</p> |
|   |   |
|   | <p>See <a href="#">“Using the Object Selector Button for Searching”</a> on page 26.</p>   |
|    | <p><b>Show History</b> Provides links to previously accessed data. You can select the link to display the data for the previous selection. Clicking Show History might be faster than performing a search if you know that you have recently worked with an item.</p>   |
|   |    |
|  | <p><b>Reset</b> Clears the current selection.</p>   |

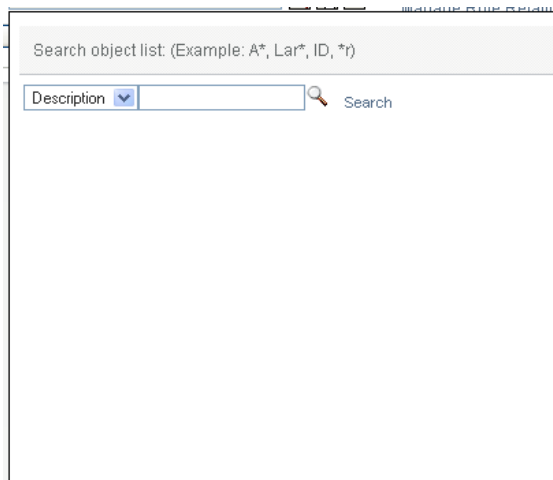
| Button  | Description  |
|---|--|
|    | <p><b>Localize</b> Displays a dialog box that lets you enter the text usually for a field name or description in any of the locales currently supported by the User Application.</p> |
|    | <p><b>Add</b> Adds a new item or object. You are prompted for additional information specific to the type of object you are adding.</p>  |
|    | <p><b>Delete</b> Deletes the currently selected item.</p>  |
|    | <p><b>Up or Down Arrow</b> Moves the currently selected object up or down on the list</p>  |
|  |  |
|  | <p><b>Legend</b> Provides a description for symbols shown in the user interface.</p>   |



## Using the Object Selector Button for Searching

To use the Object Selector button:

- 1 Click . The Search dialog displays:



**2** Specify your search criteria as follows:

**2a** Use the drop-down list to choose a field on which to search. The drop-down list fields depend on where you launched the search. In this example, you can specify *Name* or *Description*.

**2b** In the text box next to the drop-down list, type all or part of the search criteria (such as name or description). The search finds every occurrence of the type of object you are searching for that begins with the text you type. You can optionally use the asterisk (\*) as a wildcard in your text to represent zero or more of any character. For instance, all of the following examples find the role Nurse:

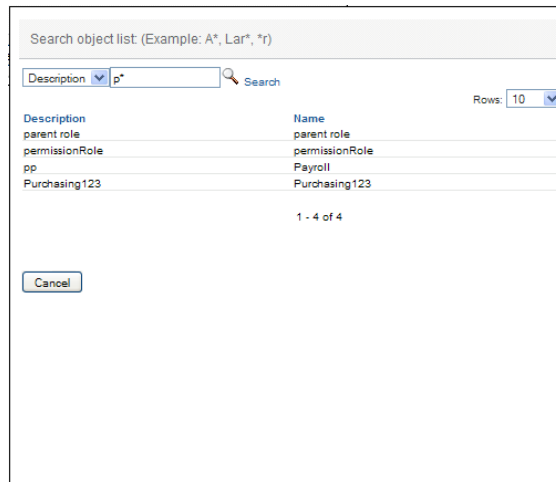
nurse

n

n\*

**3** Click *Search*.

The search results display. You can sort the search results in ascending or descending order by clicking the column headings. This example shows a list of roles.



If the result list includes the one you want, go to [Step 4](#). Otherwise, go back to [Step 2](#).

**4** Select the item you want from the list. The lookup page closes and populates the page with the data associated with your selection.

## Filtering Data

The *Work Dashboard* and *Roles and Resources* tab of the User Application provides filters so that you can display only the data that you are interested in viewing. You can additionally limit the amount of data displayed on a single page by using the Maximum rows per page setting. Some examples of filters include:

- ◆ Filtering by role or resource assignment and source (available in the Role Assignments and Resource Assignments actions)
- ◆ Filtering by role or resource name, user, and status (available in the Request Status action)
- ◆ Filtering by role level and category (available in the Role Catalog action)

To use filtering:

- 1 Specify a value in a text field (such as the *Role Name* or *Description* field) in the *Filter* dialog, as follows:
  - 1a To limit the items to those that start with a particular string of characters, type all or part of the character string. You can optionally use the asterisk (\*) as a wildcard in your text to represent zero or more of any character. The filtering applied is based on the first character in the display name.

For instance, all of the following examples find the role assignment called Nurse:

nurse

n

n\*
  - 1b To further filter the items displayed, you can specify additional filter criteria. The User Application allows you to select the criteria in different ways depending on the data. You might select a checkbox or select one or more items from a list box (using your platforms multi-select keystrokes). The criteria is ANDed so that only the items that meet all of the criteria are displayed.
  - 1c To apply the filter criteria you've specified to the display, click *Filter*.
  - 1d To clear the currently specified filter criteria, click *Clear*.
- 2 To set the maximum number of items matching the filter by criteria that are displayed on each page, select a number in the *Rows* dropdown list.

---

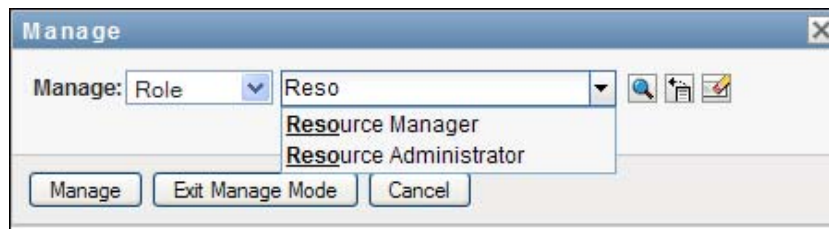
**NOTE:** A filter on Role Name does not limit the number of objects returned from the Identity Vault. It simply restricts the objects displayed on the page based on the filter criteria. Other filters (such as Status) do restrict the number of objects returned from the Identity Vault.

---

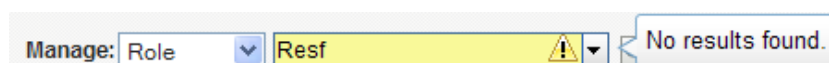
## Using the Lookahead Feature

Many of the AJAX controls within the User Application support smart look-ahead (or type ahead) processing. This support reduces the number of keystrokes required to locate items of interest. To take advantage of this feature, simply type four or more characters in the control and select one of the matching items from the automatically generated dropdown list.

Here's an example that shows how you might use the lookahead feature to search for all roles that begin with the letters Reso:



If you type a string for which there is no match, you will see an error message, as shown below:



This feature is supported by all user lookup, group lookup, or role lookup controls within the User Application where a single value is expected.

## 1.5 What's Next

Now that you've learned the basics of the Identity Manager User Application, you can start using the tabs it provides to get your work done.

---

| <b>To learn about</b>            | <b>See</b>   |
|----------------------------------|--|
| Doing identity self-service work | <a href="#">Part II, "Using the Identity Self-Service Tab," on page 31</a> |
| Doing work on the Work Dashboard | <a href="#">Part III, "Using the Work Dashboard Tab," on page 107</a>      |
| Doing roles and resources work   | <a href="#">Part IV, "Using the Roles and Resources Tab," on page 217</a>  |
| Doing compliance work            | <a href="#">Part V, "Using the Compliance Tab," on page 291</a>            |

---



---

# || Using the Identity Self-Service Tab

These sections tell you how to use the *Identity Self-Service* tab of the Identity Manager User Application to display and work with identity information.

- ♦ [Chapter 2, “Introducing the Identity Self-Service Tab,” on page 33](#)
- ♦ [Chapter 3, “Using the Organization Chart,” on page 39](#)
- ♦ [Chapter 4, “Using the Associations Report,” on page 53](#)
- ♦ [Chapter 5, “Using My Profile,” on page 57](#)
- ♦ [Chapter 6, “Using Directory Search,” on page 71](#)
- ♦ [Chapter 7, “Performing Password Management,” on page 91](#)
- ♦ [Chapter 8, “Creating Users or Groups,” on page 97](#)





---

# 2 Introducing the Identity Self-Service Tab

This section tells you how to begin using the *Identity Self-Service* tab of the Identity Manager User Application. Topics include:

- ◆ [Section 2.1, “About the Identity Self-Service Tab,” on page 33](#)
- ◆ [Section 2.2, “Accessing the Identity Self-Service Tab,” on page 33](#)
- ◆ [Section 2.3, “Exploring the Tab’s Features,” on page 34](#)
- ◆ [Section 2.4, “Identity Self-Service Actions You Can Perform,” on page 35](#)

For more general information about accessing and working with the Identity Manager User Application, see [Chapter 1, “Getting Started,” on page 15](#).

## 2.1 About the Identity Self-Service Tab

The *Identity Self-Service* tab gives you a convenient way to display and work with identity information yourself. It enables your organization to be more responsive by giving you access to the information you need whenever you need it. For example, you might use the *Identity Self-Service* tab to:

- ◆ Manage your own user account directly
- ◆ Look up other users and groups in the organization on demand
- ◆ Visualize how those users and groups are related
- ◆ List applications with which you are associated

Your system administrator is responsible for setting up the contents of the *Identity Self-Service* tab for you and the others in your organization. What you can see and do is typically determined by your job requirements and your level of authority.

---

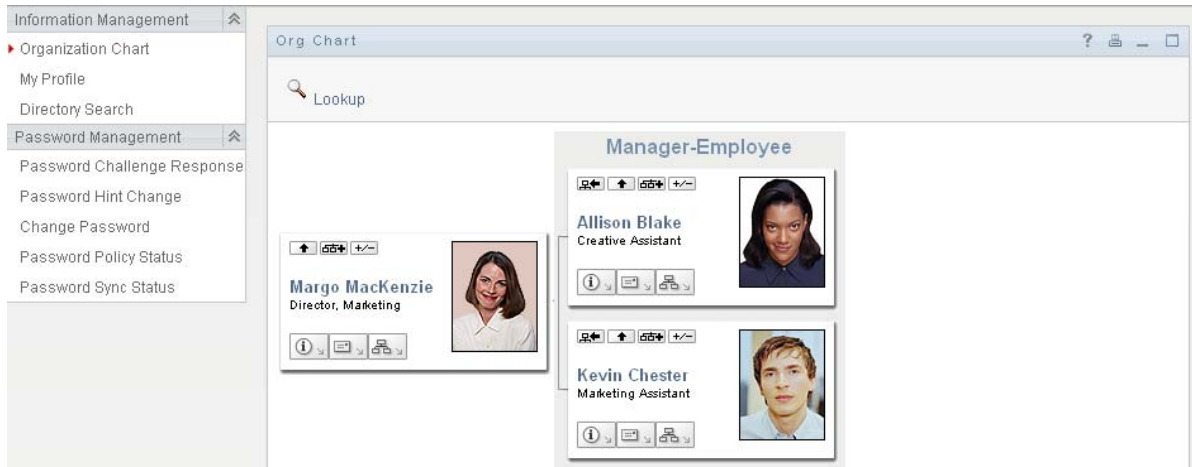
**NOTE:** In Identity Manager 4.0.2 Standard Edition, if you logon as a business user, the *Identity Self-Service* tab is the only tab you will see in the User Application. If you logon as a User Application Administrator, you see the *Administration* tab as well.

---

## 2.2 Accessing the Identity Self-Service Tab

By default, after you have logged in to the Identity Manager User Application, the *Identity Self-Service* tab opens and displays its Organization Chart page:

**Figure 2-1** The Organization Chart Page on the Identity Self-Service Tab



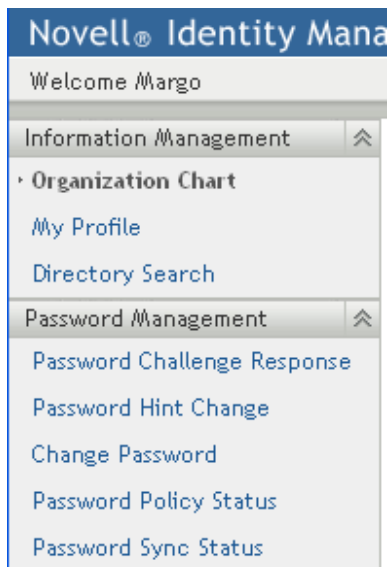
If you go to another tab in the Identity Manager User Application but then want to return, just click the *Identity Self-Service* tab to open it again.

## 2.3 Exploring the Tab's Features

This section describes the default features of the *Identity Self-Service* tab. (Your tab might look different because of customizations made for your organization; consult your system administrator.)

The left side of the *Identity Self-Service* tab displays a menu of actions you can perform. The actions are listed by category — *Information Management*, *Password Management*, and *Directory Management* (if authorized):

**Figure 2-2** The Identity Self-Service Menu of Actions



When you click an action, it displays a corresponding page on the right. The page typically contains a special window called a *portlet*, which shows the details for that action. For example, the portlet on the Organization Chart page looks like this:

**Figure 2-3** The Portlet on the Organization Chart Page







The portlet title bar typically displays a set of buttons you can click to perform standard operations. For example:



Table 2-1 describes what these buttons do:

**Table 2-1** Portlet Title-Bar Buttons and Their Functions

| Button  | What It Does                       |
|---|------------------------------------|
|  | Displays help for the portlet      |
|  | Prints the contents of the portlet |
|  | Minimizes the portlet              |
|  | Maximizes the portlet              |

If you see other buttons and aren't sure what they do, hover your mouse pointer over them to display descriptions.

## 2.4 Identity Self-Service Actions You Can Perform

Table 2-2 summarizes the actions that are available to you by default on the *Identity Self-Service* tab:

**Table 2-2** Actions Available Through the Identity Self-Service Tab

| Category               | Action                      | Description   |
|------------------------|-----------------------------|---|
| Information Management | Organization Chart          | <p>Displays the relationships among users and groups in the form of an interactive organizational chart.</p> <p>For details, see <a href="#">Chapter 3, “Using the Organization Chart,”</a> on page 39.</p>   |
|                        | Associations Report         | <p>Available to administrators. Displays applications with which a user is associated.</p> <p>For details, see <a href="#">Chapter 4, “Using the Associations Report,”</a> on page 53.</p>  |
|                        | My Profile                  | <p>Displays the details for your user account and lets you work with that information.</p> <p>For details, see <a href="#">Chapter 5, “Using My Profile,”</a> on page 57.</p>   |
|                        | Directory Search            | <p>Lets you search for users or groups by entering search criteria or by using previously saved search criteria.</p> <p>For details, see <a href="#">Chapter 6, “Using Directory Search,”</a> on page 71.</p>   |
| Password Management    | Password Challenge Response | <p>Lets you set or change your valid responses to administrator-defined challenge questions, and set or change user-defined challenge questions and responses.</p> <p>For details, see <a href="#">Chapter 7, “Performing Password Management,”</a> on page 91.</p> |
|                        | Password Hint Definition    | <p>Lets you set or change your password hint.</p> <p>For details, see <a href="#">Chapter 7, “Performing Password Management,”</a> on page 91.</p>  |
|                        | Change Password             | <p>Lets you change (reset) your password, according to the rules established by your system administrator.</p> <p>For details, see <a href="#">Chapter 7, “Performing Password Management,”</a> on page 91.</p>   |
|                        | Password Policy Status      | <p>Displays information about the effectiveness of your password management.</p> <p>For details, see <a href="#">Chapter 7, “Performing Password Management,”</a> on page 91.</p>   |
|                        | Password Sync Status        | <p>Displays the status of password synchronization for your associated applications that synchronize with the Identity Vault.</p> <p>For details, see <a href="#">Chapter 7, “Performing Password Management,”</a> on page 91.</p>                                  |

---

| Category             | Action               | Description   |
|----------------------|----------------------|---|
| Directory Management | Create User or Group | Available to administrators and authorized users. Lets you create a new user or group.<br><br>For details, see <a href="#">Chapter 8, "Creating Users or Groups,"</a> on page 97. |

---



---

# 3 Using the Organization Chart

This section tells you how to use the Organization Chart page on the *Identity Self-Service* tab of the Identity Manager User Application. Topics include:

- ♦ [Section 3.1, “About the Organization Chart,” on page 39](#)
- ♦ [Section 3.2, “Navigating the Chart,” on page 42](#)
- ♦ [Section 3.3, “Displaying Detailed Information,” on page 48](#)
- ♦ [Section 3.4, “Sending E-Mail from a Relationship Chart,” on page 49](#)

---

**NOTE:** This section describes the default features of the Organization Chart page. You might encounter some differences because of your job role, your level of authority, and customizations made for your organization; consult your system administrator for details.

---

For more general information about accessing and working with the *Identity Self-Service* tab, see [Chapter 2, “Introducing the Identity Self-Service Tab,” on page 33](#).

## 3.1 About the Organization Chart

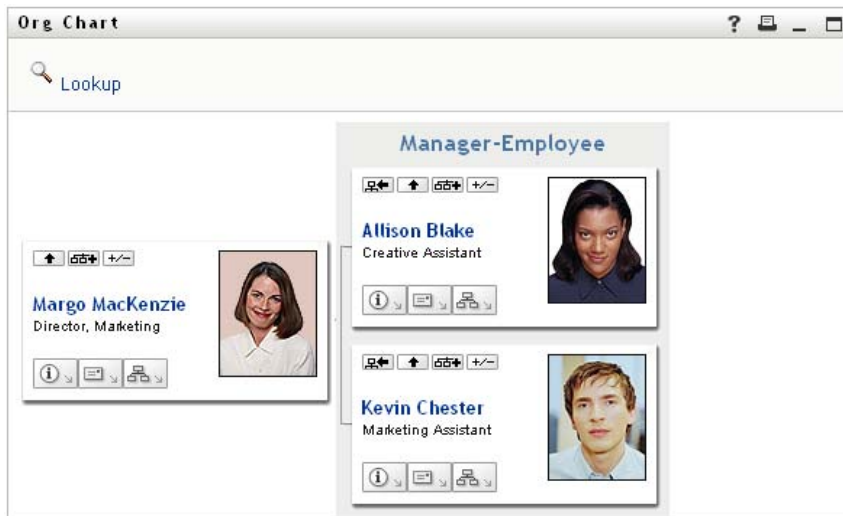
The Organization Chart page displays relationships. It can display relationships among managers, employees, and user groups in your business, and it can display other types of relationships that your administrator defines. The display is in the form of an organizational chart. In the chart, each person, group, or other entity is represented in a format that resembles a business card. The business card that is the starting point or orientation point of the organization chart is the *root* card.


The organization chart is interactive. You can:

- ♦ Select and display a type of relationship.
- ♦ Set your preferred default type of relationship, such as manager-employee, user group, or another that your administrator supplies.
- ♦ Set the default placement of a relationship chart to the left or right of the root card.
- ♦ Add up to two levels above the root card to the chart display.
- ♦ Make another user the root of the chart.
- ♦ Close (contract) or open (expand) a chart below a card.
- ♦ Look up a user to display in the chart.
- ♦ Display details (Profile page) for a selected user.
- ♦ Send user details (in the form of a link) to someone by e-mail.
- ♦ Send new e-mail to a selected user or to a manager’s team.

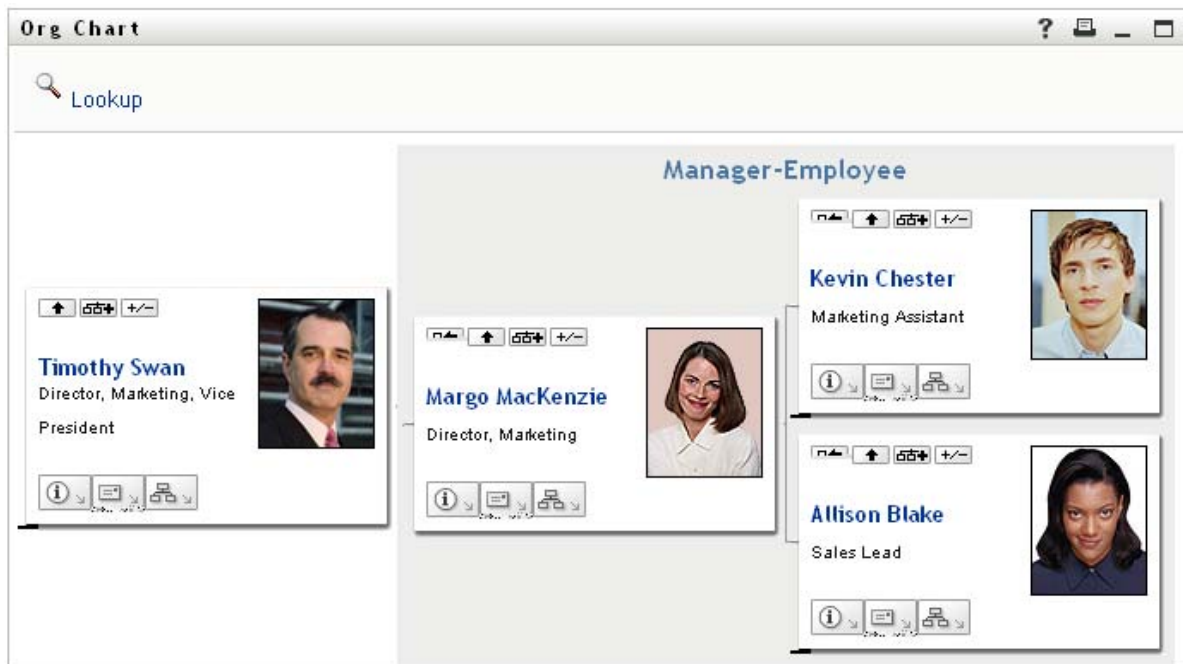
The following example introduces you to using Organization Chart. When you first display the Organization Chart page, it shows your own manager-employee relationships. For example, Margo MacKenzie (Marketing Director) logs in and sees the following default display of the Organization Chart page:

**Figure 3-1** Default View at Login



In her business card, Margo MacKenzie clicks *Go Up a Level*  to expand the chart to display her manager:

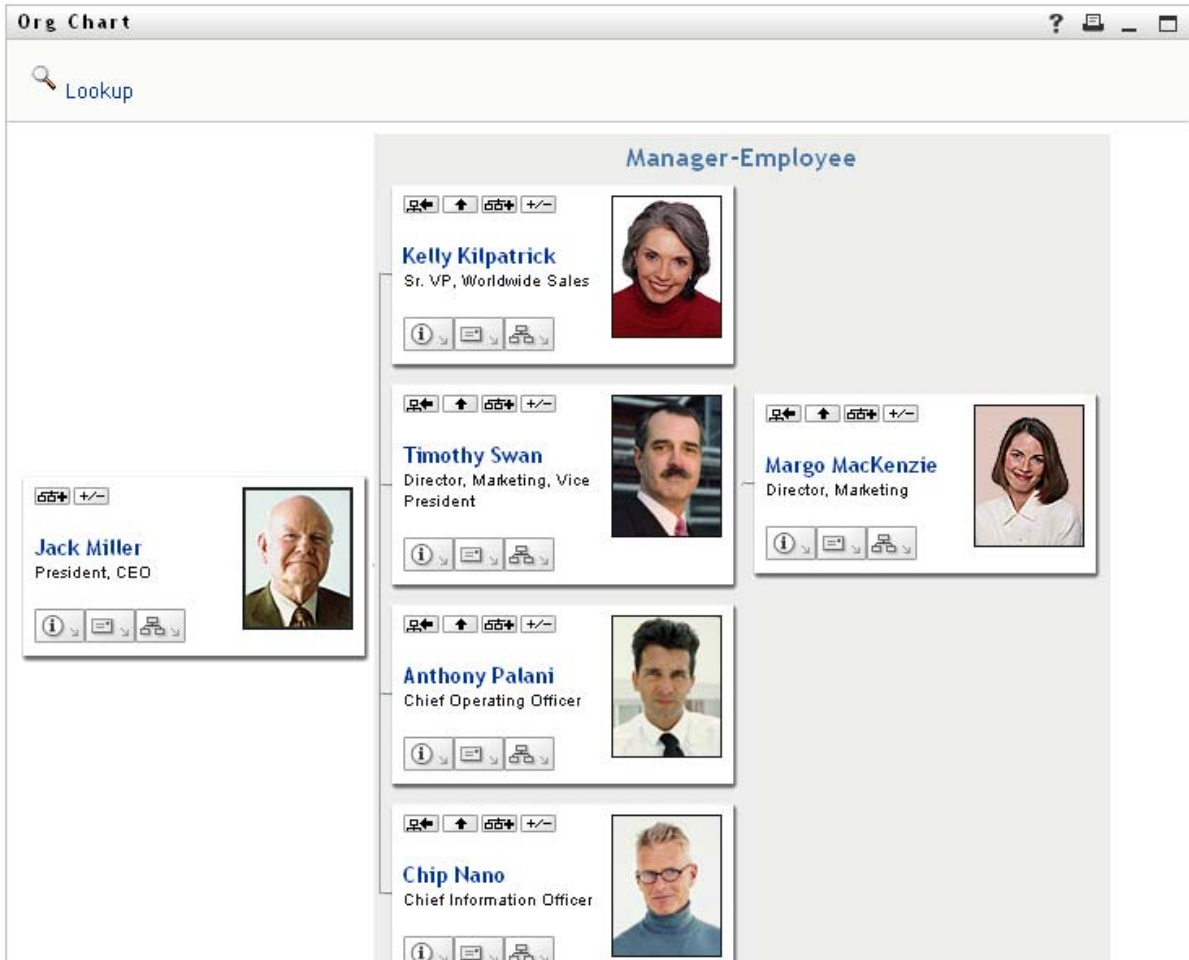
**Figure 3-2** Margo Clicks "Go Up a Level" to Show Her Manager




Margo then clicks *Go Up a Level*  in her manager's card, to show her manager's manager:

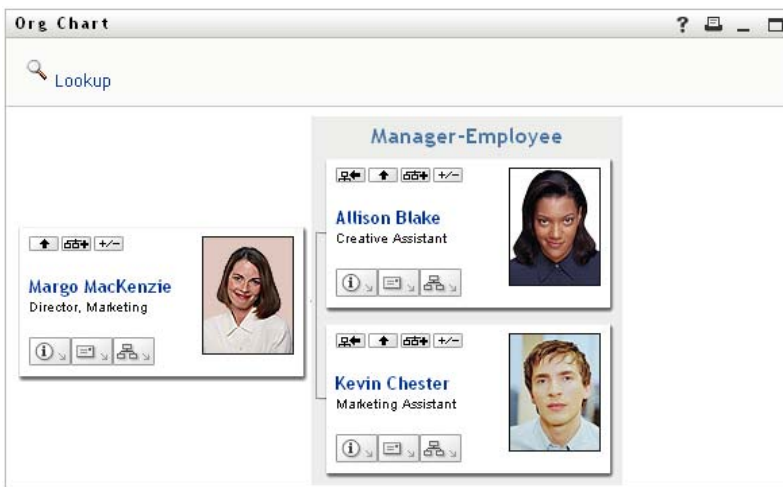


**Figure 3-3** Margo Clicks “Go Up a Level” A Second Time to Show Her Manager’s Manager



Margo then clicks *Make This Entity the New Root*  in her own card. This makes her card the root of the display again:

**Figure 3-4** Margo Clicks “Make This Entity the New Root” in Her Card




## 3.2 Navigating the Chart

This section describes how to move around a relationship chart by:

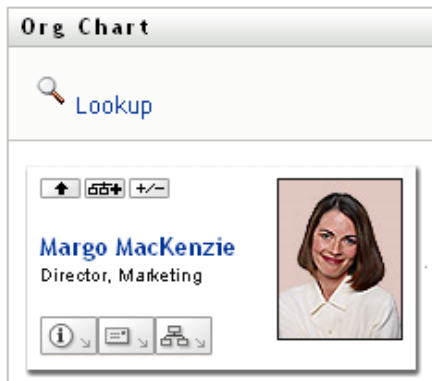
- ◆ Section 3.2.1, “Navigating to the Next Higher Level,” on page 42
- ◆ Section 3.2.2, “Resetting the Root of the Relationship,” on page 43
- ◆ Section 3.2.3, “Switching the Default Relationship,” on page 44
- ◆ Section 3.2.4, “Expanding or Collapsing the Default Chart,” on page 44
- ◆ Section 3.2.5, “Choosing a Relationship to Expand or Collapse,” on page 45
- ◆ Section 3.2.6, “Looking Up a User in Organization Chart,” on page 47

### 3.2.1 Navigating to the Next Higher Level

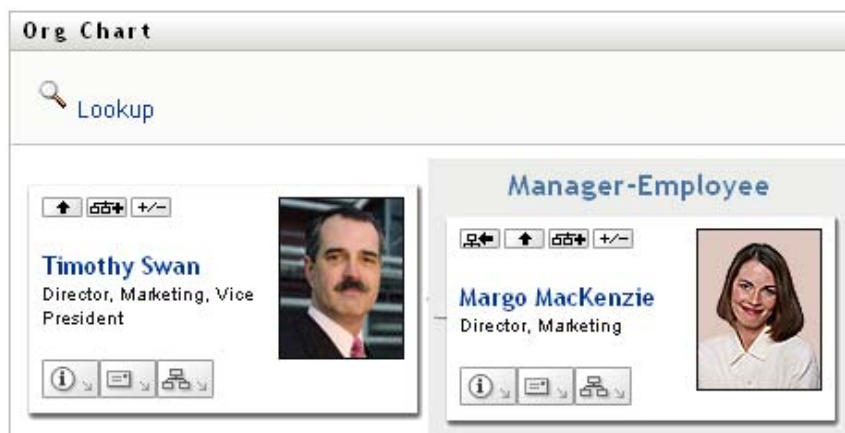
To navigate and expand to the next higher level in the relationship tree:

- 1 Click *Go Up a Level*  in the current top-level card.

For example, suppose that Margo clicks *Go Up a Level* in this view:



Her view expands to include the level above her:




*Go Up a Level* is available only if the user in the card is assigned a manager. If this function is not available to you, check with your administrator.

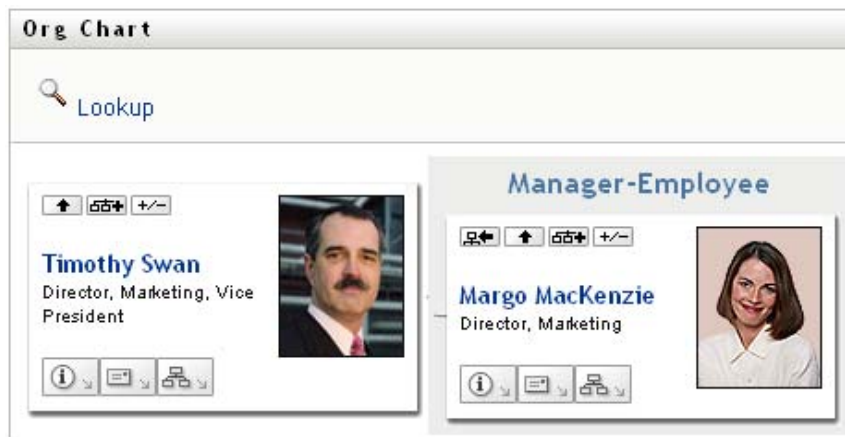
You can go up a level twice for a card.

## 3.2.2 Resetting the Root of the Relationship

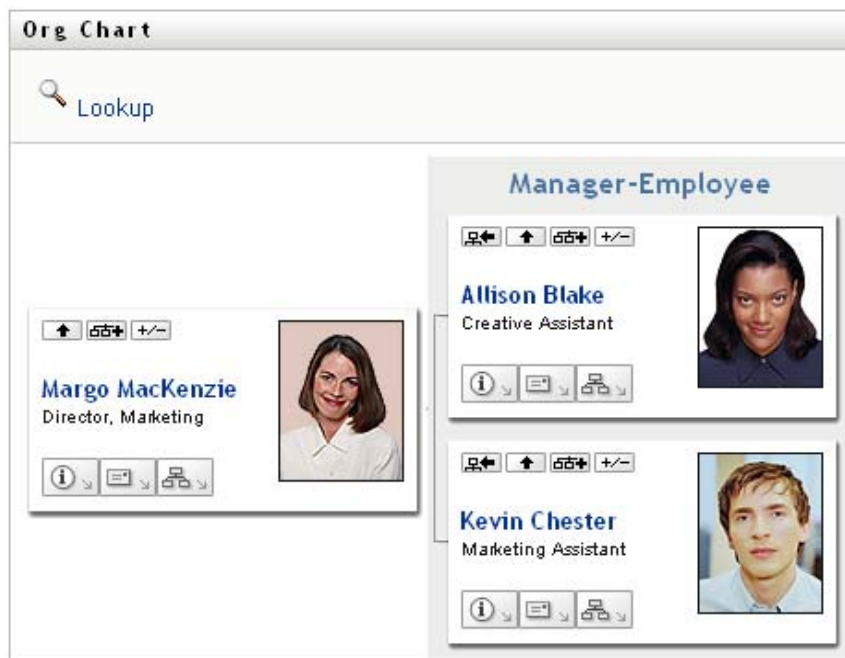
To reset the root of your view of the relationship chart:

- 1 Find the card of the user whom you want to the new root.
- 2 Click *Make This Entity the New Root* , or click the user's name (the name is a link) on that card. The chosen card becomes the root of the organization chart.


For example, suppose Margo Mackenzie clicks *Make This Entity the New Root* in her own card in this view:



Her card becomes the new root and is now at the top of her organization chart:



### 3.2.3 Switching the Default Relationship

- 1 Click *Switch to An Org Chart*  to change your default relationship.
- 2 Select the type of relationship to display. Your administrator can use relationships supplied by Novell (see [Table 3-1](#)) and can also define customized relationships.

**Table 3-1** *Types of Organization Chart Relationships Supplied by Novell*


| Type of Organizational Chart | Description   |
|------------------------------|---|
| Manager - employee           | Shows the reporting structure of managers and subordinates. |
| User group                   | Shows users and the groups in which they participate.       |

Margo Mackenzie changes her default relationship display to User Groups:

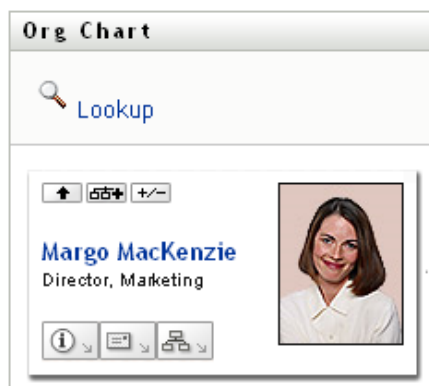
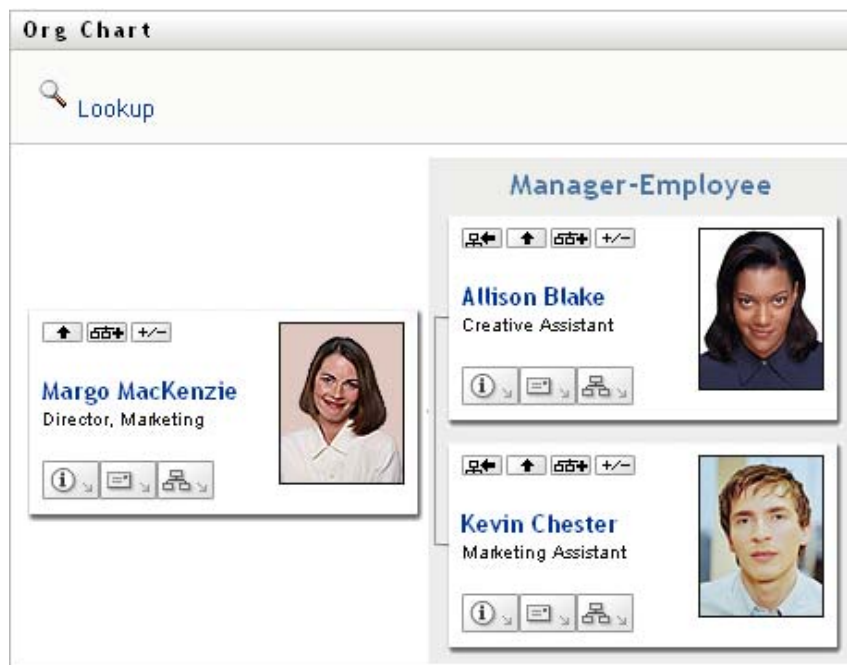


### 3.2.4 Expanding or Collapsing the Default Chart


The default relationship chart is Manager-Employee, unless you or your administrator sets it to another type. To expand or collapse the default chart:

- 1 Find a card for which you want to expand or collapse the default relationship display.
- 2 Click the *Expand/Collapse current relationship*  toggle button.

The chart expands or collapses to display or hide the subsidiary cards that are related to your chosen card. For example, the following two views show the Expand view and then the Collapse view.



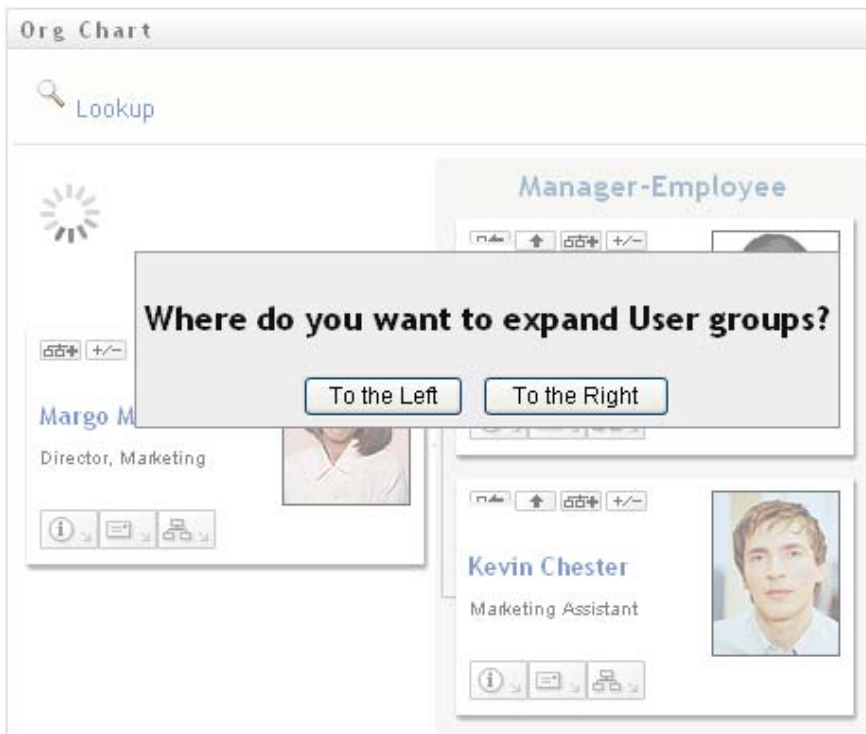
### 3.2.5 Choosing a Relationship to Expand or Collapse

- 1 Identify a card whose relationships you want to view.
- 2 Click *Choose relationship to Expand/Collapse*  in that card. A drop-down list opens.
- 3 Select a relationship and action from the drop-down list:

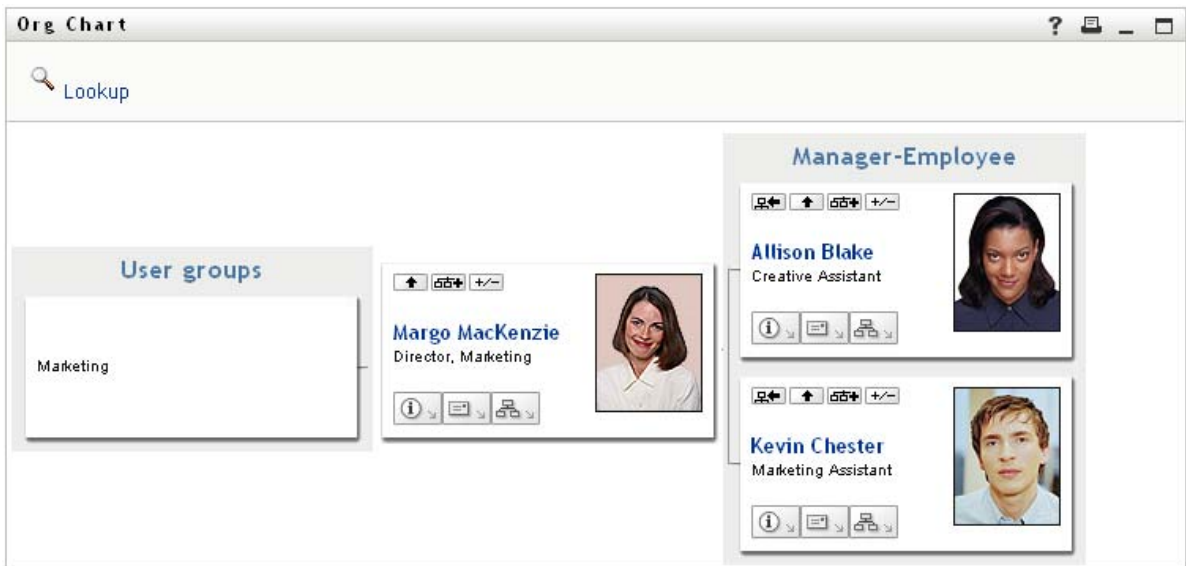
| Action                    | Description   |
|---------------------------|---|
| Expand Manager-Employee   | Select this option to open a Manager-Employee chart. Available if the chart is closed.                |
| Expand User Groups        | Select this option to open User groups. Available if User groups is closed.                           |
| Collapse Manager-Employee | Select this option to collapse the Manager-Employee chart for a card. Available if the chart is open. |
| Collapse User Groups      | Select this option to collapse User Groups for a card. Available if the chart is open.                |

Additional relationships are available in the list if your administrator defines them.

In the following example, Margo MacKenzie clicks *Choose relationship to Expand/Collapse* and selects *Expand User groups*:



She then clicks *To the Left* and sees the following:

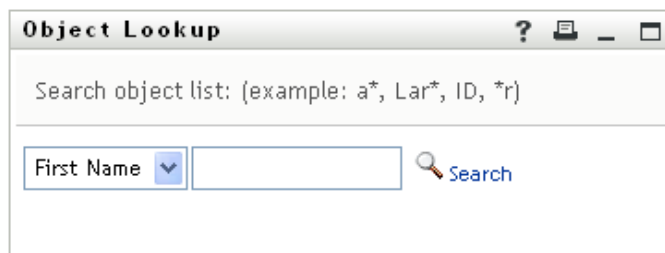


### 3.2.6 Looking Up a User in Organization Chart

You can look up a user in Organization Chart. This search is a quick way to find a user who is not in your current view or relationship chart. The looked-up user becomes the new root in your view.

- 1 Click the *Lookup* link at the top left corner of the chart.

The Lookup page displays:



- 2 Specify search criteria for the user you want:

**2a** Use the drop-down list to select whether the search is by *First Name* or *Last Name*.

**2b** In the text box next to the drop-down, type all or part of the name to search for.

The search finds every name that begins with the text you type. It is not case sensitive. You can optionally use the asterisk (\*) as a wildcard in your text to represent zero or more of any character.

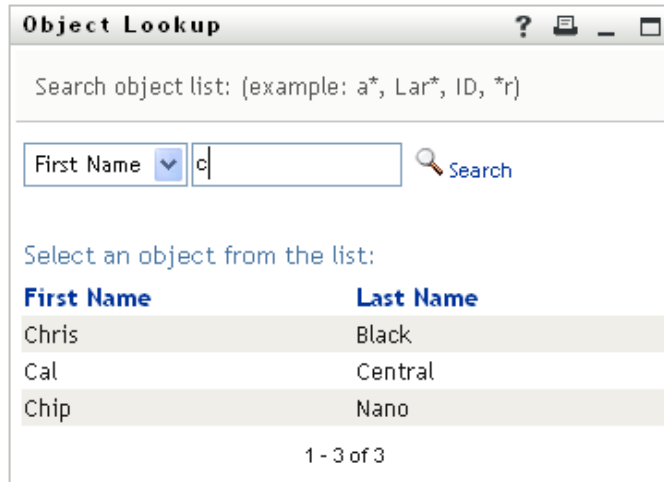
For instance, all of the following examples find the first name Chip:

- Chip
- chip
- c
- c\*
- \*p
- \*h\*

**Entity names with a dash are not supported** The search feature in the Organization Chart does not work if the entity type being displayed has a dash (-) in the name. The product does not support entities with dashes in their names.

**3** Click *Search*.

The Lookup page displays your search results:



If you see a list of users that includes the one you want, go to [Step 4](#). Otherwise, go back to [Step 2](#).

You can sort the search results in ascending or descending order by clicking the column headings.


**4** Select the user you want from the list.

The Lookup page closes and makes that user the new root in your view of the chart.

## 3.3 Displaying Detailed Information

You can display details (the Profile page) for a selected user in the chart:

**1** Find the card of a user whose details you want to display.

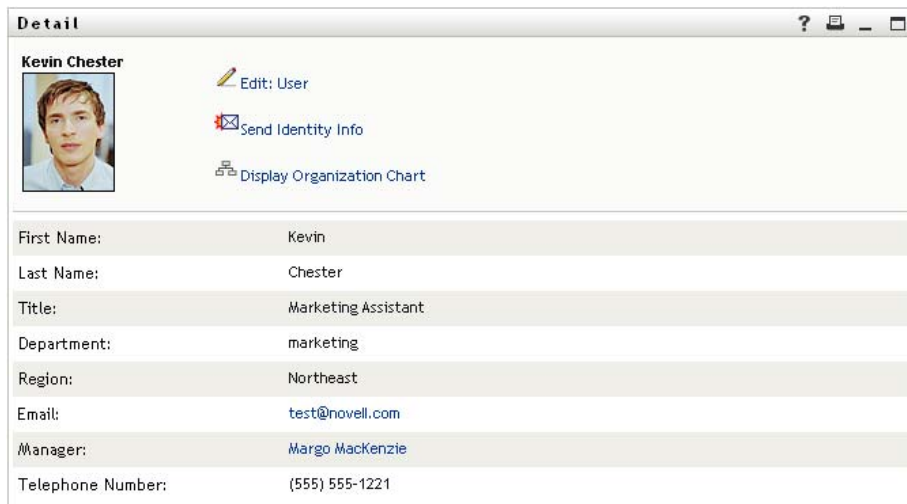
**2** Click *Identity Actions*  on that card:

A drop-down list displays.

**3** Click *Show Info* from the drop-down list. Additional options are listed if your administrator defines them.

The Profile page displays, showing detailed information about your chosen user:





This page is similar to your own My Profile page on the *Identity Self-Service* tab. However, as you view details about another user, you might not be authorized to see some of the data or perform some of the actions on the page. Consult your system administrator for assistance.

To learn about using the features of the Profile page, see [Chapter 5, “Using My Profile,” on page 57](#).

- 4 When you’re done with the Profile page, you can close its window.

## 3.4 Sending E-Mail from a Relationship Chart

This section describes:

- [Section 3.4.1, “E-Mailing Information About a User in a Chart,” on page 49](#)
- [Section 3.4.2, “Sending New E-Mail to a User in the Chart,” on page 50](#)
- [Section 3.4.3, “Sending E-Mail to a Manager’s Team,” on page 51](#)

### 3.4.1 E-Mailing Information About a User in a Chart

- 1 Find the card of a user whose details you want to e-mail to someone.

- 2 Click the e-mail icon  on the card:

A pop-up menu displays.

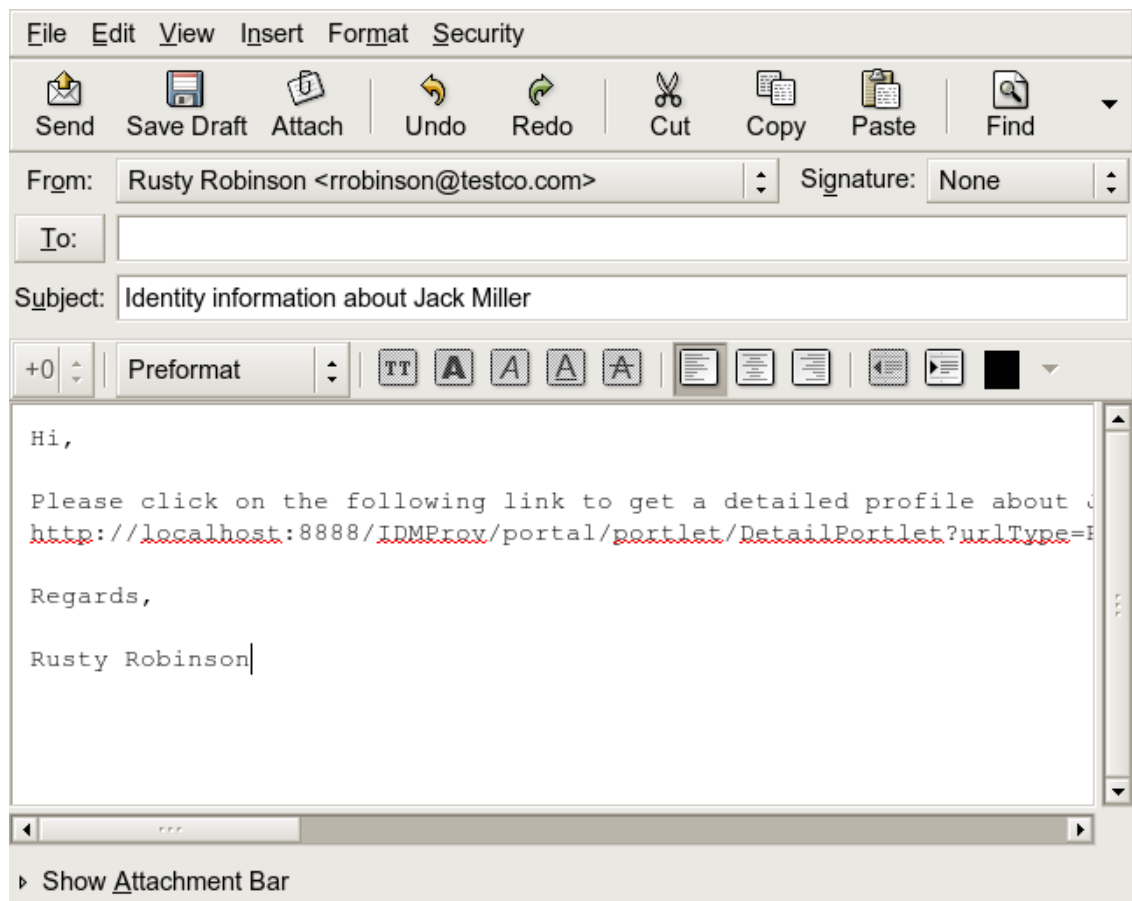
- 3 Select *Email Info*.

A new message is created in your default e-mail client. The following parts of the message are already filled in for you:

| This part of the message | Contains   |
|--------------------------|--|
| Subject                  | The text:<br><br>Identity Information for <i>user-name</i> |


| This part of the message | Contains  |
|--------------------------|---|
| Body                     | <p>Greeting, message, link, and sender's name.</p> <p>The link (URL) is to the Profile page that displays detailed information about your chosen user.</p> <p>This link prompts the recipient to log in to the Identity Manager User Application before it displays any information. The recipient must have appropriate authority to view or edit the data.</p> <p>To learn about using the features of the Profile page, see <a href="#">Chapter 5, "Using My Profile," on page 57</a>.</p> |

For example:



- 4 Specify the recipients of the message (and any additional content that you want).
- 5 Send the message.

### 3.4.2 Sending New E-Mail to a User in the Chart

- 1 Find the card of a user to whom you want to send e-mail.
- 2 Click the e-mail icon  on the card.

A pop-up menu displays.

**3** Select *New Email*.

A new message is created in your default e-mail client. The message is blank except for the *To* list, which specifies your chosen user as a recipient.

**4** Fill in the message contents.

**5** Send the message.

### 3.4.3 Sending E-Mail to a Manager's Team

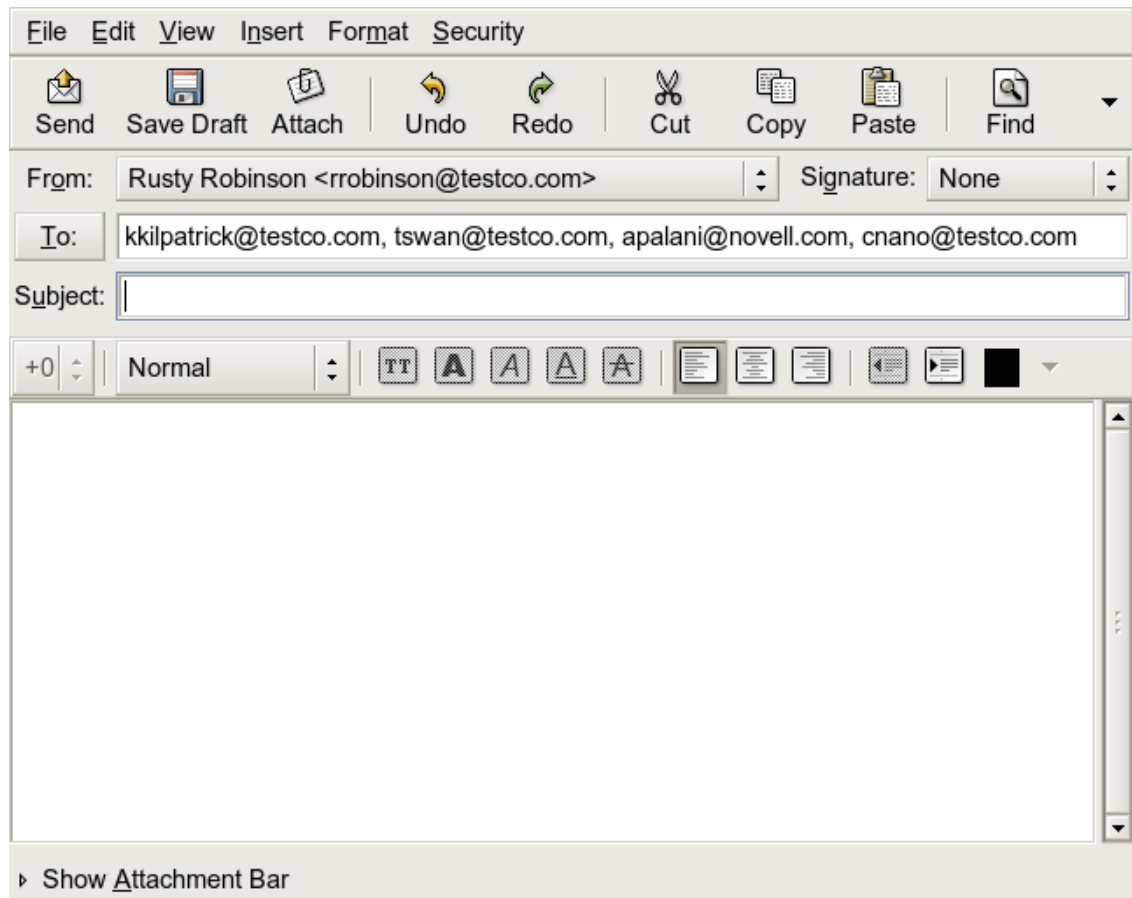
**1** Find the card of a user who manages a team to whom you want to send e-mail.

**2** Click the e-mail icon  on the card:

A pop-up menu displays.

**3** Select *Email to team*.

A new message is created in your default e-mail client. The message is blank except for the *To* list, which specifies each immediate subordinate of your chosen user (manager) as a recipient.



**4** Fill in the message contents.

**5** Send the message.



---

# 4 Using the Associations Report

This section tells you how to use the Associations Report page on the *Identity Self-Service* tab of the Identity Manager User Application. Topics include

- ♦ [Section 4.1, “About the Associations Report,” on page 53](#)
- ♦ [Section 4.2, “Displaying Associations,” on page 54](#)

---

**NOTE:** This section describes the default features of the Associations Report page. You might encounter some differences because of your job role, your level of authority, and customizations made for your organization; consult your system administrator for details.

---

For more general information about accessing and working with the *Identity Self-Service* tab, see [Chapter 2, “Introducing the Identity Self-Service Tab,” on page 33](#).

## 4.1 About the Associations Report

As an administrator, you can use the Associations Report page to list or troubleshoot some of the associations with which users have been provisioned. The application table shows:

- ♦ Application or system names for which the user has an association in the DirXML-Associations table in the Identity Vault. (The associations table is populated when the Identity Vault synchronizes a user account with a connected system through a policy or an entitlement.)
- ♦ The instance of the association.
- ♦ The status of the association. See [Table 4-1](#) for status descriptions.

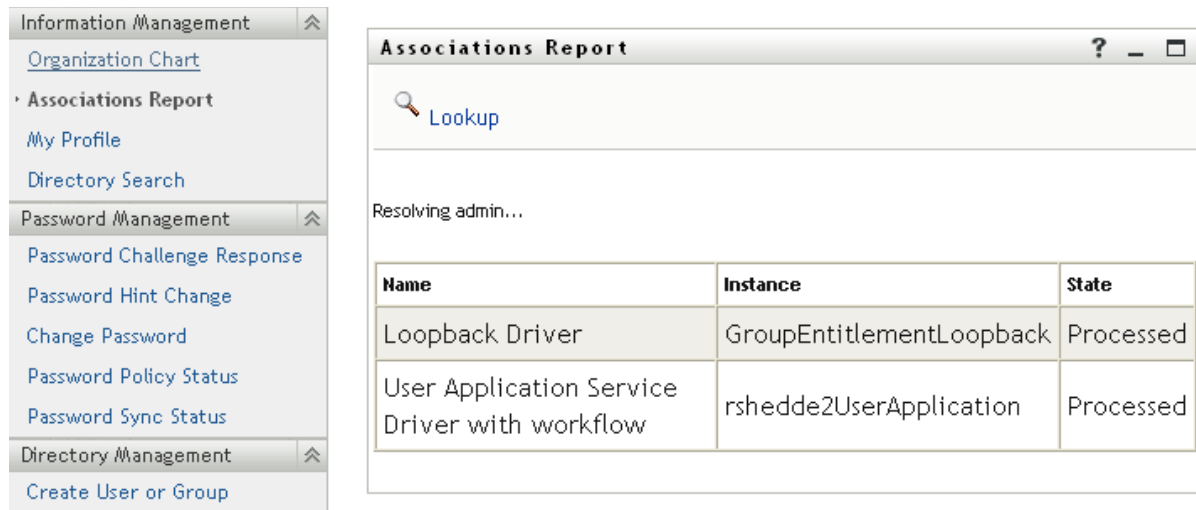
**Table 4-1** Association Status Table

| Status    | Indicates   |
|-----------|---|
| Processed | A driver recognizes the user for the driver’s target application. Users might want to check whether they need to issue a provisioning request for an application or system that does not appear in their associations lists. Or, if an application is in their lists but they cannot access it, users might want to check with their application administrators to determine the problem. |
| Disabled  | The application is probably unavailable to the user.  |
| Pending   | The association is waiting for something.   |
| Manual    | A manual process is required to implement the association.  |
| Migrate   | Migration is required.  |
| ANY       | Miscellaneous kinds of status.  |

Not all provisioned resources are represented in the Identity Vault.

Figure 4-1 on page 54 shows an example of the Associations Report page.

**Figure 4-1** The Associations Report Page



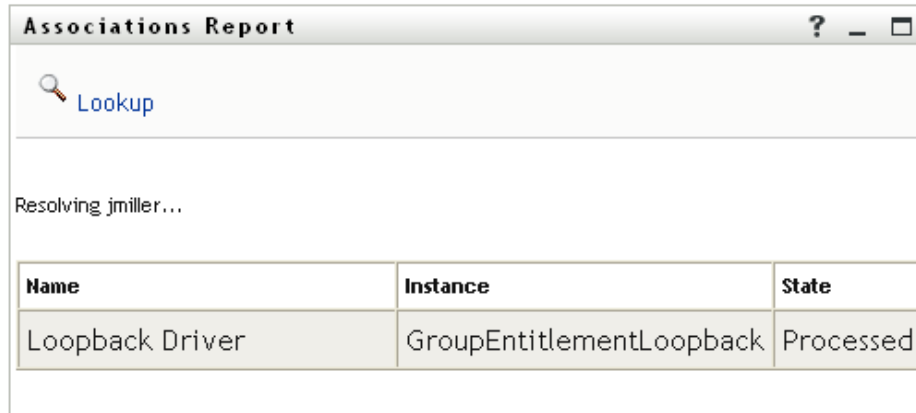
## 4.2 Displaying Associations

When you click *Associations Report*, the first associations shown are your own. To display another user's associations:

- 1 On the *Identity Self-Service* tab, under *Information Management*, click *Associations Report*.
- 2 Above the associations table, click *Lookup*.
- 3 In the Object Lookup window, select *First Name* or *Last Name* from the drop-down menu and specify a search string. The Object Lookup window displays both *First Name* and *Last Name*.



- 4 Select a name. The associations table displays associations for that name.



The screenshot shows a window titled "Associations Report" with a search bar containing "Lookup" and a magnifying glass icon. Below the search bar, the text "Resolving jmiller..." is displayed. A table with three columns: "Name", "Instance", and "State" is shown. The table contains one row with the following data:

| Name            | Instance                 | State     |
|-----------------|--------------------------|-----------|
| Loopback Driver | GroupEntitlementLoopback | Processed |





# 5 Using My Profile

This section tells you how to use the My Profile page on the *Identity Self-Service* tab of the Identity Manager User Application. Topics include:

- ◆ [Section 5.1, “About My Profile,” on page 57](#)
- ◆ [Section 5.2, “Editing Your Information,” on page 58](#)
- ◆ [Section 5.3, “E-Mailing Your Information,” on page 63](#)
- ◆ [Section 5.4, “Displaying Your Organization Chart,” on page 64](#)
- ◆ [Section 5.5, “Linking to Other Users or Groups,” on page 65](#)

---

**NOTE:** This section describes the default features of the My Profile page. You might encounter some differences because of your job role, your level of authority, and customizations made for your organization; consult your system administrator for details.

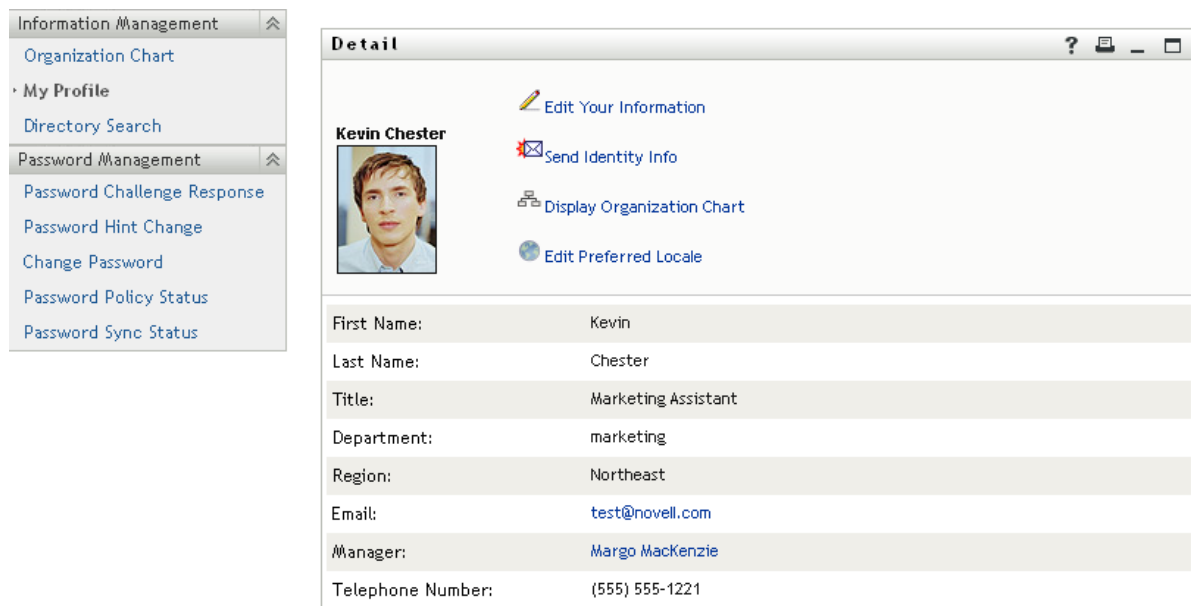
---

For more general information about accessing and working with the *Identity Self-Service* tab, see [Chapter 2, “Introducing the Identity Self-Service Tab,” on page 33](#).

## 5.1 About My Profile

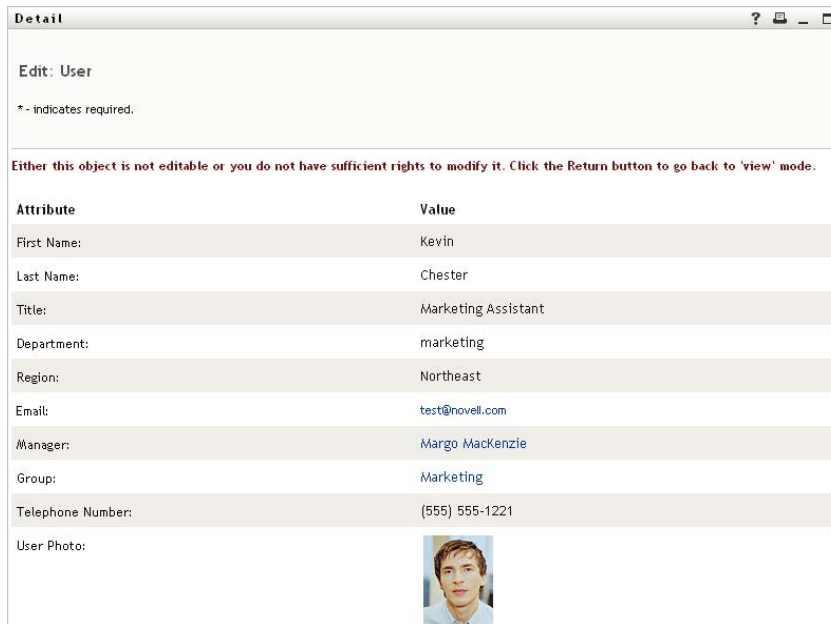
You can use the My Profile page to display the details for your user account and to work with that information, as needed. For example, here’s what Kevin Chester (Marketing Assistant) sees when he goes to the My Profile page:

**Figure 5-1** My Profile Detail Page



If you want to change some of these details, you can edit your information (although it's up to the system administrator to determine exactly what you are authorized to edit). For instance, suppose Kevin Chester clicks *Edit Your Information*. He sees a page in which he can edit Profile information, after his administrator gives him privileges to do so:

**Figure 5-2** *Edit Profile Page*




The screenshot shows a web browser window titled "Detail". The page content is as follows:

Edit: User  
\*- indicates required.

Either this object is not editable or you do not have sufficient rights to modify it. Click the Return button to go back to 'view' mode.

| Attribute         | Value               |
|-------------------|---------------------|
| First Name:       | Kevin               |
| Last Name:        | Chester             |
| Title:            | Marketing Assistant |
| Department:       | marketing           |
| Region:           | Northeast           |
| Email:            | test@novell.com     |
| Manager:          | Margo MacKenzie     |
| Group:            | Marketing           |
| Telephone Number: | (555) 555-1221      |

User Photo: 

Back on the main (viewing) page, My Profile provides links for performing other useful actions on your information. You can:

- ◆ Send your details (in the form of a link) to someone by e-mail
- ◆ Switch to displaying your organization chart instead of your details
- ◆ If authorized, select another user or group in the organization chart whose details you want to display
- ◆ Click an e-mail address to send a message to that account
- ◆ Specify a locale (language) for the instance of the User Application that you use.

## 5.2 Editing Your Information

My Profile provides an editing page that you can switch to when you want to make changes.

Some values might not be editable. Uneditable values appear on the editing page as read-only text or as links. If you have questions about what you're authorized to edit, consult your system administrator.

To edit your information:

- 1 Click the *Edit Your Information* link at the top of the My Profile page.
- 2 When the editing page displays, make your changes as needed. Use the editing buttons in [Table 5-1](#).
- 3 When you're done editing, click *Save Changes*, then click *Return*.

## 5.2.1 Hiding Information

Hiding a piece of your information hides it from everyone using the Identity Manager User Application, except you and the system administrator.







- 1 Click the *Edit Your Information* link at the top of the My Profile page.
- 2 On the editing page, find an item that you want to hide.
- 3 Click *Hide* next to that item.

*Hide* might be disabled for some items. The system administrator can enable this feature for specific items.

## 5.2.2 Using the Editing Buttons

Table 5-1 lists the editing buttons you can use to edit your profile details.

**Table 5-1** *Editing Buttons*


| Button  | What it does  |
|---|---|
|    | Looks up a value to use in an entry                       |
|    | Displays a <i>History</i> list of values used in an entry |
|    | Adds another entry  |
|  | Displays all entries for the attribute                    |
|  | Deletes an existing entry and its value                   |
|  | Lets you edit (specify and display) an image              |

**NOTE:** Add and delete groups in separate editing operations. If you remove and add groups in the same editing operation, the deleted group name reappears when the + (add) button is clicked.

The following sections tell you more about using some of these editing buttons:

- ♦ [“Looking Up a User” on page 59](#)
- ♦ [“Looking Up a Group” on page 61](#)
- ♦ [“Using the History List” on page 62](#)
- ♦ [“Editing an Image” on page 63](#)

### Looking Up a User

- 1 Click *Lookup*  to the right of an entry (for which you want to look up a user).  
The Lookup page displays:

The screenshot shows a window titled "Object Lookup" with a search bar containing the text "Search object list: (example: a\*, Lar\*, ID, \*r)". Below the search bar is a dropdown menu set to "First Name" and an empty text input field. To the right of the input field is a magnifying glass icon and the word "Search".

**2** Specify search criteria for the user you want:

**2a** Use the drop-down list to specify a search by *First Name* or *Last Name*.

**2b** In the text box next to the drop-down list, type all or part of the name to search for.

The search finds every name that begins with the text you type. It is not case sensitive. You can optionally use the asterisk (\*) as a wildcard in your text to represent zero or more of any character.

For instance, all of the following examples find the first name Chip:

```
Chip
chip
c
c*
*p
*h*
```

A manager lookup searches only for users who are managers.

**3** Click *Search*.

The Lookup page displays your search results:

The screenshot shows the "Object Lookup" window after a search. The search bar now contains the letter "c". Below the search bar, the text "Select an object from the list:" is displayed. A table with two columns, "First Name" and "Last Name", shows a single result: "Chip" and "Nano". At the bottom of the table, it says "1 - 1 of 1".

| First Name | Last Name |
|------------|-----------|
| Chip       | Nano      |


If you see a list of users that includes the one you want, go to [Step 4](#). Otherwise, go back to [Step 2](#).

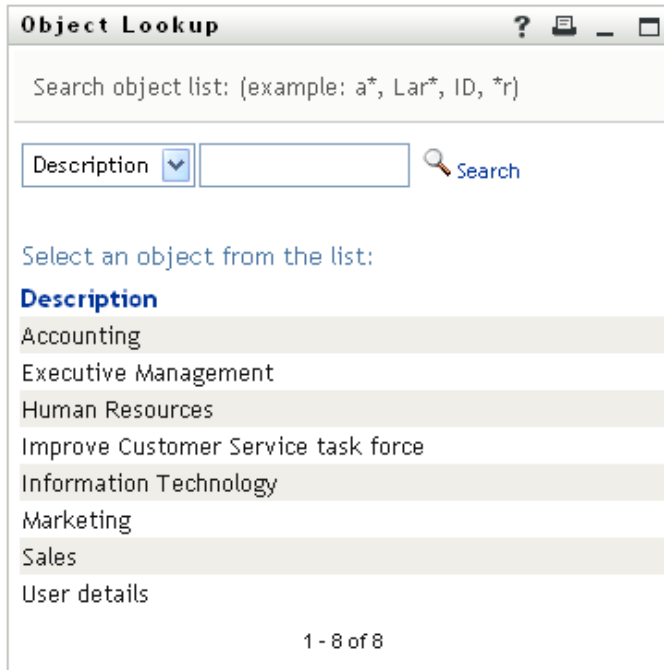
You can sort the search results in ascending or descending order by clicking the column headings.

**4** Select the user you want from the list.

The Lookup page closes and inserts the name of that user into the appropriate entry on the editing page.

## Looking Up a Group

- 1 Click *Lookup*  to the right of an entry (for which you want to look up a group).  
The Lookup page displays:



**Object Lookup** ? [minimize] [maximize] [close]

Search object list: (example: a\*, Lar\*, ID, \*r)

Description [v] [text box] Search

Select an object from the list:

**Description**

- Accounting
- Executive Management
- Human Resources
- Improve Customer Service task force
- Information Technology
- Marketing
- Sales
- User details

1 - 8 of 8

- 2 Specify search criteria for the group you want:

**2a** In the drop-down list, your only choice is to search by *Description*.

**2b** In the text box next to the drop-down list, type all or part of the description to search for.

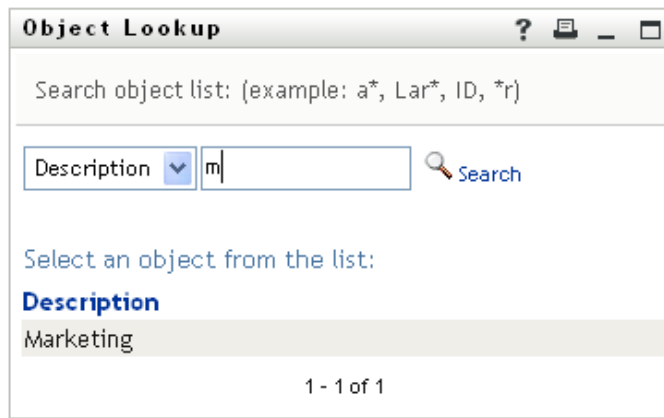
The search finds every description that begins with the text you type. It is not case sensitive. You can optionally use the asterisk (\*) as a wildcard in your text to represent zero or more of any character.

For instance, all of the following examples find the description Marketing:

```
Marketing
marketing
m
m*
*g
*|k*
```

- 3 Click *Search*.

The Lookup page displays your search results:




If you see a list of groups that includes the one you want, go to [Step 4](#). Otherwise, go back to [Step 2](#).

You can sort the search results in ascending or descending order by clicking the column heading.

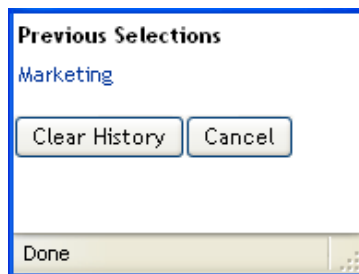
- 4 Select the group you want from the list.

The Lookup page closes and inserts the group into the appropriate entry on the editing page.

## Using the History List

- 1 Click *History*  to the right of an entry (whose previous values you want to see).

The *History* list displays. Values appear in alphabetical order.




- 2 Do one of the following:

| If you want to                    | Do this  |
|-----------------------------------|--|
| Pick from the <i>History</i> list | <p>Select a <i>value</i> that you want from the list.</p> <p>The <i>History</i> list closes and inserts that value into the appropriate entry on the editing page.</p>   |
| Clear the <i>History</i> list     | <p>Click <i>Clear History</i>.</p> <p>The <i>History</i> list closes and deletes its values for this entry. Clearing the <i>History</i> list does not change the current value of the entry on the editing page.</p> |

## Editing an Image

Editing your information might involve adding, replacing, or displaying an image:

- 1 On the editing page, click *Display* to display an image.
- 2 Click the plus sign icon  [Add Image](#) to add an image.



If an image already exists, you can click the pencil icon [Delete Image](#) to replace or remove it.

- 3 Click that button to display the File Upload page:



If this item already has an image, that image displays here.

- 4 To add an image or to replace the current one:
  - 4a Click *Browse* and select an appropriate image file (such as a GIF or JPG).
  - 4b Click *Save Changes* to upload the selected image file to the server.
- 5 Click *Close Window* to return to the editing page.

## 5.3 E-Mailing Your Information

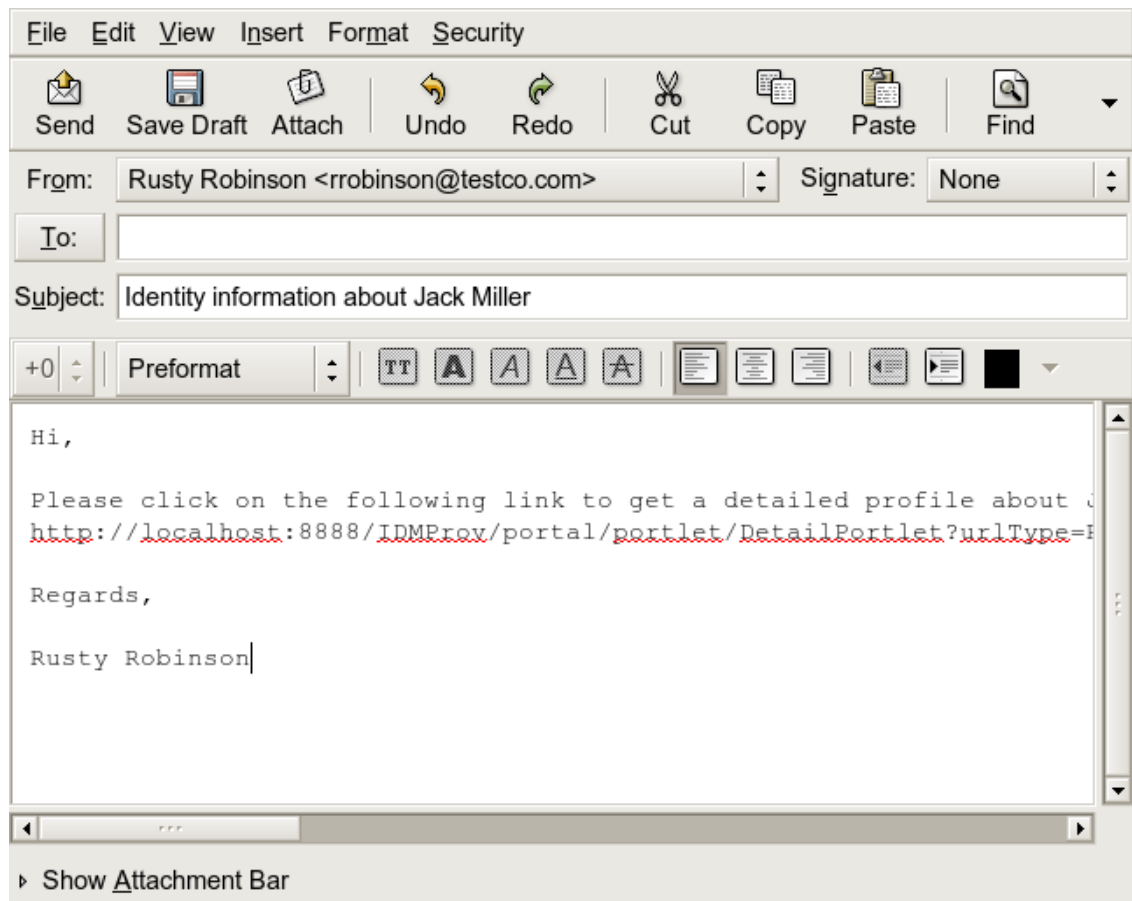
The My Profile page enables e-mailing details as links:

- 1 Click the *Send Identity Info* link toward the top of the My Profile page.

A new message is created in your default e-mail client. The following parts of the message are already filled in for you:

| This part of the message | Contains   |
|--------------------------|--|
| Subject                  | The text:<br><br><i>Identity Information for your-user-id</i>  |
| Body                     | A greeting, message, link, and your name.<br><br>The link (URL) is to the Profile page that displays detailed information about you.<br><br>This link prompts the recipient to log in to the Identity Manager User Application before it displays any information. The recipient must have appropriate authority to view or edit the data. |

For example:



- 2 Specify the recipients of the message (and any additional content that you want).
- 3 Send the message.

## 5.4 Displaying Your Organization Chart

To switch from My Profile to Organization Chart, click the *Display Organization Chart* link toward the middle of the My Profile page.

Your organization chart displays. For example:





To learn about using the features of this page, see [Chapter 3, “Using the Organization Chart,”](#) on page 39.

## 5.5 Linking to Other Users or Groups

The Detail page of your profile can include links to other users or groups. You can display the details (Profile page) for any other user or group that is listed as a link in your details.

To display detailed information about another user or group:

- 1 While viewing or editing information on the My Profile page, look for links that refer to the names of users or groups. Move your mouse cursor over text to reveal the underline that indicates a link.
- 2 Click a link to display the details for that user or group (in a separate window).
- 3 When you're done with that detail window, you can close it.

Here's a scenario that shows how someone might link to other user and group details. Timothy Swan (Vice President of Marketing) logs in to the Identity Manager User Application and goes to the My Profile page:


**Figure 5-3** The My Profile Page Shows Profile Details and Lists Profile Actions





The screenshot displays a user interface for profile management. On the left, there are two main menu sections: 'Information Management' and 'Password Management'. Under 'Information Management', the 'My Profile' link is highlighted. The 'Password Management' section includes options like 'Change Password' and 'Password Policy Status'. The main content area, titled 'Detail', features a profile picture of Timothy Swan, his name, and a list of actions: 'Edit Your Information', 'Send Identity Info', 'Display Organization Chart', and 'Edit Preferred Locale'. Below this, a table lists personal and professional details.

|                             |   |
|-----------------------------|---|
| Information Management      | ⤴ |
| Organization Chart          |   |
| My Profile                  |   |
| Directory Search            |   |
| Password Management         | ⤴ |
| Password Challenge Response |   |
| Password Hint Change        |   |
| Change Password             |   |
| Password Policy Status      |   |
| Password Sync Status        |   |

**Detail**

**Timothy Swan**



-  Edit Your Information
-  Send Identity Info
-  Display Organization Chart
-  Edit Preferred Locale

|                   |                                     |
|-------------------|-------------------------------------|
| First Name:       | Timothy                             |
| Last Name:        | Swan                                |
| Title:            | Director, Marketing, Vice President |
| Department:       | management                          |
| Region:           | Northeast                           |
| Email:            | test@novell.com                     |
| Manager:          | Terry Mellon                        |
| Telephone Number: | (555) 555-1204                      |

He clicks *Edit Your Information*.

**Figure 5-4** The Edit Detail Page

| Attribute         | Value  |
|-------------------|--|
| First Name:*      | Timothy  |
| Last Name:*       | Swan   |
| Title:            | Vice President, Marketing  |
| Department:       | management   |
| Region:           | Northeast  |
| Email:            | test@novell.com  |
| Manager:          | Terry Mellon   |
| Group:            | Executive Management<br>Improve Customer Service task force<br>Marketing |
| Telephone Number: | (555) 555-1204   |

He notices user names (Terry Mellon) and group names (Executive Management, Marketing, Improve Customer Service task force) that appear as links. He clicks *Marketing* and sees a new window:

**Figure 5-5** The Group Detail Page

[Edit: Group](#)

[Send Identity Info](#)

[Display Organization Chart](#)

**Marketing**

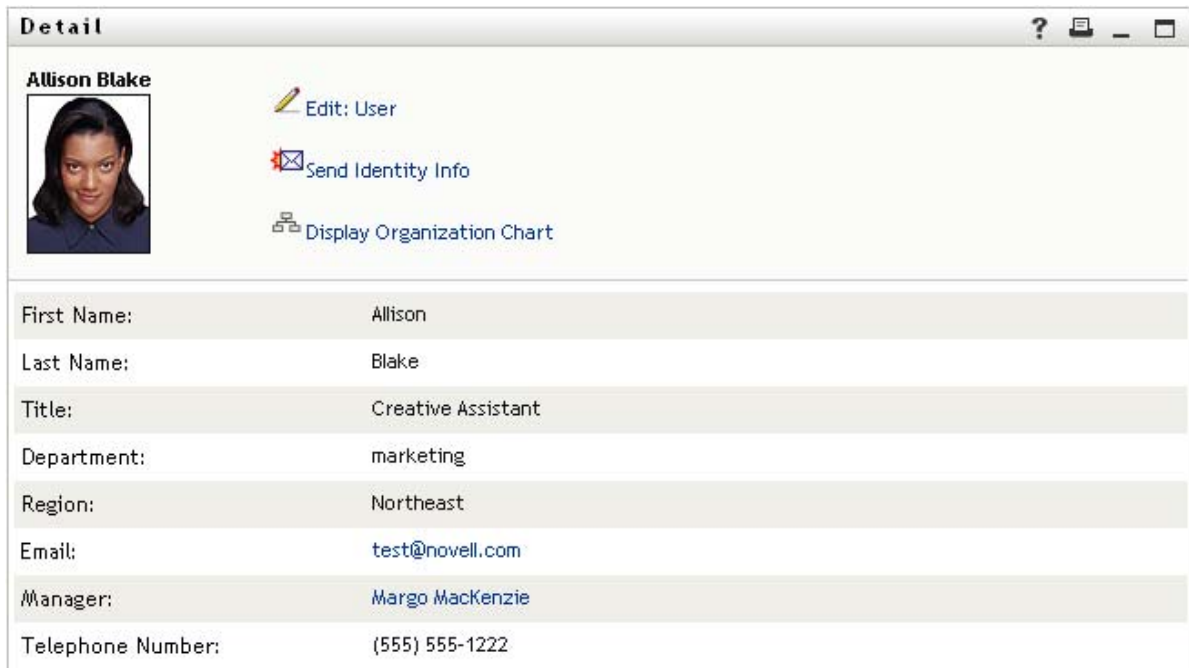
Description: Marketing





Members: [Timothy Swan](#), [Margo MacKenzie](#), [Kevin Chester](#), [Allison Blake](#)

This is the detailed information about the Marketing group. If he has permission, he can click *Edit Group* and use the *Edit Group* page to add or remove members from the group, change the group description, or even delete the group.

The names of the Marketing group's members are also links. He clicks *Allison Blake* and sees:

**Figure 5-6** The Group Detail Page Links to Group Members' Profiles



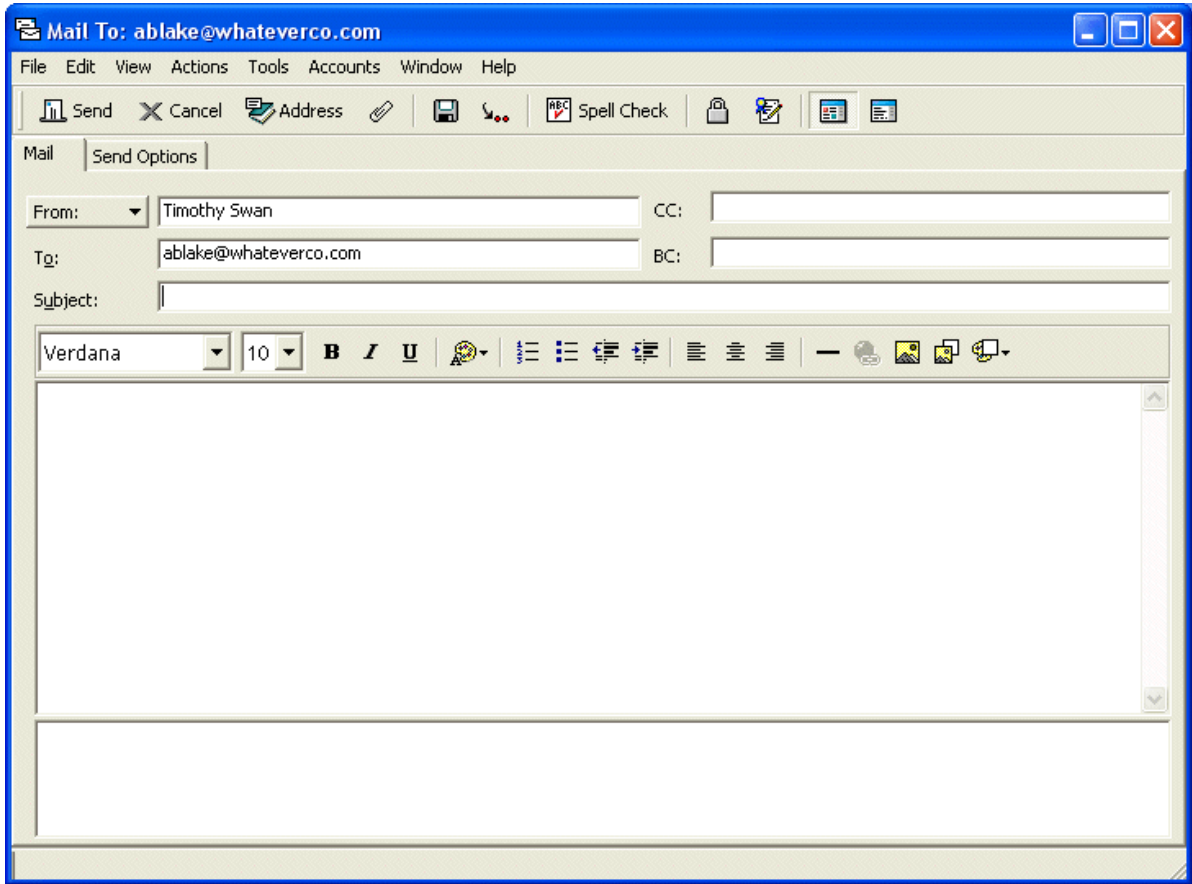
| Detail               |  |
|----------------------|--|
| <b>Allison Blake</b> |                             |
|                      |  Edit: User                 |
|                      |  Send Identity Info         |
|                      |  Display Organization Chart |
| First Name:          | Allison  |
| Last Name:           | Blake  |
| Title:               | Creative Assistant   |
| Department:          | marketing  |
| Region:              | Northeast  |
| Email:               | <a href="mailto:test@novell.com">test@novell.com</a>   |
| Manager:             | <a href="#">Margo MacKenzie</a>  |
| Telephone Number:    | (555) 555-1222   |

This is the detailed information about user Allison Blake (one of his employees).

He can click *Edit: User*, and, if the system administrator has given him the ability to do so, edit this user's details (except the Department and Region attributes) or delete this user.

Allison's e-mail address is a link. When he clicks it, his e-mail client creates a new message to her:

**Figure 5-7** E-Mail Message to User from User's Profile Page



He can now type the message contents and send it.

## 5.6 Choosing a Preferred Language

You can select the locale (language) that you prefer to use in the Identity Manager User Application. You can set the preferred locale at any time in *My Profile*.

- 1 Click *Identity Self-Service > Information Management > My Profile > Edit Preferred Locale*. The *Edit Preferred Locale* page opens.
- 2 Add a locale by opening the *Available Locales* drop-down list, selecting a locale, and clicking *Add*.
- 3 Change the order of preference by selecting a locale from the *Locales in order of preference list* and choosing *Move Up*, *Move Down*, or *Remove*.
- 4 Click *Save Changes*.

**Edit Preferred Language**

User: Chip Nano

Select your preferred languages (locales) for displaying pages in the Identity Manager User Application.

**Languages in order of preference**

Move Up  
Move Down  
Remove

**Available Languages**

Select a locale to add... Add

Save Changes Close

The Identity Manager User Application pages are displayed in one or more preferred languages (locales) according to these rules:

1. The User Application uses locales defined in the User Application, according to the order in the preferred-locale list.
2. If no preferred locale is defined for the User Application, the User Application uses the preferred browser languages in the order listed.
3. If no preferred locale is defined for the User Application or the browser, the User Application default is used.

## 5.6.1 Defining a Preferred Language in the Browser

In Firefox\*, add languages through *Tools > General > Languages > Languages*. Place your preferred language at the top of the list. In Internet Explorer, set language through *View > Encoding*.

# 6 Using Directory Search

This section tells you how to use the Directory Search page on the *Identity Self-Service* tab of the Identity Manager User Application. Topics include:

- ♦ [Section 6.1, “About Directory Search,” on page 71](#)
- ♦ [Section 6.2, “Performing Basic Searches,” on page 74](#)
- ♦ [Section 6.3, “Performing Advanced Searches,” on page 74](#)
- ♦ [Section 6.4, “Working with Search Results,” on page 83](#)
- ♦ [Section 6.5, “Using Saved Searches,” on page 89](#)

---

**NOTE:** This section describes the default features of the Directory Search page. You might encounter some differences because of your job role, your level of authority, and customizations made for your organization; consult your system administrator for details.

---

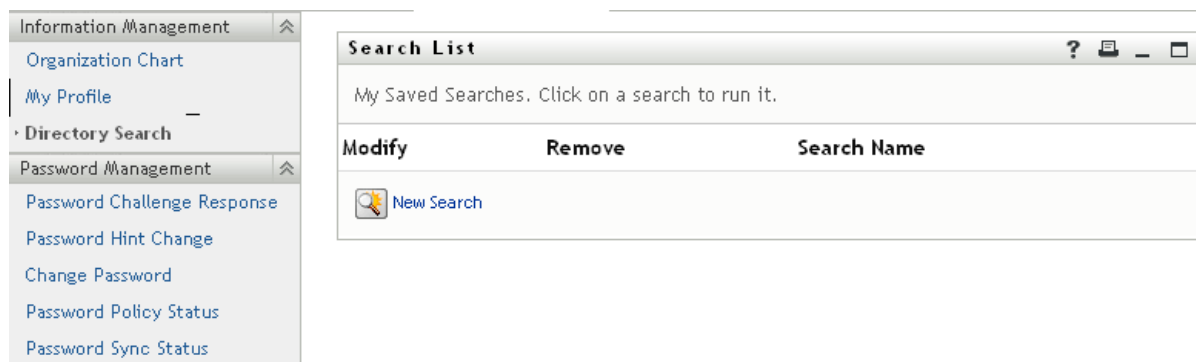
For more general information about accessing and working with the *Identity Self-Service* tab, see [Chapter 2, “Introducing the Identity Self-Service Tab,” on page 33](#).

## 6.1 About Directory Search

You can use the Directory Search page to search for users, groups, or teams by entering search criteria or by using previously saved search criteria.

For example, suppose Timothy Swan (Marketing Director) needs to search for information about someone in his organization. He goes to the Directory Search page and sees this by default:

**Figure 6-1** Directory Search Page



He doesn't yet have any saved searches to select from, so he selects *New Search*.

There's a user he wants to contact whose first name begins with the letter *C*, but he can't remember the full name. He just needs to specify a basic search with this criterion:

**Figure 6-2** Specify a Search Criterion on the Search List Page

The screenshot shows a window titled "Search List" with a search interface. At the top, it says "Basic Search." Below that, there is a "Search for:" dropdown menu set to "User". Underneath, there are three columns: "Item Category", "Expression", and "Search Term". The "Item Category" dropdown is set to "First Name", the "Expression" dropdown is set to "starts with", and the "Search Term" text box contains the letter "C". A "Search" button is located below these fields. At the bottom of the window, there are two links: "My Saved Searches" and "Advanced Search".

The search results display, enabling Timothy to examine and work with his requested information. By default, *Identity* tab information is displayed:

**Figure 6-3** Search Results

The screenshot shows a window titled "Search List" displaying search results. At the top, it says "Search Results. Use the tabs below for different views of your result set." Below that, there is a summary: "User: (First Name starts with C)", "Sorted by: Last Name", and "Total Matches: 3". There are three tabs: "Identity", "Location", and "Organization". The "Identity" tab is selected. Below the tabs is a table with the following data:

| First Name | Last Name | Title                     | Email | Telephone Number |
|------------|-----------|---------------------------|-------|------------------|
| Chris      | Black     | Sales Director, Black     | ✉     | (555) 555-1338   |
| Cal        | Central   | VP, North American Sales  | ✉     | (555) 555-1209   |
| Chip       | Nano      | Chief Information Officer | ✉     | (555) 555-1222   |

Below the table, it says "1 - 3 of 3". At the bottom of the window, there are five links: "My Saved Searches", "Save Search", "Export Results", "Revise Search", and "New Search".

Timothy clicks the *Organization* tab in the search results to get another view of the information. He recalls that the person he seeks works for Kip Keller, so that narrows it down to Cal Central:



**Figure 6-4** Use Tabs to Change Views of Search Results



In addition to the tabs for different views, the search results page provides links and buttons for performing actions on its information. You can:

- Sort the rows of information by clicking the column headings
- Display details (Profile page) for a user or group by clicking its row
- Send new e-mail to a user by clicking the e-mail icon in that user's row
- Save the search for future reuse
- Export the results to a text file
- Revise the search by changing its criteria

When generating search results, you might sometimes need more than a basic search to describe the information you want. You can use an advanced search to specify complex criteria.

If there's an advanced search that you might need to perform again, you can retain it as a saved search. Saved searches are even handy for basic searches that you run frequently. For instance, Timothy Swan has added a couple of saved searches that he often uses:

**Figure 6-5** Saved Searches, on the Search List Page



## 6.2 Performing Basic Searches

- 1 Go to the Directory Search page and click *New Search*. The Basic Search page displays by default:

| Item Category | Expression  | Search Term |
|---------------|-------------|-------------|
| First Name    | starts with |             |

- 2 In the *Search for* drop-down list, specify the type of information to find by selecting *Group* or *User*.

- 3 In the *Item Category* drop-down list, select an attribute to search on. For example:

Last Name

The list of available attributes is determined by what you're searching for (users or groups).

- 4 In the *Expression* drop-down list, select a comparison operation to perform against your chosen attribute. For example:

equals

For more information, see [Section 6.3.1, "Selecting an Expression,"](#) on page 77.

- 5 In the *Search Term* entry box, specify a value to compare against your chosen attribute. For example:

Smith

For more information, see [Section 6.3.2, "Specifying a Value for Your Comparison,"](#) on page 79.

- 6 Click *Search*.

Your search results display.

To learn about what to do next, see [Section 6.4, "Working with Search Results,"](#) on page 83.

## 6.3 Performing Advanced Searches

If you need to specify multiple criteria when searching for users or groups, you can use an advanced search. For example:

```
Last Name equals Smith AND Title contains Rep
```

If you specify multiple criteria groupings (to control the order in which criteria are evaluated), you'll use the same logical operations to connect them. For example, to perform an advanced search with the following criteria (two criteria groupings connected by an or):

(Last Name **equals** Smith **AND** Title **contains** Rep) **OR** (First Name **starts with** k **AND** Department **equals** Sales)

specify the following shown in [Figure 6-6 on page 75](#):

**Figure 6-6** Specifying an Advanced Search on the Search List Page

**Search List** ? [Icons]

Advanced Search. Specify one or more criteria for your search.

Search for: User [v]

With this criteria:

| Operator | Item Category | Expression   | Search Term | Add/Remove Criteria |
|----------|---------------|--------------|-------------|---------------------|
|          | Last Name [v] | equals [v]   | Smith       | [+] [-]             |
| and [v]  | Title [v]     | contains [v] | Rep         | [+] [-]             |

[+] Remove Criteria Grouping

or [v]

With this criteria:

| Operator | Item Category  | Expression      | Search Term | Add/Remove Criteria |
|----------|----------------|-----------------|-------------|---------------------|
|          | First Name [v] | starts with [v] | k           | [+] [-]             |
| and [v]  | Department [v] | equals [v]      | Sales       | [+] [-]             |

[+] Remove Criteria Grouping

[+] Add Criteria Grouping

Search

[Icon] My Saved Searches [Icon] Basic Search

The result of this search is shown in [Figure 6-7 on page 76](#).

**Figure 6-7** Result of Advanced Search

Search Results. Use the tabs below for different views of your result set.

**User:** (Last Name equals Smith and Title contains Rep) -or- (First Name starts with k and Department equals Sales)  
**Sorted by:** Department  
**Total Matches:** 5

Identity Location **Organization**

| First Name | Last Name | Title                    | Department | Manager          | Email |
|------------|-----------|--------------------------|------------|------------------|-------|
| Jane       | Smith     | HR, Representative       | hr         | Renee Resource   | ✉     |
| Kate       | Smith     | Sales Representative     | sales      | Sally South      | ✉     |
| Ken        | Carson    | Account Executive        | sales      | Ned North        | ✉     |
| Kevin      | Chang     | Account Executive        | sales      | Ned North        | ✉     |
| Kip        | Keller    | VP, North American Sales | sales      | Kelly Kilpatrick | ✉     |

1 - 5 of 5

My Saved Searches Save Search Export Results Revise Search New Search

To perform an advanced search:

- 1 Go to the Directory Search page and click *New Search*. The Basic Search page displays by default.
- 2 Click *Advanced Search*. The Advanced Search page displays:

Advanced Search. Specify one or more criteria for your search.

Search for: User

With this criteria:

| Item Category | Expression  | Search Term | Add/Remove Criteria |
|---------------|-------------|-------------|---------------------|
| First Name    | starts with |             | +                   |

Search Add Criteria Grouping

My Saved Searches Basic Search

- 3 In the *Search for* drop-down list, specify the type of information to find by selecting one of the following:
  - ◆ Group
  - ◆ User

You can now fill in the *With this criteria* section.
- 4 Specify a criterion of a criteria grouping:
  - 4a Use the *Item Category* drop-down list to select an attribute to search on. For example:

Last Name

The list of available attributes is determined by what you're searching for (users or groups).

- 4b** Use the *Expression* drop-down list to select a comparison operation to perform against your chosen attribute. For example:

equals

For more information, see [Section 6.3.1, "Selecting an Expression,"](#) on page 77.

- 4c** Use the *Search Term* entry to specify a value to compare against your chosen attribute. For example:

Smith

For more information, see [Section 6.3.2, "Specifying a Value for Your Comparison,"](#) on page 79.

- 5** If you want to specify another criterion of a criteria grouping:

- 5a** Click *Add Criteria* on the right side of the criteria grouping:



- 5b** On the left side of the new criterion, use the *Criteria Logical Operator* drop-down list to connect this criterion with the preceding one; select either *and* or *or*. You can use only one of the two types of logical operator within any one criteria grouping.

- 5c** Repeat this procedure, starting with [Step 4](#).

To delete a criterion, click *Remove Criteria* to its right: 

- 6** If you want to specify another criteria grouping:

- 6a** Click *Add Criteria Grouping*:



- 6b** Above the new criteria grouping, use the *Criteria Grouping Logical Operator* drop-down list to connect this grouping with the preceding one; select either *and* or *or*.

- 6c** Repeat this procedure, starting with [Step 4](#).

To delete a criteria grouping, click *Remove Criteria Grouping* directly above

it:  *Remove Criteria Grouping*

- 7** Click *Search*.

Your search results display.

To learn about what to do next, see [Section 6.4, "Working with Search Results,"](#) on page 83.

## 6.3.1 Selecting an Expression

Click *Expression* to select a comparison criterion for your search. The list of comparison (relational) operations available to you in a criterion is determined by the type of attribute specified in that criterion:

**Table 6-1** Comparison Operations for Searching

| If the attribute is a                                   | You can select one of these comparison operations  |
|---|--|
| String (text)   | <ul style="list-style-type: none"> <li>◆ starts with</li> <li>◆ contains</li> <li>◆ equals</li> <li>◆ ends with</li> <li>◆ is present</li> <li>◆ does not start with</li> <li>◆ does not contain</li> <li>◆ does not equal</li> <li>◆ does not end with</li> <li>◆ is not present</li> </ul>   |
| String (text) with a predetermined list of choices      | ◆ equals   |
| User or group (or other object identified by DN)        | ◆ is present   |
| Boolean (true or false)                                 | <ul style="list-style-type: none"> <li>◆ does not equal</li> <li>◆ is not present</li> </ul>   |
| User (item category: Manager, Group, or Direct Reports) | <ul style="list-style-type: none"> <li>◆ equals</li> <li>◆ is present</li> <li>◆ does not equal</li> <li>◆ is not present</li> </ul>   |
| Group (item category: Members)                          | <ul style="list-style-type: none"> <li>◆ equals</li> <li>◆ is present</li> <li>◆ does not equal</li> <li>◆ is not present</li> </ul>   |
| Time (in date-time or date-only format)                 | ◆ equals   |
| Number (integer)  | <ul style="list-style-type: none"> <li>◆ greater than</li> <li>◆ greater than or equal to</li> <li>◆ less than</li> <li>◆ less than or equal to</li> <li>◆ is present</li> <li>◆ does not equal</li> <li>◆ not greater than</li> <li>◆ not greater than or equal to</li> <li>◆ not less than</li> <li>◆ not less than or equal to</li> <li>◆ is not present</li> </ul> |

## 6.3.2 Specifying a Value for Your Comparison

The type of attribute specified in a criterion also determines how you specify the value for a comparison in that criterion:

**Table 6-2** Method of Entering Comparison Value

| If the attribute is a                              | You do this to specify the value   |
|--|--|
| String (text)                                      | Type your text in the text box that displays on the right.                                   |
| String (text) with a predetermined list of choices | Select a choice from the drop-down list that displays on the right.                          |
| User or group (or other object identified by DN)   | Use the <i>Lookup</i> , <i>History</i> , and <i>Reset</i> buttons that display on the right. |
| Time (in date-time or date-only format)            | Use the <i>Calendar</i> and <i>Reset</i> buttons that display on the right.                  |
| Number (integer)                                   | Type your number in the text box that displays on the right.                                 |
| Boolean (true or false)                            | Type <code>true</code> or <code>false</code> in the text box that displays on the right.     |

Don't specify a value when the comparison operation is one of the following:

- ◆ is present
- ◆ is not present

### Case in Text

Text searches are not case sensitive. You'll get the same results no matter which case you use in your value. For example, these are all equivalent:

McDonald

mcdonald

MCDONALD

### Wildcards in Text

You can optionally use the asterisk (\*) as a wildcard in your text to represent zero or more of any character. For example:

Mc\*

\*Donald




\*Don\*

McD\*d

### Using the Lookup, History, and Reset Buttons

Some search criteria display Lookup, History, and Reset buttons. This section describes how to use these buttons:

**Table 6-3** *Lookup, History, and Reset Buttons in Search Criteria*

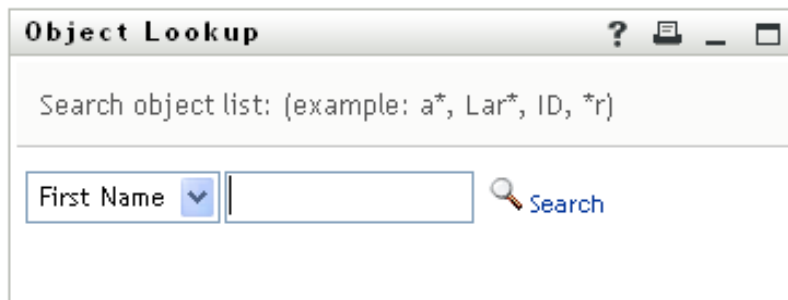
| Button  | What It Does   |
|---|--|
|  | Looks up a value to use for a comparison                       |
|  | Displays a <i>History</i> list of values used for a comparison |
|  | Resets the value for a comparison                              |

To look up a user:

- 1 Click *Lookup* to the right of an entry (for which you want to look up the user):



The Lookup page displays:



- 2 Specify search criteria for the user you want:

- 2a Use the drop-down list to select a search by *First Name* or *Last Name*.

- 2b In the text box next to the drop-down list, type all or part of the name to search for.

The search finds every name that begins with the text you type. It is not case sensitive. You can optionally use the asterisk (\*) as a wildcard in your text to represent zero or more of any character.

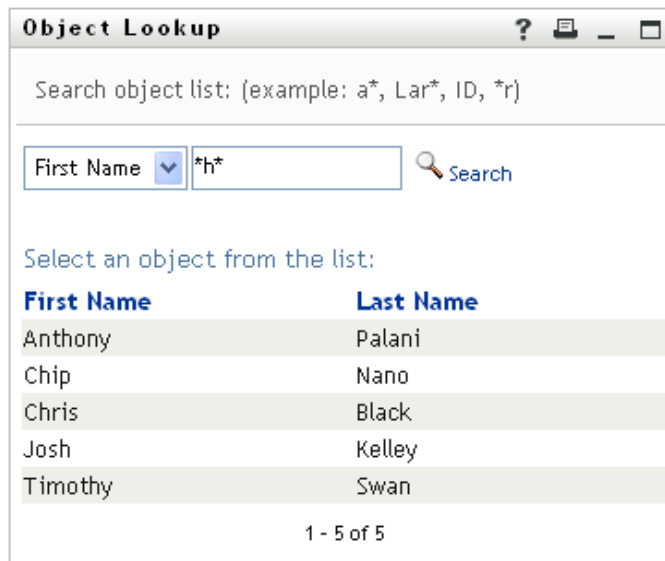
For instance, all of the following examples finds the first name Chip:

```
Chip
chip
c
c*
*p
*h*
```

- 3 Click *Search*.

The Lookup page displays your search results:





If you see a list of users that includes the one you want, go to [Step 4](#). Otherwise, go back to [Step 2](#).

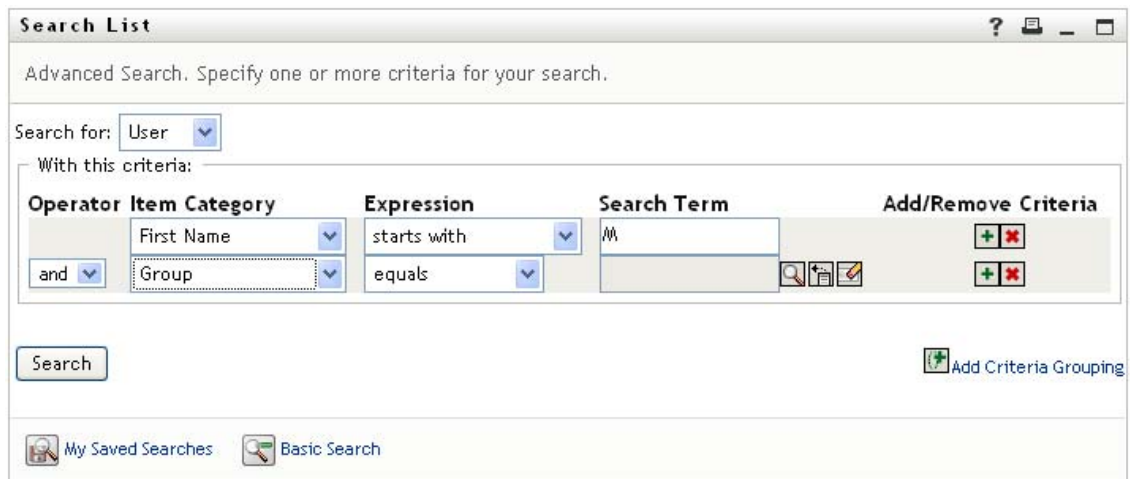
You can sort the search results in ascending or descending order by clicking the column headings.

- 4 Select the user you want from the list.

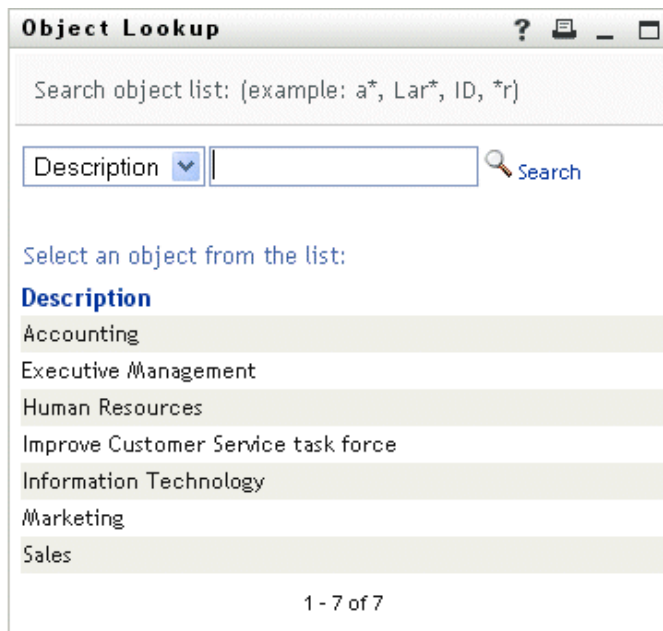
The Lookup page closes and inserts the name of that user into the appropriate entry as the value to use for your comparison.

To look up a group as a search criterion for a user:

- 1 Add *Group* as a search criterion, then click *Lookup*  to the right of the *Search Term* field:



The Lookup page displays search results:



**2** Specify search criteria for the group you want:

**2a** In the drop-down list, your only choice is to search by *Description*.

**2b** In the text box next to the drop-down list, type all or part of the description to search for.

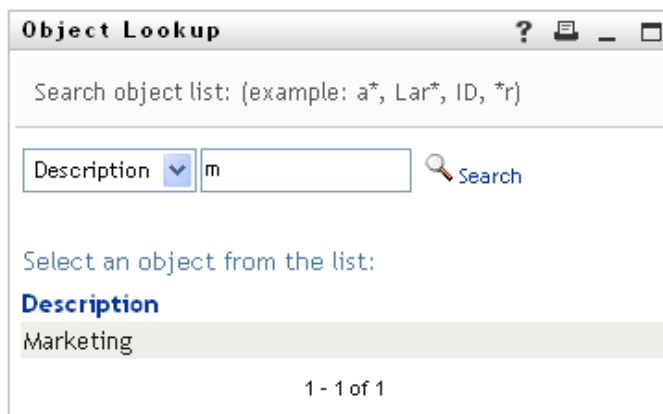
The search finds every description that begins with the text you type. It is not case sensitive. You can optionally use the asterisk (\*) as a wildcard in your text to represent zero or more of any character.

For instance, all of the following examples find the description Marketing:

```
Marketing
marketing
m
m*
*g
*|c*
```

**3** Click *Search*.

The Lookup page displays your search results:




If you see a list of groups that includes the one you want, go to [Step 4](#). Otherwise, go back to [Step 2](#).

You can sort the search results in ascending or descending order by clicking the column heading.

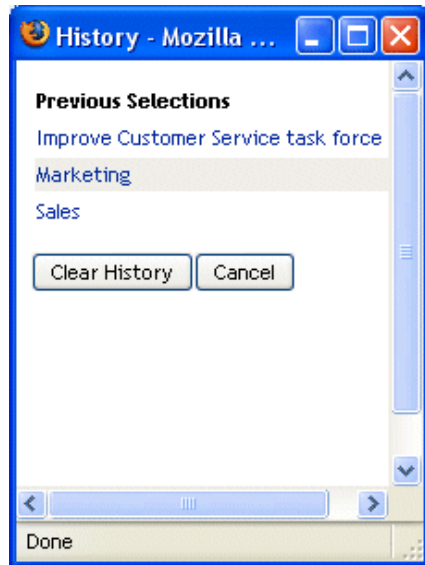
- 4 Select the group you want from the list.

The Lookup page closes and inserts the description of that group into the appropriate entry as the value to use for your comparison.

To use the *History* list:

- 1 Click *History*  to the right of an entry (whose previous values you want to see):

The *History* list displays previous values for this criterion in alphabetical order:



- 2 Do one of the following:

| If you want to                    | Do this   |
|-----------------------------------|---|
| Pick from the <i>History</i> list | Select a value that you want from the list.<br><br>The <i>History</i> list closes and inserts that value into the appropriate entry as the value to use for your comparison.                                  |
| Clear the <i>History</i> list     | Click <i>Clear History</i> .<br><br>The <i>History</i> list closes and deletes its values for this entry. Clearing the <i>History</i> list does not change the current value of the entry in your comparison. |

## 6.4 Working with Search Results

This section tells you how to work with the results that display after a successful search:

- ♦ [Section 6.4.1, “About Search Results,” on page 84](#)
- ♦ [Section 6.4.2, “Using the Search List,” on page 85](#)
- ♦ [Section 6.4.3, “Other Actions You Can Perform,” on page 87](#)

## 6.4.1 About Search Results

The content of your search results depends on the type of search you perform:

- ♦ “For a User Search” on page 84
- ♦ “For a Group Search” on page 85

On any search results page, you can select

- ♦ View My Saved Searches
- ♦ Save Search
- ♦ Revise Search
- ♦ Export Results
- ♦ Start a New Search

### For a User Search

In the results of a user search, the list of users provides tabs for three views of the information:

- ♦ *Identity* (contact information)
- ♦ *Location* (geographical information)
- ♦ *Organization* (organizational information)

**Figure 6-8** User Search Results

**Search List**

Search Results

Use the tabs below for different views of your result set.

**User:** (Group equals Marketing or Group equals Sales )  
**Sorted by:** Last Name  
**Total Matches:** 22

Identity Location Organization

| First Name | Last Name | Title                     | Email | Telephone Number |
|------------|-----------|---------------------------|-------|------------------|
| Bill       | Bender    | Technical Account Manager | ✉     | (555) 555-1320   |
| Chris      | Black     | Sales Director, Black     | ✉     | (555) 555-1338   |
| Allison    | Blake     | Creative Assistant        | ✉     | (555) 555-1222   |
| Jane       | Brown     | Technical Account Manager | ✉     | (555) 555-1316   |
| Bill       | Burke     | Sales Manager, Central    | ✉     | (555) 555-1210   |
| Ken        | Carson    | Account Executive         | ✉     | (555) 555-1315   |
| Ricardo    | Castro    | VP, Latin American Sales  | ✉     | (555) 555-1206   |
| Cal        | Central   | VP, North American Sales  | ✉     | (555) 555-1209   |
| Kevin      | Chang     | Account Executive         | ✉     | (555) 555-1212   |
| Kevin      | Chester   | Marketing Assistant       | ✉     | (555) 555-1221   |

1 - 10 of 22

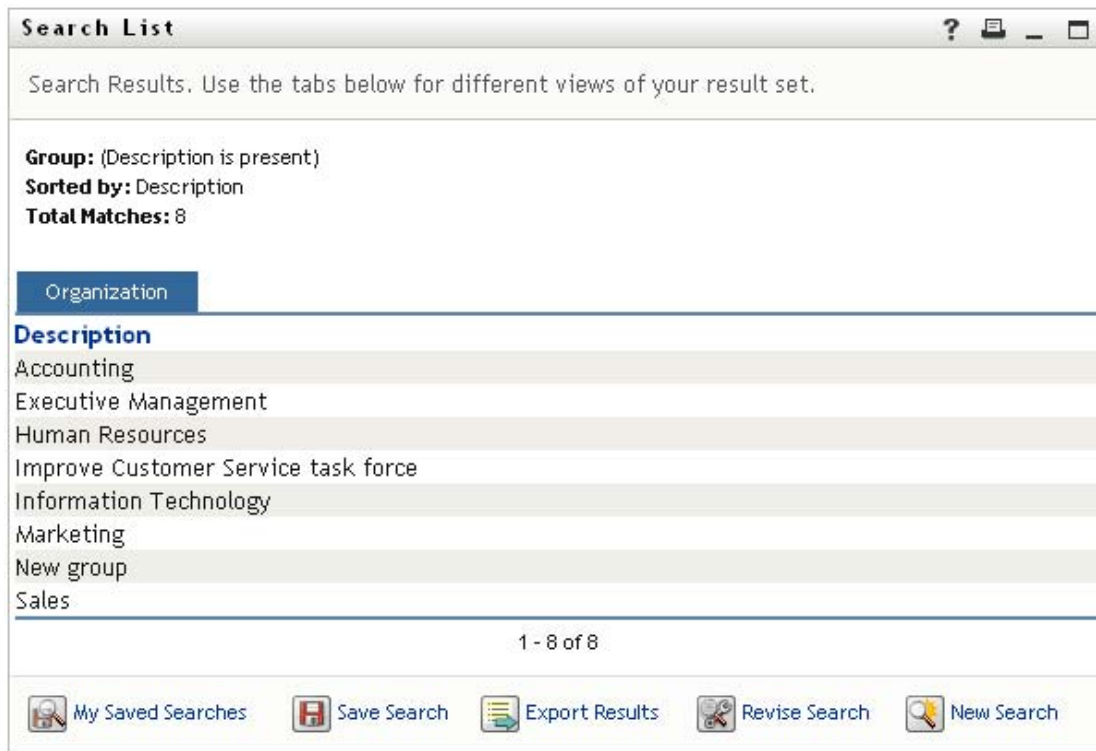
Next Last

My Saved Searches Save Search Export Results Revise Search New Search

## For a Group Search

The results of a group search provide only the Organization view of the information:

**Figure 6-9** Group Search Results



### 6.4.2 Using the Search List

You can do the following with the list of rows that displays to represent your results:

- ♦ [“To Switch to a Another View” on page 85](#)
- ♦ [“To Sort the Rows of Information” on page 85](#)
- ♦ [“To Display Details for a User or Group” on page 86](#)
- ♦ [“To Send E-Mail to a User in the Search List” on page 86](#)

#### To Switch to a Another View

- 1 Click the tab for the view you want to display.

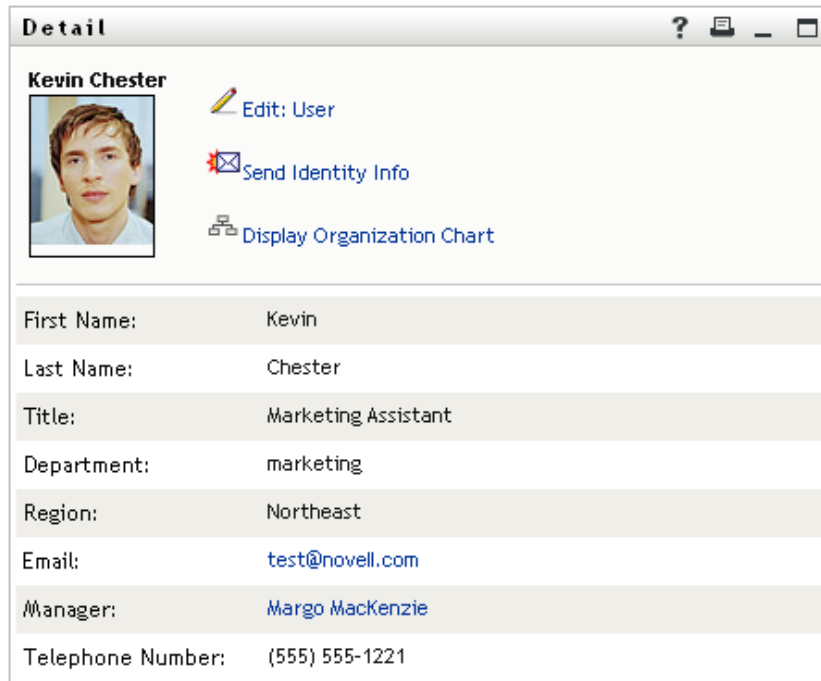
#### To Sort the Rows of Information

- 1 Click the heading of the column that you want to sort.  
The initial sort is in ascending order.
- 2 You can toggle between ascending and descending order by clicking the column heading again (as often as you like).

## To Display Details for a User or Group

- 1 Click the row for the user or group whose details you want to see (but don't click directly on an e-mail icon unless you want to send a message instead).

The Profile page displays, showing detailed information about your chosen user or group:




|                   |  |
|-------------------|--|
| First Name:       | Kevin  |
| Last Name:        | Chester  |
| Title:            | Marketing Assistant                                  |
| Department:       | marketing  |
| Region:           | Northeast  |
| Email:            | <a href="mailto:test@novell.com">test@novell.com</a> |
| Manager:          | <a href="#">Margo MacKenzie</a>                      |
| Telephone Number: | (555) 555-1221                                       |

This page is just like the My Profile page on the *Identity Self-Service* tab. The only difference is that, when you are viewing details about another user or group (instead of yourself), you might not be authorized to see some of the data or perform some of the actions on the page. Consult your system administrator for assistance.

To learn about using the features of the Profile page, see [Chapter 5, "Using My Profile," on page 57](#).

- 2 When you're done with the Profile page, you can close its window.

## To Send E-Mail to a User in the Search List

- 1 Find the row of a user to whom you want to send e-mail.
- 2 Click *Send E-Mail*  in that user's row:

A new message is created in your default e-mail client. The message is blank except for the *To* list, which specifies your chosen user as a recipient.

- 3 Fill in the message contents.
- 4 Send the message.

## 6.4.3 Other Actions You Can Perform

While displaying search results, you can also:

- ♦ [“Save a Search” on page 87](#)
- ♦ [“Export Search Results” on page 87](#)
- ♦ [“Revise Search Criteria” on page 88](#)

### Save a Search

To save the current set of search criteria for future reuse:

- 1 Click *Save Search* (at the bottom of the page).
- 2 When prompted, specify a name for this search.

If you’re viewing the results of an existing saved search, that search name displays as the default. This enables you to update a saved search with any criteria changes you’ve made.

Otherwise, if you type a search name that conflicts with the name of an existing saved search, a version number is automatically added to the end of the name when your new search is saved.

- 3 Click *OK* to save the search.

The Search List page displays a list of My Saved Searches.

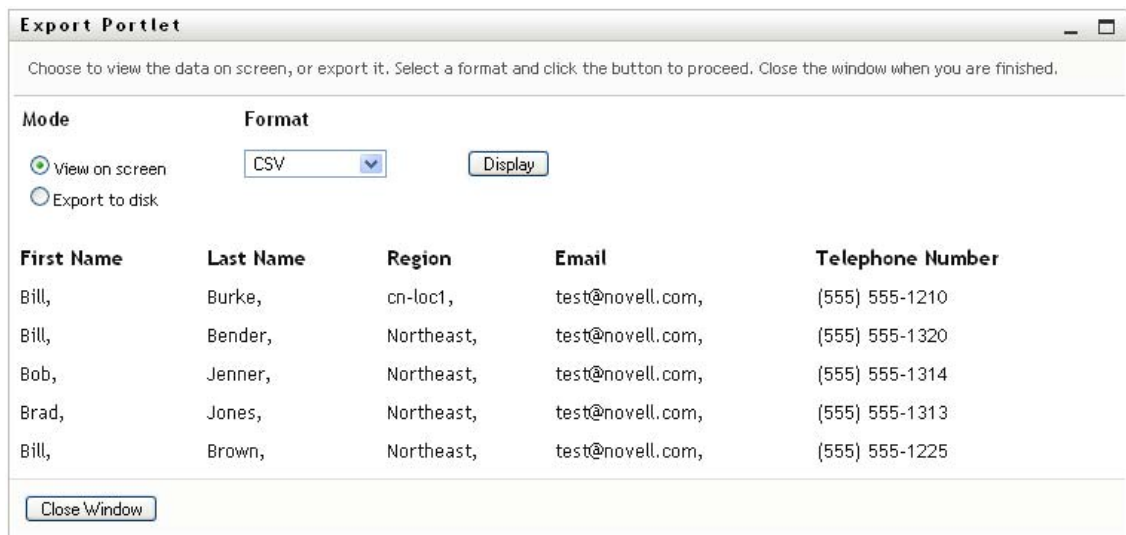
To learn more about working with saved searches, see [Section 6.5, “Using Saved Searches,” on page 89](#).

### Export Search Results

To export search results to a text file:

- 1 Click *Export Results* (at the bottom of the page).

The Export page displays:

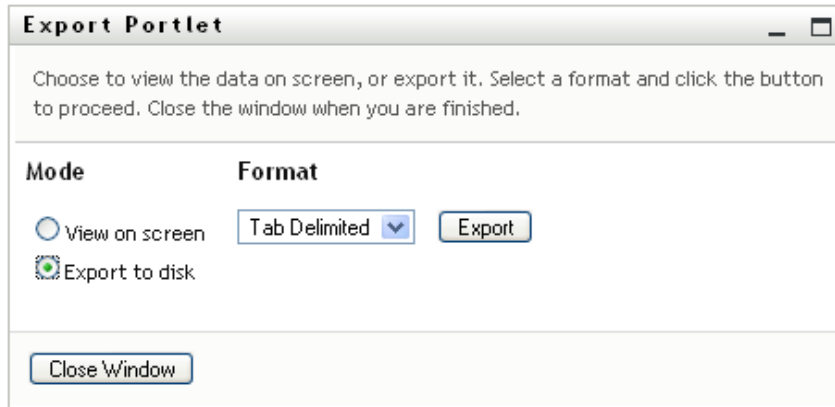


The screenshot shows a window titled "Export Portlet" with a close button in the top right corner. Below the title bar is a text instruction: "Choose to view the data on screen, or export it. Select a format and click the button to proceed. Close the window when you are finished." The window contains two sections: "Mode" and "Format". In the "Mode" section, there are two radio buttons: "View on screen" (which is selected) and "Export to disk". In the "Format" section, there is a dropdown menu currently set to "CSV" and a "Display" button. Below these controls is a table with five columns: "First Name", "Last Name", "Region", "Email", and "Telephone Number". The table contains five rows of data. At the bottom of the window, there is a "Close Window" button.

| First Name | Last Name | Region     | Email            | Telephone Number |
|------------|-----------|------------|------------------|------------------|
| Bill,      | Burke,    | cn-loc1,   | test@novell.com, | (555) 555-1210   |
| Bill,      | Bender,   | Northeast, | test@novell.com, | (555) 555-1320   |
| Bob,       | Jenner,   | Northeast, | test@novell.com, | (555) 555-1314   |
| Brad,      | Jones,    | Northeast, | test@novell.com, | (555) 555-1313   |
| Bill,      | Brown,    | Northeast, | test@novell.com, | (555) 555-1225   |

By default, *View on screen* is selected, and *CSV* is chosen in the format drop-down list. Consequently, the Export page shows your current search results in CSV (Comma Separated Value) format.

- 2 If you want to see what those search results look like in Tab Delimited format instead, select *Tab Delimited* in the drop-down list, then click *Continue*.
- 3 When you're ready to export your current search results to a text file, select *Export to disk*.  
The Export page displays:



- 4 Use the *Format* drop-down list to select an export format for the search results:

| Export Format                                | Default Name of Generated File   |
|--|--|
| CSV  | SearchListResult. <i>date.time</i> .csv<br>For example:<br>SearchListResult.27-Sep-05.11.21.47.csv |
| Tab Delimited                                | SearchListResult. <i>date.time</i> .txt<br>For example:<br>SearchListResult.27-Sep-05.11.20.51.txt |
| XML (available if you are exporting to disk) | SearchListResult. <i>date.time</i> .xml<br>For example:<br>SearchListResult.27-Sep-05.11.22.51.xml |

- 5 Click *Export*.
- 6 When prompted, specify where to save the file of exported search results.
- 7 When you're finished exporting, click *Close Window*.

## Revise Search Criteria

- 1 Click *Revise Search* (at the bottom of the page).  
This returns you to your previous search page to edit your search criteria.
- 2 Make your revisions to the search criteria according to the instructions in these sections:
  - ♦ [Section 6.2, "Performing Basic Searches," on page 74](#)
  - ♦ [Section 6.3, "Performing Advanced Searches," on page 74](#)



## 6.5 Using Saved Searches

When you go to Directory Search, the My Saved Searches page displays by default. This section describes what you can do with saved searches:

- ◆ [Section 6.5.1, “To List Saved Searches,” on page 89](#)
- ◆ [Section 6.5.2, “To Run a Saved Search,” on page 89](#)
- ◆ [Section 6.5.3, “To Edit a Saved Search,” on page 89](#)
- ◆ [Section 6.5.4, “To Delete a Saved Search,” on page 90](#)

### 6.5.1 To List Saved Searches

- 1 Click the *My Saved Searches* button at the bottom of a Directory Search page. The My Saved Searches page displays. [Figure 6-10 on page 89](#) shows an example.

**Figure 6-10** *The My Saved Searches Page*



### 6.5.2 To Run a Saved Search

- 1 In the *My Saved Searches* list, find a saved search that you want to perform.
- 2 Click the name of the saved search (or click the beginning of that row).  
Your search results display.  
To learn about what to do next, see [Section 6.4, “Working with Search Results,” on page 83](#).

### 6.5.3 To Edit a Saved Search

- 1 In the *My Saved Searches* list, find a saved search that you want to revise.
- 2 Click *Edit* in the row for that saved search.  
This takes you to the search page to edit the search criteria.
- 3 Make your revisions to the search criteria according to the instructions in these sections:
  - ◆ [Section 6.2, “Performing Basic Searches,” on page 74](#)
  - ◆ [Section 6.3, “Performing Advanced Searches,” on page 74](#)
- 4 To save your changes to the search, see [Section 6.4, “Working with Search Results,” on page 83](#).

## 6.5.4 To Delete a Saved Search

- 1 In the *My Saved Searches* list, find a saved search that you want to delete.
- 2 Click *Delete* in the row for that saved search.
- 3 When prompted, click *OK* to confirm the deletion.

---

# 7 Performing Password Management

This section tells you how to use the Password Management pages on the *Identity Self-Service* tab of the Identity Manager User Application. Topics include:

- ◆ [Section 7.1, “About Password Management,” on page 91](#)
- ◆ [Section 7.2, “Password Challenge Response,” on page 92](#)
- ◆ [Section 7.3, “Password Hint Change,” on page 92](#)
- ◆ [Section 7.4, “Change Password,” on page 93](#)
- ◆ [Section 7.5, “Password Policy Status,” on page 95](#)
- ◆ [Section 7.6, “Password Sync Status,” on page 95](#)

---

**NOTE:** This section describes the default features of the Password Management pages. You might encounter some differences because of your job role, your level of authority, and customizations made for your organization; consult your system administrator for details.

---

For more general information about accessing and working with the *Identity Self-Service* tab, see [Chapter 2, “Introducing the Identity Self-Service Tab,” on page 33](#).

## 7.1 About Password Management

You can use the Password Management pages to do any of the functions listed in [Table 7-1](#):

**Table 7-1** *Password Management Functions*

| This Password Management page | Enables you to  |
|-------------------------------|---|
| Password Challenge Response   | Set or change either of the following: <ul style="list-style-type: none"><li>◆ Your valid responses to administrator-defined challenge questions</li><li>◆ User-defined challenge questions and responses</li></ul> |
| Password Hint Change          | Set or change your password hint  |
| Change Password               | Change (reset) your password, according to the rules established by your system administrator   |
| Password Policy Status        | Review your password policy requirements.   |
| Password Sync Status          | Display the status of synchronization of application passwords with the Identity Vault  |

**NOTE:** Accessing applications prior to completion of synchronization causes application access issues.

---

## 7.2 Password Challenge Response

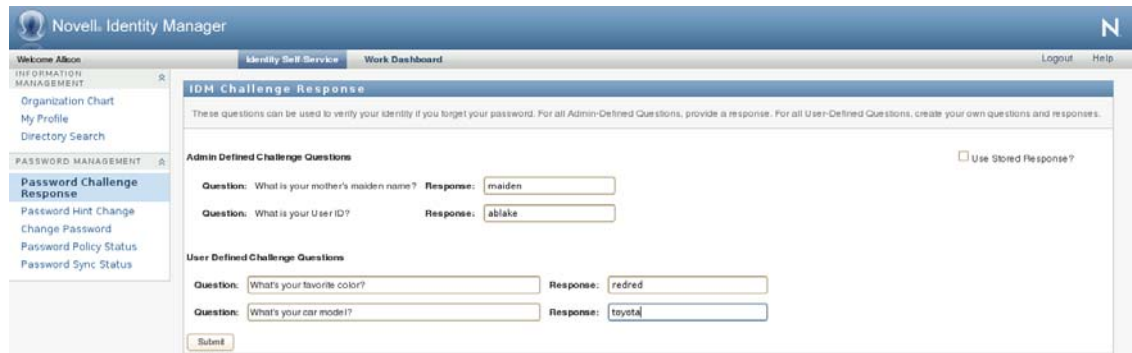
Challenge questions are used to verify your identity during login when you have forgotten your password. If the system administrator has set up a password policy that enables this feature for you, you can use the Password Challenge Response page to:

- ◆ Specify responses that are valid for you when answering administrator-defined questions
- ◆ Specify your own questions and the valid responses for them (if your password policy enables this)

To use the Password Challenge Response page:

- 1 On the *Identity Self-Service* tab, click *Password Challenge Response* in the menu (under *Password Management*).

The Password Challenge Response page displays. For example:



- 2 Type an appropriate response in each *Response* text box (they are all required), or use your previously stored response. When *Use Stored Response* is selected, the challenge answers, including the labels, are not shown. In addition, user-defined challenge questions are disabled.

Make sure you specify responses that you can remember later.

- 3 Specify or change any user-defined questions that are required. You may not use the same question more than once.
- 4 Click *Submit*.

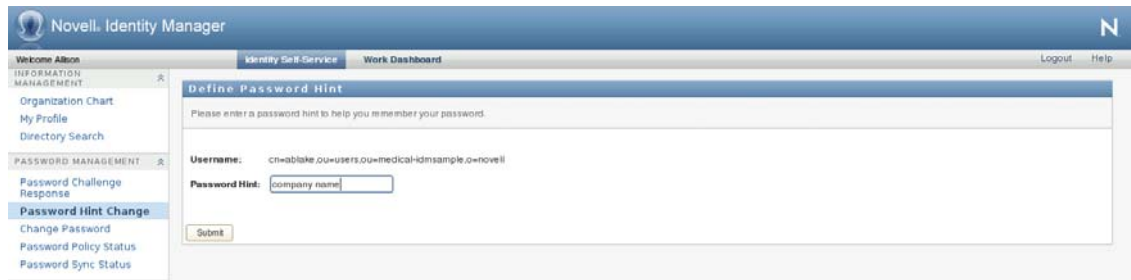
After you save the challenge responses, the User Application displays a message indicating that the challenge responses were saved successfully and displays the challenge response screen again with "Use Stored Response?" selected.

## 7.3 Password Hint Change

A password hint is used during login to help you remember your password when you have forgotten it. Use the Password Hint Change page to set or change your password hint.

- 1 On the *Identity Self-Service* tab, click *Password Hint Change* in the menu (under *Password Management*).

The Password Hint Definition page displays:



- 2 Type the new text for your hint.  
Your password cannot appear within the hint text.
- 3 Click *Submit*.  
The status of your request displays.

## 7.4 Change Password

You can use this page whenever you need to change your password (providing that the system administrator has enabled you to do so).

- 1 On the *Identity Self-Service* tab, click *Change Password* in the menu (under *Password Management*).  
The Change Password page displays. If the system administrator has set up a password policy for you, the Change Password page typically provides information about how to specify a password that meets the policy's requirements. For example:



If no password policy applies, you'll see the basic Change Password page, which simply provides fields for changing your password.

In version 4.0.2, the User Application supports the following password syntax types:

- ◆ Microsoft complexity policy  
This password syntax type is used for backward compatibility with Active Directory 2003.
- ◆ Microsoft Server 2008 Password Policy  
This is a new password syntax type that has been added to eDirectory 8.8.7 to support Active Directory 2008.

The following settings are supported with Microsoft Server 2008 Password Policy:

- ◆ Use Microsoft Server 2008 Password Policy
- ◆ Maximum number of complexity policy violations in password (0-5)

- ◆ Novell syntax

The following new settings are supported with the Novell syntax:

- ◆ Minimum number of non-alphabetic characters (1-512)
- ◆ Maximum number of non-alphabetic characters (1-512)

For all three types password syntax types, the User Application supports these new features in version 4.0.2:

- ◆ Number of characters different from current password and passwords from history (0-6)
- ◆ Number of passwords in history to be considered for character exclusion (0-10)

If your administrator has enabled the Microsoft Server 2008 Policy syntax, you will see information similar to the following:

**Change Password**

Your password policy supports Microsoft AD2008 Password Complexity Policy rules:

Minimum number of characters in password: 3.

Maximum number of characters in password: 512.

Your password should contain characters from at least 3 of the following 5 categories:

1. Uppercase characters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters).
2. Lowercase characters of European languages (a through z, sharp-s, with diacritic marks, Greek and Cyrillic characters).
3. Base 10 digits (0 through 9).
4. Non-alphanumeric characters: ~!@#\$%^&\* \_+=~!@[]:;'"<>.,?/
5. Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase. This includes Unicode characters from Asian languages.

You may use numbers in your password.

The password is case sensitive.

You may use special characters in your password.

You must use a unique password.

You may not use the following attribute values for your password:

- CN

Old password:

New password:

Retype password:

- 2 Type your current password in the *Old password* text box.
- 3 Type your new password in the *New password* text box.
- 4 Type your new password again in the *Retype password* text box.
- 5 Click *Submit*.

If your new password violates any of the password rules defined by your administrator, you will see an error message on the Change Password page. If you are using Microsoft Server 2008 Policy, and your password is in violation, the user interface will show this message at the top of the page:

Password AD2008 complexity policy violation.

If your new password is in violation, review the password rules defined by your administrator, and try again.

---

**NOTE:** In Identity Manager 4.0.2, the password self-service capabilities have been enhanced to support the new, optional password policy capability provided by eDirectory 8.8.7. Prior versions of Identity Manager (that are in general support), though supported with eDirectory 8.8.7, may not provide full context in the error messages for failures with new password policies. We recommend using the latest versions of the products to get the full benefits of the latest features and fixes. For more information on the eDirectory 8.8.7 password policy enhancements,

see “Microsoft Windows Server 2008 Password Policy Support” (<http://www.netiq.com/documentation/edir88/edir88new/index.html?page=/documentation/edir88/edir88new/data/bz9jze9.html>).

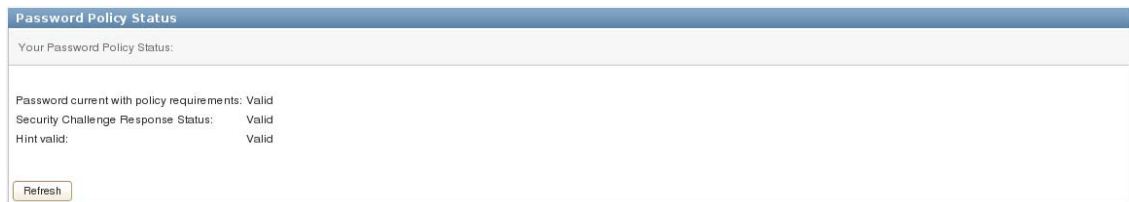
- 6 You might be prompted to supply a password hint, if your administrator configured your security policy to do so. If so, see [Section 7.3, “Password Hint Change,”](#) on page 92.
- 7 The status of your request is displayed.

## 7.5 Password Policy Status

You are assigned a password policy by your administrator. The policy determines the security measures associated with your password. You can check your password policy requirements as follows:

- 1 On the *Identity Self-Service* tab, click *Password Policy Status* in the menu (under *Password Management*).

The *Password Policy Status* page displays. For example:



Items labeled invalid are items that you cannot change.

## 7.6 Password Sync Status

Use the Password Sync Status page to determine if your password has been synchronized across applications. Access another application only after your password has synchronized. Accessing applications prior to completion of synchronization causes application access issues.

- 1 On the *Identity Self-Service* tab, click *Password Sync Status* in the menu (under *Password Management*).

The *Password Sync Status* page displays. Full-color icons indicate applications for which the password is synchronized. Dimmed icons indicate applications that are not yet synchronized. For example:



---

**NOTE:** Only the administrator can see the *Select User* box.

---



---

# 8 Creating Users or Groups

This section tells you how to use the Create User or Group page on the *Identity Self-Service* tab of the Identity Manager User Application. Topics include:

- ♦ [Section 8.1, “About Creating Users or Groups,” on page 97](#)
- ♦ [Section 8.2, “Creating a User,” on page 97](#)
- ♦ [Section 8.3, “Creating a Group,” on page 99](#)
- ♦ [Section 8.4, “Using the Editing Buttons,” on page 101](#)

For general information about accessing and working with the *Identity Self-Service* tab, see [Chapter 2, “Introducing the Identity Self-Service Tab,” on page 33](#).

## 8.1 About Creating Users or Groups

System administrators can use the Create User or Group page to create users and groups. The system administrator can give others (typically, selected people in administration or management positions) access to this page.

You might encounter some differences from functions documented in this section because of your job role, your level of authority, and customizations made for your organization. Consult your system administrator for details.

Details on enabling access to the Create User or Group page are in the “Page Administration” section of the *Identity Manager User Application: Administration Guide* (<http://www.netiq.com/documentation/idm402/index.html>). To enable access, open iManager, add the user as a Trustee, and add the Assigned Right called Create to the Trustee.

To check which users or groups already exist, use the Directory Search page. See [Chapter 6, “Using Directory Search,” on page 71](#).

## 8.2 Creating a User

- 1 On the *Identity Self-Service* tab, click *Create User or Group* in the menu (under *Directory Management*, if displayed).

The *Select an object to create* panel displays.

- 2 Use the *Object type* drop-down list to select *User*, then click *Continue*.

The *User - Set Attributes* panel displays:

**Create** ? \_ □

User - Set Attributes  
\* - indicates required.

User Id:\*

Container:\*  🔍 📄 ✎

First Name:\*  +

Last Name:\*  +

Title:  +

Department:  +

Region:  +

Email:  +

Manager:  ▾ 🔍 📄 ✎ ✖

Telephone Number:  +

← Back Continue →

**3** Specify values for the following required attributes:

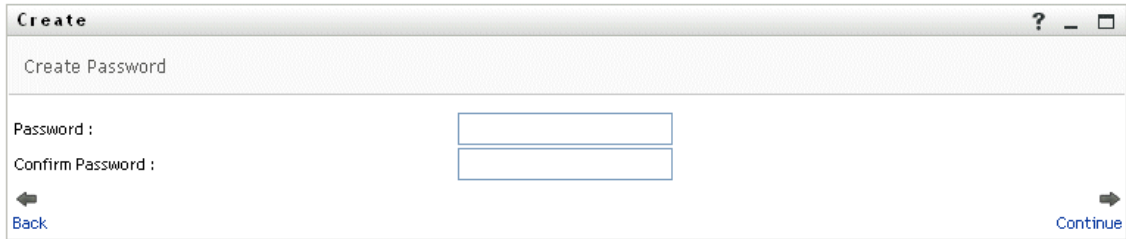
| Attribute  | What to Specify   |
|------------|---|
| User ID    | The username for this new user.   |
| Container  | An organizational unit in the Identity Vault under which you want the new user stored (such as an OU named users). For example:<br><br>ou=users,ou=MyUnit,o=MyOrg<br><br>To learn about using the buttons provided to specify a container, see <a href="#">Section 8.4, "Using the Editing Buttons," on page 101</a> .<br><br>You won't be prompted for Container if the system administrator has established a default create container for this type of object. |
| First Name | First name of the user.   |
| Last Name  | Last name of the user.  |

**4** Specify optional details about this new user, such as Title, Department, Region, E-mail, Manager, or Telephone Number.

To learn about using the buttons provided to specify values for certain attributes, see [Section 8.2, "Creating a User," on page 97](#).

**5** Click *Continue*.

The *Create Password* panel displays:

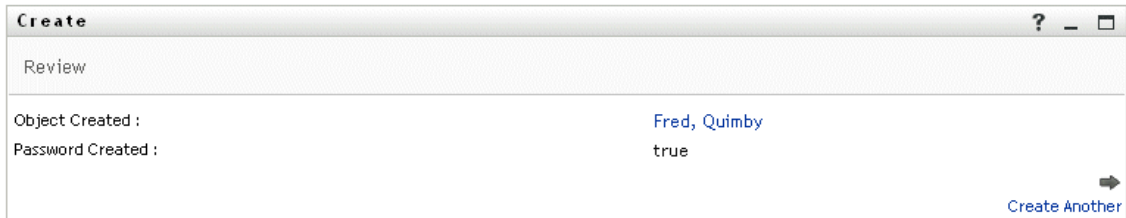


If a password policy is in effect for the target container, this panel provides information about how to specify a password that meets the policy's requirements. The password is also validated against that policy.

- 6 Type a password for the new user in the *Password* and *Confirm Password* text boxes, then click *Continue*.

This sets the new user's initial password. When that user first logs in, the Identity Manager User Application prompts the user to change this password.

The user and password are created, then the *Review* panel displays to summarize the result:



The *Review* panel provides optional links that you might find handy:

- Click the new user's name to display the Profile page of detailed information for this user. From the Profile page, you can edit the user's details to make changes or delete the user.
- Click *Create Another* to return to the initial panel of the Create User or Group page

## 8.3 Creating a Group

- 1 On the *Identity Self-Service* tab, click *Create User or Group* in the menu (under *Directory Management*, if displayed).

The *Select an object to create* panel displays.

- 2 Use the *Object type* drop-down list to select *Group*, then click *Continue*.

The *Set attributes for this Group* panel displays:

**Create** ? \_ □

Group - Set Attributes  
\*- indicates required.

Group Id:\*

Container:\*  🔍 📄 ✎

Description:\*

← Back Continue →

3 Specify values for the following required attributes:

| Attribute   | What to Specify   |
|-------------|---|
| Group ID    | The group name for this new group.  |
| Container   | <p>An organizational unit in the identity vault under which you want the new group stored (such as an OU named groups). For example:</p> <p>ou=groups , ou=MyUnit , o=MyOrg</p> <p>To learn about using the buttons provided to specify a container, see <a href="#">Section 8.2, “Creating a User,” on page 97.</a></p> <p><b>NOTE:</b> You won't be prompted for <i>Container</i> if the system administrator has established a default create container for this type of object.</p> |
| Description | A description of this new group.  |

4 Click *Continue*.

The group is created, then the *Review* panel displays to summarize the result:

**Create** ? \_ □

Review

Object Created: [New group](#)

→  
Create Another







The *Review* panel provides optional links that you might find handy:

- ♦ Click the new group's name to display the Profile page of detailed information for this group  
From the Profile page, you can edit the group's details to make changes or delete the group.
- ♦ Click *Create Another* to return to the initial panel of the Create User or Group page

## 8.4 Using the Editing Buttons

Table 8-1 lists the editing buttons you can use to specify values for attributes.

**Table 8-1** *Editing Buttons for Specifying Users and Groups*

| Button  | What It Does  |
|---|---|
|  | Looks up a value to use in an entry                       |
|  | Displays a <i>History</i> list of values used in an entry |
|  | Resets the value of a selected entry                      |
|  | Adds a new entry. You can add more than one entry.        |
|  | Indicates that more than one entry exists.                |
|  | Deletes a selected entry and its value                    |

**IMPORTANT:** It is possible to use the Edit User page of the *Identity Self-Service* tab to break the hierarchical reporting structure. For example, you can add a direct report to a manager even if the direct report has another manager assigned, or you can have a manager report to a person in his or her own organization.

### 8.4.1 To Look Up a Container

- 1 Click *Lookup* to the right of an entry for which you want to look up a container:



The Lookup page displays a tree of containers:



You can expand or collapse the nodes in this tree (by clicking the + or - buttons) to look for the container you want.

- 2 If necessary, specify search criteria for the container you want.

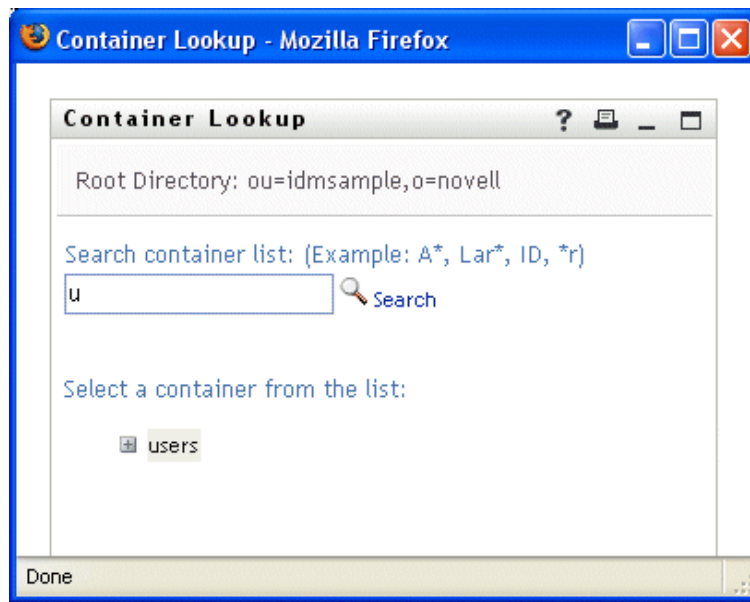
In the text box, type all or part of the container name to search for. The search finds every container name that begins with the text you type. It is not case sensitive. You can optionally use the asterisk (\*) as a wildcard in your text to represent zero or more of any character.

For instance, all of the following examples find the container named users:

```
Users  
users  
u  
u*  
*s  
*r*
```

- 3 Click *Search*.

The Lookup page displays your search results:



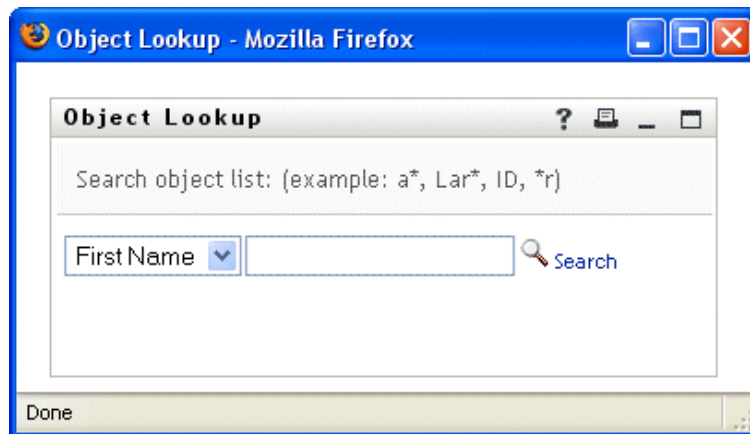
- 4 Select the container you want from the tree.  
The Lookup page closes and inserts the name of that container into the appropriate entry.

## 8.4.2 To Look Up a User

- 1 Click *Lookup* to the right of an entry (for which you want to look up a user):



The Lookup page displays:



- 2 Specify search criteria for the user you want:
  - 2a Use the drop-down list to select a search by *First Name* or *Last Name*.
  - 2b In the text box next to the drop-down list, type all or part of the name to search for.

The search finds every name that begins with the text you type. It is not case sensitive. You can optionally use the asterisk (\*) as a wildcard in your text to represent zero or more of any character.

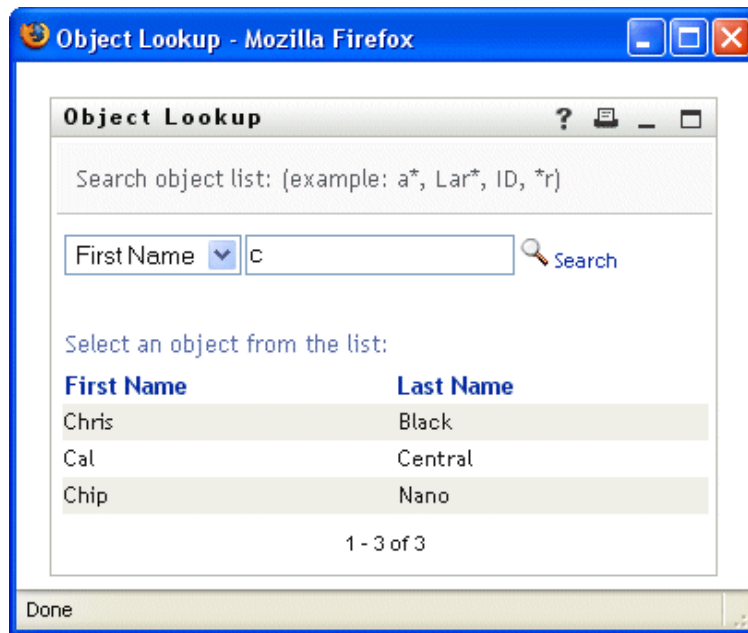
For instance, all of the following examples find the first name Chip:

Chip  
chip  
c  
c\*  
\*p  
\*h\*

A manager lookup searches only for users who are managers.

**3** Click *Search*.

The Lookup page displays your search results:



If you see a list of users that includes the one you want, go to [Step 4](#). Otherwise, go back to [Step 2](#).

You can sort the search results in ascending or descending order by clicking the column headings.

**4** Select the user you want from the list.

The Lookup page closes and inserts the name of that user into the appropriate entry.

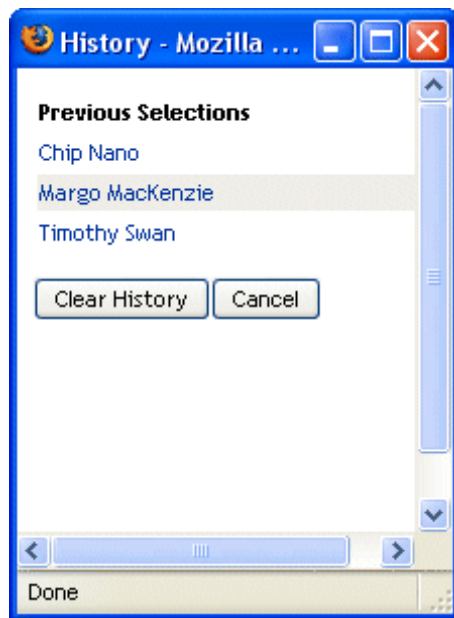
### 8.4.3 To Use the History List

**1** Click *History* to the right of an entry (whose previous values you want to see):



The *History* list displays, with values in alphabetical order:





2 Do one of the following:

---

**If you want to**

**Do this**

Pick from the *History* list

Select a value that you want from the list.

The *History* list closes and inserts that value into the appropriate entry.

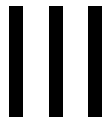
Clear the *History* list

Click *Clear History*.

The *History* list closes and deletes its values for this entry. Clearing the *History* list does not change the current value of the entry.

---





# Using the Work Dashboard Tab

These sections tell you how to use the *Work Dashboard* tab of the Identity Manager User Application.

- ♦ [Chapter 9, “Introducing the Work Dashboard Tab,” on page 109](#)
- ♦ [Chapter 10, “Managing Your Work,” on page 125](#)
- ♦ [Chapter 11, “Managing Work for Users, Groups, Containers, Roles, and Teams,” on page 173](#)
- ♦ [Chapter 12, “Controlling Your Settings,” on page 179](#)
- ♦ [Chapter 13, “Making a Process Request,” on page 209](#)
- ♦ [Chapter 14, “Launching the Identity Reporting Module,” on page 215](#)



---

# 9 Introducing the Work Dashboard Tab

This section provides an overview of the *Work Dashboard* tab. Topics include:

- ◆ [Section 9.1, “About the Work Dashboard Tab,” on page 109](#)
- ◆ [Section 9.2, “Accessing the Work Dashboard Tab,” on page 109](#)
- ◆ [Section 9.3, “Exploring the Tab’s Features,” on page 110](#)
- ◆ [Section 9.4, “Work Dashboard Actions You Can Perform,” on page 112](#)
- ◆ [Section 9.5, “Understanding the Icons on the Work Dashboard,” on page 113](#)
- ◆ [Section 9.6, “Security Permissions for the Work Dashboard,” on page 115](#)

## 9.1 About the Work Dashboard Tab

The *Work Dashboard* tab provides a single, consolidated user interface for all end-user functions within the Identity Manager User Application. The *Work Dashboard* tab provides a convenient way to manage tasks, resources, and roles. In addition, it allows you to review the status of requests, and change settings within the User Application. The *Work Dashboard* tab presents only the most relevant features of the application, allowing you to focus on your work.

When a request requires permission from one or more individuals in an organization, the request starts a workflow. The workflow coordinates the approvals needed to fulfill the request. Some requests require approval from a single individual; others require approval from several individuals. In some instances, a request can be fulfilled without any approvals.

When a request is initiated, the User Application tracks the initiator and the recipient. The initiator is the person who made the request. The recipient is the person for whom the request was made.

Your workflow designer and system administrator are responsible for setting up the contents of the *Work Dashboard* tab for you and the others in your organization. The flow of control for a workflow, as well as the appearance of forms, can vary depending on how the designer and administrator configured the application. In addition, what you can see and do is typically determined by your job requirements and your level of authority.

---

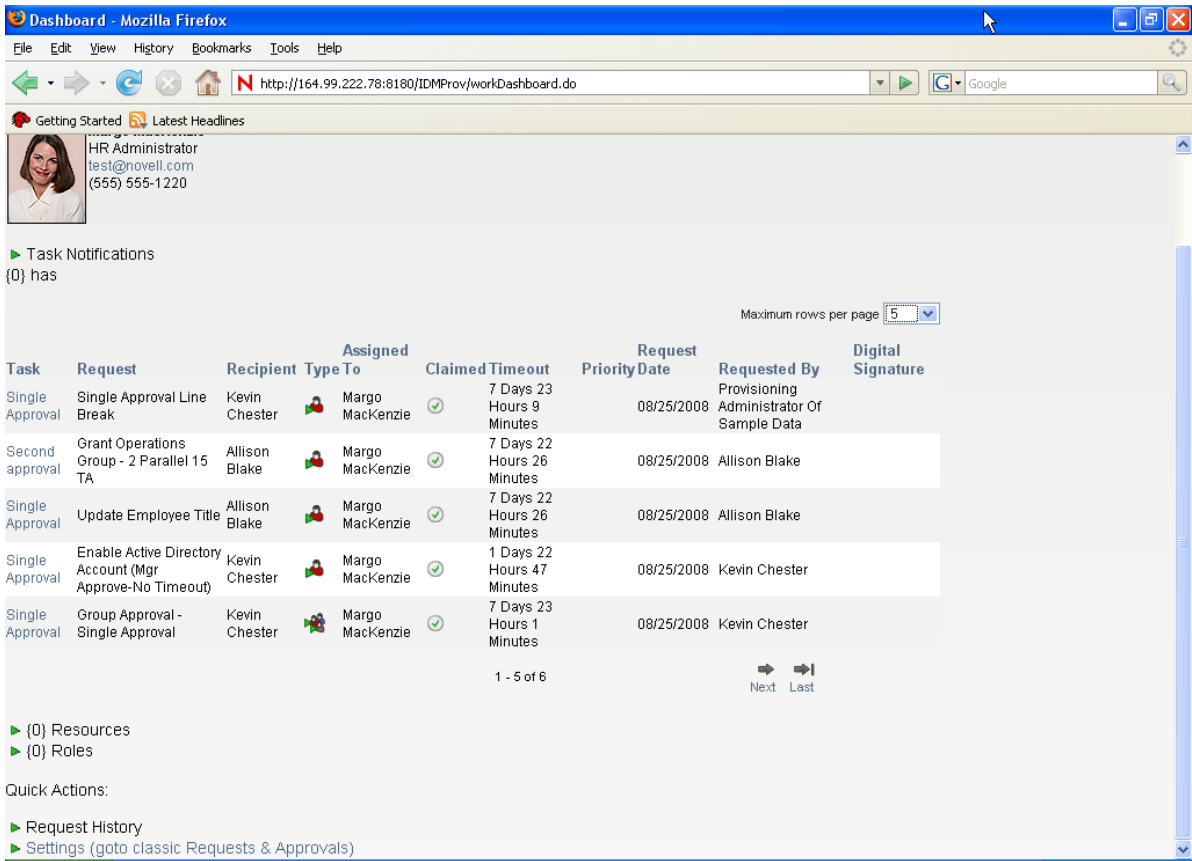
**NOTE:** The *Work Dashboard* tab is available only with Identity Manager 4.0.2 Advanced Edition. Standard Edition does not support this feature.

---

## 9.2 Accessing the Work Dashboard Tab

By default, after you have logged in to the Identity Manager user interface, the *Work Dashboard* tab opens:

**Figure 9-1** Work Dashboard



If you go to another tab in the Identity Manager user interface but then want to return, you just need to click the *Work Dashboard* tab to open it again.

### 9.3 Exploring the Tab’s Features

This section describes the default features of the *Work Dashboard* tab. (Your tab might look different because of customizations made for your organization; consult your system administrator or workflow designer.)

The right side of the *Work Dashboard* tab displays several sections that give you access to typical Work Dashboard actions. The sections are described below:

**Table 9-1** Sections of the Work Dashboard

| Section                   | Description  |
|---------------------------|--|
| <i>Task Notifications</i> | Lets you check the workflow queue for tasks that have been assigned to you or to a user whose tasks you are permitted to manage. |

| Section                     | Description  |
|-----------------------------|--|
| <i>Resource Assignments</i> | Allows you to see what resource assignments you have, and also make requests for additional resource assignments.  |
| <i>Role Assignments</i>     | Allows you to see what roles you have, and also make requests for additional role assignments.   |
| <i>Request Status</i>       | <p>Allows you to see the status of the requests you've made. It lets you see the current state of each request. In addition, it gives you the option to retract a request that is still in process if you have changed your mind and do not need to have the request fulfilled.</p> <p>The <i>Request Status</i> display includes provisioning requests, role requests, and resource requests in a single consolidated list.</p> |

The Work Dashboard also includes a User Profile section in the upper-left corner of the screen. This section of the page lets you manage work for other users, groups, containers, and roles. In addition, it lets you manage your settings and team settings, and also make process requests (also known as provisioning requests).

The actions available within the User Profile section are described below:

**Table 9-2** *Actions Available From the User Profile Section*

| Action          | Description  |
|-----------------|--|
| <i>Manage</i>   | Allows the current user to select a particular user, group, container, role, or team and use the Work Dashboard interface to manage work for the selected entity type. After the user selects an entity, the data and access permissions on the Work Dashboard pertain to the selected entity, rather than to the user currently logged on. However, when the user is in Manage mode, the <i>Settings</i> and <i>Make a Process Request</i> menus still apply to the logged-in-user, not the selected entity in the <i>Manage</i> control. |
| <i>Settings</i> | Give you the ability to act as a proxy for another user. In addition, they allow you to view your proxy and delegate assignments. If you are a team manager or Provisioning Application Administrator, you might also be permitted to define proxy and delegate assignments, as well as team availability settings.  |

| Action                        | Description   |
|-------------------------------|---|
| <i>Make a Process Request</i> | <p>Allows you to initiate a process request (also known as a provisioning request). By default, this action is not included in the User Profile section of the Work Dashboard.</p> <p>The <i>Make a Process Request</i> menu does not allow you to make attestation, resource, or role requests. The interface for submitting these requests depends on the type of request you want to make, as described below:</p> <ul style="list-style-type: none"> <li>♦ To make an attestation request, you need to use the <i>Attestation Requests</i> actions on the <i>Compliance</i> tab.</li> <li>♦ To make a resource request, you need to use the <i>Resource Assignments</i> section of the <i>Work Dashboard</i> tab, or the <i>Resource Catalog</i> on the <i>Roles and Resources</i> tab.</li> <li>♦ To make a role request, you need to use the <i>Role Assignments</i> section of the <i>Work Dashboard</i> tab, or the <i>Role Catalog</i> on the <i>Roles and Resources</i> tab.</li> </ul> |

## 9.4 Work Dashboard Actions You Can Perform

The Work Dashboard sections support the following actions:

**Table 9-3** Common Work Dashboard Actions

| Action           | Description   |
|------------------|---|
| <i>Assign</i>    | <p>Assigns a role or resource.</p> <p>Only available with the <i>Role Assignments</i> and <i>Resource Assignments</i> actions.</p>            |
| <i>Remove</i>    | <p>Removes a role or resource assignment.</p> <p>Only available with the <i>Role Assignments</i> and <i>Resource Assignments</i> actions.</p> |
| <i>Refresh</i>   | Refreshes the display.  |
| <i>Customize</i> | Allows you to specify which columns appear in the display, and what order they appear in.   |
| <i>Filter</i>    | Allows you to filter the data based on selection criteria.  |
| <i>Rows</i>      | Gives you the ability to control how many rows appear on each page of the display.  |

You can also sort the data in the list by clicking the headings in the display.

**Saving User Preferences** When you use the *Customize*, *Filter*, and *Rows* actions to customize the display within any of the sections of the Work Dashboard, or change the sort order of the data displayed, your customizations are saved in the Identity Vault along with your other user

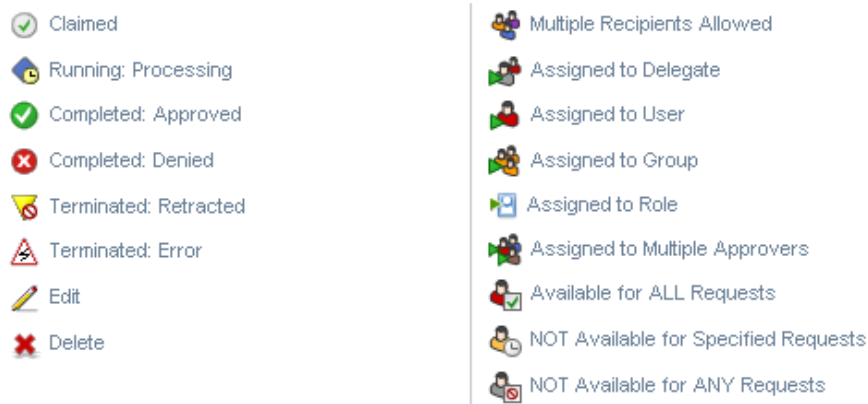


preferences. To allow the user preferences to be saved, the administrator must ensure that the permissions on the `srvprvUserPrefs` and `srvprvQueryList` attributes are set so that the user is able to write to these attributes.

## 9.5 Understanding the Icons on the Work Dashboard

When you use the Work Dashboard, you see icons in many places that convey important information. These are the icons you see:

**Figure 9-2** *Icons Used on the Work Dashboard*



The table below provides detailed descriptions of the icons used on the Work Dashboard:

**Table 9-4** *Work Dashboard Icons*

| Icon                         | Description   |
|------------------------------|---|
| <i>Claimed</i>               | Indicates whether a particular workflow task has been claimed by a user.<br><br>Appears in the <i>Task Notifications</i> section of the Work Dashboard.   |
| <i>Running: Processing</i>   | Indicates that a particular request is still in process.<br><br>Appears in the <i>Request Status</i> section of the Work Dashboard.   |
| <i>Completed: Approved</i>   | Indicates that a particular request has completed its processing and has been approved.<br><br>Appears in the <i>Request Status</i> section of the Work Dashboard.  |
| <i>Completed: Denied</i>     | Indicates that a particular request has completed its processing and has been denied.<br><br>Appears in the <i>Request Status</i> section of the Work Dashboard.  |
| <i>Terminated: Retracted</i> | Indicates that a particular request was retracted by a user (either the user who submitted the request, a Team Manager, or an Domain Administrator or Domain Manager).<br><br>Appears in the <i>Request Status</i> section of the Work Dashboard. |

| Icon                               | Description   |
|------------------------------------|---|
| <i>Terminated: Error</i>           | <p>Indicates that a particular request was terminated because of an error.</p> <p>Appears in the <i>Request Status</i> section of the Work Dashboard.</p>   |
| <i>Edit</i>                        | <p>Lets you edit a proxy or delegate assignment. To edit the assignment, select it and click the <i>Edit</i> icon.</p> <p>Appears on the <i>My Proxy Assignments</i>, <i>My Delegate Assignments</i>, <i>Team Proxy Assignments</i>, <i>Team Delegate Assignments</i>, <i>Edit Availability</i>, and <i>Team Availability</i> pages.</p>  |
| <i>Delete</i>                      | <p>Lets you delete a proxy or delegate assignment. To delete the assignment, select it and click the <i>Delete</i> icon.</p> <p>Appears on the <i>My Proxy Assignments</i>, <i>My Delegate Assignments</i>, <i>Team Proxy Assignments</i>, <i>Team Delegate Assignments</i>, <i>Edit Availability</i>, and <i>Team Availability</i> pages.</p>                                      |
| <i>Multiple Recipients Allowed</i> | <p>Indicates that this resource provides support for multiple recipients. When a resource supports multiple recipients, the <i>Make Team Process Requests</i> action lets you select multiple users as recipients.</p> <p>Appears on the <i>Make Team Process Requests</i> page.</p>  |
| <i>Assigned to Delegate</i>        | <p>Indicates that a particular workflow task has been delegated by another user. This task appears in the current user's queue because the original assignee has declared himself or herself unavailable. Because the current user is the original assignee's delegate, this user sees the task.</p> <p>Appears in the <i>Task Notifications</i> section of the Work Dashboard.</p> |
| <i>Assigned to User</i>            | <p>Indicates that a particular workflow task was assigned to a user.</p> <p>Appears in the <i>Task Notifications</i> section of the Work Dashboard.</p>   |
| <i>Assigned to Group</i>           | <p>Indicates that a particular workflow task was assigned to a group.</p> <p>Appears in the <i>Task Notifications</i> section of the Work Dashboard.</p>  |
| <i>Assigned to Role</i>            | <p>Indicates that a particular workflow task was assigned to a role.</p> <p>Appears in the <i>Task Notifications</i> section of the Work Dashboard.</p>   |

| Icon  | Description  |
|---|--|
| <i>Assigned to Multiple Approvers</i>       | <p>Indicates that a particular workflow task was assigned to more than one user.</p> <p>This icon applies in the following situations:</p> <ul style="list-style-type: none"> <li>♦ The task has been assigned to a group of addressees, but only one addressee can claim and approve the task. When this approval is given, task execution is considered finished.</li> <li>♦ The task has been assigned to multiple addressees, and all of them must claim and approve the task before the activity can be considered complete.</li> <li>♦ The task has been assigned to multiple addressees, and a quorum of users must claim and approve the task before the activity can be considered complete. The definition of a quorum is configured by the administrator. To define the quorum, the administrator specifies an approval condition that specifies the precise number of approvals or the percentage of approvals needed.</li> </ul> <p>Appears in the <i>Task Notifications</i> section of the Work Dashboard.</p> |
| <i>Available for ALL Requests</i>           | <p>Indicates that a particular user is available for all kinds of process requests. This setting applies to delegation.</p> <p>Appears on the <i>Edit Availability</i> and <i>Team Availability</i> pages.</p>   |
| <i>NOT Available for Specified Requests</i> | <p>Indicates that a particular user is not available for certain kinds of process requests during a particular period. This setting applies to delegation. During the time period when a particular user is unavailable for these requests, the user delegated to act on these requests can work on them.</p> <p>Appears on the <i>Edit Availability</i> and <i>Team Availability</i> pages.</p>   |
| <i>NOT Available for ANY Requests</i>       | <p>Indicates that a particular user is not available for any process requests currently in the system. This setting applies to delegation. During the time period when a particular user is unavailable for a request, the user delegated to act on that request can work on it.</p> <p>Appears on the <i>Edit Availability</i> and <i>Team Availability</i> pages.</p>  |

## 9.6 Security Permissions for the Work Dashboard

This section describes the permissions needed by each user to perform various actions on the Work Dashboard. Topics include:

- ♦ [Section 9.6.1, “User Self-Service,” on page 116](#)
- ♦ [Section 9.6.2, “Domain Administrator in Manage Mode,” on page 117](#)
- ♦ [Section 9.6.3, “Domain Manager in Manage Mode,” on page 120](#)
- ♦ [Section 9.6.4, “Team Manager in Manage Mode,” on page 122](#)

## 9.6.1 User Self-Service

The authenticated user can perform self-service actions for tasks on the Work Dashboard without any security permissions, as outlined in the table below.

**Table 9-5** *Task Notifications for User Self-Service*

| To perform this action...      | Authenticated user must be...  | And the user must have these permissions... |
|--------------------------------|--|---|
| View task in list              | <p>Addressee for task.</p> <p>Alternatively the task may be delegated to this user by the addressee, or be claimed by this user for a group.</p> <p><b>NOTE:</b> In self-service mode, the Domain Administrator or Domain Manager can also view tasks for which he/she is a recipient.</p> | None.                                       |
| View and work with task detail | <p>Addressee for task.</p> <p>Alternatively the task may be delegated to this user by the addressee, or be claimed by this user for a group.</p>   | None.                                       |
| View workflow comments         | <p>Addressee for task.</p> <p>Alternatively the task may be delegated to this user by the addressee, or be claimed by this user for a group.</p>   | None.                                       |

The authenticated user requires entry browse rights to assign or remove role and resource assignments, as outlined in the table below.

**Table 9-6** *Role and Resource Assignments for User Self-Service*

| To perform this action...                        | Authenticated user must be...  | And the user must have these permissions... |
|--|--|---|
| View role or resource in list                    | <p>Recipient.</p> <p>The list of assignments includes assignments for groups and containers to which the user belongs.</p> | None.                                       |
| Assign or remove assignment for role or resource | <p>Recipient.</p> <p>Grant and Revoke operations apply to the authenticated user only</p>                                  | Trustee (Entry Browse)                      |

The authenticated user requires entry browse rights for some request status actions, as outlined in the table below.

**Table 9-7** Request Status for User Self-Service

| To perform this action...                            | Authenticated user must be...  | And the user must have these permissions... |
|--|--|---|
| View process requests in list                        | Initiator or recipient   | None.                                       |
| View and work with process request detail            | Initiator or recipient (if the <i>Restrict View</i> option is set to false in Designer).<br><br>If the <i>Restrict View</i> option is set to true, the display is restricted to tasks initiated by the user, even if the user has browse rights. | Trustee (Entry Browse)                      |
| Retract process requests                             | Initiator and recipient<br><br>The request must be in a retractable state, which means that it has not been approved, denied, canceled or provisioned.   | Trustee (Entry Browse)                      |
| View workflow comments for process requests          | Initiator or recipient (if the <i>Restrict View</i> option is set to false in Designer).<br><br>If the <i>Restrict View</i> option is set to true, the display is restricted to tasks initiated by the user, even if the user has browse rights. | Trustee (Entry Browse)                      |
| View role or resource requests in list               | Initiator or recipient   | None.                                       |
| View and work with role or resource request detail   | Initiator or recipient   | Trustee (Entry Browse)                      |
| Retract role or resource requests                    | Initiator and recipient.<br><br>The request must be in a retractable state, which means that it has not been approved, denied, canceled or provisioned.  | Trustee (Entry Browse)                      |
| View workflow comments for role or resource requests | Initiator or recipient   | Role/Resource Trustee (Entry Browse)        |

## 9.6.2 Domain Administrator in Manage Mode

In manage mode, the Domain Administrator can perform actions for tasks on the Work Dashboard without any security permissions, as outlined in the table below.

**Table 9-8** Task Notifications for Domain Administrator in Manage Mode

| To perform this action...      | Managed User, Group, Container, or Role must be...  | And the Domain Administrator must have these permissions... |
|--------------------------------|---|---|
| View task in list              | <p>Addressee or recipient for task.</p> <p><b>NOTE:</b> A role cannot be the recipient for a task. It can only be the addressee for a task.</p> <p>Alternatively the task may be delegated to this user by the addressee, or be claimed by this user for a group.</p> | None.   |
| View and work with task detail | <p>Addressee or recipient for task.</p> <p>Alternatively the task may be delegated to this user by the addressee, or be claimed by this user for a group.</p>   | None.   |
| View workflow comments         | <p>Addressee or recipient for task.</p> <p>Alternatively the task may be delegated to this user by the addressee, or be claimed by this user for a group.</p>   | None.   |

In manage mode, the Domain Administrator can perform all actions for role and resource assignments on the Work Dashboard without any security permissions, as outlined in the table below.

**Table 9-9** Role and Resource Assignments for Domain Administrators in Manage Mode

| To perform this action...     | Managed User, Group, or Container must be...   | And the Domain Administrator must have these permissions... |
|-------------------------------|--|---|
| View role or resource in list | <p>Recipient.</p> <p>The list of assignments includes assignments for groups and containers to which the user belongs.</p> | None.   |

| To perform this action...                        | Managed User, Group, or Container must be...  | And the Domain Administrator must have these permissions...  |
|--|---|--|
| Assign or remove assignment for role or resource | Recipient.<br><br>The list of assignments includes assignments for groups and containers to which the user belongs. | None.<br><br>On the Work Dashboard, the Domain Administrator can edit, assign, or remove all role assignments, except system role assignments that are not in the domain he is authorized to administer. This means that the Role Domain Administrator can remove Role Administrator and Role Manager assignments, but not Resource Administrator or Resource Manager assignments.<br><br>Domain Administrator can view and edit any resource. |

In manage mode, the Domain Administrator can perform self-service actions for request status on the Work Dashboard without any security permissions, as outlined in the table below.

**Table 9-10** Request Status for Domain Administrators in Manage Mode

| To perform this action....                         | Managed User, Group, or Container must be...   | And the Domain Administrator must have these permissions....  |
|--|--|---|
| View process requests in list                      | Initiator or recipient   | None.   |
| View and work with process request detail          | Initiator or recipient   | None.   |
| Retract process requests                           | Initiator or recipient   | None.   |
| View workflow comments for process requests        | Initiator or recipient   | None.   |
| View role or resource requests in list             | Initiator or recipient   | None.   |
| View and work with role or resource request detail | Initiator or recipient.<br><br>The Domain Administrator cannot see requests for system roles.  | None.<br><br>Domain Administrator can view all role requests, except for system role requests.<br><br>Domain Administrator can view and edit any resource.    |
| Retract role or resource requests                  | Initiator or recipient.<br><br>The request must be in retractable state.<br><br>The Domain Administrator cannot retract requests for system roles. | None.<br><br>Domain Administrator can retract all role requests, except for system role requests.<br><br>Domain Administrator can view and edit any resource. |

| To perform this action....                           | Managed User, Group, or Container must be...  | And the Domain Administrator must have these permissions....   |
|--|---|--|
| View workflow comments for role or resource requests | Initiator or recipient.<br><br>The Domain Administrator cannot view workflow comments for system roles. | None.<br><br>Domain Administrator can view and edit all roles except system roles.<br><br>Domain Administrator can view and edit any resource. |

### 9.6.3 Domain Manager in Manage Mode

In manage mode, the Domain Manager can view tasks without any security permissions, but must have permission to view task details and workflow comments, as outlined in the table below.

**Table 9-11** Task Notifications for Domain Managers in Managed Mode

| To perform this action... | Managed User, Group, Container, or Role must be...   | And the Domain Manager must have these permissions... |
|---------------------------|--|---|
| View task in list         | Addressee or recipient for task.<br><br><b>NOTE:</b> A role cannot be the recipient for a task. It can only be the addressee for a task.<br><br>Alternatively the task may be delegated to this user by the addressee, or be claimed by this user for a group. | None.   |
| View task detail          | Addressee or recipient for task.<br><br>Alternatively the task may be delegated to this user by the addressee, or be claimed by this user for a group.   | Manage Addressee Task                                 |
| View workflow comments    | Addressee or recipient for task.<br><br>Alternatively the task may be delegated to this user by the addressee, or be claimed by this user for a group.   | Manage Addressee Task                                 |

In manage mode, the Domain Manager can view role and resource assignments without any security permissions, but must have permission to assign roles and resources or to remove existing assignments, as outlined in the table below.



**Table 9-12** Role and Resource Assignments for Domain Managers in Manage Mode

| To perform this action...                        | Managed User, Group, or Container must be...  | And the Domain Manager must have these permissions...   |
|--|---|---|
| View role or resource in list                    | Recipient.<br><br>The list of assignments includes assignments for groups and containers to which the user belongs. | None.   |
| Assign or remove assignment for role or resource | Recipient.<br><br>The list of assignments includes assignments for groups and containers to which the user belongs. | One or more of the following trustee permissions for a role: <ul style="list-style-type: none"> <li>◆ Assign Role To User</li> <li>◆ Revoke Role From User</li> <li>◆ Assign Role To Group And Container</li> <li>◆ Revoke Role From Group And Container</li> </ul> One or more of the following trustee permissions for a resource: <ul style="list-style-type: none"> <li>◆ Assign Resource</li> <li>◆ Revoke Resource</li> </ul> |

In manage mode, the Domain Manager can view process, role, and resource requests without any security permissions, but must have permission to view request details and workflow comments, as well as to retract requests, as outlined in the table below.

**Table 9-13** Request Status for Domain Managers in Manage Mode

| To perform this action...                          | Managed User, Group, or Container must be... | And the Domain Manager must have these permissions...  |
|--|--|--|
| View process requests in list                      | Initiator or recipient                       | None.  |
| View and work with process request detail          | Initiator or recipient                       | View Running PRD   |
| Retract process requests                           | Initiator or recipient                       | Retract PRD  |
| View workflow comments for process requests        | Initiator or recipient                       | View Running PRD   |
| View role or resource requests in list             | Initiator or recipient                       | None.  |
| View and work with role or resource request detail | Initiator or recipient                       | View Role or View Resource<br><br>The View Role permission controls whether you can see details for role requests in the Request Status section of the Work Dashboard. The View Resource permissions controls whether you can see details for resource requests. |

| To perform this action...                            | Managed User, Group, or Container must be...                              | And the Domain Manager must have these permissions...  |
|--|---|--|
| Retract role or resource requests                    | Initiator or recipient.<br><br>The request must be in a retractable state | One or more of the following trustee permissions for a role: <ul style="list-style-type: none"> <li>◆ Assign Role To User</li> <li>◆ Assign Role To Group And Container</li> <li>◆ Update Role</li> <li>◆ Revoke Role From User</li> <li>◆ Revoke Role From Group And Container</li> </ul><br>The following trustee permission for a resource: <ul style="list-style-type: none"> <li>◆ Revoke Resource</li> </ul> |
| View workflow comments for role or resource requests | Initiator or recipient  | View Role or View Resource   |

## 9.6.4 Team Manager in Manage Mode

In manage mode, the Team Manager can view tasks without any security permissions, but must have permission to view task details and workflow comments, as outlined in the table below.

**Table 9-14** Task Notifications for Team Managers in Manage Mode

| To perform this action... | Managed User must be...   | And the Team Manager must have these permissions... |
|---------------------------|---|---|
| View task in list         | A member of the team and also the addressee for the task.<br><br>Alternatively the task may be delegated to this user by the addressee, or be claimed by this user for a group. | None.   |
| View task detail          | A member of the team and also the addressee for the task.<br><br>Alternatively the task may be delegated to this user by the addressee, or be claimed by this user for a group. | Manage Addressee Task                               |
| View workflow comments    | A member of the team and also the addressee for the task.<br><br>Alternatively the task may be delegated to this user by the addressee, or be claimed by this user for a group. | Manage Addressee Task                               |

In manage mode, the Team Manager can view role and resource assignments without any security permissions, but must have permission to assign roles and resources or to remove existing assignments, as outlined in the table below.

**Table 9-15** Role and Resource Assignments for Team Managers in Manage Mode

| To perform this action...                        | Managed user must be...  | And the Team Manager must have these permissions...   |
|--|--|---|
| View role or resource in list                    | A member of the selected team.<br><br>The user must also be the recipient.<br><br>The list of role assignments includes assignments for groups and containers to which the user belongs.<br><br>The list of resource assignments includes assignments for the managed user only. | None.   |
| Assign or remove assignment for role or resource | A member of the selected team.<br><br>The user must also be the recipient.<br><br>The list of assignments includes assignments for groups and containers to which the user belongs.  | One or more of the following trustee permissions for a role: <ul style="list-style-type: none"> <li>◆ Assign Role To User</li> <li>◆ Revoke Role From User</li> <li>◆ Assign Role To Group And Container</li> <li>◆ Revoke Role From Group And Container</li> </ul> One or more of the following trustee permissions for a resource: <ul style="list-style-type: none"> <li>◆ Assign Resource</li> <li>◆ Revoke Resource</li> </ul> |

In manage mode, the Team Manager can view process, role, and resource requests without any security permissions, but must have permission to view request details and workflow comments, as well as to retract requests, as outlined in the table below.

**Table 9-16** Request Status for Team Managers in Manage Mode

| To perform this action...                   | Managed user must be... | And the Team Manager must have these permissions... |
|---|-------------------------|---|
| View process requests in list               | Initiator or recipient  | None.   |
| View and work with process request detail   | Initiator or recipient  | View Running PRD                                    |
| Retract process requests                    | Initiator or recipient  | Retract PRD   |
| View workflow comments for process requests | Initiator or recipient  | View Running PRD                                    |

| To perform this action...                            | Managed user must be...   | And the Team Manager must have these permissions...  |
|--|---|--|
| View role or resource requests in list               | Initiator or recipient  | None.  |
| View and work with role or resource request detail   | Initiator or recipient  | <p>View Role or View Resource</p> <p>The View Role permission controls whether you can see details for role requests in the Request Status section of the Work Dashboard. The View Resource permissions controls whether you can see details for resource requests.</p>  |
| Retract role or resource requests                    | <p>Initiator or recipient.</p> <p>The request must be in a retractable state.</p> | <p>One or more of the following trustee permissions for a role:</p> <ul style="list-style-type: none"> <li>◆ Assign Role To User</li> <li>◆ Assign Role To User and Group</li> <li>◆ Update Role</li> <li>◆ Revoke Role From User</li> <li>◆ Revoke Role From Group And Container</li> </ul> <p>The following trustee permission for a resource:</p> <ul style="list-style-type: none"> <li>◆ Revoke Resource</li> </ul> |
| View workflow comments for role or resource requests | Initiator or recipient  | View Role or View Resource   |

---

# 10 Managing Your Work

This section describes the actions supported by the Work Dashboard page. Topics include:

- ♦ [Section 10.1, “Working with Tasks,” on page 125](#)
- ♦ [Section 10.2, “Working with Resources,” on page 143](#)
- ♦ [Section 10.3, “Working with Roles,” on page 151](#)
- ♦ [Section 10.4, “Viewing Your Request Status,” on page 159](#)

## 10.1 Working with Tasks

The *Task Notifications* action lets you check the workflow queue for tasks that have been assigned to you or to a user, group, container, or role whose tasks you are permitted to manage. When a task is in your queue, you need to perform one of the following actions:

- ♦ Claim the task so you begin working on it
- ♦ Reassign the task to another user, group, or role

---

**NOTE:** To reassign a task, you must be a Provisioning Administrator or Provisioning Manager (or Team Manager) who has the *Manage Addressee Task* permission. If you do not have this permission, the *Reassign* button is not available.

---

The business user who does not have any administrative privileges can only see tasks for which he is the addressee. The business user does not see tasks for which he is the recipient. The list of tasks shown to the business user includes unclaimed tasks.

Alternatively the task may be delegated to the business user by the addressee, or be claimed by this user for a group.

---

**NOTE:** The business user does not need to have directory browse rights to the provisioning request definition that started the workflow in order to see a task for which he is the addressee.

---

The Provisioning Administrator and Provisioning Manager have the ability to manage tasks for other users, as described below:

- ♦ When nothing is selected in the *Manage* control, the task list shows the current user’s tasks. These tasks include those for which he is either recipient or addressee, as well as tasks for which the recipient or addressee is a group, container, or role to which the current user belongs. The Provisioning Administrator or Provisioning Manager can do anything with his own tasks, since no rights are required to work with one’s own tasks.
- ♦ When a user is selected in the *Manage* control, the list shows tasks that have the selected user as addressee, as well as those for which the user is the recipient. The Provisioning Administrator or Provisioning Manager can filter the task list to show only those tasks for which the managed user is addressee. Alternatively, the user can filter the list to show only those tasks for which the managed user is the recipient.

- ◆ When a group is selected, the list shows tasks that have the selected group as addressee, as well as those for which the group is recipient. The Provisioning Administrator, Provisioning Manager, or Team Manager can filter the task list to show only those tasks for which the managed group is addressee. Alternatively, the user can filter the list to show only those tasks for which the managed group is the recipient.
- ◆ When a role is selected, the list shows tasks that have the selected role as addressee. A role cannot be specified as the recipient for a task.
- ◆ When a container is chosen, the list shows tasks that have the selected container as recipient. A container cannot be specified as the addressee for a task.

A Team Manager for the Provisioning domain has the ability to manage tasks for team members. Before selecting a team member, the Team Manager must select a team.

The *Task Notifications* action allows you to work on tasks associated with resource requests, role requests, process requests, and attestation requests. In some cases, the user interface may differ depending on which type of task you select to work on. For attestation requests, the *Task Notifications* action shows only those tasks for which the current user is designated as an attester.

When you claim a task associated with a resource, role, or process request, you have the ability to take an action that forwards the workitem to the next activity within the workflow. The actions you can perform are described below:

**Table 10-1** Forward Actions

| Forward Action | Description  |
|----------------|--|
| Approve        | Allows you to give your approval to the task. When you approve the task, the workitem is forwarded to the next activity in the workflow.   |
| Deny           | Allows you to explicitly deny your approval to the task. When you deny the task, the workitem is forwarded to the next activity in the workflow and the request is denied. Typically, the workflow process terminates when a request is denied.  |
| Refuse         | Allows you to explicitly refuse the task. When you refuse the task, the workitem is forwarded to the next activity for the refused action in the workflow.<br><br>The Refuse action applies to individual tasks. The user interface does not permit to you to perform this action on a set of tasks. |

When you claim a task associated with an attestation request, you need to review the information displayed in the attestation form. In addition, you need to answer the required attestation question, which indicates whether you attest to the correctness of the data, and, in some cases, respond to one or more survey questions. For user profile attestation processes, the form includes your user attribute data, which you need to verify for accuracy. For role assignment, user assignment, and SoD attestation processes, the form includes a report that shows the role assignment, user assignment, or SoD data you need to verify.

## 10.1.1 Viewing the Task List

To see the tasks that have been assigned to you:

- 1 Click *Task Notifications* in the group of actions on the Work Dashboard.  
The list of tasks in your queue is displayed.

Novell Identity Manager

Welcome Allison | Identity Self-Service | Work Dashboard | Logout | Help

Task Notifications

| Task                          | Request                                   | Recipient     | Type | Request Date           | Comments |
|-------------------------------|---|---------------|------|------------------------|----------|
| Approve Role Request (Serial) | Role Approval - test 1 polina june        | Chris Black   | →    | 06/09/2009 04:09:58 AM |          |
| Approve Role Request (Serial) | Role Approval - test 1 polina june        | Chip Nano     | →    | 06/09/2009 04:09:59 AM |          |
| Resource Request              | Add Resource To User - Alan Resource Test | Kevin Chester | →    | 06/19/2009 03:52:40 AM |          |
| Resource Request              | Add Resource To User - Alan Resource Test | Timothy Swan  | →    | 06/19/2009 03:55:12 AM |          |
| Attestation Approval          | User Profile - Default (2009/06/23)       | Allison Blake | →    | 06/23/2009 06:43:15 PM |          |
| Resource Request              | Add Resource To User - Alan Resource Test | Jay West      | →    | 06/25/2009 08:46:07 AM |          |
| Resource Request              | Add Resource To User - Alan Resource Test | Chris Black   | →    | 06/25/2009 08:46:07 AM |          |
| Resource Request              | Add Resource To User - Alan Resource Test | Kip Keller    | →    | 06/25/2009 08:46:07 AM |          |
| Attestation Approval          | User Profile - Default (2009/06/30)       | Allison Blake | →    | 06/30/2009 03:58:03 AM |          |

1 - 9 of 9

Resource Assignments

Role Assignments

Request Status

For resource and role requests, the *Recipient* column in the task list specifies the user(s) or group(s) that will receive the resource or role in the event that the required approvals are given. For attestation requests, the *Recipient* column specifies the name of the attester.

The *Type* column in the task list includes an icon that indicates whether the task is currently assigned to a user, group, delegate, or to multiple approvers. The type *Assigned to Multiple Approvers* applies in the following situations:

- ◆ The task has been assigned to a group of addressees, but only one addressee can claim and approve the task. After this approval is given, task execution is considered complete.
- ◆ The task has been assigned to multiple addressees, and all of them must claim and approve the task before the activity can be considered complete.
- ◆ The task has been assigned to multiple addressees, and a quorum of users must claim and approve the task before the activity can be considered complete. The definition of a quorum is configured by the administrator. To define the quorum, the administrator specifies an approval condition that specifies the precise number of approvals or the percentage of approvals needed.

The workflow system performs *short circuit evaluation* to optimize quorums. Whenever a quorum approval condition reaches the point where a quorum is not possible, the activity is denied and the task is removed from the queues of all addressees.

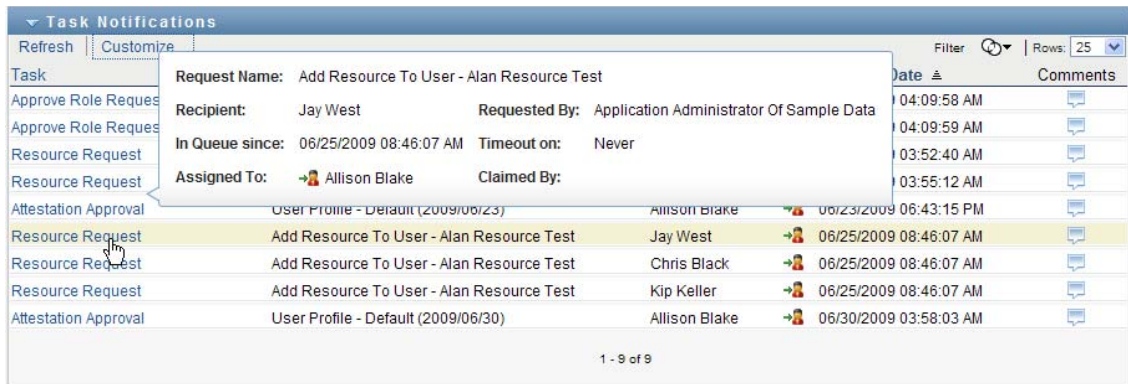
The *Priority* column shows a flag for the high priority tasks. You can sort the list of tasks by priority by clicking the *Priority* column.

Workflow tasks associated with attestation requests show a task name of *Attestation Approval*.

## 10.1.2 Viewing the Summary for a Task

To see the summary information for a task:

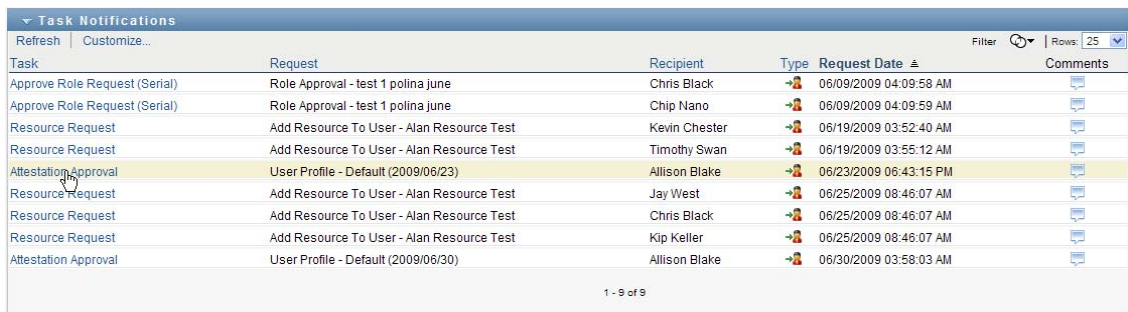
- 1 Hover over the task name in the task list.



## 10.1.3 Selecting a Task

To select a task in the queue list:

- 1 Click the name of the task in the queue.



The Task Detail form is displayed, either in a message window, or inline with the list of tasks. This behavior is controlled by a setting in the *Customize* dialog. The image below shows the Task Detail form inline:



**Request Name:** User Profile - Default (2009/06/23)

**Recipient:** Allison Blake      **Requested By:** Application Administrator Of Sample Data

**In Queue since:** 06/23/2009 06:43:15 PM      **Timeout on:** Never

**Assigned To:** Allison Blake      **Claimed By:**

[Comment and Flow History](#)

**Form Detail**  
\* - indicates required.

**Attributes List**

|                   |                |
|-------------------|----------------|
| First Name:       | Allison        |
| Last Name:        | Blake          |
| Title:            | Payroll        |
| Telephone Number: | (555) 555-1222 |

**Attestation Question**  
Do you attest that you have reviewed the details on your user profile and updated as needed? \*

The image below shows the Task Detail form in a message window:

**Task Notifications**  
Refresh | Customize...

**Task**

- Approve Role Request (Serial)
- Approve Role Request (Serial)
- Resource Request
- Resource Request
- Attestation Approval
- Resource Request
- Resource Request
- Resource Request
- Resource Request
- Attestation Approval

[Resource Assignments](#)

[Role Assignments](#)

[Request Status](#)

**Attestation Approval**

**Request Name:** User Profile - Default (2009/06/23)

**Recipient:** Allison Blake      **Requested By:** Application Administrator Of Sample Data

**In Queue since:** 06/23/2009 06:43:15 PM      **Timeout on:** Never

**Assigned To:** Allison Blake      **Claimed By:**

[Comment and Flow History](#)

**Form Detail**  
\* - indicates required.

**Attributes List**

|                   |                |
|-------------------|----------------|
| First Name:       | Allison        |
| Last Name:        | Blake          |
| Title:            | Payroll        |
| Telephone Number: | (555) 555-1222 |

**Attestation Question**  
Do you attest that you have reviewed the details on your user profile and updated as needed? \*

**Request Date** | Filter | Rows: 25

| Request Date          | Comments |
|-----------------------|----------|
| 6/09/2009 04:09:58 AM |          |
| 6/09/2009 04:09:59 AM |          |
| 6/19/2009 03:52:40 AM |          |
| 6/19/2009 03:55:12 AM |          |
| 6/23/2009 06:43:15 PM |          |
| 6/25/2009 08:46:07 AM |          |
| 6/25/2009 08:46:07 AM |          |
| 6/25/2009 08:46:07 AM |          |
| 6/30/2009 03:58:03 AM |          |

When a task is assigned to multiple approvers, the Task Detail form displays the *Multiple Approvers* icon next to the *Assigned To* field, and displays text below the icon to indicate that multiple approvals are necessary.

**Assigned To:** Multiple Approvers\*\*      **Claimed By:**

\*\*A number of approvals necessary. This task is in your queue because it has been delegated to you.

- To display more information about a task assigned to multiple approvers, click the text under the *Multiple Approvers* icon:



A pop-up window displays to indicate how many approvals are required, who the current addressees are, and what the approval status currently is.



The requirements for the task depend on how the task was configured by your administrator:

- ◆ If the approval type is *group*, the task has been assigned to several users within a group, but only one is expected to claim and approve the task.
- ◆ If the approval type is *role*, the task has been assigned to several users within a role, but only one is expected to claim and approve the task.
- ◆ If the approval type is *multiple approvers*, the task has been assigned to several addressees, and all of the addressees must claim and approve the task.
- ◆ If the approval type is *quorum*, the task has been assigned to several addressees, and a quorum of addressees is sufficient to approve the task. The definition of a quorum is configured by the administrator. To define the quorum, the administrator specifies an approval condition that specifies the precise number of approvals or the percentage of approvals needed.

The workflow system performs *short circuit evaluation* to optimize quorums. Whenever a quorum approval condition reaches the point where a quorum is not possible, the activity is denied and the task is removed from the queues of all addressees.

- 3 To claim a task, follow the instructions under [Section 10.1.4, “Claiming a Task,”](#) on page 132.
- 4 To view the comment history for the task, click *View Comment History*.

A pop-up window lets you see user and system comments. The order in which comments appear is determined by the time stamp associated with each comment. Comments entered first are displayed first. For parallel approval flows, the order of activities being processed concurrently can be unpredictable.

- 4a Click *Comment and Flow History*.
- 4b To display user comments, click *User Comments*.

**Attestation Approval**

Request Name: User Profile - Default (2009/06/23)

Recipient: Allison Blake      Requested By: Application Administrator Of Sample Data

In Queue since: 06/23/2009 06:43:15 PM      Timeout on: Never

Assigned To: Allison Blake      Claimed By:

**Comment and Flow History**

Refresh       User Comments       System Comments      Rows: 25

| Date                   | Activity             | User    | Comments                                     |
|------------------------|----------------------|---------|--|
| 06/23/2009 06:43:16 PM | Attestation Approval | IDMProv | User task assigned to reviewer Allison Blake |

1 - 1 of 1

Claim    Release    Close

**Form Detail**

\* - indicates required.

**Attributes List**

|             |         |
|-------------|---------|
| First Name: | Allison |
| Last Name:  | Blake   |

User comments include the following kinds of information:

- ◆ The date and time when each comment was added.
- ◆ The name of the activity to which each comment applies. The list of activities displayed includes user and provisioning activities that have been processed or are currently being processed.
- ◆ The name of the user who made the comment. If the comment is generated by the workflow system, the name of the application (for example, `IDMProv`) is the user name. Comments generated by the workflow system are localized automatically.
- ◆ The comment text, which includes the name of the user who is the current assignee for each activity.

The workflow designer can disable the generation of user comments for a workflow. For more information, see the *Identity Manager User Application: Design Guide*. (<http://www.netiq.com/documentation/idm402/index.html>)

**4c** To display system comments, click *Show System Comments*.

System comments include the following kinds of information:

- ◆ The date and time when each comment was added.
- ◆ The name of the activity to which each comment applies. When you display system comments, all activities in the workflow are listed. The list of activities includes those that have been processed or are currently being processed.

- ♦ The name of the user who made the comment. If the comment is generated by the workflow system, the name of the application (for example, IDMP<sub>Prov</sub>) is the user name. Comments generated by the workflow system are localized automatically.
- ♦ The comment text, which indicates what action was taken for the activity.

System comments are intended primarily for debugging purposes. Most business users do not need to look at the system comments for a workflow.

- 4d To scroll through a long list of comments, click the arrows at the bottom of the screen. For example, to scroll to the next page, click the *Next* arrow.



- 4e Click *Close* to close the window.

- 5 To return to the task list, click *Back*.

## 10.1.4 Claiming a Task

To claim a task to work on:

- 1 Click *Claim*.

For resource, role, and process requests, the *Form Detail* section of the page is updated to include the *Deny* and *Approve* buttons, as well as any other action buttons included by the flow definition, and the appropriate fields become editable.

For attestation requests, the *Form Detail* section of the page is updated to include the attestation form. The appearance of the form varies, depending on the attestation type. For user profile attestation processes, the form shows the user profile data you need to review:

Form Detail

### Attributes List

|                   |                |
|-------------------|----------------|
| First Name:       | Allison        |
| Last Name:        | Blake          |
| Title:            | Payroll        |
| Telephone Number: | (555) 555-1222 |

[Go to your profile](#)

---

### Attestation Question

Do you attest that you have reviewed the details on your user profile and updated as needed? \*

Comment:

For role assignment, user assignment, and SoD attestation processes, the form includes a report that shows the data you need to review:

Form Detail

### Report

**Role Assignment Attestation Report** Report Date: May 8, 2008 9:41 AM

---

**IT Role (Total: 2)**

**Role Name:** Compliance Module Administrator (IT Role)  
**Container:** Compliance Module Administrator.Level20.RoleDefs  
**Role Categories:** System Roles  
**Description:** Compliance Administrator

**Assignments to this Role** **Approver(s)**  
 Application Administrator Of Sample Data (User)

---

**Role Name:** Role Module Administrator (IT Role)  
**Container:** Role Module Administrator.Level20.RoleDefs  
**Role Categories:** System Roles  
**Description:** Role Module Administrator

**Assignments to this Role** **Approver(s)**  
 Application Administrator Of Sample Data (User)

---

**Business Role (Total: 2)**

**Role Name:** Conflict1 (Business Role)  
**Container:** Conflict1.Level30.RoleDefs  
**Role Categories:**  
**Description:** Conflict1

**Assignments to this Role** **Approver(s)**

For all attestation types, the form shows controls that allow you to answer the required attestation question, as well as any additional survey questions included in the attestation process:

### Survey Questions

Have you read the Role Assignment policy statement?  Comment:

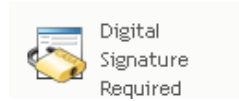
---

### Attestation Question

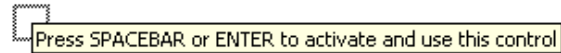
Do you attest that the role assignments in this Role Assignment report are valid and appropriate? \*

Comment:

If your administrator has configured your system for digital signatures, and the task requires a digital signature, the *Digital Signature Required* icon appears in the upper right corner of the page.



In addition, on Internet Explorer, a message appears indicating that you need to press the Spacebar or the Enter key to activate the digital signature applet.



- 2 If you're working on a task that requires a digital signature, perform these steps:
  - 2a If you're using a smart card, insert the smart card into the smart card reader.
  - 2b On Internet Explorer, press the Spacebar or the Enter key to activate the applet.

At this point, your browser might display a security warning message.
  - 2c Click *Run* to proceed.
  - 2d Fill in the fields in the approval form. The fields on the form vary depending on which resource you requested.
  - 2e Click the checkbox next to the digital signature confirmation message to indicate that you are ready to sign.

The digital signature confirmation message varies depending on how the provisioning resource was configured by the administrator.

The applet then displays a pop-up window that allows you to select a certificate. The pop-up window lists certificates imported to the browser as well as certificates imported to the smart card (if one is currently connected).

| Issued To /                                      | Issued By | Expiration ... | Intended ... |
|--|-----------|----------------|--------------|
| O=novell,OU=idmsample-lumberg,OU=users,CN=ablake | O=SL      | 09.10.2008     | <All>        |
| O=novell,OU=idmsample-tdb,OU=users,CN=jmiller    | O=SI      | 26.10.2008     | <All>        |

- 2f Select the certificate you want to use and click *Select*.
- 2g If you select a certificate that has been imported into your browser, type the password for the certificate in the *Password* field on the request form.
- 2h If you select a certificate that has been imported to your smart card, type the PIN for your smart card and click *OK*.

You do not need to type the password for the certificate if you're using a smart card, because the certificate password has already been transmitted to the card.



If your administrator has enabled the ability to preview the user agreement, the *Preview* button is enabled.

- 2i Click *Preview* to see the user agreement.

If the digital signature type is set to Form, a PDF document is displayed.

If the digital signature type is set to data, an XML document is displayed.

- 3 To deny a resource or role request, click *Deny*.

Form Detail

### Manager Approval

Please select the appropriate button to approve or reject the request.

Requested by: Allison Blake Recipient: Allison Blake

Request Date: 12/04/2006

Reason: test

Comment:

View Comment History

Deny Approve

- 4 To approve a resource or role request, click *Approve*.

Form Detail

### Manager Approval

Please select the appropriate button to approve or reject the request.

Requested by: Allison Blake Recipient: Allison Blake

Request Date: 12/04/2006

Reason: test

Comment:

View Comment History

Deny Approve

The User Application displays a message indicating whether the action was successful.

---

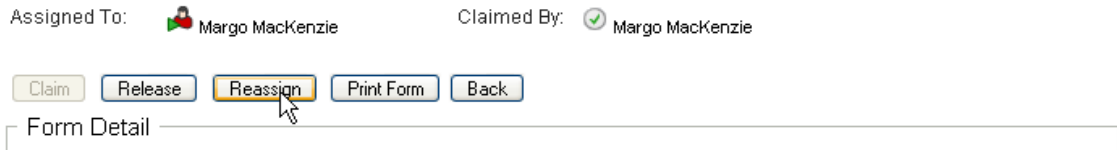
**NOTE:** If you accessed the task through the task list on the Work Dashboard, the task completion window provides a close button (X) in the upper right corner. However, the close button on the task completion window is not available if you accessed and completed the task via an e-mail link, or through deep linking.



---

## 10.1.5 Reassigning a Task

To reassign a task:

- 1 Click *Reassign* in the Task Detail window.




Assigned To:  Margo MacKenzie      Claimed By:  Margo MacKenzie

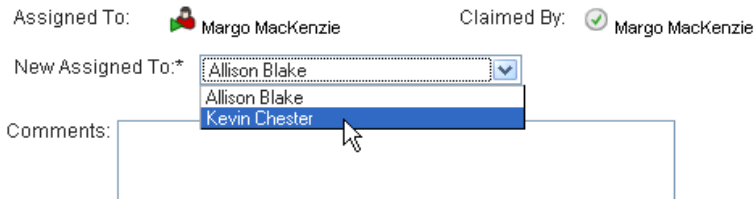
Form Detail



---


**NOTE:** To reassign a task, you must be a Provisioning Administrator or Provisioning Manager (or Team Manager) who has the *Manage Addressee Task* permission. If you do not have this permission, the *Reassign* button is not available.

---

- 2 Click the *Object Selector* icon  next to your chosen entry box.
- 3 In the *New Assigned To* drop-down list, select the user to whom you want to reassign the task.



Assigned To:  Margo MacKenzie      Claimed By:  Margo MacKenzie

New Assigned To:\*  

Comments:

*Allison Blake*  
*Allison Blake*  
*Kevin Chester*

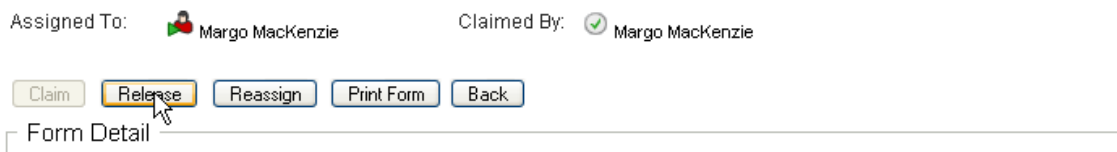
- 4 (Optional) Type a comment in the *Comments* field to explain the reason for the reassignment.
- 5 Click *Submit*.



The User Application displays a message indicating whether the action was successful.

## 10.1.6 Releasing a Task

You release a task so that it can be assigned to or claimed by another team member.

- 1 Click *Release* in the Task Detail window.



Assigned To:  Margo MacKenzie      Claimed By:  Margo MacKenzie

Form Detail

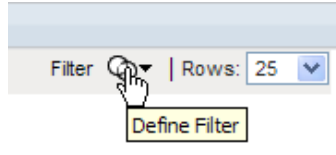


## 10.1.7 Filtering the Task List

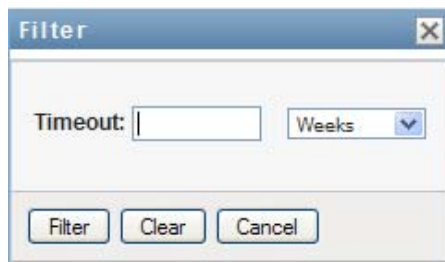
You can apply a filter to the task list to limit the number of rows returned. By filtering the task list, you can find what you're looking for more easily, and also improve performance.

To define a filter for the task list:

- 1 Click the *Define Filter* button.



The Filter dialog displays, showing several fields you can use to specify how you want to filter the data:



- 2 To narrow the search to tasks for which the current entity profile (either the currently logged-on user or a user, group, container, or role selected in the *Manage* control) is the addressee, select *Assigned to* in the *Tasks By* field.

---

**NOTE:** The *Tasks By* field is not available to end users, since end users can only see tasks for which they are the addressees. The *Tasks By* field is only visible to Domain Administrators, Domain Managers, and Team Managers.

---

- 3 To narrow the search to tasks for which the current entity profile is the recipient, select *Recipient* in the *Tasks By* field.
- 4 To include all tasks for which the current entity profile is either the addressee or the recipient, be sure that nothing is selected in the *Tasks By* field.
- 5 To narrow the search to tasks that timeout by a particular point in time, select the timeout unit (*Weeks*, *Days*, or *Hours*) and enter a value in the *Timeout* field.
- 6 Click *Filter* to perform a new query for tasks, using the selection criteria you've specified in the Filter dialog.

When you define a filter for the task list, your filter definition is saved in the Identity Vault along with your other user preferences.

---

**NOTE:** The preferences saved always apply to the user currently logged on to the User Application, regardless of whether a different user has been selected in the *Manage* control.

---

To see what filter points have been defined previously:

- 1 Look at the boxes to the left of the *Define Filter* icon.

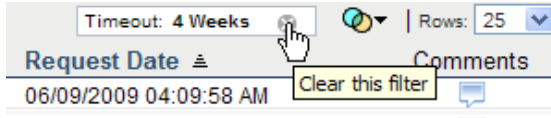
When no filters are defined, the *Define Filter* icon shows two empty rings, as shown below:



When one or more filter points have been defined, each filter point appears in a separate box, as shown below:

To remove a filter point previously specified in the Filter dialog:

- 1 Click the *Clear this filter* icon (which looks like an X) next to the filter point you want to remove:



To remove all previously defined filters and update the search results to include all tasks.

- 1 Click the *Define Filters* button to open the Filter dialog.
- 2 Click the *Clear Filters* button.

The Filter dialog closes and the task list is updated to include all tasks.

## 10.1.8 Customizing the Task Columns

The Task Notifications section of the Work Dashboard page allows you to select and deselect columns, and also reorder columns within the task list display. This behavior is controlled by a setting within the Customize Task Notifications Display dialog.

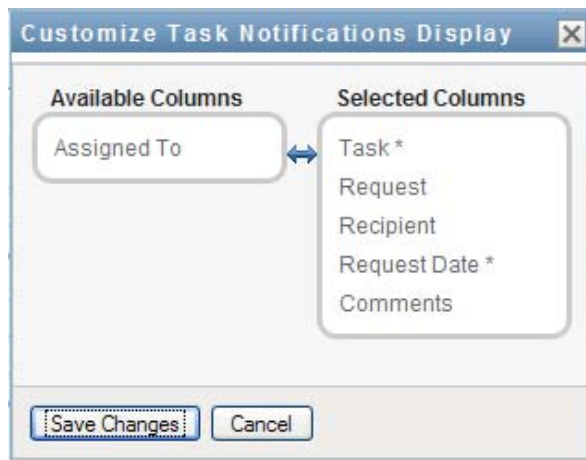
When you modify the column list or reorder the columns, your customizations are saved in the Identity Vault along with your other user preferences.

To customize the display of columns in the task list:

- 1 Click the *Customize Task Notifications Display* button in the *Task Notifications* section of the Work Dashboard page.



The User Application displays the list of columns currently selected for the display, and a list of additional columns that are available for selection.



- 2 To include an additional column in the display, select the column in the *Available Columns* list box, and drag it to the *Selected Columns* list box.

To select multiple columns in the list, hold down the Ctrl key and select the columns. To select a range of columns that appear together in the list, hold down the Shift key and select the columns.

You can reorder the columns in the display by moving them up or down in the *Selected Columns* list box.

- 3 To remove a column from the display, select the column in the *Selected Columns* list box, and drag it to the *Available Columns* list box.

The *Task* and *Priority* columns are mandatory columns and cannot be removed from the task list display.

- 4 To save your changes, click *Save*.

## 10.1.9 Controlling Whether the Task List is Expanded by Default

The Work Dashboard page allows you to specify whether you want the task list to be expanded by default in the Task Notifications section of the page. This behavior is controlled by a setting within the Customize Task Notifications Display dialog.

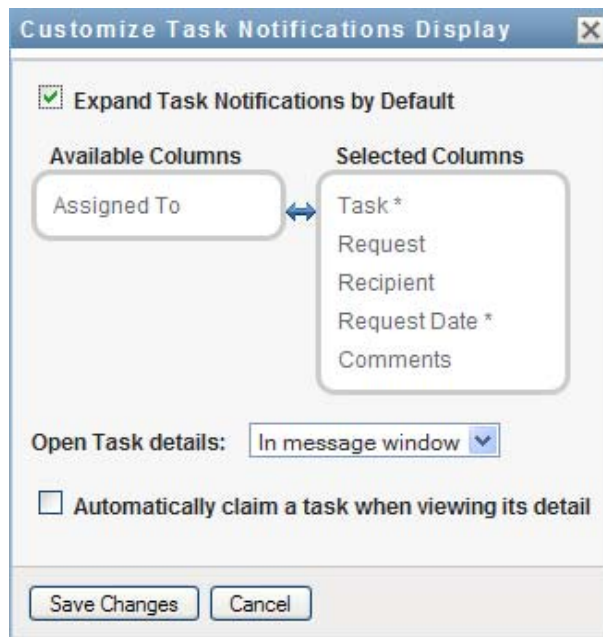
When you modify this setting, your preference is saved in the Identity Vault along with your other user preferences.

To specify whether you want the task list to be expanded by default:

- 1 Click the *Customize Task Notifications Display* button in the *Task Notifications* section of the Work Dashboard page.



The User Application displays the Customize Task Notifications Display dialog, which allows you to customize the task list display. The set of controls shown may vary depending on which settings the administrator has designated as available for user override.



- 2 To expand the task list display by default, select the *Expand Task Notifications by Default* checkbox. To hide the task list display by default, deselect the *Expand Task Notifications by Default* checkbox.

The *Expand Task Notifications by Default* checkbox controls the initial appearance of the Task Notifications section of the Work Dashboard. Note that you can expand or collapse the task list within the Task Notifications section of the page, regardless of whether you select or deselect this checkbox.

- 3 To save your changes, click *Save Changes*.

## 10.1.10 Controlling the Display of Task Details

The Work Dashboard page allows you to specify how you want to display the details for a task you click on in the Task Notifications section of the page. You can display the task details within the list or in a separate modal dialog. This behavior is controlled by a setting within the Customize Task Notifications Display dialog.

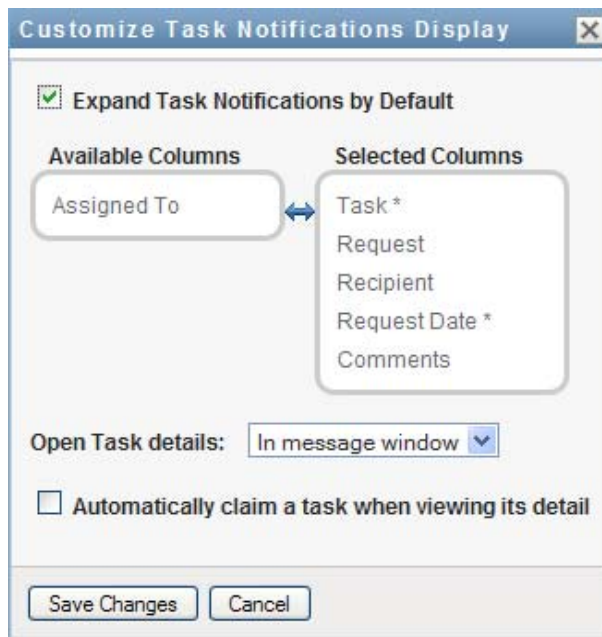
When you modify this setting, your preference is saved in the Identity Vault along with your other user preferences.

To control the display of task details:

- 1 Click the *Customize Task Notifications Display* button in the *Task Notifications* section of the Work Dashboard page.



The User Application displays the Customize Task Notifications Display dialog, which allows you to customize the task list display. The set of controls shown may vary depending on which settings the administrator has designated as available for user override.



- 2 To display the details within the task list display, select *In line with list* in the *Open Task details* dropdown. To display the details in a separate modal dialog, select *In message window*.
- 3 To save your changes, click *Save Changes*.

## 10.1.11 Setting the Claim Action for Open Tasks

The Work Dashboard page allows you to control what action is required to claim a task. You can specify that a task must be claimed explicitly, or you can specify that the action of opening a task automatically claims the task for your use. This behavior is controlled by a setting within the Customize Task Notifications Display dialog.

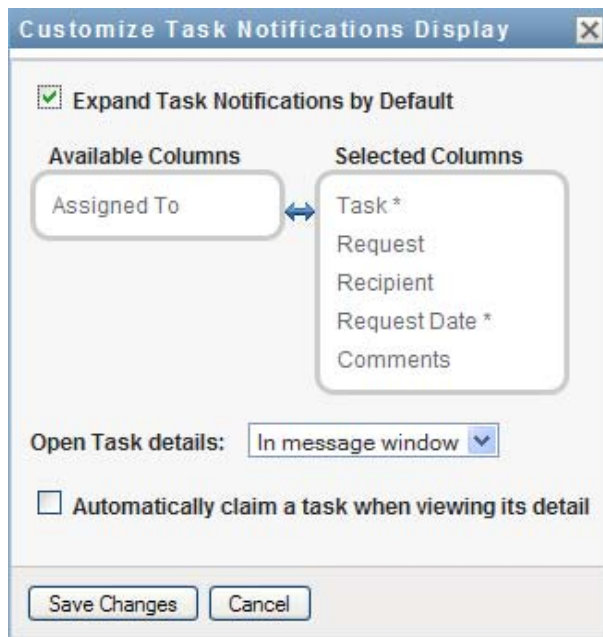
When you modify this setting, your preference is saved in the Identity Vault along with your other user preferences.

To specify what action is required to claim a task:

- 1 Click the *Customize Task Notifications Display* button in the *Task Notifications* section of the Work Dashboard page.



The User Application displays the Customize Task Notifications Display dialog, which allows you to customize the claim action. The set of controls shown may vary depending on which settings the administrator has designated as available for user override.



- 2 To specify that the action of opening a task automatically claims the task for your use, select the *Automatically claim a task when viewing its details* checkbox. To specify that a task must be claimed explicitly, deselect this checkbox.
- 3 To save your changes, click *Save Changes*.

## 10.1.12 Sorting the Task List

To sort the task list:

- 1 Click the header for the column you want to sort on.

The pyramid-shaped sort indicator shows you which column is the new primary sort column. When the sort is ascending, the sort indicator is shown in its normal, upright position.

| Task                          | Request                                   | Recipient ▲   | Request Date           | Comments |
|-------------------------------|---|---------------|------------------------|----------|
| Attestation Approval          | User Profile - Default (2009/06/23)       | Allison Blake | 06/23/2009 06:43:15 PM |          |
| Attestation Approval          | User Profile - Default (2009/06/30)       | Allison Blake | 06/30/2009 03:58:03 AM |          |
| Approve Role Request (Serial) | Role Approval - test 1 pollina june       | Chip Nano     | 06/09/2009 04:09:59 AM |          |
| Resource Request              | Add Resource To User - Alan Resource Test | Chris Black   | 06/25/2009 08:46:07 AM |          |
| Approve Role Request (Serial) | Role Approval - test 1 pollina june       | Chris Black   | 06/09/2009 04:09:58 AM |          |
| Resource Request              | Add Resource To User - Alan Resource Test | Jay West      | 06/25/2009 08:46:07 AM |          |
| Resource Request              | Add Resource To User - Alan Resource Test | Kevin Chester | 06/19/2009 03:52:40 AM |          |
| Resource Request              | Add Resource To User - Alan Resource Test | Kip Keller    | 06/25/2009 08:46:07 AM |          |
| Resource Request              | Add Resource To User - Alan Resource Test | Timothy Swan  | 06/19/2009 03:55:12 AM |          |

When the sort is descending, the sort indicator is upside down.

The initial sort column is set by the RBPM Configuration Administrator. If you sort the list on any column other than the Request column, the Request column is used as the secondary sort column.

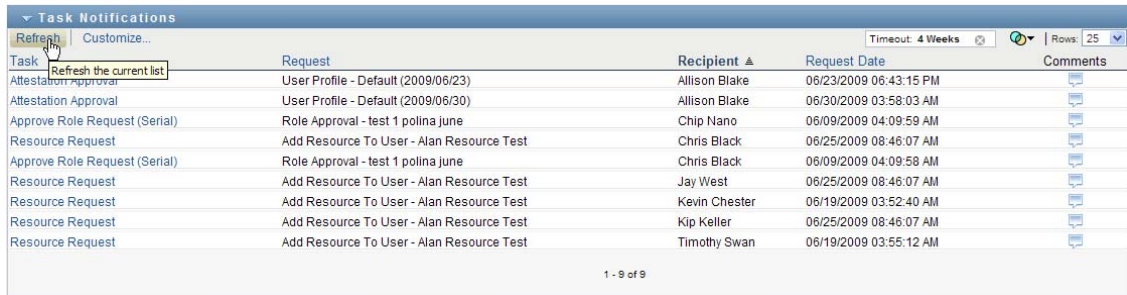
If you override the initial sort column, your sort column is added to the list of required columns in the *Customize Task Notifications Display* dialog. Required columns are indicated with an asterisk (\*).

When you modify the sort order for the task list, your preference is saved in the Identity Vault along with your other user preferences.

## 10.1.13 Refreshing the Task List

To refresh the task list:

- 1 Click the *Refresh* button.



| Task                          | Request                                   | Recipient     | Request Date           | Comments |
|-------------------------------|---|---------------|------------------------|----------|
| Attestation Approval          | User Profile - Default (2009/06/23)       | Allison Blake | 06/23/2009 06:43:15 PM |          |
| Attestation Approval          | User Profile - Default (2009/06/30)       | Allison Blake | 06/30/2009 03:58:03 AM |          |
| Approve Role Request (Serial) | Role Approval - test 1 polina june        | Chip Nano     | 06/09/2009 04:09:59 AM |          |
| Resource Request              | Add Resource To User - Alan Resource Test | Chris Black   | 06/25/2009 08:46:07 AM |          |
| Approve Role Request (Serial) | Role Approval - test 1 polina june        | Chris Black   | 06/09/2009 04:09:58 AM |          |
| Resource Request              | Add Resource To User - Alan Resource Test | Jay West      | 06/25/2009 08:46:07 AM |          |
| Resource Request              | Add Resource To User - Alan Resource Test | Kevin Chester | 06/19/2009 03:52:40 AM |          |
| Resource Request              | Add Resource To User - Alan Resource Test | Kip Keller    | 06/25/2009 08:46:07 AM |          |
| Resource Request              | Add Resource To User - Alan Resource Test | Timothy Swan  | 06/19/2009 03:55:12 AM |          |

The task list is updated to reflect the current state of the task queue for the current user.

## 10.1.14 Controlling the Number of Items Displayed on a Page

To specify the number of items you want displayed on each page:

- 1 Select a number in the *Rows* dropdown list.

When you modify the *Rows* setting, your preference is saved in the Identity Vault along with your other user preferences.

## 10.1.15 Viewing the Comments for a Task

- 1 To display the comment text for a task, click the Comments icon in the task list.



---

**NOTE:** To see the comments for a task, you must include the Comments column in the list of selected columns. For details on adding columns to the task list, see [Section 10.1.8, “Customizing the Task Columns,”](#) on page 138.

---

## 10.2 Working with Resources

The *Resource Assignments* action allows you to see what resource assignments you have, and also make requests for additional resource assignments.

The Resource Administrator and Resource Manager have the ability to view resource assignments for other users, as described below:

- ♦ When nothing is selected in the *Manage* control, the resource assignment list shows the current user’s resource assignments. These resource assignments include those for which he is either recipient or addressee, as well as resources for which the recipient or addressee is a group, container, or role to which the current user belongs. The user can do anything with his own resource assignments, since no rights are required to work with one’s own resources.
- ♦ When a user is selected in the *Manage* control, the list shows resources assignments that have the selected user as recipient.

- ◆ When a group is selected, the list shows resource assignments assigned indirectly to the selected group through role assignments.
- ◆ When a role is selected, the *Resource Assignments* section displays a message indicating that resources that are granted through role assignments are not shown. To see the resource assignments for a role, you need to look at the *Roles* tab.
- ◆ When a container is chosen, the list shows resource assignments assigned indirectly to the selected container through role assignments.

A Team Manager for the Resource domain has the ability to manage resources for team members. Before selecting a team member, the Team Manager must select a team.

When a Team Manager is in manage mode, the *Resource Assignments* list includes only resource assignments associated with the domain specified for the selected team configuration.

**Proxy Mode** The *Resource Assignments* action is not available in proxy mode.




## 10.2.1 Viewing Your Resource Assignments

To see the resource assignments for yourself, or for a user, group, or container selected in the *Manage* control:

- 1 Click *Resource Assignments* in the group of actions on the Work Dashboard.

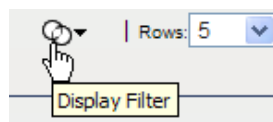
The list of resources is displayed. If you are not in managed mode, the resource assignments shown are those for which you are the recipient. If you are in managed mode, the resource assignments shown are those for which the selected user, group, or container is the recipient. For groups and containers, the resources listed are those resources assigned indirectly to the selected group or container through role assignments. The list of resource assignments for a group or container does not contain resources assigned directly to a user within the selected group or container.

**NOTE:** Resources can only be assigned directly to a user. However, a role that contains a resource can be assigned to a group or container, in which case the resource will be assigned indirectly to all users within the group or container. The *Resource Assignments* list on the dashboard shows direct assignments for users, as well as indirect assignments for groups and containers.

| ▼ Resource Assignments                         |   |                    |                   |                             |   |
|--|---|--------------------|-------------------|-----------------------------|---|
| Assign...   Remove...   Refresh   Customize... |   |                    |                   |                             | Filter    Rows: 5            |
| <input type="checkbox"/>                       | Resource ▲  | Request Date       | Description       | Initial Request Description | Parameters  |
| <input type="checkbox"/>                       |  A Van             | 7/23/09 4:46:47 PM | A Van             | test                        |   |
| <input type="checkbox"/>                       |  Van Resource Test | 7/23/09 4:47:41 PM | Van Resource Test | test assignment             | Field Label 1 : test field label<br>Select membership van : !METACARPALSTREE!novellidmsample-mysql/groups/Nursing |

### Filtering the Resource Assignment List

- 1 Click the Display Filter button in the upper right corner of the *Resource Assignments* display.





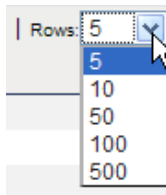
- Specify a filter string for the initial request description, resource name, description, or parameters associated with the resource assignment.

The image shows a 'Filter' dialog box with a title bar and a close button. It contains four text input fields labeled 'Initial Request Description:', 'Resource:', 'Description:', and 'Parameters:'. At the bottom, there are three buttons: 'Filter', 'Clear', and 'Cancel'.

- Click *Filter* to apply your selection criteria.
- To remove the current filter, click *Clear*.

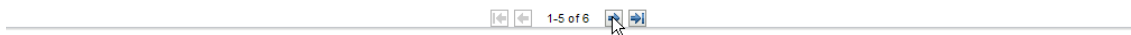
## Setting the Maximum Number of Rows on a Page

- Click on the *Rows* dropdown list and select the number of rows you want to be displayed on each page:



## Scrolling within the Resource Assignment List

- To scroll to another page in the resource assignment list, click on the Next, Previous, First or Last button at the bottom of the list:



## Sorting the Resource Assignment List

To sort the resource assignment list:

- Click the header for the column you want to sort on.

The pyramid-shaped sort indicator shows you which column is the new primary sort column. When the sort is ascending, the sort indicator is shown in its normal, upright position.

| Resource Assignments                       |                    |                   |                             |   |
|--|--------------------|-------------------|-----------------------------|---|
| Resource                                   | Request Date ▲     | Description       | Initial Request Description | Parameters  |
| <input type="checkbox"/> A Van             | 7/23/09 4:46:47 PM | A Van             | test                        |   |
| <input type="checkbox"/> Van Resource Test | 7/23/09 4:47:41 PM | Van Resource Test | test assignment             | Field Label 1 : test field label<br>Select membership van : METACARPALSTREE\novellnidmsample-mysql/groups/Nursing |

When the sort is descending, the sort indicator is upside down.

The initial sort column is determined by the RBPM Configuration Administrator.

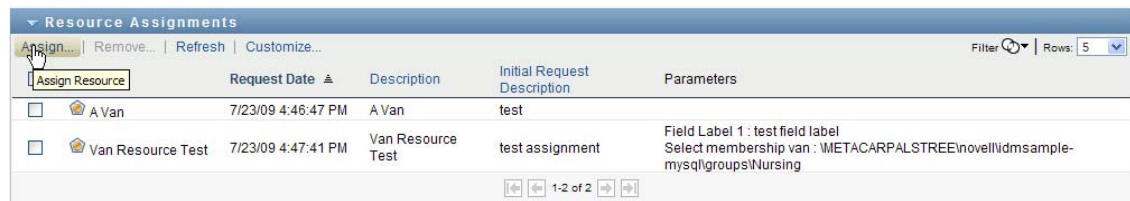
If you override the initial sort column, your sort column is added to the list of required columns. Required columns are indicated with an asterisk (\*).

When you modify the sort order for the resource assignment list, your preference is saved in the Identity Vault along with your other user preferences.

## 10.2.2 Requesting a Resource Assignment

To make a resource assignment request:

- 1 Click the *Assign* button at the top of the Resource Assignments section of the page.

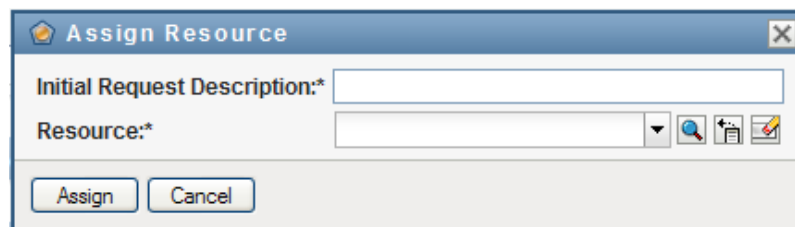


The screenshot shows a table titled "Resource Assignments" with columns: Request Date, Description, Initial Request Description, and Parameters. The "Assign Resource" button is highlighted in the top left corner of the table area.

|                          | Request Date       | Description       | Initial Request Description | Parameters  |
|--------------------------|--------------------|-------------------|-----------------------------|---|
| <input type="checkbox"/> | 7/23/09 4:46:47 PM | A Van             | test                        |   |
| <input type="checkbox"/> | 7/23/09 4:47:41 PM | Van Resource Test | test assignment             | Field Label 1 : test field label<br>Select membership van : METACARPALSTREE\novellidmsample-mysqlgroups\nursing |

**NOTE:** You need to have the *Resources Assign* navigation permission to see the *Assign* button.

The Work Dashboard displays the *Assign Resource* dialog, which allows you to specify which resource you want to request:



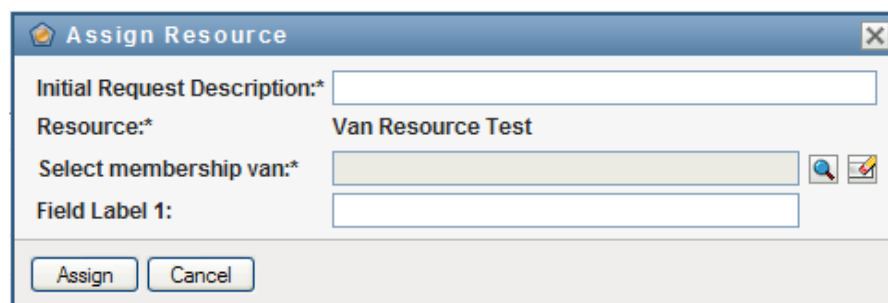
The dialog box "Assign Resource" contains the following fields:

- Initial Request Description:\*
- Resource:\*

Buttons: Assign, Cancel

- 2 Type text that describes the assignment in the *Initial Request Description* field.
- 3 Click the Object Selector to search for a resource to assign.
- 4 In the Object Selector, enter a search string and click Search.
- 5 Select the resource you want.

The Add Resource dialog now shows the selected resource, as well as any other fields defined in the resource request form:

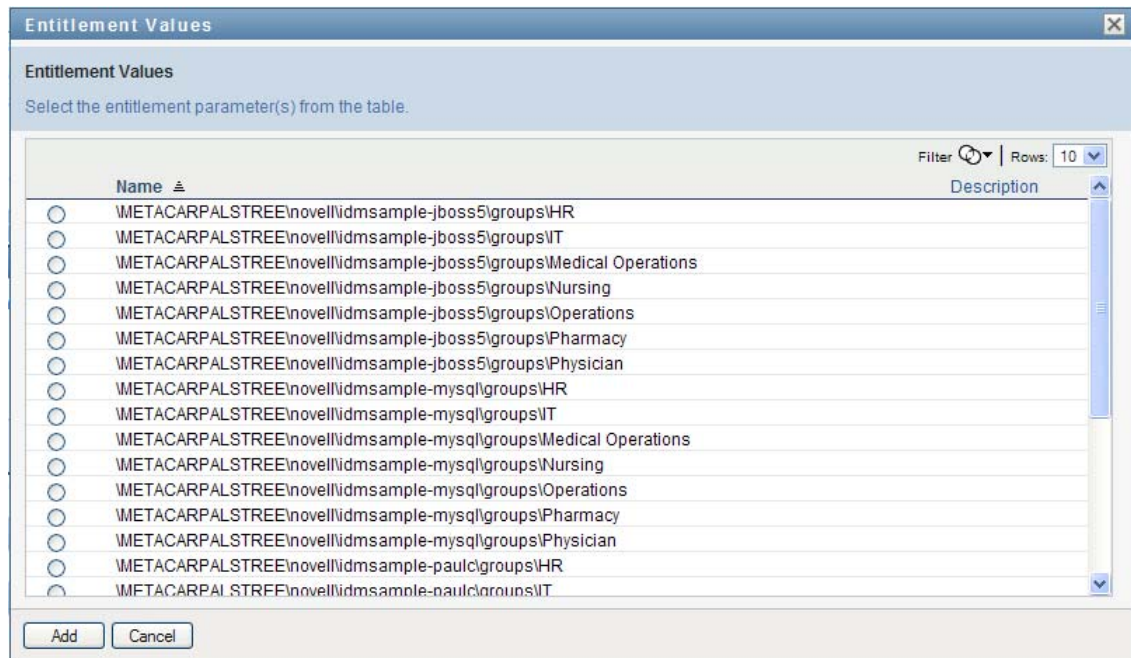


The dialog box "Assign Resource" now shows the selected resource "Van Resource Test" in the Resource:\* field. Additional fields are visible:

- Initial Request Description:\*
- Resource:\*
- Select membership van:\*
- Field Label 1:

Buttons: Assign, Cancel

- 6 If the resource requires an entitlement parameter value, you need to use the Object Selector to select the value you want to use for this resource assignment, as shown below:



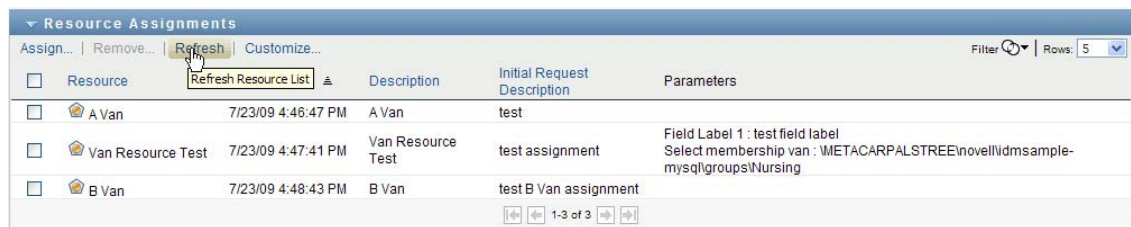
Select the parameter you want to use, and click *Add*.

- 7 If there are additional custom fields on the form, fill these out as well.
- 8 Click *Submit* to make your resource request.

## 10.2.3 Refreshing the Resource Assignment List

To refresh the resource assignment list:

- 1 Click *Refresh*.



## 10.2.4 Removing a Resource Assignment

To remove a resource assignment:

- 1 Select a previously defined resource assignment, and click *Remove*:

| Resource Assignments                           |                   |                    |                   |                             |   |
|--|-------------------|--------------------|-------------------|-----------------------------|---|
| Assign...   Remove...   Refresh   Customize... |                   |                    |                   |                             |   |
| <input type="checkbox"/>                       | Resource          | Request Date       | Description       | Initial Request Description | Parameters  |
| <input checked="" type="checkbox"/>            | A Van             | 7/23/09 4:46:47 PM | A Van             | test                        |   |
| <input type="checkbox"/>                       | Van Resource Test | 7/23/09 4:47:41 PM | Van Resource Test | test assignment             | Field Label 1 : test field label<br>Select membership van : METACARPALSTREE\novell\ldmsample-mysql\groups\Nursing |
| <input type="checkbox"/>                       | B Van             | 7/23/09 4:48:43 PM | B Van             | test B Van assignment       |   |

**NOTE:** You need to have the *Resources Remove* navigation permission to see the *Remove* button.

## 10.2.5 Customizing the Resource Assignment List Display

The *Resource Assignments* section of the dashboard allows you to select and deselect columns, and also reorder columns within the task list display. The column selection and order are controlled by settings within the *Customize Resource Assignment Display* dialog. When you modify the column list or reorder the columns, your customizations are saved in the Identity Vault along with your other user preferences.

To customize the display of columns:

- 1 Click *Customize* in the *Resource Assignments* section of the dashboard:

| Resource Assignments                           |                   |                    |                   |                             |   |
|--|-------------------|--------------------|-------------------|-----------------------------|---|
| Assign...   Remove...   Refresh   Customize... |                   |                    |                   |                             |   |
| <input type="checkbox"/>                       | Resource          | Request Date       | Description       | Initial Request Description | Parameters  |
| <input checked="" type="checkbox"/>            | A Van             | 7/23/09 4:46:47 PM | A Van             | test                        |   |
| <input type="checkbox"/>                       | Van Resource Test | 7/23/09 4:47:41 PM | Van Resource Test | test assignment             | Field Label 1 : test field label<br>Select membership van : METACARPALSTREE\novell\ldmsample-mysql\groups\Nursing |
| <input type="checkbox"/>                       | B Van             | 7/23/09 4:48:43 PM | B Van             | test B Van assignment       |   |

The *User Application* displays the list of columns currently selected for the display, and a list of additional columns that are available for selection.

**Customize Resource Assignment Display** [X]

|   |   |  |
|---|---|--|
| <p><b>Available Columns</b></p> <div style="border: 1px solid gray; padding: 5px; margin-bottom: 5px;">Status</div> | ↔ | <p><b>Selected Columns</b></p> <div style="border: 1px solid gray; padding: 5px; margin-bottom: 5px;">Resource *</div> <div style="border: 1px solid gray; padding: 5px; margin-bottom: 5px;">Request Date</div> <div style="border: 1px solid gray; padding: 5px; margin-bottom: 5px;">Description</div> <div style="border: 1px solid gray; padding: 5px; margin-bottom: 5px;">Initial Request Description</div> <div style="border: 1px solid gray; padding: 5px; margin-bottom: 5px;">Parameters</div> |
| <div style="display: flex; justify-content: space-around;"> <span>Save Changes</span> <span>Cancel</span> </div>    |   |  |

- 2 To include an additional column in the display, select the column in the *Available Columns* list box, and drag it to the *Selected Columns* list box.

To select multiple columns in the list, hold down the **Ctrl** key and select the columns. To select a range of columns that appear together in the list, hold down the **Shift** key and select the columns.

You can reorder the columns in the display by moving them up or down in the *Selected Columns* list box.

- 3 To remove a column from the display, select the column in the *Selected Columns* list box, and drag it to the *Available Columns* list box.

The *Resource Name* column is a mandatory column and cannot be removed from the task list display.

- 4 To save your changes, click *Save Changes*.

## 10.2.6 Printing the List of Resource Assignments

The *Resource Assignments* section of the dashboard allows you to print the list of resource assignments displayed on the page. What you see on the screen is essentially the same as what you see when you print a resource assignments list, except that the printout includes only the text on the screen. Any images shown in the *Assigned To* column or the *Status* column will not appear on the printout.

To print resource assignments, you need to have the *Resource Assignments Print* navigation permission within the *Work Dashboard* navigation area.

To print the list of resource assignments:

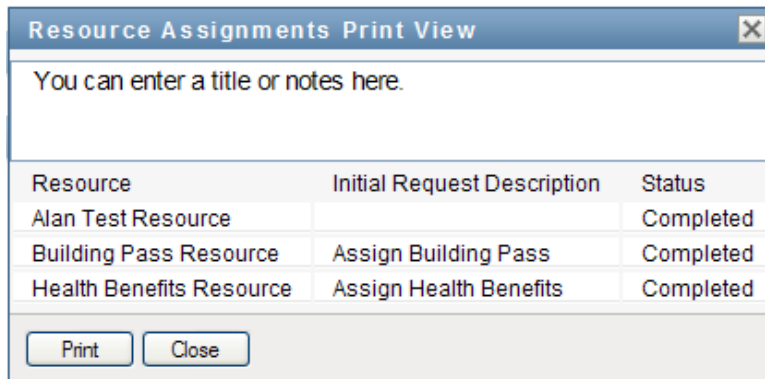
- 1 Click *Print View* in the *Resource Assignments* section of the dashboard:



The screenshot shows the 'Resource Assignments' section of a dashboard. At the top, there are navigation buttons: 'Assign...', 'Remove...', 'Refresh', 'Customize...', and 'Print View...'. A tooltip 'Open a printable version' is visible over the 'Print View...' button. Below the buttons is a table with three columns: 'Resource', 'Initial Request Description', and 'Status'. The table contains three rows of data. At the bottom right of the table, there are pagination controls showing '1-3 of 3'.

| Resource                 | Initial Request Description | Status    |
|--------------------------|-----------------------------|-----------|
| Alan Test Resource       |                             | Completed |
| Building Pass Resource   | Assign Building Pass        | Completed |
| Health Benefits Resource | Assign Health Benefits      | Completed |

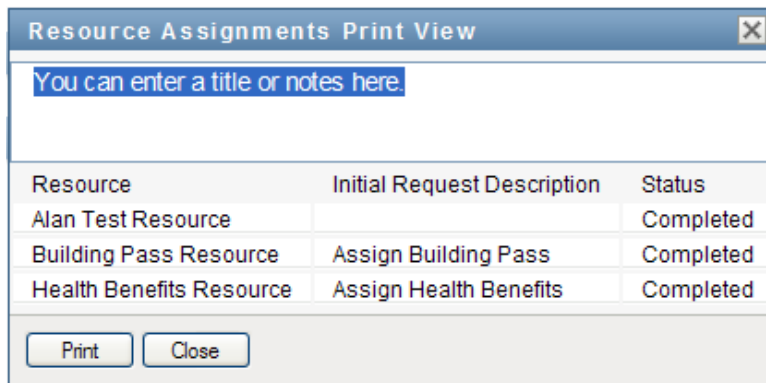
The User Application displays a printable version of the resource assignment list in a separate window:



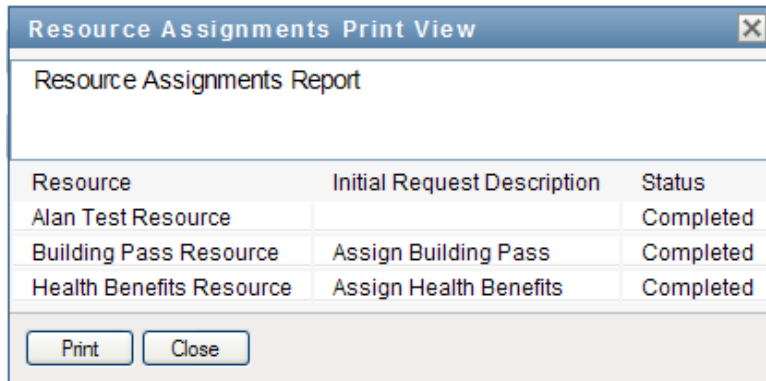
The screenshot shows a window titled 'Resource Assignments Print View'. At the top, there is a text box with the placeholder text 'You can enter a title or notes here.'. Below the text box is a table with three columns: 'Resource', 'Initial Request Description', and 'Status'. The table contains three rows of data. At the bottom of the window, there are two buttons: 'Print' and 'Close'.

| Resource                 | Initial Request Description | Status    |
|--------------------------|-----------------------------|-----------|
| Alan Test Resource       |                             | Completed |
| Building Pass Resource   | Assign Building Pass        | Completed |
| Health Benefits Resource | Assign Health Benefits      | Completed |

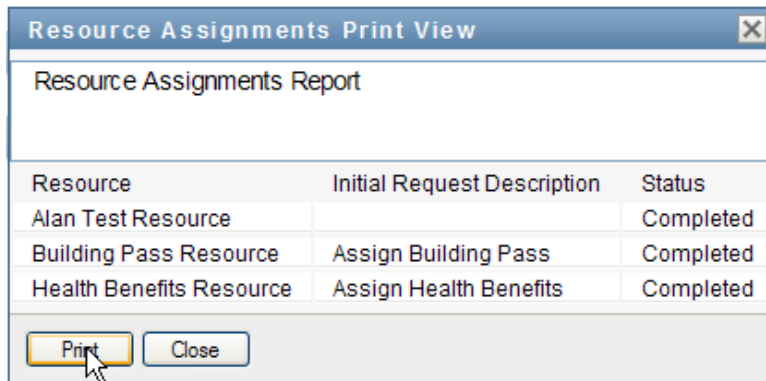
- 2 Select the text in the text box at the top of the print view:



Type a title or add notes to the text box:

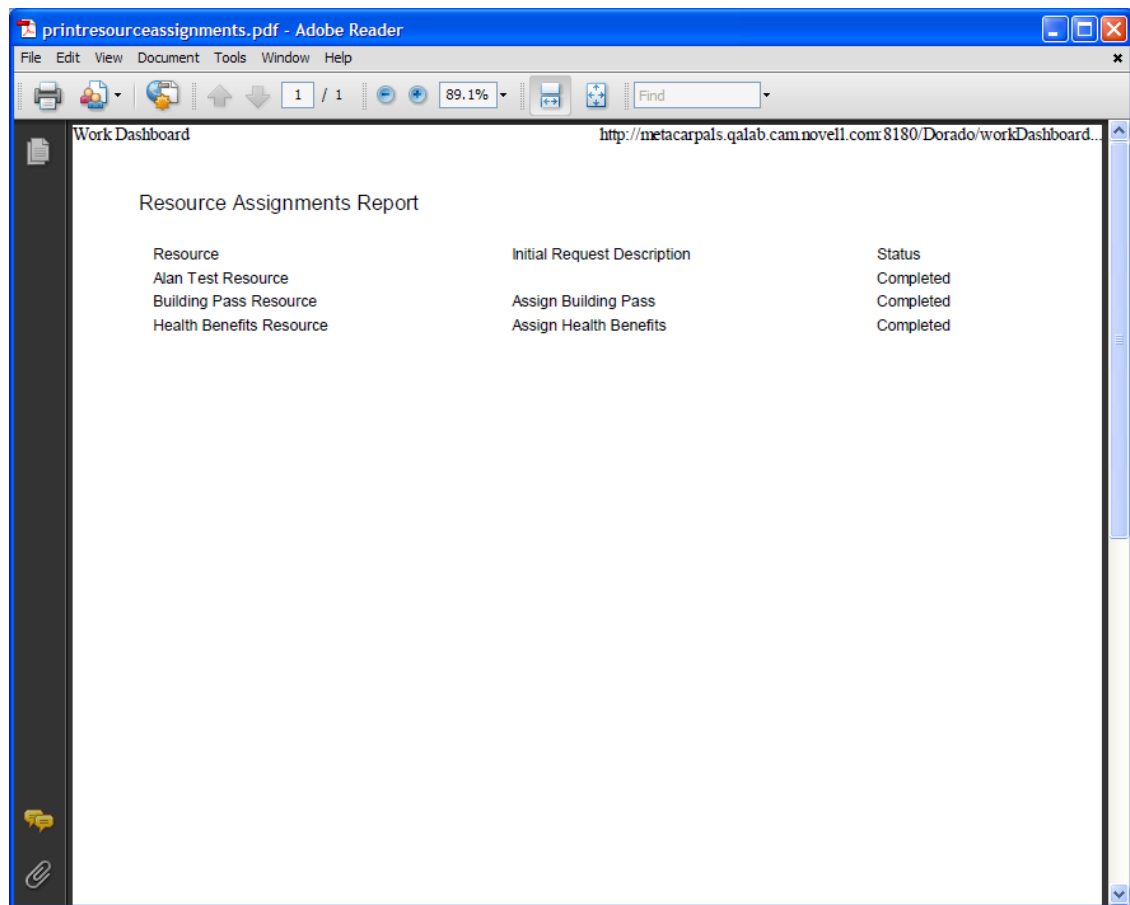


3 Click *Print*:



You can print directly to a printer, or print to a PDF file.

Here is a sample PDF showing what the printout looks like:



All rows shown on the screen will be printed, unless the number of rows displayed reaches the limit defined in the *Maximum number of results returned from a query* setting, which is specified by a Configuration Administrator on the *Administration* tab. If you reach this limit, you should see a confirmation dialog that allows you to specify whether you want to continue. Click *OK* if you want to include all of the rows shown on the screen in the printout. This message is displayed only once for each user session.

## 10.3 Working with Roles

The *Role Assignments* action allows you to see what role assignments you have, and also make requests for additional role assignments.

The Role Administrator and Role Manager have the ability to view role assignments for other users, as described below:

- ◆ When nothing is selected in the *Manage* control, the role assignment list shows the current user's assignments. These role assignments include those for which he is either recipient or addressee, as well as roles for which the recipient or addressee is a group, container, or role to which the current user belongs. The user can do anything with his own role assignments, since no rights are required to work with one's own roles.
- ◆ When a user is selected in the *Manage* control, the list shows direct and indirect role assignments that have the selected user as recipient. Before selecting a user, the Team Manager must select a team.

- ◆ When a group is selected, the list shows roles assigned directly to the selected group. The list of role assignments does not contain roles assigned to a user within the selected group or container. In addition, it does not include roles that are related to those roles assigned directly to the group.
- ◆ When a role is selected, the *Role Assignments* section displays a message indicating that role assignments are not shown. To see the role relationships for a particular role, you need to look at the *Roles* tab.
- ◆ When a container is chosen, the list shows roles assigned directly to the selected container. The list of role assignments does not contain roles assigned to a user within the selected container. In addition, it does not include roles that are related to those roles assigned directly to the container.

A Team Manager for the Role domain has the ability to manage role assignments for team members. Before selecting a team member, the Team Manager must select a team.

Role relationships are not shown in the Role Assignments section. To see the role relationships for a particular role, you need to look at the Role Relationships tab, which is available from the Roles Catalog action on the Roles tab.

**Proxy Mode** The *Role Assignments* action is not available in proxy mode.

## 10.3.1 Viewing Your Role Assignments

To see the role assignments for yourself, or for a user, group, or container selected in the *Manage* control:

- 1 Click *Role Assignments* in the group of actions on the Work Dashboard.

The list of roles is displayed. If you are not in managed mode, the role assignments shown are those for which you are the recipient.

| <input type="checkbox"/> | Role                          | Assignments                              | Source                | Effective Date | Expiration Date |
|--------------------------|-------------------------------|--|-----------------------|----------------|-----------------|
| <input type="checkbox"/> | Role Module Administrator     | Application Administrator Of Sample Data | User Assigned to Role | May 11, 2009   |                 |
| <input type="checkbox"/> | Resource Module Administrator | Application Administrator Of Sample Data | User Assigned to Role | May 11, 2009   |                 |
| <input type="checkbox"/> | Provisioning Administrator    | Application Administrator Of Sample Data | User Assigned to Role | May 11, 2009   |                 |
| <input type="checkbox"/> | Compliance Administrator      | Application Administrator Of Sample Data | User Assigned to Role | May 11, 2009   |                 |

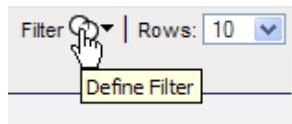
If you are in manage mode, the role assignments shown are those for which the selected user, group, or container is the recipient.

A role can be assigned to a group or container, in which case the role will be assigned indirectly to all users within the group or container. The *Role Assignments* list on the dashboard shows direct assignments for users, as well as indirect assignments for groups and containers. In addition, if a user is assigned directly to a parent role, the list includes this assignment, as well as assignments to any child roles related to this parent role. For example, if a level 30 role (parent) has a role relationship added to a level 20 role (child), and a user is directly assigned to the parent role, the *Role Assignments* display shows both assignments (parent and child). If you look at the child role in the *Role Catalog*, you will see the relationship between the roles on the *Role Relationships* tab, but not on the *Role Assignments* tab.

### Filtering the Role Assignment List

- 1 Click the Define Filter button in the upper right corner of the *Role Assignments* display.





- 2 Specify a filter string for the initial request description or for the role name, or narrow the search by selecting a type of assignment (*User*, *Group*, *Container*, or *Role*) and a set of identities that are of the selected assignment type. Alternatively, you can narrow the search by selecting a source type for the role assignment (*User Assigned to Role*, *Group Assigned to Role*, *Container Assigned to Role*, or *Role Associated with Role*).

---

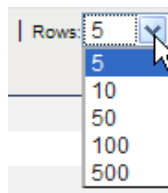
**NOTE:** When selecting *Group* as the type of assignment to use for filtering, the filter title will display a CN, while the results display another related field.

---

- 3 Click *Filter* to apply your selection criteria.
- 4 To remove the current filter, click *Clear*.

## Setting the Maximum Number of Rows on a Page

- 1 Click on the *Rows* dropdown list and select the number of rows you want to be displayed on each page:



## Scrolling within the Role Assignment List

- 1 To scroll to another page in the role assignment list, click on the *Next*, *Previous*, *First* or *Last* button at the bottom of the list.

## Sorting the Role Assignment List

To sort the role assignment list:

- 1 Click the header for the column you want to sort on.  
The pyramid-shaped sort indicator shows you which column is the new primary sort column. When the sort is ascending, the sort indicator is shown in its normal, upright position.  
When the sort is descending, the sort indicator is upside down.  
The initial sort column is determined by the RBPM Configuration Administrator.

If you override the initial sort column, your sort column is added to the list of required columns. Required columns are indicated with an asterisk (\*).

When you modify the sort order for the role assignment list, your preference is saved in the Identity Vault along with your other user preferences.

### 10.3.2 Requesting a Role

To make a role assignment request:

- 1 Click the *Assign* button at the top of the *Role Assignments* section of the page.

| Assign Role              | Assigned To        | Source                                    | Effective Date        | Expiration Date | Initial Request Description           | Status    |
|--------------------------|--------------------|---|-----------------------|-----------------|---------------------------------------|-----------|
| <input type="checkbox"/> | Role Administrator | Roles Module Administrator Of Sample Data | User Assigned to Role | Jul 24, 2009    | Role administrator assignment request | Completed |

---

**NOTE:** You need to have the *Roles Assign* navigation permission to see the *Assign* button.

---

The Work Dashboard displays the *Assign Role* dialog, which allows you to specify which role you want to request:

**Assign Role**

Initial Request Description:\*

Role:\*

Effective Date:

(mm/dd/yyyy hh:mm:ss a)

If no date is entered, effective date is immediate.

Expiration Date:  No Expiration  Specify Expiration

- 2 Fill in the fields on the *Add Role Assignment* dialog:
  - 2a Provide text describing the reason for the request in the *Initial Request Description* field.
  - 2b In the Object Selector, enter a search string and click Search.  
Select the role you want to assign.  
Click the Object Selector to search for a role to assign.
  - 2c Specify the start date for the role assignment in the *Effective Date* field.
  - 2d Specify the expiration date for the role assignment in the *Expiration Date* field.
- 3 Click *Assign* to submit your request.

### 10.3.3 Refreshing the Role Assignment List

To refresh the role assignment list:

- 1 Click *Refresh*.

The screenshot shows the 'Role Assignments' table with the following data:

| Role                          | Assignments                              | Source                | Effective Date | Expiration Date |
|-------------------------------|--|-----------------------|----------------|-----------------|
| Role Module Administrator     | Application Administrator Of Sample Data | User Assigned to Role | May 11, 2009   |                 |
| Compliance Administrator      | Application Administrator Of Sample Data | User Assigned to Role | May 11, 2009   |                 |
| Provisioning Administrator    | Application Administrator Of Sample Data | User Assigned to Role | May 11, 2009   |                 |
| Resource Module Administrator | Application Administrator Of Sample Data | User Assigned to Role | May 11, 2009   |                 |

### 10.3.4 Removing a Role Assignment

To remove a role assignment:

- 1 Select a previously defined role assignment, and click *Remove*:

The screenshot shows the 'Role Assignments' table with the following data:

| Role   | Assignments                              | Source                | Effective Date | Expiration Date |
|--|--|-----------------------|----------------|-----------------|
| Role Module Administrator                      | Application Administrator Of Sample Data | User Assigned to Role | May 11, 2009   |                 |
| Compliance Administrator                       | Application Administrator Of Sample Data | User Assigned to Role | May 11, 2009   |                 |
| Provisioning Administrator                     | Application Administrator Of Sample Data | User Assigned to Role | May 11, 2009   |                 |
| Resource Module Administrator                  | Application Administrator Of Sample Data | User Assigned to Role | May 11, 2009   |                 |
| <input checked="" type="checkbox"/> Nurse      | Application Administrator Of Sample Data | User Assigned to Role | May 12, 2009   |                 |
| <input type="checkbox"/> Administer Drugs      | Nurse                                    | Role Relationship     | May 12, 2009   |                 |
| <input type="checkbox"/> Perform Medical Tests | Nurse                                    | Role Relationship     | May 12, 2009   |                 |

---

**NOTE:** You need to have the *Roles Remove* navigation permission to see the *Remove* button.

---

### 10.3.5 Customizing the Role Assignment List Display

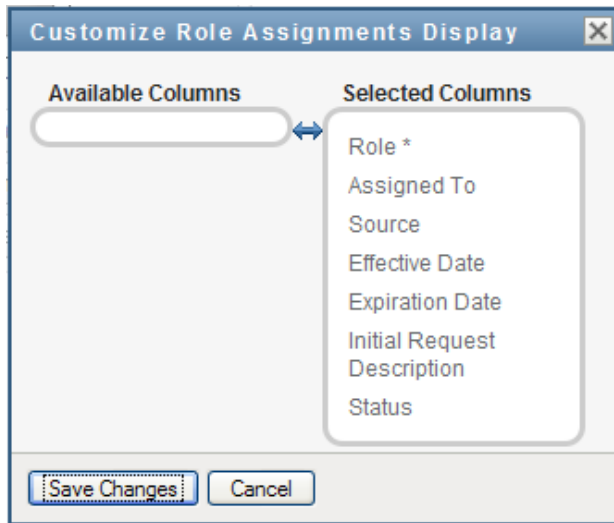
The *Role Assignments* section of the dashboard allows you to select and deselect columns, and also reorder columns within the task list display. The column selection and order are controlled by settings within the *Customize Role Assignment Display* dialog. When you modify the column list or reorder the columns, your customizations are saved in the Identity Vault along with your other user preferences.

To customize the display of columns:

- 1 Click *Customize* in the Role Assignments section of the dashboard:



The User Application displays the list of columns currently selected for the display, and a list of additional columns that are available for selection.



- 2 To include an additional column in the display, select the column in the *Available Columns* list box, and drag it to the *Selected Columns* list box.

To select multiple columns in the list, hold down the Ctrl key and select the columns. To select a range of columns that appear together in the list, hold down the Shift key and select the columns.

You can reorder the columns in the display by moving them up or down in the *Selected Columns* list box.

- 3 To remove a column from the display, select the column in the *Selected Columns* list box, and drag it to the *Available Columns* list box.

The *Role* column is a mandatory column and cannot be removed from the task list display.

- 4 To save your changes, click *Save Changes*.

## 10.3.6 Printing the List of Role Assignments

The *Role Assignments* section of the dashboard allows you to print the list of role assignments displayed on the page. What you see on the screen is essentially the same as what you see when you print a role assignments list, except that the printout includes only the text on the screen. Any images shown in the *Assigned To* column or the *Status* column will not appear on the printout.

To print role assignments, you need to have the *Role Assignments Print* navigation permission within the *Work Dashboard* navigation area.

To print the list of role assignments:

- 1 Click *Print View* in the *Role Assignments* section of the dashboard:

| Role                       | Expiration Date | Assigned To                      | Effective Date | Source                | Status    | Initial Request Description                    |
|----------------------------|-----------------|----------------------------------|----------------|-----------------------|-----------|--|
| Role Administrator         |                 | User: Application Of Sample Data | Aug 26, 2009   | User Assigned to Role | Completed | Role administrator assignment request.         |
| Role Administrator         |                 | User: Application Of Sample Data | Mar 23, 2010   | User Assigned to Role | Completed | Role administrator assignment request.         |
| Resource Administrator     |                 | User: Application Of Sample Data | Sep 23, 2009   | User Assigned to Role | Completed | Resource administrator assignment request.     |
| Provisioning Manager       |                 | User: Application Of Sample Data | Aug 26, 2009   | User Assigned to Role | Completed | Provisioning manager assignment request.       |
| Provisioning Manager       |                 | User: Application Of Sample Data | Mar 23, 2010   | User Assigned to Role | Completed | Provisioning manager assignment request.       |
| Provisioning Administrator |                 | User: Application Of Sample Data | Aug 26, 2009   | User Assigned to Role | Completed | Provisioning administrator assignment request. |
| Provisioning Administrator |                 | User: Application Of Sample Data | Mar 23, 2010   | User Assigned to Role | Completed | Provisioning administrator assignment request. |
| Compliance Administrator   |                 | User: Application Of Sample Data | Aug 26, 2009   | User Assigned to Role | Completed | Compliance administrator assignment request.   |
| Compliance Administrator   |                 | User: Application Of Sample Data | Mar 23, 2010   | User Assigned to Role | Completed | Compliance administrator assignment request.   |
| AmberTestRole              |                 | User: Application Of Sample Data | Sep 1, 2009    | User Assigned to Role | Completed | AmberTestRole assignment request.              |

The User Application displays a printable version of the role assignment list in a separate window:

You can enter a title or notes here.

| Role                       | Expiration Date | Assigned To                      | Effective Date | Source                | Status    | Initial Request Description                    |
|----------------------------|-----------------|----------------------------------|----------------|-----------------------|-----------|--|
| Role Administrator         |                 | User: Application Of Sample Data | Aug 26, 2009   | User Assigned to Role | Completed | Role administrator assignment request.         |
| Role Administrator         |                 | User: Application Of Sample Data | Mar 23, 2010   | User Assigned to Role | Completed | Role administrator assignment request.         |
| Resource Administrator     |                 | User: Application Of Sample Data | Sep 23, 2009   | User Assigned to Role | Completed | Resource administrator assignment request.     |
| Provisioning Manager       |                 | User: Application Of Sample Data | Aug 26, 2009   | User Assigned to Role | Completed | Provisioning manager assignment request.       |
| Provisioning Manager       |                 | User: Application Of Sample Data | Mar 23, 2010   | User Assigned to Role | Completed | Provisioning manager assignment request.       |
| Provisioning Administrator |                 | User: Application Of Sample Data | Aug 26, 2009   | User Assigned to Role | Completed | Provisioning administrator assignment request. |
| Provisioning Administrator |                 | User: Application Of Sample Data | Mar 23, 2010   | User Assigned to Role | Completed | Provisioning administrator assignment request. |
| Compliance Administrator   |                 | User: Application Of Sample Data | Aug 26, 2009   | User Assigned to Role | Completed | Compliance administrator assignment request.   |
| Compliance Administrator   |                 | User: Application Of Sample Data | Mar 23, 2010   | User Assigned to Role | Completed | Compliance administrator assignment request.   |
| AmberTestRole              |                 | User: Application Of Sample Data | Sep 1, 2009    | User Assigned to Role | Completed | AmberTestRole assignment request.              |

Print Close

- 2 Select the text in the text box at the top of the print view:

You can enter a title or notes here.

| Role                       | Expiration Date | Assigned To                      | Effective Date | Source                | Status    | Initial Request Description                    |
|----------------------------|-----------------|----------------------------------|----------------|-----------------------|-----------|--|
| Role Administrator         |                 | User: Application Of Sample Data | Aug 26, 2009   | User Assigned to Role | Completed | Role administrator assignment request.         |
| Role Administrator         |                 | User: Application Of Sample Data | Mar 23, 2010   | User Assigned to Role | Completed | Role administrator assignment request.         |
| Resource Administrator     |                 | User: Application Of Sample Data | Sep 23, 2009   | User Assigned to Role | Completed | Resource administrator assignment request.     |
| Provisioning Manager       |                 | User: Application Of Sample Data | Aug 26, 2009   | User Assigned to Role | Completed | Provisioning manager assignment request.       |
| Provisioning Manager       |                 | User: Application Of Sample Data | Mar 23, 2010   | User Assigned to Role | Completed | Provisioning manager assignment request.       |
| Provisioning Administrator |                 | User: Application Of Sample Data | Aug 26, 2009   | User Assigned to Role | Completed | Provisioning administrator assignment request. |
| Provisioning Administrator |                 | User: Application Of Sample Data | Mar 23, 2010   | User Assigned to Role | Completed | Provisioning administrator assignment request. |
| Compliance Administrator   |                 | User: Application Of Sample Data | Aug 26, 2009   | User Assigned to Role | Completed | Compliance administrator assignment request.   |
| Compliance Administrator   |                 | User: Application Of Sample Data | Mar 23, 2010   | User Assigned to Role | Completed | Compliance administrator assignment request.   |
| AmberTestRole              |                 | User: Application Of Sample Data | Sep 1, 2009    | User Assigned to Role | Completed | AmberTestRole assignment request.              |

Print Close

Type a title or add notes to the text box:

| Role Assignments Print View |                 |                                  |                |                       |           |  |
|-----------------------------|-----------------|----------------------------------|----------------|-----------------------|-----------|--|
| Role Assignments Report     |                 |                                  |                |                       |           |  |
| Role                        | Expiration Date | Assigned To                      | Effective Date | Source                | Status    | Initial Request Description                    |
| Role Administrator          |                 | User: Application Of Sample Data | Aug 26, 2009   | User Assigned to Role | Completed | Role administrator assignment request.         |
| Role Administrator          |                 | User: Application Of Sample Data | Mar 23, 2010   | User Assigned to Role | Completed | Role administrator assignment request.         |
| Resource Administrator      |                 | User: Application Of Sample Data | Sep 23, 2009   | User Assigned to Role | Completed | Resource administrator assignment request.     |
| Provisioning Manager        |                 | User: Application Of Sample Data | Aug 26, 2009   | User Assigned to Role | Completed | Provisioning manager assignment request.       |
| Provisioning Manager        |                 | User: Application Of Sample Data | Mar 23, 2010   | User Assigned to Role | Completed | Provisioning manager assignment request.       |
| Provisioning Administrator  |                 | User: Application Of Sample Data | Aug 26, 2009   | User Assigned to Role | Completed | Provisioning administrator assignment request. |
| Provisioning Administrator  |                 | User: Application Of Sample Data | Mar 23, 2010   | User Assigned to Role | Completed | Provisioning administrator assignment request. |
| Compliance Administrator    |                 | User: Application Of Sample Data | Aug 26, 2009   | User Assigned to Role | Completed | Compliance administrator assignment request.   |
| Compliance Administrator    |                 | User: Application Of Sample Data | Mar 23, 2010   | User Assigned to Role | Completed | Compliance administrator assignment request.   |
| AmberTestRole               |                 | User: Application Of Sample Data | Sep 1, 2009    | User Assigned to Role | Completed | ...  |

Print Close

### 3 Click *Print*:

| Role Assignments Print View |                 |                                  |                |                       |           |  |
|-----------------------------|-----------------|----------------------------------|----------------|-----------------------|-----------|--|
| Role Assignments Report     |                 |                                  |                |                       |           |  |
| Role                        | Expiration Date | Assigned To                      | Effective Date | Source                | Status    | Initial Request Description                    |
| Role Administrator          |                 | User: Application Of Sample Data | Aug 26, 2009   | User Assigned to Role | Completed | Role administrator assignment request.         |
| Role Administrator          |                 | User: Application Of Sample Data | Mar 23, 2010   | User Assigned to Role | Completed | Role administrator assignment request.         |
| Resource Administrator      |                 | User: Application Of Sample Data | Sep 23, 2009   | User Assigned to Role | Completed | Resource administrator assignment request.     |
| Provisioning Manager        |                 | User: Application Of Sample Data | Aug 26, 2009   | User Assigned to Role | Completed | Provisioning manager assignment request.       |
| Provisioning Manager        |                 | User: Application Of Sample Data | Mar 23, 2010   | User Assigned to Role | Completed | Provisioning manager assignment request.       |
| Provisioning Administrator  |                 | User: Application Of Sample Data | Aug 26, 2009   | User Assigned to Role | Completed | Provisioning administrator assignment request. |
| Provisioning Administrator  |                 | User: Application Of Sample Data | Mar 23, 2010   | User Assigned to Role | Completed | Provisioning administrator assignment request. |
| Compliance Administrator    |                 | User: Application Of Sample Data | Aug 26, 2009   | User Assigned to Role | Completed | Compliance administrator assignment request.   |
| Compliance Administrator    |                 | User: Application Of Sample Data | Mar 23, 2010   | User Assigned to Role | Completed | Compliance administrator assignment request.   |
| AmberTestRole               |                 | User: Application Of Sample Data | Sep 1, 2009    | User Assigned to Role | Completed | ...  |

Print Close

You can print directly to a printer, or print to a PDF file.

Here is a sample PDF showing what the printout looks like:

The screenshot shows a PDF document titled 'printroleassignments.pdf' in Adobe Reader. The document content is a 'Role Assignments Report' from a web application. The report is a table with the following columns: Role, Expiration Date, Assigned To, Effective Date, Source, Status, and Initial Request Description. The table contains 11 rows of data, all with a status of 'Completed'. The roles listed include Role Administrator, Resource Administrator, Provisioning Manager, Provisioning Administrator, Compliance Administrator, and AmberTestRole.

| Role                       | Expiration Date | Assigned To                      | Effective Date | Source                | Status    | Initial Request Description                    |
|----------------------------|-----------------|----------------------------------|----------------|-----------------------|-----------|--|
| Role Administrator         |                 | User: Application Of Sample Data | Aug 26, 2009   | User Assigned to Role | Completed | Role administrator assignment request.         |
| Role Administrator         |                 | User: Application Of Sample Data | Mar 23, 2010   | User Assigned to Role | Completed | Role administrator assignment request.         |
| Resource Administrator     |                 | User: Application Of Sample Data | Sep 23, 2009   | User Assigned to Role | Completed | Resource administrator assignment request.     |
| Provisioning Manager       |                 | User: Application Of Sample Data | Aug 26, 2009   | User Assigned to Role | Completed | Provisioning manager assignment request.       |
| Provisioning Manager       |                 | User: Application Of Sample Data | Mar 23, 2010   | User Assigned to Role | Completed | Provisioning manager assignment request.       |
| Provisioning Administrator |                 | User: Application Of Sample Data | Aug 26, 2009   | User Assigned to Role | Completed | Provisioning administrator assignment request. |
| Provisioning Administrator |                 | User: Application Of Sample Data | Mar 23, 2010   | User Assigned to Role | Completed | Provisioning administrator assignment request. |
| Compliance Administrator   |                 | User: Application Of Sample Data | Aug 26, 2009   | User Assigned to Role | Completed | Compliance administrator assignment request.   |
| Compliance Administrator   |                 | User: Application Of Sample Data | Mar 23, 2010   | User Assigned to Role | Completed | Compliance administrator assignment request.   |
| AmberTestRole              |                 | User: Application Of Sample Data | Sep 1, 2009    | User Assigned to Role | Completed | ...  |

All rows shown on the screen will be printed, unless the number of rows displayed reaches the limit defined in the *Maximum number of results returned from a query* setting, which is specified by a Configuration Administrator on the *Administration* tab. If you reach this limit, you should see a confirmation dialog that allows you to specify whether you want to continue. Click *OK* if you want to include all of the rows shown on the screen in the printout. This message is displayed only once for each user session.

## 10.4 Viewing Your Request Status

The *Request Status* action allows you to see the status of the requests you've made. It lets you see the current state of each request. In addition, it gives you the option to retract a request that is still in process if you have changed your mind and do not need to have the request fulfilled.

The *Request Status* action includes process (provisioning) requests, role requests, and resource requests in a single consolidated list. The list provides a *Type* column that allows you to see the type for each request. The requests appear in a single list, but the list can be sorted or filtered by request type. You can retract requests that are still in a retractable state from the *Request Status* list.

The Domain Administrator and Domain Manager have the ability to view requests for other users, as described below:

- ◆ When nothing is selected in the *Manage* control, the request list shows the current user's requests. These requests include those for which he is either recipient or addressee, as well as requests for which the recipient or addressee is a group, container, or role to which the current user belongs.

- ◆ When a user is selected in the *Manage* control, the list shows requests that have the selected user as recipient.
- ◆ When a group is selected, the list shows requests that have the selected group as recipient.
- ◆ When a role is selected, the list shows requests that have the selected role as recipient.
- ◆ When a container is chosen, the list shows requests that have the selected container as recipient.

When a Domain Administrator or Domain Manager is in manage mode, the *Request Status* list includes only requests associated with the domain specified for the administrator or manager assignment.

A Team Manager has the ability view requests for team members. Before selecting a team member, the Team Manager must select a team.

When a Team Manager is in manage mode, the *Request Status* list includes only requests associated with the domain specified for the selected team configuration.

**Proxy Mode** The *Request Status* action is not available in proxy mode.

## 10.4.1 Viewing the Request List

To see the requests you have made:

- 1 Click *Request Status* in the group of actions on the Work Dashboard.

The list of requests is displayed. If you are not in managed mode, the requests shown are those for which you are the recipient or the requester. If you are in managed mode, the requests shown are those for which the selected user, group, or container is the recipient or the requester.

| Type | Item Requested                      | Request Date           | Status                  | Comments |
|------|-------------------------------------|------------------------|-------------------------|----------|
|      | Nurse                               | 05/25/2009 05:13:58 AM | ✓ Completed             |          |
|      | Add Resource To User - lingresrouce | 05/23/2009 03:44:01 AM | 🔄 Running: Processing   |          |
|      | Role Approval - lingtest            | 05/22/2009 07:16:01 PM | ✗ Terminated: Retracted |          |
|      | lingtest                            | 05/22/2009 07:16:00 PM | ✗ Terminated            |          |
|      | Compliance Administrator            | 05/22/2009 02:52:59 PM | ✓ Completed             |          |
|      | Compliance Administrator            | 05/22/2009 02:52:59 PM | ✓ Completed             |          |
|      | Provisioning Administrator          | 05/22/2009 01:03:51 PM | ✓ Completed             |          |
|      | Compliance Administrator            | 05/22/2009 01:03:51 PM | ✓ Completed             |          |
|      | Role Module Administrator           | 05/22/2009 01:03:51 PM | ✓ Completed             |          |

The list includes active requests, as well as requests that have already been approved or denied. The administrator can control how long workflow results are retained for. By default, the Workflow system retains workflow results for 120 days.

**NOTE:** If you assign a resource to a user that has multiple values from an entitlement, on the *Request Status* tab only one entry will be listed. The first value selected will be the one displayed. On the *Assignments* tab, multiple entries will be listed, and the user will appear as many times as there were values selected.




To see the type of the request, you need to include the *Type* column in the list of columns for the display. When the *Type* column is included, the User Application shows an icon indicating whether the request was a process (provisioning) request, role request, or resource request.






The columns in the Request Status list are described below:








- ◆ The *Item Requested* column provides the name of the role, resource, or process specified for the request.






- ◆ The *Requester* column identifies the user who made the request.
- ◆ The *Recipient* column identifies the user, group, or container that will receive the item requested, if the request is approved. In the case of role relationships, the *Recipient* column shows the name of the role related to the role named in the *Item Requested* column.
- ◆ The *Status* column shows a detailed status for the request as well as an icon that indicates the status summary. The status summary shows the general status of the request and can be selected from the Filter menu to narrow the results when searching for requests with a particular status:

| Status summary icon  | Detailed Status                | Description  |
|--|--------------------------------|--|
|  Running/Processing | New Request                    | <p>Indicates that this is a new request that is currently being processed.</p> <p>A request with this status can be retracted.</p>   |
|  Running/Processing | SoD Approval Start - Pending   | <p>Indicates that the Role Service driver is attempting to restart a separation of duties approval process for the request following an SoD Approval Start - Suspended condition.</p> <p>A request with this status can be retracted.</p>  |
|  Running/Processing | SoD Approval Start - Suspended | <p>Indicates that the Role Service driver is unable to start a separation of duties approval process and the process has been suspended temporarily.</p> <p>When the Role Service driver tries to start a workflow and cannot (for example, when the User Application is down or unreachable), the request transitions to a pending retry state to wait for up to a minute before transitioning to a retry state (SoD Approval Start - Pending state) that triggers the driver to try and start the workflow again. These states prevent requests that don't depend on workflows from being backed up behind requests that are blocked by a workflow that can't be started.</p> <p>If a request shows this status for an extended period of time, make sure the User Application is running. If it is running, check the connection parameters given to the Role Service driver to be sure they are correct.</p> <p>A request with this status can be retracted.</p> |

| Status summary icon  | Detailed Status                  | Description   |
|--|----------------------------------|---|
|  Running/Processing | Approval Start - Pending         | <p>Indicates that the Role Service driver is attempting to restart an approval process for the request following an Approval Start - Suspended condition.</p> <p>A request with this status can be retracted.</p>   |
|  Running/Processing | Approval Start - Suspended       | <p>Indicates that an approval process has been initiated for the request, but the process has been suspended temporarily.</p> <p>When the Role Service driver tries to start a workflow and cannot (for example, when the User Application is down or unreachable), the request transitions to a pending retry state to wait for up to a minute before transitioning to a retry state (Approval Start - Pending state) that triggers the driver to try and start the workflow again. These states prevent requests that don't depend on workflows from being backed up behind requests that are blocked by a workflow that can't be started.</p> <p>If a request shows this status for an extended period of time, make sure the User Application is running. If it is running, check the connection parameters given to the Role Service driver to be sure they are correct.</p> <p>A request with this status can be retracted.</p> |
|  Pending Approval | SoD Exception - Approval Pending | <p>Indicates that a separation of duties approval process has been started and is waiting for one or more approvals.</p> <p>A request with this status can be retracted.</p>  |
|  Pending Approval | Approval Pending                 | <p>Indicates that an approval process has been started for the request and is waiting for one or more approvals.</p> <p>A request with this status can be retracted.</p>  |
|  Approved         | SoD Exception - Approved         | <p>Indicates that a separation of duties exception has been approved for this request.</p> <p>A request with this status can be retracted.</p>  |

| Status summary icon   | Detailed Status        | Description   |
|---|------------------------|---|
|  Approved                | Approved               | <p>Indicates that the request has been approved.</p> <p>A request with this status can be retracted.</p>  |
|  Approved                | Provisioning           | <p>Indicates that the request has been approved (if approvals were required), and the activation time for the assignment has been reached. The Role Service driver is in the process of granting the assignment.</p> <p>You are not permitted to retract a request with this status.</p>  |
|  Pending Activation      | Pending Activation     | <p>Indicates that the request has been approved, but the activation time for the assignment has not yet been reached. The Pending Activation does not have a roll-up category, or summary status icon. This means that you cannot filter the list of requests by the Pending Activation status.</p> <p>A request with this status can be retracted.</p> |
|  Denied                 | SoD Exception - Denied | <p>Indicates that a separation of duties exception has been denied for this request.</p> <p>You are not permitted to retract a request with this status.</p>  |
|  Denied                | Denied                 | <p>Indicates that the request has been denied.</p> <p>You are not permitted to retract a request with this status.</p>  |
|  Completed Provisioned | Provisioned            | <p>Indicates the request has been approved (if approvals were required), and the assignment has been granted.</p> <p>You are not permitted to retract a request with this status.</p>   |
|  Completed Provisioned | Cleanup                | <p>Indicates that the request has been processed and the Role Service driver is in the process removing the internal objects created for the request.</p> <p>You are not permitted to retract a request with this status.</p>   |

| Status summary icon  | Detailed Status    | Description  |
|--|--------------------|--|
|  Terminated | Canceling          | <p>Indicates that the Role Service driver is canceling the request because of a user action.</p> <p>You are not permitted to retract a request with this status.</p>   |
|  Terminated | Canceled           | <p>Indicates that the request has been canceled by a user action.</p> <p>You are not permitted to retract a request with this status.</p>  |
|  Terminated | Provisioning Error | <p>Indicates that an error occurred during the course of provisioning (granting) or deprovisioning (revoking) the assignment.</p> <p>The precise error message for a provisioning error is written to the trace or audit log, if either is active. If a provisioning error occurs, check your trace or audit log to see if the error message indicates a serious problem that must be fixed.</p> <p>You are not permitted to retract a request with this status.</p> |

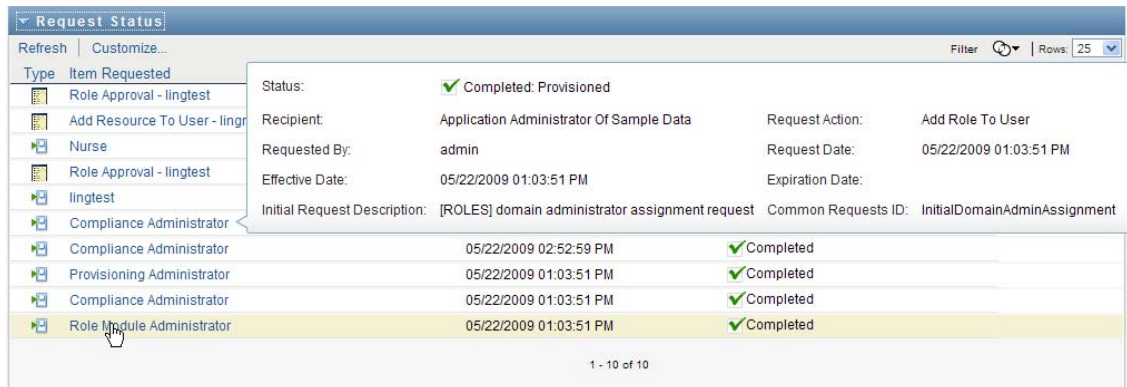
**NOTE:** If the system clock on the server where the Role Service driver resides is not synchronized with the system clock on the server where the User Application is running, the request status might appear to be different on the Request Status and Role Assignments lists. For example, if you request a role assignment that does not require approval, you might see the status as Provisioned in the Request Status section, but the status on the Role Assignments section shows Pending Activation. If you wait for a minute or so, you might then see the status on the Role Assignments section change to Provisioned. To ensure that the status is shown correctly throughout the User Application, check your system clocks to be sure they are synchronized appropriately.

- ◆ The *Request Date* column shows the date when the request was made.

## 10.4.2 Viewing the Summary for a Request

To see the summary information for a request:

- 1 Hover over the request name in the *Item Requested* column.



The screenshot shows a table titled "Request Status" with columns "Type" and "Item Requested". A tooltip is displayed over the "Role Module Administrator" row, showing the following details:

|                              |   |                  |                        |
|------------------------------|---|------------------|------------------------|
| Status:                      | ✓ Completed: Provisioned                        |                  |                        |
| Recipient:                   | Application Administrator Of Sample Data        | Request Action:  | Add Role To User       |
| Requested By:                | admin   | Request Date:    | 05/22/2009 01:03:51 PM |
| Effective Date:              | 05/22/2009 01:03:51 PM                          | Expiration Date: |                        |
| Initial Request Description: | [ROLES] domain administrator assignment request |                  |                        |
| Common Requests ID:          | InitialDomainAdminAssignment                    |                  |                        |

The table below shows the list of requests with their status:

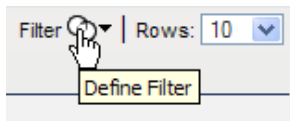
| Type                       | Item Requested | Status      |
|----------------------------|----------------|-------------|
| Compliance Administrator   |                | ✓ Completed |
| Provisioning Administrator |                | ✓ Completed |
| Compliance Administrator   |                | ✓ Completed |
| Role Module Administrator  |                | ✓ Completed |

## 10.4.3 Filtering the Request List

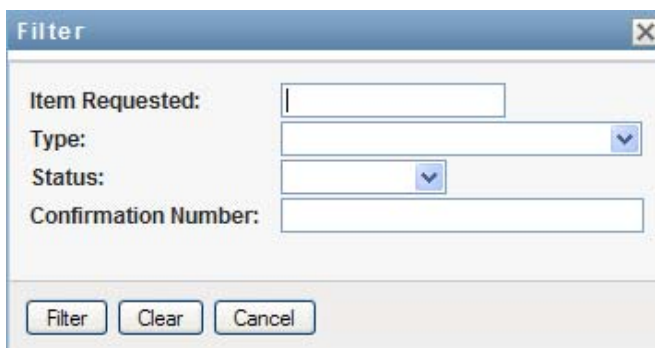
You can apply a filter to the request list to limit the number of rows returned. By filtering the request list, you can find what you're looking for more easily, and also improve performance.

To define a filter for the request list:

- 1 Click the *Define Filter* button.



The Filter dialog displays, showing several fields you can use to specify how you want to filter the data:



The screenshot shows the "Filter" dialog box with the following fields:

- Item Requested:
- Type:
- Status:
- Confirmation Number:

Buttons: Filter, Clear, Cancel

- 2 To narrow the search to requests that have a request name that matches a particular string, type the first characters of the string in the *Item Requested* field.
- 3 To narrow the search to requests of a particular type, select the type in the *Type* dropdown.
- 4 To narrow the search to requests that have a particular status, select the status in the *Status* dropdown.

The status categories available for selection vary depending on which type you've selected in the *Type* dropdown.

- 5 To narrow the search to requests that have a particular confirmation number, type the ID in the *Confirmation Number* field.

The confirmation number is an internal identifier that correlates a set of role assignments that were requested at the same time. Here are some situations in which a set of role assignments will share a confirmation number:

- ♦ A single request assigns multiple roles to a single user.
- ♦ A single request assigns a single role to multiple users. This might occur when a requester assigns a role to a group or container.

When a set of role assignments share a confirmation number, a user can retract each assignment individually. In addition, each role assignment can be approved or denied separately.

- 6 Click *Filter* to perform a new query for requests, using the selection criteria you've specified in the Filter dialog.

When you define a filter for the request list, your filter definition is saved in the Identity Vault along with your other user preferences.

---

**NOTE:** The preferences saved always apply to the user currently logged on to the User Application, regardless of whether a different user has been selected in the *Manage* control.

---

To see what filter points have been defined previously:

- 1 Look at the boxes to the left of the Define Filter icon.

When no filters are defined, the Define Filter icon shows two empty rings, as shown below:



When one or more filter points have been defined, each filter point appears in a separate box, as shown below:



To remove a filter point previously specified in the Filter dialog:

- 1 Click the *Clear this filter* icon (which looks like an X) next to the filter point you want to remove:



To remove all previously defined filters and update the search results to include all requests.

- 1 Click the *Define Filters* button to open the Filter dialog.

- 2 Click the *Reset* button.

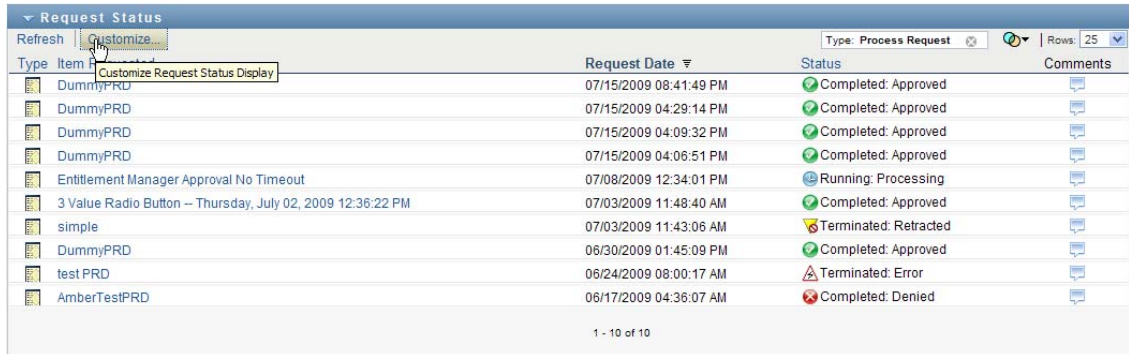
The Filter dialog closes and the request list is updated to include all requests.

## 10.4.4 Customizing the Request Status Columns

The Request Status section of the Work Dashboard page allows you to select and deselect columns, and also reorder columns within the request list display. Any customizations you make to the display are saved for future use.

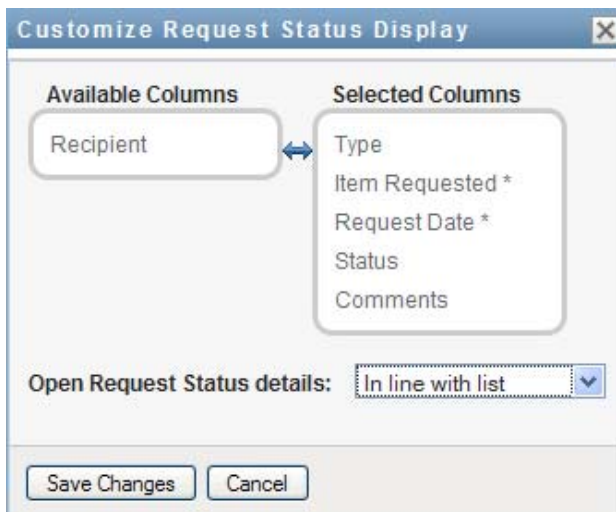
To customize the display of columns in the request status list:

- 1 Click the *Customize* button in the *Request Status* section of the Work Dashboard page.



| Type  | Item                             | Request Date           | Status                | Comments |
|---|----------------------------------|------------------------|-----------------------|----------|
| DummyPRD  | Customize Request Status Display | 07/15/2009 08:41:49 PM | Completed: Approved   |          |
| DummyPRD  |                                  | 07/15/2009 04:29:14 PM | Completed: Approved   |          |
| DummyPRD  |                                  | 07/15/2009 04:09:32 PM | Completed: Approved   |          |
| DummyPRD  |                                  | 07/15/2009 04:06:51 PM | Completed: Approved   |          |
| Entitlement Manager Approval No Timeout                     |                                  | 07/08/2009 12:34:01 PM | Running: Processing   |          |
| 3 Value Radio Button -- Thursday, July 02, 2009 12:36:22 PM |                                  | 07/03/2009 11:48:40 AM | Completed: Approved   |          |
| simple  |                                  | 07/03/2009 11:43:06 AM | Terminated: Retracted |          |
| DummyPRD  |                                  | 06/30/2009 01:45:09 PM | Completed: Approved   |          |
| test PRD  |                                  | 06/24/2009 08:00:17 AM | Terminated: Error     |          |
| AmberTestPRD  |                                  | 06/17/2009 04:36:07 AM | Completed: Denied     |          |

The User Application displays the list of columns currently selected for the display, and a list of additional columns that are available for selection.



- 2 To include an additional column in the display, select the column in the *Available Columns* list box, and drag it to the *Selected Columns* list box.

To select multiple columns in the list, hold down the Ctrl key and select the columns. To select a range of columns that appear together in the list, hold down the Shift key and select the columns.

You can reorder the columns in the display by moving them up or down in the *Selected Columns* list box.

- 3 To remove a column from the display, select the column in the *Selected Columns* list box, and drag it to the *Available Columns* list box.

The *Item Requested* and *Request Date* columns are mandatory columns and cannot be removed from the request list display.

- 4 To save your changes, click *OK*.

## 10.4.5 Controlling the Number of Items Displayed on a Page

To specify the number of items you want displayed on each page:

- 1 Select a number in the *Rows* dropdown list.

When you modify the *Rows* setting, your preference is saved in the Identity Vault along with your other user preferences.

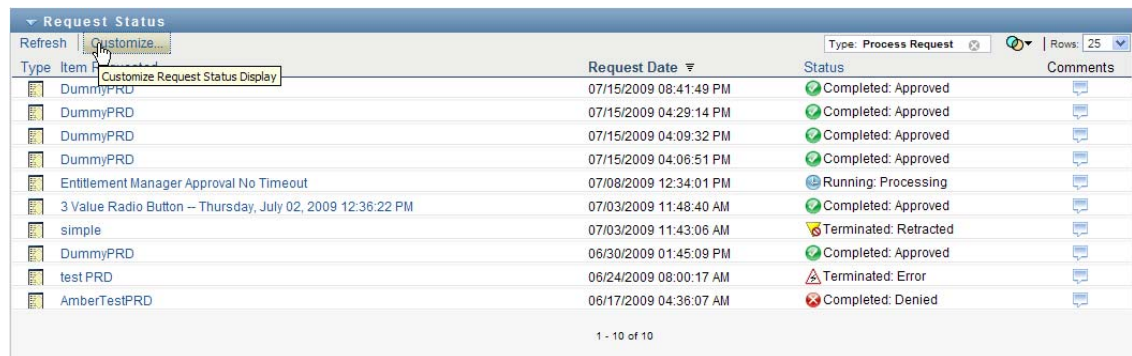
## 10.4.6 Controlling the Display of Request Status Details

The Work Dashboard page allows you to specify how you want to display the details for a request you click on in the Request Status section of the page. You can display the task details within the list or in a separate modal dialog. This behavior is controlled by a setting within the Customize Request Status Display dialog.

When you modify this setting, your preference is saved in the Identity Vault along with your other user preferences.

To control the display of task details:

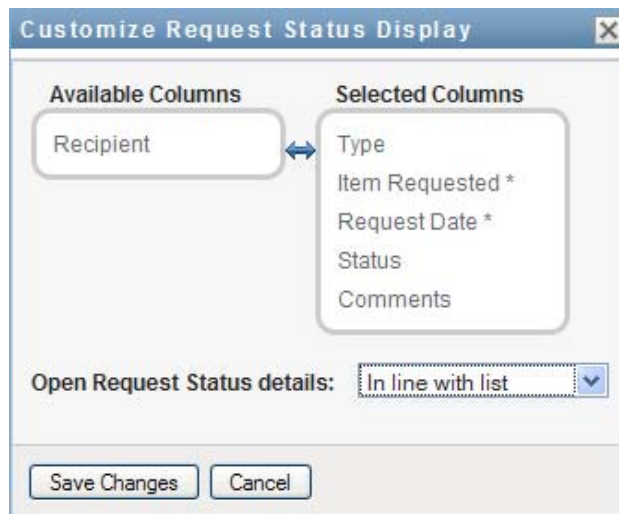
- 1 Click the *Customize* button in the *Request Status* section of the Work Dashboard page.



| Type  | Item     | Request Date           | Status                | Comments |
|---|----------|------------------------|-----------------------|----------|
| DummyPRD  | DummyPRD | 07/15/2009 08:41:49 PM | Completed: Approved   |          |
| DummyPRD  | DummyPRD | 07/15/2009 04:29:14 PM | Completed: Approved   |          |
| DummyPRD  | DummyPRD | 07/15/2009 04:09:32 PM | Completed: Approved   |          |
| DummyPRD  | DummyPRD | 07/15/2009 04:06:51 PM | Completed: Approved   |          |
| Entitlement Manager Approval No Timeout                     |          | 07/08/2009 12:34:01 PM | Running: Processing   |          |
| 3 Value Radio Button -- Thursday, July 02, 2009 12:36:22 PM |          | 07/03/2009 11:48:40 AM | Completed: Approved   |          |
| simple  |          | 07/03/2009 11:43:06 AM | Terminated: Retracted |          |
| DummyPRD  | DummyPRD | 06/30/2009 01:45:09 PM | Completed: Approved   |          |
| test PRD  |          | 06/24/2009 08:00:17 AM | Terminated: Error     |          |
| AmberTestIPRD   |          | 06/17/2009 04:36:07 AM | Completed: Denied     |          |

The User Application displays the *Customize Request Status Display* dialog, which allows you to customize the request list display. The set of controls shown may vary depending on which settings the administrator has designated as available for user override.





- 2 To display the details within the task list display, select *In line with list* in the *Open Request Status details* dropdown. To display the details in a separate modal dialog, select *In message window*.
- 3 To save your changes, click *Save Changes*.

## 10.4.7 Sorting the Request List

To sort the request list:

- 1 Click the header for the column you want to sort on.

The pyramid-shaped sort indicator shows you which column is the new primary sort column. When the sort is ascending, the sort indicator is shown in its normal, upright position. When the sort is descending, the sort indicator is upside down.

You can sort the list on multiple columns by clicking the header for each sort column. The default sort is descending order by Request Date, which causes the most recent requests to display first. If you sort the list on any column other than the Request Date column, the Request Date column is used as the secondary sort column.

When you modify the sort order for the request list, your preference is saved in the Identity Vault along with your other user preferences.

## 10.4.8 Refreshing the Request List

To refresh the request list:

- 1 Click the *Refresh* button.

The request list is updated to reflect the current state of the request list for the current user. The *Refresh* button does not remove any filters you have applied to the request list. When you refresh the request list, any filters you have defined are used to update the list, and the filters remain in effect until you reset them.

## 10.4.9 Viewing the Comments for a Request

- 1 To display the comment text for a request, click the Comments icon in the request list.



**NOTE:** To see the comments for a request, you must include the Comments column in the list of selected columns. For details on adding columns to the task list, see [Section 10.4.4, “Customizing the Request Status Columns,”](#) on page 167.

## 10.4.10 Viewing the Details for a Request

To view the details for a request:

- 1 Click the request name in the *Item Requested* column.

The User Application displays the details for the request.

The screenshot shows a 'Request Status' window with a table of requests and a detailed view for a 'Nurse' request.

| Type | Item Requested                      | Request Date           | Status                | Comments |
|------|-------------------------------------|------------------------|-----------------------|----------|
|      | Role Approval - lingtest            | 05/22/2009 07:16:01 PM | Terminated: Retracted |          |
|      | Add Resource To User - lingresrouce | 05/23/2009 03:44:01 AM | Running: Processing   |          |
|      | Nurse                               | 05/26/2009 05:14:42 PM | Completed             |          |

**Nurse**

Status: ✔ Completed: Provisioned

Recipient: Bob Jenner      Request Action: Add Role To User

Requested By: Bob Jenner      Request Date: 05/26/2009 05:14:42 PM

Effective Date: 05/26/2009 05:14:42 PM      Expiration Date:

Initial Request Description: TDBTestRoleAssignment      Common Requests ID: f01005149d914a3fab49321b59088726

Retract    Close

|  |                            |                        |                       |  |
|--|----------------------------|------------------------|-----------------------|--|
|  | Role Approval - lingtest   | 05/22/2009 07:16:01 PM | Terminated: Retracted |  |
|  | lingtest                   | 05/22/2009 07:16:00 PM | Terminated            |  |
|  | Compliance Administrator   | 05/22/2009 02:52:59 PM | Completed             |  |
|  | Compliance Administrator   | 05/22/2009 02:52:59 PM | Completed             |  |
|  | Provisioning Administrator | 05/22/2009 01:03:51 PM | Completed             |  |
|  | Compliance Administrator   | 05/22/2009 01:03:51 PM | Completed             |  |
|  | Role Module Administrator  | 05/22/2009 01:03:51 PM | Completed             |  |

1 - 10 of 10

## 10.4.11 Retracting a Request

The Request Status section of the Work Dashboard page gives you the option to retract a request that is still in process if you have changed your mind and do not need to have the request fulfilled.

An end user can retract any request that for which this user is the initiator, as long as the request is still in a retractable state. A Domain Administrator can retract any request within the domain for which the administrator has authority. A Domain Manager must have the proper security permission to retract requests. Specifically, you must have permission to revoke assignments, which implicitly gives you the ability to retract a request as well.

To retract a request:

- 1 Click *Retract* on the Request Detail window.

Request Status

Refresh | Customize... Filter | Rows: 25

| Type | Item Requested                       | Request Date           | Status                | Comments |
|------|--------------------------------------|------------------------|-----------------------|----------|
|      | Role Approval - llingtest            | 05/22/2009 07:16:01 PM | Terminated: Retracted |          |
|      | Add Resource To User - llingresrouce | 05/23/2009 03:44:01 AM | Running: Processing   |          |

**Add Resource To User - llingresrouce**

Status: Running: Processing

Recipient: Abby Spencer

Requested By: Application Administrator Of Sample Data Request Date: 05/23/2009 03:44:01 AM

Comment and Flow History

Retract Close

|  |                            |                        |                       |  |
|--|----------------------------|------------------------|-----------------------|--|
|  | Nurse                      | 05/26/2009 05:14:42 PM | Completed             |  |
|  | Role Approval - llingtest  | 05/22/2009 07:16:01 PM | Terminated: Retracted |  |
|  | llingtest                  | 05/22/2009 07:16:00 PM | Terminated            |  |
|  | Compliance Administrator   | 05/22/2009 02:52:59 PM | Completed             |  |
|  | Compliance Administrator   | 05/22/2009 02:52:59 PM | Completed             |  |
|  | Provisioning Administrator | 05/22/2009 01:03:51 PM | Completed             |  |
|  | Compliance Administrator   | 05/22/2009 01:03:51 PM | Completed             |  |
|  | Role Module Administrator  | 05/22/2009 01:03:51 PM | Completed             |  |

1 - 10 of 10

The *Retract* button is enabled only when the process associated with the request is still running.



# 11 Managing Work for Users, Groups, Containers, Roles, and Teams

This section explains how to use the Manage control to manage work for other users, and for groups, containers, roles, and teams. Topics include:

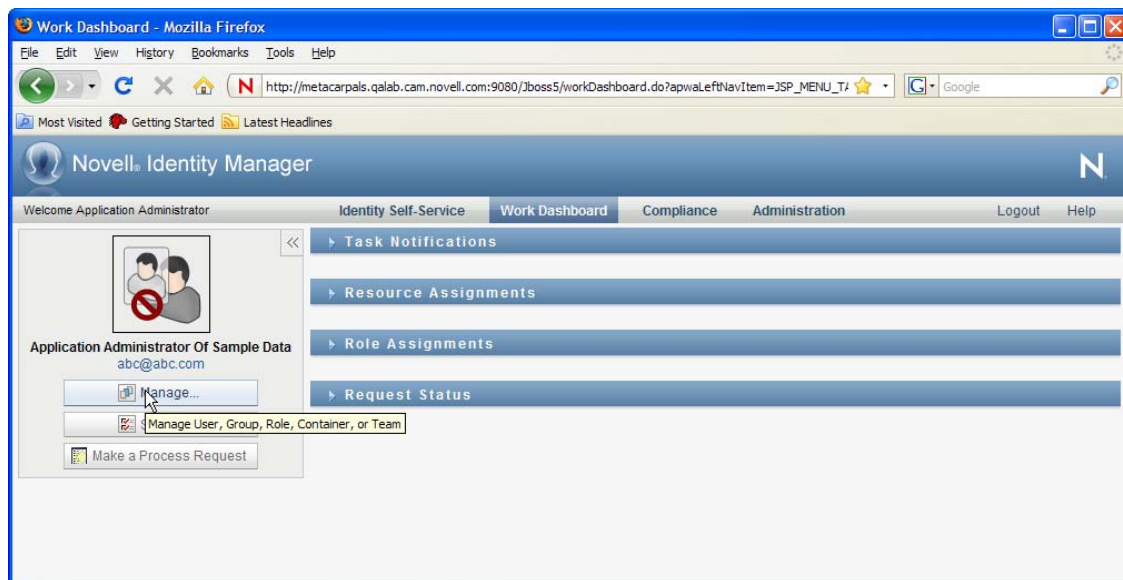
- [Section 11.1, “Selecting a User, Group, Container, Role, or Team,” on page 173](#)
- [Section 11.2, “Changing to a Different Managed Entity,” on page 176](#)
- [Section 11.3, “Minimizing the Screen Space Used by The User Profile Section,” on page 176](#)
- [Section 11.4, “Exiting Manage Mode,” on page 177](#)

## 11.1 Selecting a User, Group, Container, Role, or Team

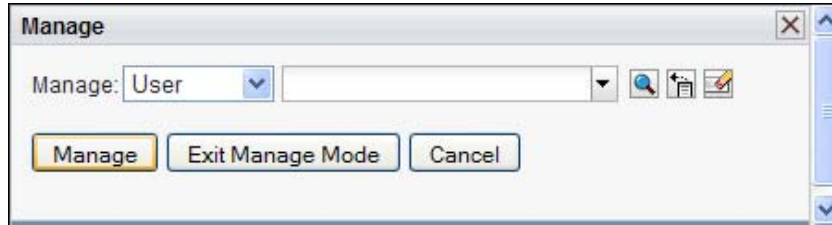
When a Domain Administrator or Domain Manager logs in to the User Application, the Work Dashboard shows the *Manage* control, which is a global lookup control. The *Manage* control allows the current user to select a particular user, group, container, role, or team member and use the Work Dashboard interface to manage work for the selected entity type. After the user selects an entity, the data and access permissions on the Work Dashboard pertain to the selected entity, rather than to the user currently logged on. However, when the user is in Manage mode, the *Settings* and *Make a Process Request* menus still apply to the logged-in-user, not the selected entity in the *Manage* control.

To select a user, group, container, role, or team member:

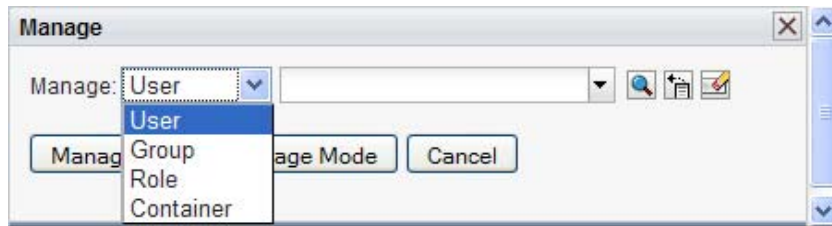
- 1 Click *Manage* in the upper-left corner of the Work Dashboard.



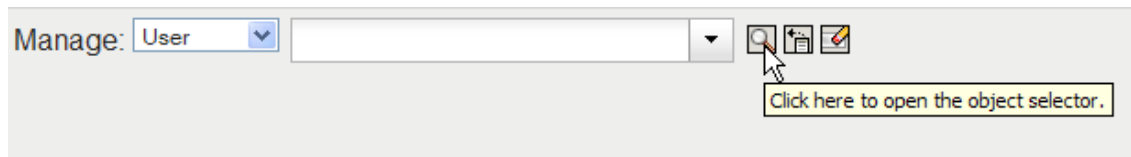
The Work Dashboard displays the Manage pop-up window:



2 In the *Manage* control, select the entity type:

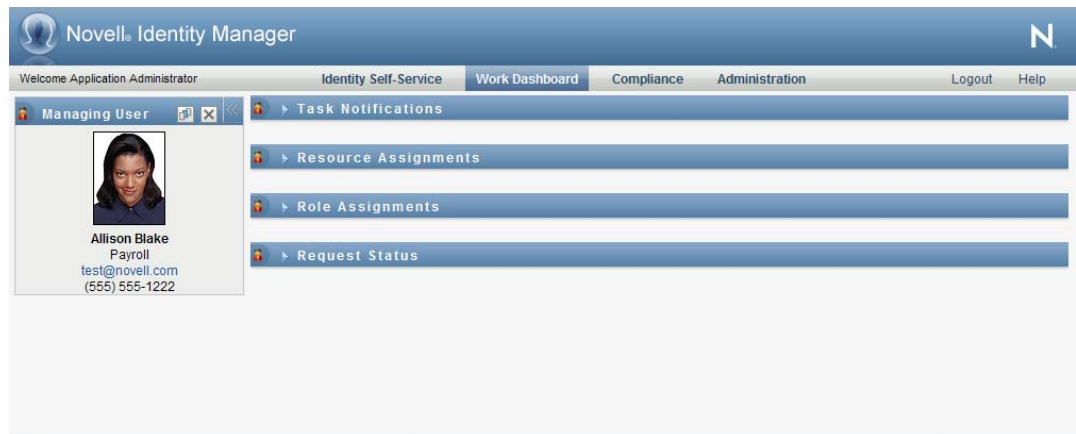


3 Use the object selector to select a particular user, group, container, role, or team:



When you select a user, group, container, role, or team, the Work Dashboard puts you in manage mode and updates the User Profile section on the left side of the screen. The User Profile updates its display, as follows:

- ◆ When a user is chosen, it shows the photo, name, title, email, and phone number of the selected user.

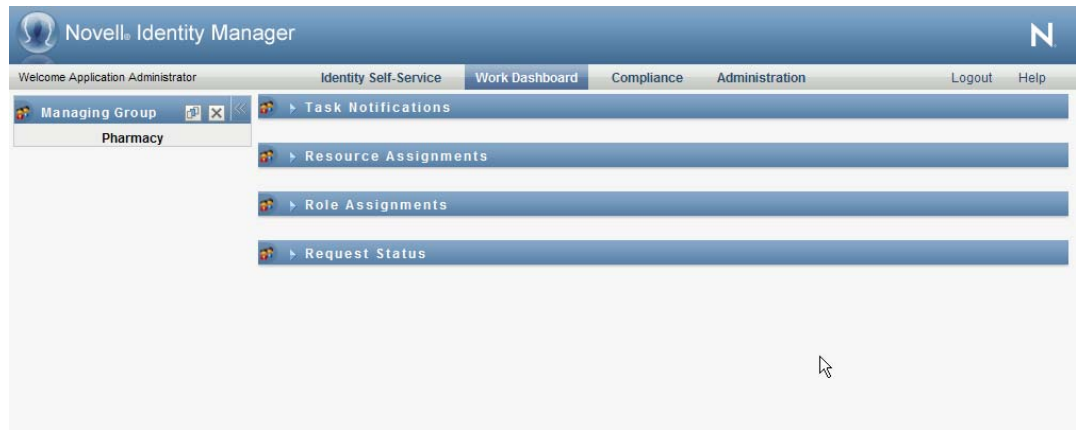


When you select a user, the User Profile section and the Task Notifications, Resource Assignments, Role Assignments, and Request Status sections of the page show this icon:



This icon indicates that the data and access permissions for these sections of the Work Dashboard pertain to the selected user, rather than to the user currently logged on.

- ◆ When a group, container, or role is chosen, it shows the DN, display name, and description (if available) of the group, container or role.



When you select a container, the User Profile section and the Task Notifications, Resource Assignments, Role Assignments, and Request Status sections of the page show this icon:



When you select a group, the User Profile section and the Task Notifications, Resource Assignments, Role Assignments, and Request Status sections of the page show this icon:



When you select a role, the User Profile section and the Task Notifications, Resource Assignments, Role Assignments, and Request Status sections of the page show this icon:



These icons indicate that the data and access permissions for these sections of the Work Dashboard pertain to the selected entity, rather than to the user currently logged on.

- ◆ When a team is selected, it shows the team dropdown to allow you to select a team. In addition, it shows a dropdown that lets you pick a team member.

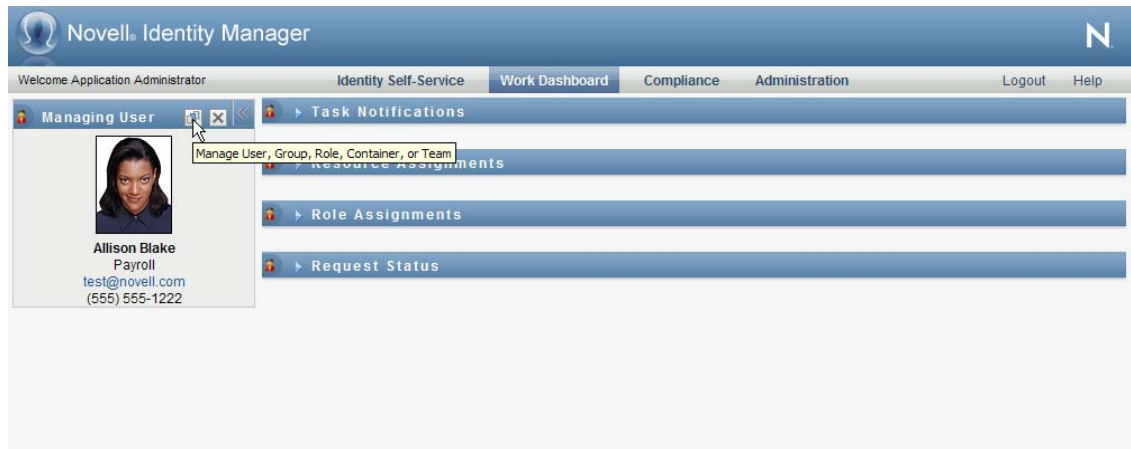
When you select a team member, the User Profile section and the Task Notifications, Resource Assignments, Role Assignments, and Request Status sections of the page show this icon:



## 11.2 Changing to a Different Managed Entity

To change to a different managed entity:

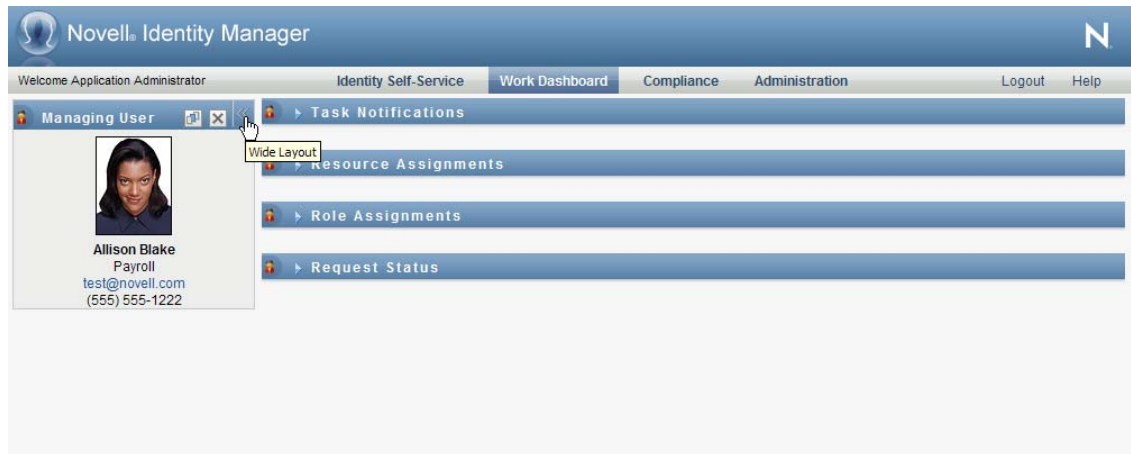
- 1 Click the *Manage User, Group, Role, or Container* button in the User Profile section.



## 11.3 Minimizing the Screen Space Used by The User Profile Section

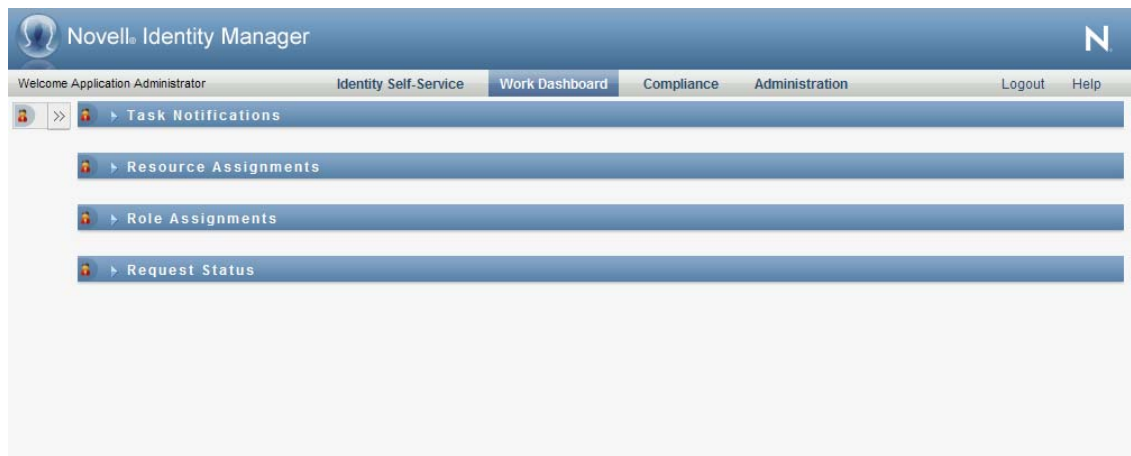
To minimize the screen space used by the User Profile section:

- 1 Click the *Wide Layout* button in the User Profile section.

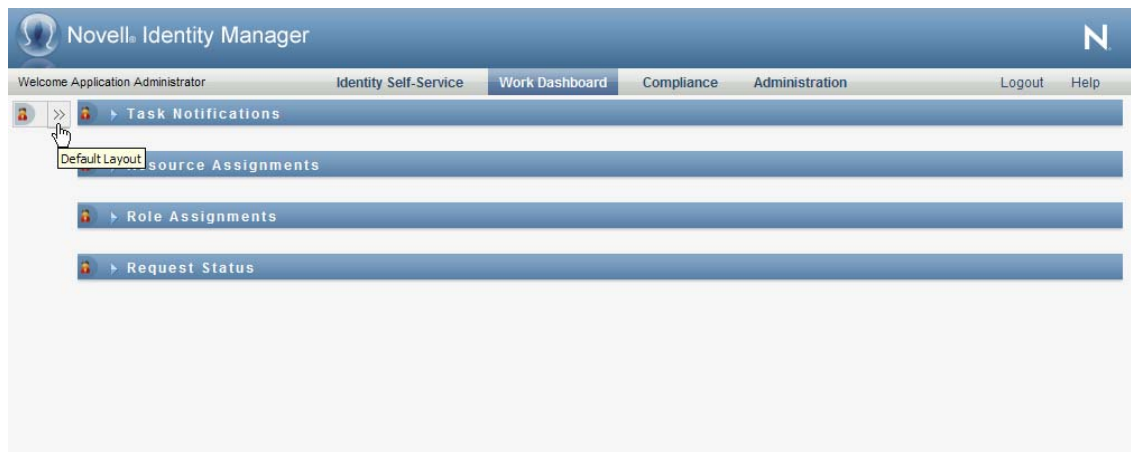


The User Profile section hides the details about the currently selected entity to give you more space to work with the Task Notifications, Resource Assignments, Role Assignments, and Request Status sections of the page.





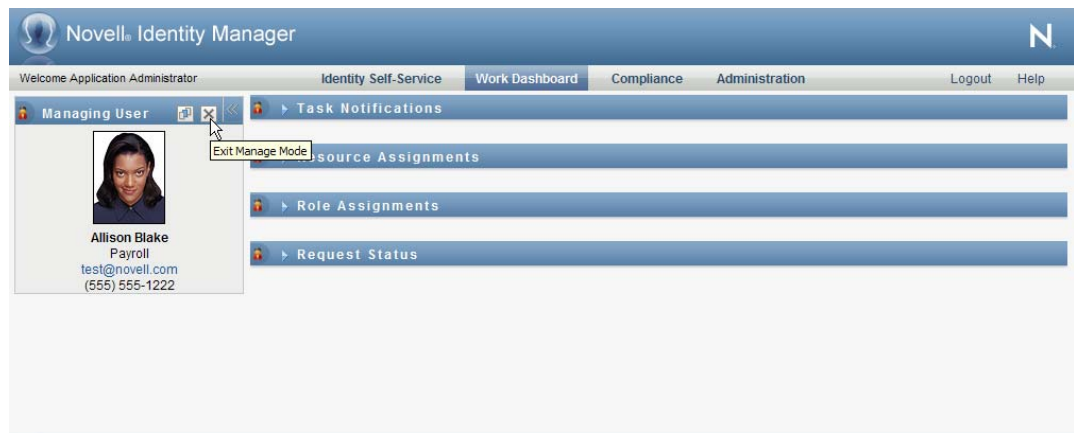
To return the User Profile section to its normal display size so that the entity details are visible, click the *Default Layout* button.



## 11.4 Exiting Manage Mode

To exit manage mode and reset the Work Dashboard to show data and access permissions for the current logged in user:

- 1 Use either of the following methods:
  - ◆ Click the X on the User Profile section:



- ◆ In the Manage dialog, click the *Exit Manage Mode* button.

**Proxy Mode** The *Manage* control is not available in proxy mode, even if a user is proxying for a user that is a Domain Administrator or Domain Manager. When a user is in proxy mode, the navigation access permissions for menu items on the Work Dashboard show the proxied user's permissions, not the permissions for the logged in user.

---

# 12 Controlling Your Settings

This section provides information about how to use the *Settings* menu on the Work Dashboard. Topics include:

- ◆ [Section 12.1, “About the Settings Menu,” on page 179](#)
- ◆ [Section 12.2, “Acting as a Proxy,” on page 183](#)
- ◆ [Section 12.3, “Specifying Your Availability,” on page 184](#)
- ◆ [Section 12.4, “Viewing and Editing Your Proxy Assignments,” on page 190](#)
- ◆ [Section 12.5, “Viewing and Editing Your Delegate Assignments,” on page 192](#)
- ◆ [Section 12.6, “Viewing and Editing Your Team Proxy Assignments,” on page 195](#)
- ◆ [Section 12.7, “Viewing and Editing Your Team Delegate Assignments,” on page 199](#)
- ◆ [Section 12.8, “Specifying Your Team’s Availability,” on page 203](#)
- ◆ [Section 12.9, “Making a Team Process Request,” on page 206](#)

## 12.1 About the Settings Menu

The *Settings* actions give you the ability to act as a proxy for another user. In addition, they allow you to view your proxy and delegate assignments. If you are a Provisioning Administrator, or a Provisioning Manager or Team Manager for the Provisioning Domain, you might also be permitted to define proxy and delegate assignments, as well as team availability settings.

### 12.1.1 About Proxies and Delegates

A *delegate* is a user authorized to perform work for another user. A delegate assignment applies to a particular type of request.

A *proxy* is a user authorized to perform any and all work (and also define provisioning settings) for one or more users, groups, or containers. Unlike delegate assignments, proxy assignments are independent of process requests, and therefore apply to all work and settings actions.

**Proxy and Delegate Assignments Have Time Periods:** Both proxy and delegate assignments are associated with time periods. The time period for a proxy or delegate assignment can be as short or as long as you need it to be. The time period can also have no expiration date.

**Proxy and Delegate Actions Are Logged:** If logging is enabled, any actions taken by a proxy or delegate are logged along with actions taken by other users. When an action is taken by a proxy or delegate, the log message clearly indicates that the action was performed by a proxy or delegate for another user. In addition, each time a new proxy or delegate assignment is defined, this event is logged as well.

**Delegate Assignments When a Role Is the Approver:** The User Application does not perform delegate processing when a workflow approver is a role. Any user in a role can perform approvals assigned to the role so delegation is not necessary.

**Proxy Assignments When a Role Is the Approver:** When you make proxy assignments, the User Application does not perform any checks on the roles already held by the user. It is possible that the user might already be assigned to all of the same roles as the person for whom they are acting as proxy. It is also possible that there are conflicts with the roles of the person for whom they will act as proxy.

## 12.1.2 Sample Usage Scenarios

This section describes two business scenarios where proxies and delegates might be used:

- ♦ [“Proxy Usage Scenario” on page 180](#)
- ♦ [“Delegate Usage Scenario” on page 180](#)

### Proxy Usage Scenario

Suppose you are a manager who is responsible for approving (or denying) a large number of workflow tasks on a daily basis. In addition, you are also responsible for editing provisioning settings for a large number of users in your organization. In this situation, you might want to assign a proxy so that some of your work can be off-loaded to a trusted member of your team.

### Delegate Usage Scenario

Suppose you are a manager who is responsible for approving or denying requests for ten different types of provisioned resources. All ten request types need regular attention, but you would rather have another individual in your organization attend to six of them. In this case, you could define a delegate for these six process request types. If necessary, you could restrict this delegate relationship to a period of hours, days, or weeks. Alternatively, you could specify no expiration for the delegate relationship, thereby establishing this relationship as a more permanent arrangement.

## 12.1.3 User Access to the Settings Menu

The *Settings* menu on the Work Dashboard displays the following options to all users who log in to the User Application:

**Table 12-1** *Settings Menu Options Available to All Authenticated Users*

| Settings Menu Option | Description   |
|----------------------|---|
| Edit Proxy Mode      | Lets you act as a proxy for another user.<br><br>For details, see <a href="#">Section 12.2, “Acting as a Proxy,” on page 183</a> .  |
| Edit Availability    | Lets you view or edit the requests you are available to act on, and which requests your assigned delegates can act on. To edit availability, you must have the Configure Availability permission.<br><br>For details, see <a href="#">Section 12.3, “Specifying Your Availability,” on page 184</a> . |

| Settings Menu Option    | Description  |
|-------------------------|--|
| My Proxy Assignments    | <p>Lets you view or edit your proxy assignments. To edit proxy assignments, you must have the Configure Proxy permission.</p> <p>For details, see <a href="#">Section 12.4, “Viewing and Editing Your Proxy Assignments,”</a> on page 190.</p>             |
| My Delegate Assignments | <p>Lets you view or edit your delegate assignments. To edit delegate assignments, you must have the Configure Delegate permission.</p> <p>For details, see <a href="#">Section 12.5, “Viewing and Editing Your Delegate Assignments,”</a> on page 192.</p> |

When a Provisioning Administrator, Provisioning Manager, or Team Manager logs in to the User Application, the *Settings* menu shows the following additional menu options:

**Table 12-2** *Settings Menu Options Available to Administrators and Team Managers*

| Settings Menu Option                    | Description  |
|---|--|
| Team Settings>Team Availability         | <p>Lets you specify which requests your team members are available to act on, and which requests the team member’s delegates can act on.</p> <p>The Configure Availability permission must be enabled in the team configuration. When this permission is disabled, this action is not allowed.</p> <p>For details, see <a href="#">Section 12.8, “Specifying Your Team’s Availability,”</a> on page 203.</p>   |
| Team Settings>Team Proxy Assignments    | <p>Lets you specify proxy assignments for members of your team.</p> <p>The Configure Proxy permission must be enabled in the team configuration. When this capability is disabled, this action is not allowed.</p> <p>For details, see <a href="#">Section 12.6, “Viewing and Editing Your Team Proxy Assignments,”</a> on page 195.</p>   |
| Team Settings>Team Delegate Assignments | <p>Lets you specify delegate assignments for members of your team.</p> <p>The Configure Delegate permission must be enabled in the team configuration. If the team rights allow managers to make a team member a delegate for other team member’s provisioning requests, this action is allowed for these requests. When this permission is disabled in the team configuration, this action is not allowed.</p> <p>For details, see <a href="#">Section 12.7, “Viewing and Editing Your Team Delegate Assignments,”</a> on page 199.</p> |

| Settings Menu Option                     | Description   |
|--|---|
| Team Settings>Make Team Process Requests | <p>Lets you make a process request for a member of your team.</p> <p>The Initiate PRD permission must be enabled in the team configuration. When this permission is disabled in the team configuration, this action is not allowed.</p> <p>For details, see <a href="#">Section 12.9, “Making a Team Process Request,”</a> on page 206.</p> |

The behavior of the Team Settings menu options varies depending on whether the current user is an administrator or team manager, and on which permissions have been granted, as described below:

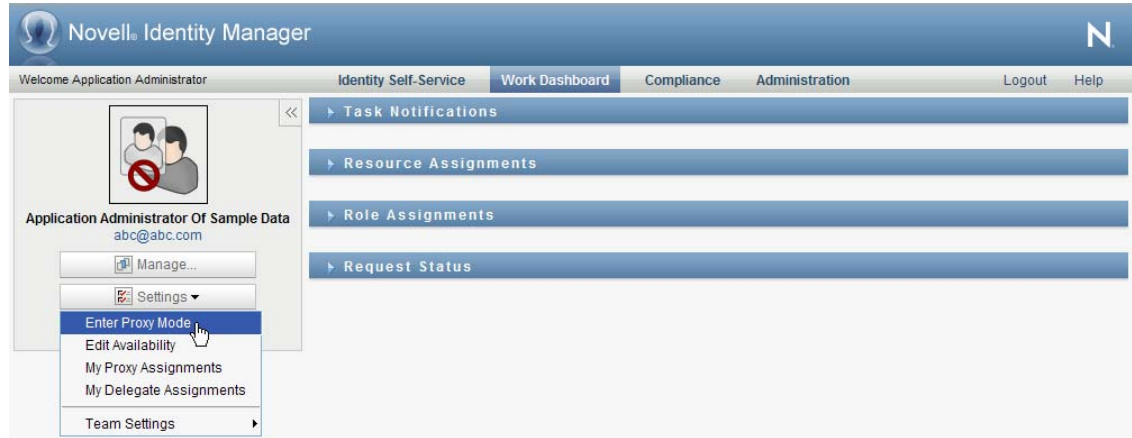
**Table 12-3** *User Access to the Team Settings Menu Options*

| User  | Capabilities   |
|---|--|
| Provisioning Administrator (or Security Domain Administrator) | <p>Can select a user without having to select a team.</p> <p>Has all permissions associated with the Provisioning Domain, and can therefore see the Team Proxy Assignments, Team Delegate Assignments, and Team Availability menu options.</p> <p>Can access the <i>New</i> button on the Team Proxy Assignments, Team Delegate Assignments, and Team Availability pages.</p>  |
| Provisioning Manager  | <p>Can select a user without having to select a team.</p> <p>Needs to be given security rights to see the Team Proxy Assignments, Team Delegate Assignments, and Team Availability menu options.</p> <p>Can access the <i>New</i> button on the Team Proxy Assignments, Team Delegate Assignments, and Team Availability pages, if the proper security rights have been given.</p> <p>In the Team Delegate Assignments user interface, the Provisioning Manager is only able to select provisioning requests that they have rights to assign. When the Provisioning Manager submits a delegate assignment request, only assignments they are allowed to make are successfully completed.</p> |
| Team Manager  | <p>Must select a team before choosing a user.</p> <p>Needs to be given security rights to see the Team Proxy Assignments, Team Delegate Assignments, and Team Availability menu options.</p> <p>Can access the <i>New</i> button on the Team Proxy Assignments, Team Delegate Assignments, and Team Availability pages, if the proper security rights have been given.</p>   |

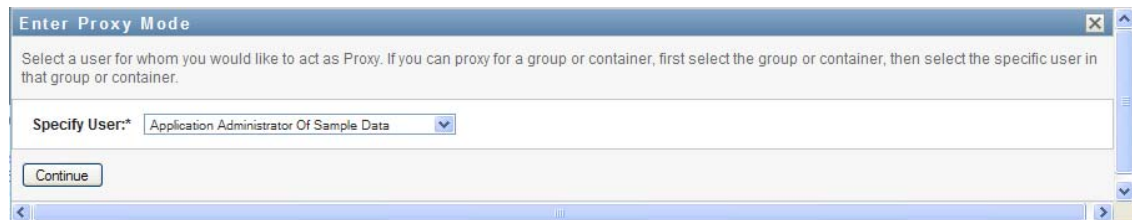
## 12.2 Acting as a Proxy

The *Enter Proxy Mode* action allows you to act as a proxy for another user.

- 1 Click *Enter Proxy Mode* in the *Settings* group of actions in the User Profile section of the Work Dashboard.



If you are authorized to act as a proxy for at least one other user, the User Application displays a list of users.



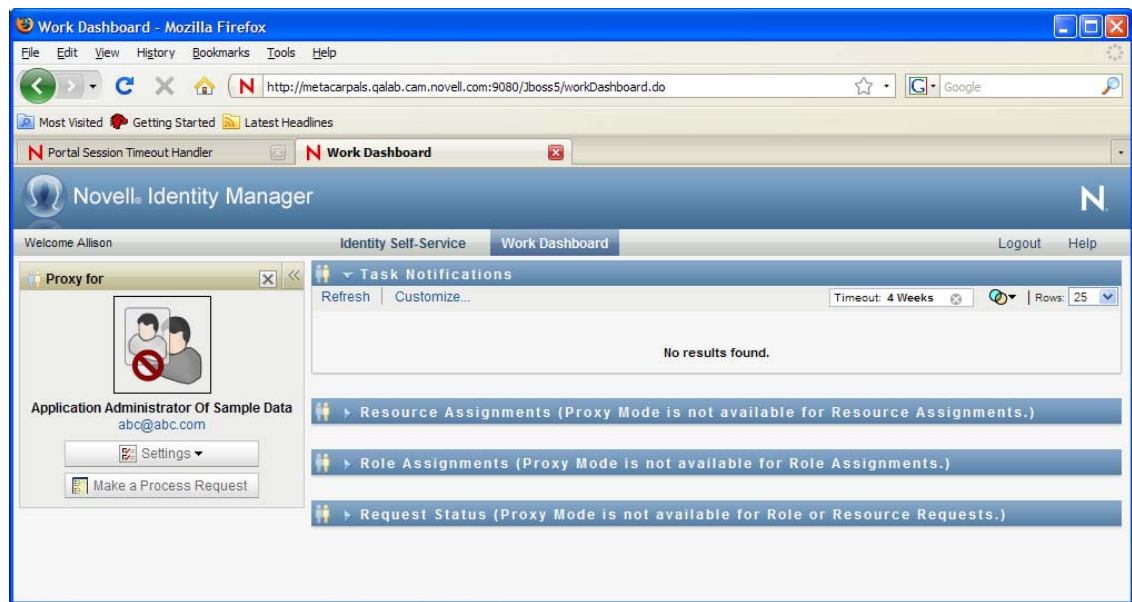
If you are not authorized to act as a proxy for any other user, the User Application displays this message:



- 2 Select the user for whom you want to act as proxy and click *Continue*.

If you are designated as a proxy for a group or container, you must select the group or container before you can select the user. The User Application provides a dropdown list to allow you to select the group or container.

The User Application refreshes the display and returns you to the *My Tasks* action, the default action when you log on. The task lists shows tasks assigned to the user for whom you are acting as proxy. A message appears above the *My Work* group (as well as in the title bar) indicating that you are now acting as a proxy for another user.



At this point, you can perform any action that the user for whom you are acting as proxy could perform. The list of actions available changes depending on your authority and the authority of the user for whom you are acting as proxy.

## 12.3 Specifying Your Availability

The *Edit Availability* action allows you to specify which process requests with a delegate assignment you are unavailable to work on during a particular time period. During the time period when you are unavailable for a particular request, the user delegated to act on that request can work on it.

If you prefer not to specify your availability for each process request definition individually, you can use the *Edit Availability* action to establish global settings pertaining to delegation.

---

**TIP:** Before using the *Edit Availability* action, you need to have at least one delegate assignment to work on. You need to have a Provisioning Administrator (or a Provisioning Manager or Team Manager) create delegate assignments for you.

---

- ♦ [Section 12.3.1, “Setting Your Availability Status,” on page 184](#)
- ♦ [Section 12.3.2, “Creating or Editing an Availability Setting,” on page 186](#)
- ♦ [Section 12.3.3, “Deleting an Availability Setting,” on page 189](#)

### 12.3.1 Setting Your Availability Status

- 1 Click *Edit Availability* in the *Settings* group of actions.

The User Application displays the Edit Availability page. If you do not have any existing availability settings, the display list is empty:



Edit Availability

Edit, delete, or create a new "Selectively Available" setting, or change the status across all requests.

User: Allison Blake

Status:  Available for ALL Requests

Change Status: (Select One) ▼

| User          | Unavailable From | Unavailable Until | Resource |
|---------------|------------------|-------------------|----------|
| Allison Blake | --               | --                | All      |

0 - 0 of 0

Refresh New

If no delegates have been assigned for you, the User Application displays a message indicating that you cannot change your status on the Edit Availability page.

If you have one or more availability settings, the display list shows these settings:



Edit Availability

Edit, delete, or create a new "Selectively Available" setting, or change the status across all requests.

User: Allison Blake

Status:  NOT Available for ANY Requests

Change Status: (Select One) ▼

| User  | Unavailable From       | Unavailable Until | Resource |
|---|------------------------|-------------------|----------|
|   Allison Blake | 12/05/2006 10:28:13 AM | No Expiration     | All      |

1 - 1 of 1

Refresh New

- To see details about a particular process associated with an availability assignment, click the name of the process.

The page then displays a pop-up window that provides information about the delegate assignment:

**Delegate Assignment** [X]

User: Allison Blake  
 Delegate Assigned: Kevin Chester  
 Expiration: No Expiration

This information is particularly helpful in situations where the same process name appears more than once in the availability settings list.

- 3 Specify your status by selecting one of the following options in the *Change Status* drop-down list:

| Status                                      | Description   |
|---|---|
| <i>Available for ALL Requests</i>           | <p>This is the default status. It indicates that you are globally available. When this status is in effect, requests assigned to you are not delegated, even if you have assigned delegates.</p> <p>The <i>Available for ALL Requests</i> status overrides other settings. If you change the status to one of the other settings, and then change it back to <i>Available for ALL Requests</i>, any <i>Selectively Available</i> settings previously defined are removed.</p>                         |
| <i>NOT Available for ANY Requests</i>       | <p>Specifies that you are globally unavailable for any request definitions currently in the system.</p> <p>Choosing the <i>Not Available for ANY Requests</i> status indicates that you are unavailable for each existing delegate assignment and changes the current status to <i>Not Available for Specified Requests</i>. Assignments are effective immediately until the delegate assignment expires. This setting does not affect availability for new assignments created after this point.</p> |
| <i>NOT Available for Specified Requests</i> | <p>Specifies that you are not available for certain process request definitions. During the time period when you are unavailable for a particular request, the user delegated to act on that request can work on it.</p> <p>The <i>NOT Available for Specified Requests</i> option takes you to the Edit Availability page. It is the same action as clicking the <i>New</i> button.</p>  |

## 12.3.2 Creating or Editing an Availability Setting

- 1 To create a new availability setting, click *New* (or select *NOT Available for Specified Requests* in the *Change Status* drop-down list).
- 2 To edit an existing setting, click *Edit* next to the setting you want to modify:



The User Application displays a set of controls that allow you to specify the time period for which you are unavailable and select the requests to which this setting applies.


The list of process requests displayed includes only those that have a delegate assignment.

Edit Availability

Selective Availability

\* - indicates required.

User: Allison Blake

Unavailable From:\*  

Unavailable Until:\*  No Expiration  
 Specify Duration (Weeks, Days, Hours)  
 Specify End Date

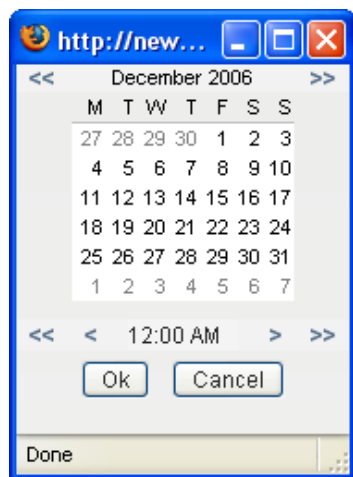
Notify other users of these changes.

All Request Types

Request Type Selection

**3** Specify the time period during which you will be unavailable:

- 3a** Specify when the time period begins by typing the start date and time in the *Unavailable From* box, or by clicking the calendar button and selecting the date and time.



- 3b** Specify when the time period ends by clicking one of the following:

| Button               | Description  |
|----------------------|--|
| <i>Duration</i>      | Lets you specify the time period in weeks, days, or hours.   |
| <i>End date</i>      | Lets you specify the end date and time. You can type the date and time, or click the calendar button and select the date and time from the calendar. |
| <i>No Expiration</i> | Indicates that this unavailability setting does not expire.  |

The end date you specify must be within the time period allowed by the delegate assignment. For example, if the delegate assignment expires on October 31, 2009, you cannot specify an expiration date of November 15, 2009 for the availability setting. If you specify an expiration date of November 15, 2009, it is automatically adjusted when it is submitted to expire on October 31, 2009.

- 4 Specify whether you want to send e-mail notifications to other users by filling in these fields:

| Field                                      | Description  |
|--|--|
| <i>Notify other users of these changes</i> | Indicates whether you want to send an e-mail message to notify one or more users of this availability assignment.                                    |
| <i>Addressee</i>                           | Specifies which users should receive e-mail notifications:<br><br><b>Selective:</b> Allows you to send e-mail notifications to any users you select. |

- 5 Select one or more process requests in the *Types of Requests* list, and click *Add*.

On this page, you select the types of requests not to accept during the time you are unavailable. This has the effect of delegating these requests to other users.

Request Type Selection

Select the types of requests that you will not accept during the time you are unavailable. Only requests with a delegate assignment are available for selection below.

Types of Requests:

Enable Active Directory Account

Declined for the Specified Period:\*

Each process request you add is included in the *Declined for the Specified Period* list.

**Request Type Selection**

Select the types of requests that you will not accept during the time you are unavailable. Only requests with a delegate assignment are available for selection below.

Types of Requests:

Declined for the Specified Period:\*

- 6 To indicate that this availability setting applies to all request types, click *All Request Types* instead of selecting the request types individually.

All Request Types

The *All Request Types* check box is only available when the type of request for the delegate assignment is set to *All*.

- 7 To remove a request from the list, click *Remove*.
- 8 Click *Submit* to commit your changes.

### 12.3.3 Deleting an Availability Setting

To delete an existing availability setting:

- 1 Click *Remove* next to the setting:



## 12.4 Viewing and Editing Your Proxy Assignments

The *My Proxy Assignments* action allows you to view your proxy assignments. If you are a Provisioning Administrator, Provisioning Manager, or Team Manager, you can also use this action to edit proxy assignments.

Only Provisioning Administrators, Provisioning Managers, and Team Managers can assign proxies, as described below:

- ♦ The Provisioning Administrator and the Provisioning Manager have the ability to define proxy assignments for any user in the organization.
- ♦ A Team Manager might have the ability to define proxy settings for users on his team, depending on how the team was defined. The proxies must also be within the team. To define a proxy, a Team Manager must use the *Team Proxy Assignments* action.

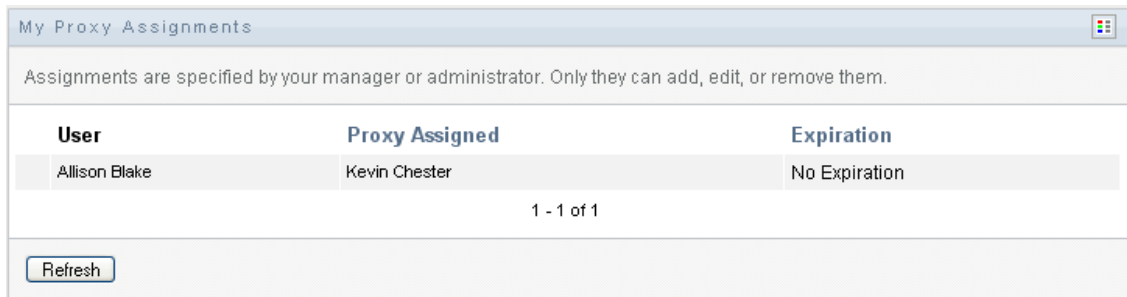
If a Team Manager needs to select a proxy who is not within the team, the manager must request that the Provisioning Administrator or Provisioning Manager define the proxy relationship.

### 12.4.1 Displaying Your Proxy Settings

- 1 Click *My Proxy Assignments* in the *Settings* group of actions.

The User Application displays your current settings. The proxy assignments displayed are those that specify you as proxy for someone else, as well as those that specify someone else as proxy for you.

If you are not a Provisioning Administrator, Provisioning Manager, or Team Manager, you see a read-only view of your proxy assignments:



| User          | Proxy Assigned | Expiration    |
|---------------|----------------|---------------|
| Allison Blake | Kevin Chester  | No Expiration |

1 - 1 of 1

Refresh

If you have administrative privileges, you are provided with buttons that let you create and edit proxy assignments.

- 2 To refresh the list, click *Refresh*.

### 12.4.2 Creating or Editing Proxy Assignments

- 1 To create a new proxy assignment, click *New*.
- 2 To edit an existing proxy assignment, click *Edit* next to the assignment:



If you are the Provisioning Application Administrator, the User Application presents the following interface to allow you to define proxy assignments:

My Proxy Assignments




Complete and submit the assignment.




\* - indicates required.




Proxy Authorization

Select one or more users, groups or containers for which you would like to assign a proxy. A selection of at least one of the available options is required in order to grant a proxy assignment.




Proxy For:\*

User:    

Group:    

Container:    

Proxy Assigned:\*

Notify other users of these changes.

Timeframe

- 3 If you are a Provisioning Administrator, select one or more users, groups, and containers for which you want to define a proxy.  
Use the *Object Selector* or the *Show History* tool to select a user, group, or container.
- 4 If you are a team manager, select one or more users for whom you want to define a proxy.
- 5 Specify a user to be the proxy in the *Proxy Assigned* field.
- 6 Specify when the time period ends by clicking one of the following:

| Button                    | Description  |
|---------------------------|--|
| <i>No Expiration</i>      | Indicates that this proxy assignment does not expire.  |
| <i>Specify Expiration</i> | Lets you specify the end date and time. You can type the date and time, or click the calendar button and select the date and time from the calendar. |

- 7 Click *Submit* to commit your changes.

### 12.4.3 Deleting Proxy Assignments

To delete an existing proxy assignment:

- 1 Click *Remove* next to the assignment:



---

**NOTE:** The User Application does not log you out of proxy mode right after you change permissions for a proxy assignment. This allows you to change a value if you have made a mistake. Therefore, if you delete a proxy assignment while in proxy mode, you are still able to edit the proxy assignment and also work on the proxy user's tasks even after removing the proxy assignment.

---

## 12.5 Viewing and Editing Your Delegate Assignments

The *My Delegate Assignments* action allows you to view your delegate assignments. If you are a Provisioning Administrator, Provisioning Manager, or Team Manager, you can also use this action to edit delegate assignments.

Only Provisioning Administrators, Provisioning Managers, and Team Managers can assign delegates, as described below:

- ♦ The Provisioning Administrator and Provisioning Manager have the ability to define delegate assignments for any user in the organization.
- ♦ A Team Manager might have the ability to define delegate settings for users on his team, depending on how the team rights have been defined. The delegates must also be within the team. To define a delegate, a Team Manager must use the *Team Delegate Assignments* action.

If a team manager needs to define a delegate relationship for users who are not within his or her scope of authority, he or she must request that the Provisioning Administrator define the delegate relationship.

---

**TIP:** Before using the *Edit Availability* action, you need to have at least one delegate assignment to work on.

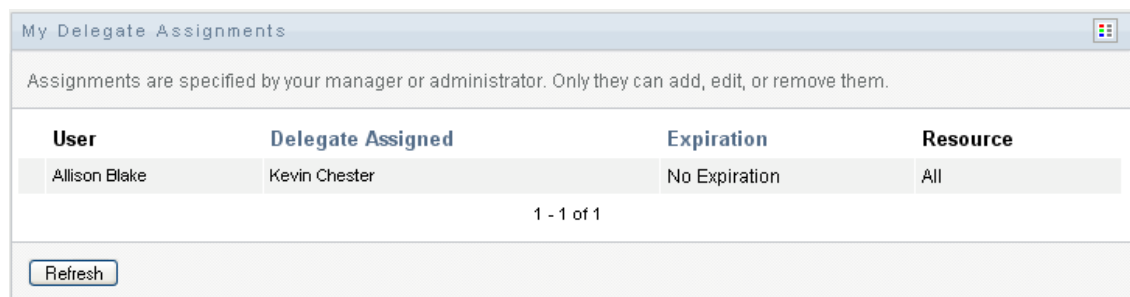
---

### 12.5.1 Displaying Your Delegate Settings

- 1 Click *My Delegate Assignments* in the *Settings* group of actions.

The User Application displays your current settings.

If you are not a Provisioning Administrator, Provisioning Manager, or Team Manager, you see a read-only view of your delegate assignments:



| User          | Delegate Assigned | Expiration    | Resource |
|---------------|-------------------|---------------|----------|
| Allison Blake | Kevin Chester     | No Expiration | All      |

1 - 1 of 1

Refresh

If you have administrative privileges, you are provided with buttons that let you create and edit delegate assignments.





- 2 To refresh the list, click *Refresh*.

## 12.5.2 Creating or Editing Delegate Assignments

- 1 To edit an existing delegate assignment, click *Edit* next to the assignment:



Or, to create a new delegate assignment, click *New*.

If you are the Provisioning Application Administrator, the User Application presents the following interface to allow you to define delegate assignments:

- 2 Select one or more users, groups, and containers for which you want to define a delegate. Use the *Object Selector* or the *Show History* tool to select a user, group, or container.
- 3 Click *Assign Delegate*. Specify the user who is the delegate in the *Delegate Assigned* field. Alternatively, click *Assign by Relationship*, then select a relationship in the *Delegate Relationship* field.
- 4 Specify when the time period ends by clicking one of the following:

| Button                    | Description  |
|---------------------------|--|
| <i>No Expiration</i>      | Indicates that this delegate assignment does not expire.   |
| <i>Specify Expiration</i> | Lets you specify the end date and time. You can type the date and time, or click the calendar button and select the date and time from the calendar. |

- 5 Select the category of process requests in the *Type of Request* field. Select *All* to include requests from all available categories.
- 6 Select one or more requests that you want to delegate in the *Available Requests in Selected Category* list, then click *Add*.

Request Type Selection

Select the types of requests for this delegate assignment. Select a Resource Category to display the available requests.

Resource Search Criteria: Entitlements ▼

Available Requests in Selected Category:

Enable Active Directory Account

Add Remove

Selected Requests:\*

Each process request you add is included in the *Selected Requests* list.

Request Type Selection

Select the types of requests for this delegate assignment. Select a Resource Category to display the available requests.

Resource Search Criteria: Entitlements ▼

Available Requests in Selected Category:

Add Remove

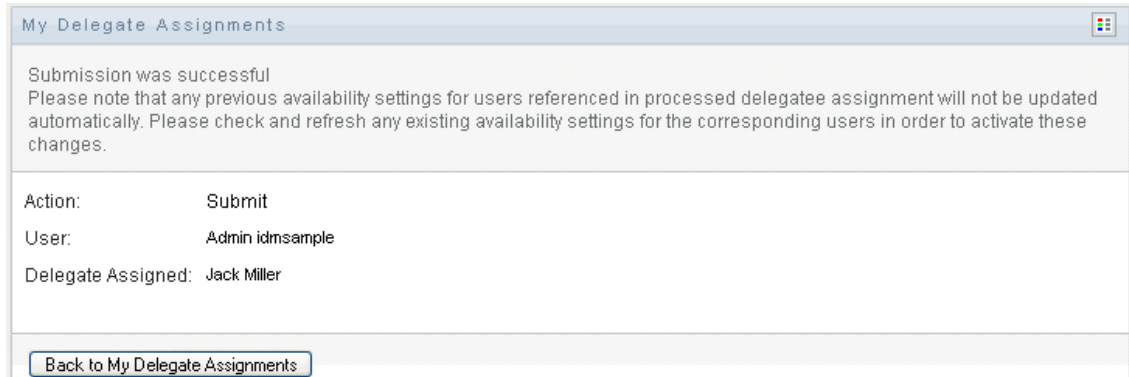
Selected Requests:\*

Enable Active Directory Account

If you add multiple requests, each request is treated as an individual object that can be edited separately.

- 7 To remove a request from the list, click *Remove*.
- 8 Click *Submit* to commit your changes.

The User Application displays a confirmation message indicating whether the delegate assignment was successfully submitted:



### 12.5.3 Deleting a Delegate Assignment

To delete an existing delegate assignment:

- 1 Click *Remove* next to the assignment:



## 12.6 Viewing and Editing Your Team Proxy Assignments

The *Team Proxy Assignments* action lets you manage the proxy assignment for any of your team members. The rules for defining proxies are:

- ♦ If you are the Team Manager, you might be allowed to define proxies for the members of your team. To define proxies, the Team Manager must have the Configure Proxy permission in the team definition.
- ♦ The Provisioning Administrator has the ability to set proxies for any user, group, or container in the organization.
- ♦ The Provisioning Manager may have the ability to set proxies for any user, group, or container in the organization. To define proxies, the Provisioning Manager must have the Configure Proxy permission.

To assign a proxy for a team member:


- 1 Click *Team Proxy Assignments* in the *Settings>Team Settings* group of actions.

- 2 Click *Select a team* to select a team for which you have been designated as a Team Manager.

If you are a Provisioning Administrator or Provisioning Manager, you do not see the *Select a team* box.

The list of teams includes teams for which team managers are permitted to set proxies, as well as teams for which the ability to set proxies has been disabled. If a particular team definition does not permit Team Managers to set proxies, the manager can still view proxy settings defined for the team members by the administrator or by a manager of another team to which these users belong. However, the Team Manager cannot edit these settings, view details for these settings, or create new proxy assignments.

- 3 Click *Continue*.
- 4 In the *Team Member* selection box, type at least four characters of the user's first name to select the user.

Alternatively, use the *Object Selector* icon  beside the *Team Member* selection box to select a team member. In this case, click the icon to open the Object Lookup window. Specify search criteria for the team member, click *Search*, and select the team member.

- 5 Click *Continue*.

The proxy assignments for the selected team member, if any, are displayed. You can sort the proxy assignments by clicking the *Proxy Assigned* field.

- 6 Click *New*.

The *New* button is only enabled for those teams for which team managers are permitted to set proxies for team members.

- 7 Fill in the fields as follows:

| Field       | Description  |
|-------------|--|
| <i>User</i> | Select the team member for whom you want to assign a proxy. You can select multiple users. |

| Field                                      | Description   |
|--|---|
| <i>Proxy Assigned</i>                      | Select the team member who is to act as proxy.  |
| <i>Notify other users of these changes</i> | Indicates whether you want to send an e-mail message to notify one or more users of this proxy assignment.  |
| <i>Addressee</i>                           | Specifies which users should receive e-mail notifications:<br><br><b>All:</b> Specifies that the user assigned as proxy, as well as the team member(s) for whom the proxy has been assigned, receives e-mail notifications.<br><br><b>Assign From:</b> Specifies that only the team member(s) for whom the proxy has been assigned receives an e-mail notification.<br><br><b>Assign To:</b> Specifies that only the team member who is to act as proxy receives an e-mail notification.<br><br><b>Selective:</b> Allows you to send e-mail notifications to any users you select, including users who are not on the team. |
| <i>Expiration</i>                          | <b>No Expiration:</b> Select <i>No Expiration</i> if you want the proxy assignment to remain in effect until it is removed or modified.<br><br><b>Specify Expiration:</b> Select <i>Specify Expiration</i> to define an <i>End Date</i> . Click the Calendar and select a date and time when the proxy assignment expires.  |

- 8 Click *Submit* to save your selections.

If the assignment is successful, you'll see a message like this:

```
Submission was successful
Changes will be reflected upon the assigned's next login.
```

- 9 Click *Back to Team Proxy Assignments* to create a new or edit an existing proxy assignment.


To change existing proxy assignments:

- 1 Click *Team Proxy Assignments* in the *Settings>Team Settings* group of actions.
- 2 Click *Select a team* to select a team for which you have been designated as a Team Manager.

If you are a Provisioning Administrator or Provisioning Manager, you do not see the *Select a team* box.

The list of teams includes teams for which team managers are permitted to set proxies, as well as teams for which the ability to set proxies has been disabled. If a particular team definition does not permit Team Managers to set proxies, the manager can still view proxy settings defined for the team members by the administrator or by a manager of another team to which these users belong. However, the Team Manager cannot edit these settings, view details for these settings, or create new proxy assignments.

- 3 Click *Continue*.
- 4 In the *Team Member* selection box, type at least four characters of the user's first name to select the user.

Alternatively, use the *Object Selector* icon  beside the *Team Member* selection box to select a team member. In this case, click the icon to open the Object Lookup window. Specify search criteria for the team member, click *Search*, and select the team member.

- 5 Click *Continue*.

The proxy assignments for the selected team member, if any, are displayed.

- 6 To change a proxy assignment, click the edit button next to the assignment you want to modify.



If the team definition does not permit team managers to set proxies, the edit button is disabled.

- 7 Fill in the fields as follows:

| Field                                      | Description  |
|--|--|
| <i>User</i>                                | Select the team member for whom you want to assign a proxy. You can select multiple users.   |
| <i>Proxy Assigned</i>                      | Select the team member who is to act as proxy.   |
| <i>Notify other users of these changes</i> | Indicates whether you want to send an e-mail message to notify one or more users of this proxy assignment.   |
| <i>Addressee</i>                           | Specifies which users should receive e-mail notifications:<br><br><b>All:</b> Specifies that the user assigned as proxy, as well as the team member for whom the proxy has been assigned, receives e-mail notifications.<br><br><b>Assign From:</b> Specifies that only the team member(s) for whom the proxy has been assigned receives an e-mail notification.<br><br><b>Assign To:</b> Specifies that only the team member who is to act as proxy receives an e-mail notification.<br><br><b>Selective:</b> Allows you to send e-mail notifications to any users you select, including users who are not on the team. |
| <i>Expiration</i>                          | <b>No Expiration:</b> Select <i>No Expiration</i> if you want the proxy assignment to remain in effect until it is removed or modified.<br><br><b>Specify Expiration:</b> Select <i>Specify Expiration</i> to define an <i>End Date</i> . Click the Calendar and select a date and time when the proxy assignment expires.   |

- 8 Click *Submit* to save your selections.

If the change was successful, you'll see a message like this:

```
Submission was successful
Changes will be reflected upon the assigned's next login.
```

To delete proxy assignments:

- 1 Click *Team Proxy Assignments* in the *Settings>Team Settings* group of actions.
- 2 To remove a proxy setting, click *Delete*.



You are prompted to confirm the delete. When the deletion is complete, you'll see a confirmation like this:

```
Submission was successful.Changes will be reflected upon the assigned's next
login.
```

---

**NOTE:** As an alternative, you can also delete a proxy assignment during the edit proxy assignment process.

---

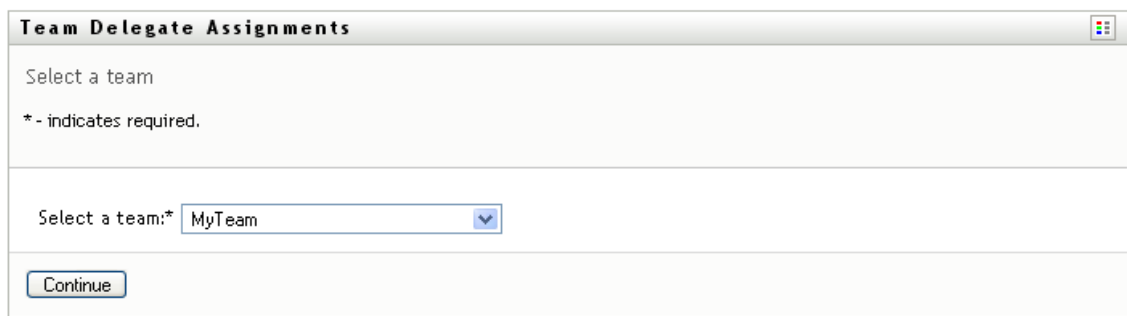
## 12.7 Viewing and Editing Your Team Delegate Assignments

The *Team Delegate Assignments* action allows you to manage the delegate assignments for team members. The rules for defining delegates are as follows:

- ♦ You are allowed to define delegates for the members of a team for which you have been designated as team manager, as long as the team definition gives you this permission. To configure team delegate assignments, the Team Manager must have the Configure Delegate permission.
- ♦ The Provisioning Administrator has the ability to define delegate assignments for any user, group, or container in the organization.
- ♦ The Provisioning Manager may have the ability to set delegates for any user, group, or container in the organization. To define delegates, the Provisioning Manager must have the Configure Delegate permission.

To define a delegate assignment:

- 1 Click *Team Delegate Assignments* in the *Settings>Team Settings* group of actions.
- 2 Click *Select a team* to select a team for which you have been designated as a team manager.




The screenshot shows a dialog box titled "Team Delegate Assignments". Inside the dialog, there is a text label "Select a team" followed by a note "\* - indicates required.". Below this is a dropdown menu with the label "Select a team:\*" and the value "MyTeam" selected. At the bottom of the dialog is a "Continue" button.

If you are a Provisioning Administrator or Provisioning Manager, you do not see the *Select a team* box.

The list of teams includes teams for which team managers are permitted to define delegates (specified in the team request rights), as well as teams for which the ability to set delegates has been disabled. If the team request rights do not permit team managers to define delegates, the manager can still view delegate settings defined for the team members by the administrator or by a manager of another team to which these users belong. However, the team manager cannot edit or delete these settings, view details for these settings, or create new delegate assignments.

If you are a Provisioning Application Administrator, you do not see the *Select a team* box.

- 3 Click *Continue*.
- 4 In the *Team Member* selection box, type at least four characters of the user's first name to select the user.

Alternatively, use the *Object Selector* icon  beside the *Team Member* selection box to select a team member. In this case, click the icon to open the Object Lookup window. Specify search criteria for the team member, click *Search*, and select the team member.

**Team Delegate Assignments**

Select a user to view or edit his or her assigned delegates.

\* - indicates required.

---

Team Member:\*

---

5 Select a team member from the list, and click *Continue*.

Any existing assignments for the team member are displayed.

6 Click *New*.

The *New* button is only enabled for those teams for which team managers are permitted to define delegates for team members.

7 Fill in the fields as follows:

| Field                                      | Description  |
|--|--|
| <i>User</i>                                | Select one or more users whose work you want to delegate.  |
| <i>Assignment Type</i>                     | Assign the user who can perform the delegated work by selecting one of the following: <ul style="list-style-type: none"> <li>◆ <b>Assign Delegate:</b> Select a user from the list.</li> <li>◆ <b>Assign by Relationship:</b> Select the delegate relationship from the drop-down list.</li> </ul>   |
| <i>Notify other users of these changes</i> | Indicates whether you want to send an e-mail message to notify one or more users of this delegate assignment.  |
| <i>Addressee</i>                           | Specifies which users should receive e-mail notifications: <p><b>All:</b> Specifies that the user assigned as delegate, as well as the team member for whom the delegate has been assigned, receives e-mail notifications.</p> <p><b>Assign From:</b> Specifies that only the team member(s) for whom the delegate has been assigned receives an e-mail notification.</p> <p><b>Assign To:</b> Specifies that only the team member who is to act as delegate receives an e-mail notification.</p> <p><b>Selective:</b> Allows you to send e-mail notifications to any users you select, including users who are not on the team.</p> |
| <i>Expiration</i>                          | <p><b>No Expiration:</b> Select <i>No Expiration</i> if you want the delegation to remain in effect until it is removed or modified. This, in effect, makes the delegation permanent.</p> <p><b>Specify Expiration:</b> Select <i>Specify Expiration</i> to define an <i>End Date</i>. Click the Calendar and select a date and time when the delegate assignment expires.</p>   |
| <i>Type of Request</i>                     | Select a category from the list.<br><br>This populates the list of <i>Available Requests</i> in <i>Selected Category</i> .   |



| Field  | Description   |
|--|---|
| <i>Available Requests in Selected Category</i> | Select one or more process requests from this list and click <i>Add</i> .   |
| <i>Selected Requests</i>                       | This list shows the process request types that have been delegated. To remove a request type, select it from the list and click <i>Remove</i> . |

**8** Click *Submit* to save your assignments.

If the save is successful, you'll see a message like this:

```
Submission was successful
Please note that any previous availability settings for users referenced in
processed delegatee assignment will not be updated automatically. Please check
and refresh any existing availability settings for the corresponding users in
order to activate these changes.
```

To modify delegate assignments:

**1** Click *Team Delegate Assignments* in the *Team Settings* group of actions.


**2** Click *Select a team* to select a team for which you have been designated as a team manager.

The list of teams includes teams for which team managers are permitted to define delegates (specified in the team request rights), as well as teams for which the ability to set delegates has been disabled. If the team request rights do not permit team managers to define delegates, the manager can still view delegate settings defined for the team members by the administrator or by a manager of another team to which these users belong. However, the team manager cannot edit or delete these settings, view details for these settings, or create new delegate assignments.

If you are a Provisioning Application Administrator, you do not see the *Select a team* box.

**3** Click *Continue*.

**4** In the *Team Member* selection box, type at least four characters of the user's first name to select the user.

Alternatively, use the *Object Selector* icon  beside the *Team Member* selection box to select a team member. In this case, click the icon to open the Object Lookup window. Specify search criteria for the team member, click *Search*, and select the team member.

The delegate assignments for the selected team member, if any, are displayed.

**5** Select a team member from the list, and click *Continue*.

Any existing assignments for the team member are displayed.

**6** To edit a delegate assignment, click the edit button in the same row as the assignment you want to modify.



If the team request rights do not permit team managers to define delegates, the edit button is disabled.

**7** Fill in the fields as follows:

| Field  | Description   |
|--|---|
| <i>User</i>                                    | Select one or more users whose work you want to delegate.   |
| <i>Assignment Type</i>                         | Assign the user who can perform the delegated work by selecting one of the following: <ul style="list-style-type: none"> <li>♦ <b>Assign Delegate:</b> Select a user from the list.</li> <li>♦ <b>Assign by Relationship:</b> Select the delegate relationship from the drop-down list.</li> </ul>  |
| <i>Notify other users of these changes</i>     | Indicates whether you want to send an e-mail message to notify one or more users of this delegate assignment.   |
| <i>Addressee</i>                               | Specifies which users should receive e-mail notifications: <p><b>All:</b> Specifies that the user assigned as delegate, as well as the team member for whom the delegate has been assigned, receives e-mail notifications.</p> <p><b>Assign From:</b> Specifies that only the team member for whom the delegate has been assigned receives an e-mail notification.</p> <p><b>Assign To:</b> Specifies that only the team member who is to act as delegate receives an e-mail notification.</p> <p><b>Selective:</b> Allows you to send e-mail notifications to any users you select, including users who are not on the team.</p>   |
| <i>Expiration</i>                              | <p><b>No Expiration:</b> Select <i>No Expiration</i> if you want the delegation to remain in effect until it is removed or modified. This, in effect, makes the delegation permanent.</p> <p><b>Specify Expiration:</b> Select <i>Specify Expiration</i> to define an <i>End Date</i>. Click the Calendar and select a date and time when the delegate assignment expires.</p>  |
| <i>Type of Request</i>                         | <p>Select a category from the list.</p> <p>This populates the list of <i>Available Requests</i> in <i>Selected Category</i>.</p> <p>To specify that this delegate assignment applies to all categories, set the type of request for the delegate assignment to <i>All</i>.</p> <div data-bbox="737 1377 1360 1493" style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p>Request Type Selection</p> <p>Select the types of requests for this delegate assignment. Select a Resource Category to display the available requests.</p> <p>Resource Search Criteria: <input type="text" value="All"/></p> </div> <p><b>NOTE:</b> The All option is available only if the Provisioning Administrator has enabled the Allow All Requests option for your application.</p> |
| <i>Available Requests in Selected Category</i> | <p>Select one or more process requests from this list and click <i>Add</i>.</p> <p>The list of provisioning requests includes only those requests that are within the domain of the team. If the team request rights do not permit team managers to define delegates, the provisioning requests associated with the team are not included in the list.</p>  |

| Field                    | Description   |
|--------------------------|---|
| <i>Selected Requests</i> | This list shows the process request types that have been delegated. To remove a request type, select it from the list and click <i>Remove</i> . |

8 Click *Submit* to save your selections.

To delete a delegate assignment:

- 1 Click *Team Delegate Assignments* in the *Settings>Team Settings* group of actions to view assignments delegated to this team member and also assignments delegated away from this team member.
- 2 To remove a delegate assignment, click the delete button in the row of the assignment you want to delete.



You are prompted to confirm the deletion. When the deletion is complete, you'll see a confirmation message.

## 12.8 Specifying Your Team's Availability

The *Team Availability* action allows you to specify the process requests your team members are not available to work on. During the time period when you or your team members are not available, any process requests of that type are forwarded to the delegate's queue.

You can specify availability for each process request individually or globally. You can only specify the availability for users who have delegates already assigned.

- 1 Click *Team Availability* in the *Settings>Team Settings* group of actions.
- 2 Click *Select a team* to select a team for which you have been designated as a team manager.

**Team Availability** ☰

Select a team

\* - indicates required.


---

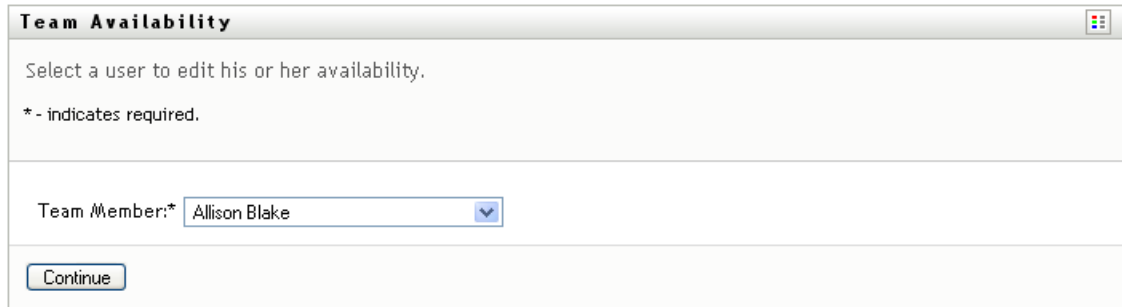
Select a team:\*  ▼

If you are a Provisioning Administrator or Provisioning Manager, you do not see the *Select a team* box.

The list of teams includes teams for which team managers are permitted to define availability (specified in the team definition), as well as teams for which the ability to define availability has been disabled. If the team definition does not permit team managers to define availability, the manager can still view availability settings defined for the team members by the administrator or by a manager of another team to which these users belong. However, the team manager cannot edit or delete these settings, view details for these settings, or create new availability assignments.

- 3 Click *Continue*.
- 4 In the *Team Member* selection box, type at least four characters of the user's first name to select the user.

Alternatively, use the *Object Selector* icon  beside the *Team Member* selection box to select a team member. In this case, click the icon to open the Object Lookup window. Specify search criteria for the team member, click *Search*, and select the team member.



The availability settings for the selected team member, if any, are displayed.

- 5 To see details about a particular resource associated with an availability assignment, click the name of the resource:

### Resource

[Enable Active Directory Account](#)

The page then displays a pop-up window that provides information about the delegate assignment:



This information is particularly helpful in situations where the same resource name appears more than once in the availability settings list.

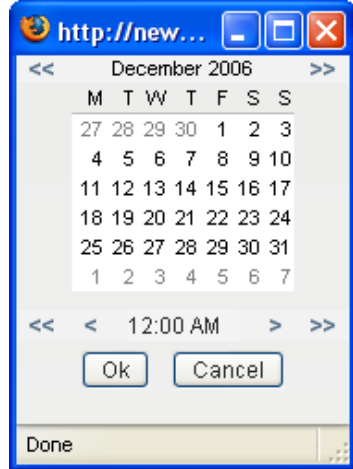
- 6 Click *New*.  
The *New* button is enabled only for those teams for which team managers are permitted to define availability settings for team members.
- 7 Specify the status by selecting one of the options in the *Change Status* drop-down list:

| Status                     | Description   |
|----------------------------|---|
| Available for ALL Requests | This is the default status. It indicates that the team member is globally available. When this status is in effect, requests assigned to the team member are not delegated, even if there are delegates assigned.<br><br><b>NOTE:</b> If you change the status and then change it back to <i>Available for ALL Requests</i> , any <i>Selectively Available</i> settings previously defined are removed. |

| Status                               | Description  |
|--------------------------------------|--|
| NOT Available for ANY Requests       | <p>Specifies that the team member is not available for any process requests currently in the system. (This is also known as globally unavailable.)</p> <p>Choosing this status indicates that the team member is unavailable for each existing delegate assignment and changes the current status to <i>Not Available for Specified Requests</i>.</p> <p>Assignments are effective immediately and last until the delegate assignment expires.</p> <p><b>NOTE:</b> This setting does not affect availability for new assignments created after this point.</p> |
| NOT Available for Specified Requests | <p>When you select this option, you are prompted to specify the team member's availability. (This is the same as clicking the <i>New</i> button.) You'll be prompted to specify:</p> <ul style="list-style-type: none"> <li>◆ The types of requests the team member is not available for.</li> <li>◆ The time period when the team member is unavailable.</li> </ul> <p>During the time period when the team member is unavailable for a particular request, the user delegated to act on that request can work on it.</p>                                     |

**8** Specify the time period when the team member is unavailable:

- 8a** Specify when the time period begins by typing the start date and time in the *Unavailable From* box, or by clicking the calendar and selecting the date and time.



- 8b** Specify when the time period ends by clicking one of the following:

| Button                  | Description   |
|-------------------------|---|
| <i>No Expiration</i>    | Indicates that this unavailability setting does not expire.   |
| <i>Specify Duration</i> | Lets you specify the time period in weeks, days, or hours.  |
| <i>Specify End Date</i> | Lets you specify the end date and time. You can type the date and time, or click the calendar and select the date and time from the calendar. |

- Specify whether you want to send e-mail notifications to other users by filling in these fields:

| Field                                      | Description   |
|--|---|
| <i>Notify other users of these changes</i> | Indicates whether you want to send an e-mail message to notify one or more users of this availability assignment.   |
| <i>Addressee</i>                           | Specifies which users should receive e-mail notifications:<br><br><b>Selective:</b> Allows you to send e-mail notifications to any users you select, including users who are not on the team. |

- Select one or more requests in the *Types of Requests* list box, then click *Add*.

On this page, you select the types of requests that the team member does not accept during the unavailable period. This has the effect of delegating these requests to other users.

Each request you add is included in the *Declined for the Specified Period* list box.

If you add multiple requests for this time period, each request is treated as an individual object that can be edited separately.

- To indicate that this availability setting applies to all request types, click *All Request Types* instead of selecting the request types individually.

All Request Types

The *All Request Types* check box is only available when the type of request for the delegate assignment is set to *All*.

- To remove a request from the list, click *Remove*.
- Click *Submit* to save your changes.

## 12.9 Making a Team Process Request

The *Make Team Process Request* action enables you to make process requests for team members.

- Click *Make Team Process Request* in the *Settings>Team Settings* group of actions.

The *Make Team Process Requests* page is displayed.


- Click *Select a team* to select a team for which you have been designated as a Team Manager. Then click *Continue*.

The application displays a page that lets you pick a category.

- 3 Select the category of the request in the *Type of Request* drop-down list. Select *All* to include requests from all available categories.
- 4 Click *Continue*.

The Make Team Process Requests page displays a list of processes that you can request. The list includes only those processes for which Team Managers are permitted to initiate requests.

- 5 Click a resource name to select it.
- 6 Click a *Recipient* name to select it. The team member you select is the recipient for the request.

Depending on how the team was defined, you might see an *Object Selector* icon  beside the *Recipient* selection box, instead of a list of team members. In this case, click the icon to open the Object Lookup window. Specify search criteria for the team member, click *Search*, and select the team member.

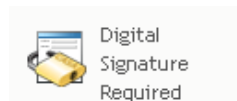
The *History* icon will also appear, if you are a Provisioning Manager or a Provisioning Administrator. Otherwise, this icon is not available.

If the *flow strategy* for the workflow has been defined to support multiple recipients, the application lets you pick a group, container, or team as the recipient. Depending on how the workflow is configured, the User Application might spawn a separate workflow for each recipient (so that the request can be approved or denied independently for each recipient), or initiate a single flow that includes multiple provisioning steps, one for each recipient. In the latter case, the approval or denial of the request applies to all recipients.

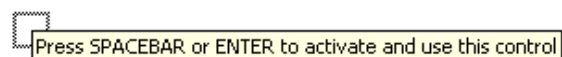
- 7 Click *Continue*.
- 8 The Make Team Process Request page displays the request form. Fill in the fields on the request form. In the following example, the only required field is *Reason for request*.

The fields on the form vary according to the process you requested.

If your administrator has configured your system for digital signatures, and the process you've requested requires a digital signature, the *Digital Signature Required* icon appears in the upper right corner of the page.



In addition, on Internet Explorer, a message appears indicating that you need to press the Spacebar or the Enter key to activate the digital signature applet:



- 9 If you're making a request that requires a digital signature, perform these steps:
  - 9a If you're using a smart card, insert the smart card into the smart card reader.
  - 9b On Internet Explorer, press the Spacebar or the Enter key to activate the applet.

At this point, your browser might display a security warning message.
  - 9c Click *Run* to proceed.
  - 9d Fill in the fields in the initial request form. The fields on the form vary depending on which resource you requested.
  - 9e Click the check box next to the digital signature confirmation message to indicate that you are ready to sign.

The digital signature confirmation message varies depending on how the provisioning resource was configured by the administrator.

The applet then displays a pop-up window that allows you to select a certificate. The pop-up window lists certificates imported to the browser as well as certificates imported to the smart card (if one is currently connected).

| Issued To /                                      | Issued By | Expiration ... | Intended ... |
|--|-----------|----------------|--------------|
| O=novell,OU=idmsample-lumberg,OU=users,CN=ablake | O=SL      | 09.10.2008     | <All>        |
| O=novell,OU=idmsample-tdb,OU=users,CN=jmiller    | O=SI      | 26.10.2008     | <All>        |

- 9f** Select the certificate you want to use and click *Select*.
- 9g** If you select a certificate that has been imported into your browser, you need to type the password for the certificate in the *Password* field on the request form.
- 9h** If you select a certificate that has been imported to your smart card, type the PIN for your smart card and click *OK*.

You do not need to type the password for the certificate if you're using a smart card, because the certificate password has already been transmitted to the card.



If your administrator has enabled the ability to preview the user agreement, the *Preview* button is enabled.



- 9i** Click *Preview* to see the user agreement.  
If the digital signature type is set to Form, a PDF document is displayed. If the digital signature type is set to data, an XML document is displayed.
- 10** Click *Submit*.

A workflow starts for the user.

The Make Team Process Request page displays a status message indicating whether the request was submitted successfully.

If your request requires permission from one or more individuals in an organization, the request starts one or more workflows to obtain those approvals.



---

# 13 Making a Process Request

This section provides information about making process requests. Topics include:

- ♦ [Section 13.1, “About Process Requests,” on page 209](#)
- ♦ [Section 13.2, “Making a Process Request,” on page 210](#)
- ♦ [Section 13.3, “Deep Linking to a Request,” on page 213](#)

## 13.1 About Process Requests

The *Make a Process Request* menu allows you to initiate a process request (also known as a provisioning request). The *Make a Process Request* menu does not allow you to make attestation, resource, or role requests. The interface for submitting these requests depends on the type of request you want to make, as described below:

- ♦ To make an attestation request, you need to use the *Attestation Requests* actions on the *Compliance* tab.
- ♦ To make a resource request, you need to use the *Resource Assignments* section of the *Work Dashboard* tab, or the *Resource Catalog* on the *Roles and Resources* tab.
- ♦ To make a role request, you need to use the *Role Assignments* section of the *Work Dashboard* tab, or the *Role Catalog* on the *Roles and Resources* tab.

The list of process requests shown on the *Make a Process Request* menu depends on which user is currently logged in to the User Application:

- ♦ If you are a Provisioning Administrator (Domain Administrator for the Provisioning Domain), you are able to select any process request.
- ♦ If you are a Provisioning Manager (Domain Manager for the Provisioning Domain), you see only those requests for which you have been given appropriate permissions.
- ♦ If you are a Team Manager, you see only those requests for which you have been given appropriate permissions.

Before selecting a process request, you need to select a category. The list of categories includes all categories.

---

**NOTE:** By default, the list includes the Attestations and Roles categories. These categories do not give you the ability to initiate standard, out-of-the-box attestation or role assignment requests. Instead, these categories are included to allow your administrator to define custom process requests that perform special attestation or role-based functions.

---

When you initiate the request, the User Application displays the initial request form. This form lets you specify all of the information needed for the request.

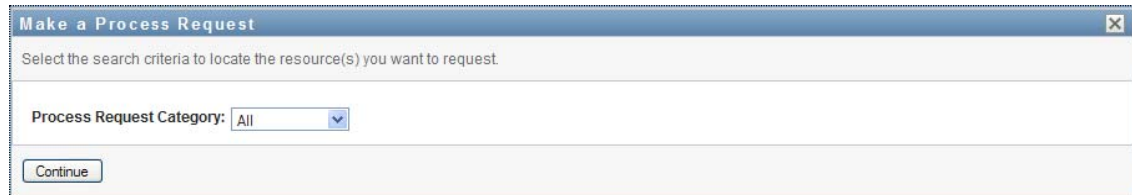
When a process request is submitted, the request starts a workflow. The workflow coordinates the approvals needed to fulfill the request. Some process requests require approval from a single individual; others require approval from several individuals. In some instances, a request can be fulfilled without any approvals.

## 13.2 Making a Process Request

To make a process request:

- 1 Click *Make a Process Request* in the User Profile section of the Work Dashboard.

The Make a Process Request page is displayed.



- 2 Select the category of the request in the *Process Request Category* drop-down list. Select *All* to include requests from all available categories.

- 3 Click *Continue*.

The Make a Process Request page displays a list of process requests available to the current user.

The User Application enforces security constraints to ensure that you see only those request types to which you have access rights.

- 4 Select the desired process by clicking the process name.

The Make a Process Request page displays the initial request form.

If your administrator has configured your system for digital signatures, and the process you've requested requires a digital signature, the *Digital Signature Required* icon appears in the upper right corner of the page. In addition, on Internet Explorer, a message appears indicating that you need to press the Spacebar or the Enter key to activate the digital signature applet.

- 5 If you're making a request that requires a digital signature, perform these steps:

- 5a If you're using a smart card, insert the smart card into the smart card reader.

- 5b On Internet Explorer, press the Spacebar or the Enter key to activate the applet.

At this point, your browser might display a security warning message.

- 5c Click *Run* to proceed.

- 5d Fill in the fields in the initial request form. The fields on the form vary depending on which resource you requested.

- 5e Click the check box next to the digital signature confirmation message to indicate that you are ready to sign.

The digital signature confirmation message varies depending on how the provisioning resource was configured by the administrator.

The applet then displays a pop-up window that allows you to select a certificate. The pop-up window lists certificates imported to the browser as well as certificates imported to the smart card (if one is currently connected).

| Issued To /                                      | Issued By | Expiration ... | Intended ... |
|--|-----------|----------------|--------------|
| O=novell,OU=idmsample-lumberg,OU=users,CN=ablake | O=SL      | 09.10.2008     | <All>        |
| O=novell,OU=idmsample-tdb,OU=users,CN=jmiller    | O=SI      | 26.10.2008     | <All>        |

- 5f Select the certificate you want to use and click *Select*.
- 5g If you select a certificate that has been imported into your browser, you need to type the password for the certificate in the *Password* field on the request form.
- 5h If you select a certificate that has been imported to your smart card, type the PIN for your smart card and click *OK*.

You do not need to type the password for the certificate if you're using a smart card, because the certificate password has already been transmitted to the card.



If your administrator has enabled the ability to preview the user agreement, the *Preview* button is enabled.

Step 3 of 3: Confirm and complete resource request.  
\* - indicates required.

Digital Signature Required

Resource: digsigtest  
Recipient: Jack Miller  
Resource Search Criteria: Entitlements  
Description: asf

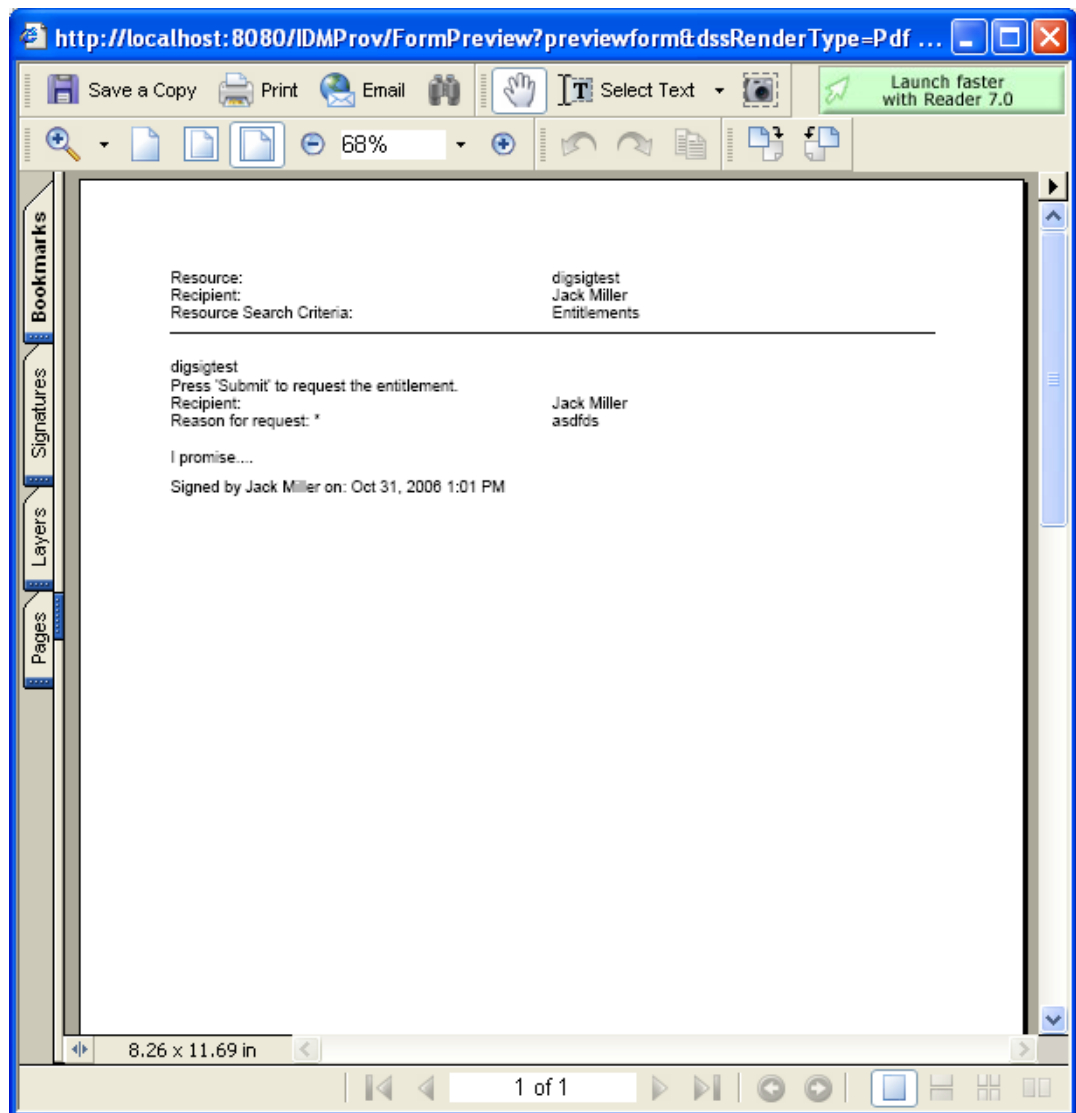
Form Detail  
Gathering data to sign ...  
Form signature successfully attached

**digsigtest**  
Press "Submit" to request the entitlement.

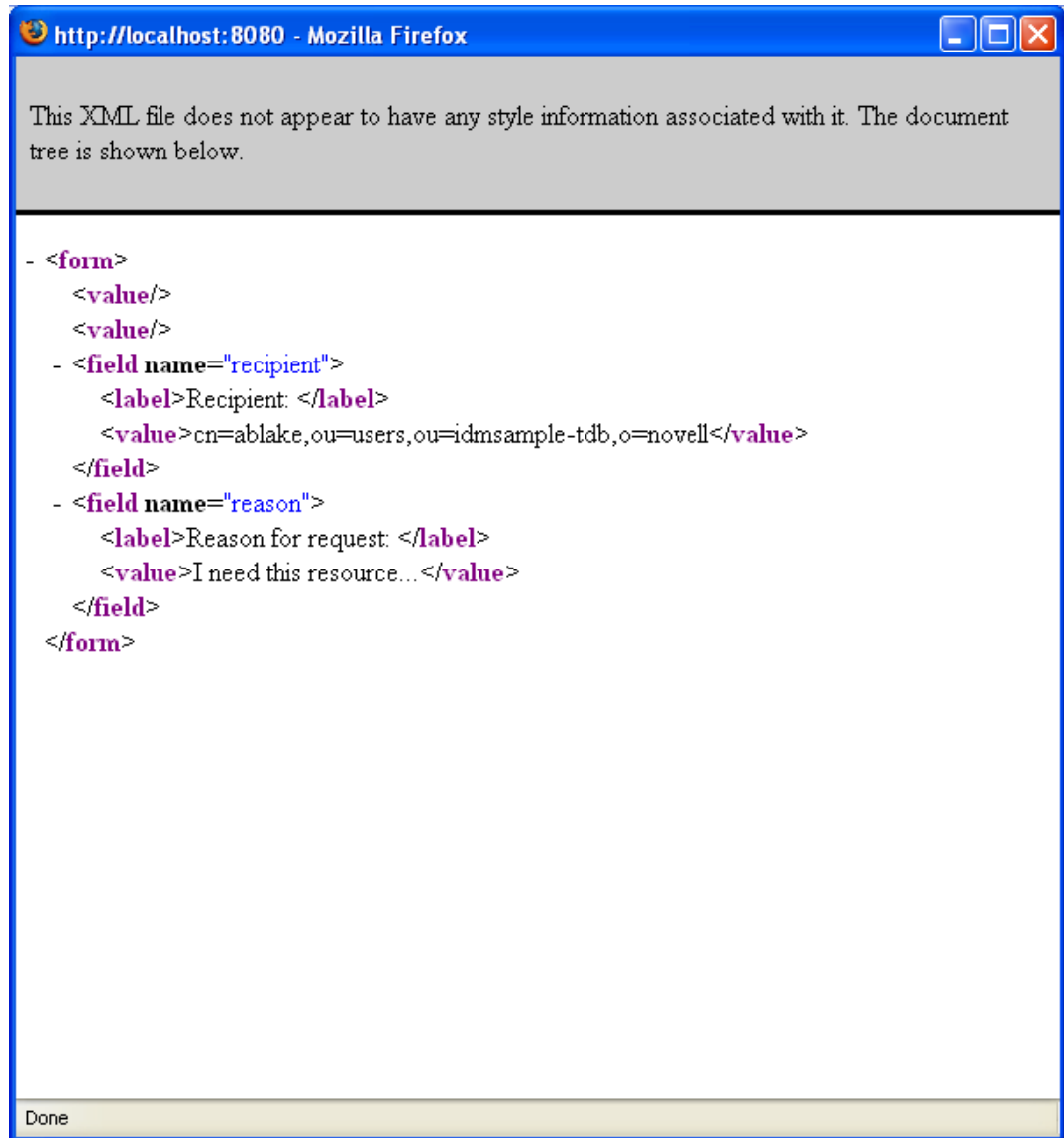
Recipient: Jack Miller  
Reason for request: \*

I promise...

- 5i Click *Preview* to see the user agreement.
- If the digital signature type is set to Form, a PDF document is displayed.



If the digital signature type is set to data, an XML document is displayed.



6 If the request you're making does not require a digital signature, simply fill in the fields on the initial request form. The fields on the form vary depending on which resource you requested.

7 Click *Submit*.

The Make a Process Request page displays a status message indicating whether the request was submitted successfully.

## 13.3 Deep Linking to a Request

The User Application provides the ability to deep link to a specific process request (also known as a provisioning request) for the current user. This feature gives a manager the ability to send a specific process request URL to an employee, so this employee can request the process quickly without having to go through the User Application interface.

When you deep link to a process request, the request form is displayed in the body of the page, along with the header for the User Application:

The screenshot displays the Novell Identity Manager web interface. At the top, the header includes the logo and the text 'Novell Identity Manager' on the left, and the date 'Wednesday, February 25, 2009' on the right. Below the header is a navigation menu with tabs for 'Identity Self-Service', 'Work Dashboard', 'Roles', 'Compliance', 'Administration', 'Logout', and 'Help'. The 'Work Dashboard' tab is currently selected. The main content area is titled 'EmailChange-B' and shows the following details:

- Recipient: Application Administrator Of Sample Data
- Description: EmailChange-B Process Request Category: Accounts

Below this information is a 'Form Detail' section. It starts with a note: '\* - indicates required.' The form is titled 'Email Change' and includes the instruction: 'Press 'Submit' to request the entitlement.' The form fields are:

- Recipient: Application Administrator Of Sample Data
- Reason for request: \* (text input field)
- Current Email Address: (text input field)
- New Email Address: (text input field)

At the bottom of the form are two buttons: 'Submit' and 'Cancel'.

Once a request is made, it appears in the list of requests that the requester sees in the Work Dashboard under *Request Status*. In addition, the approver sees the task in the Work Dashboard under *Task Notifications*.

The URL used for deep linking to a process request takes this form:

```
http://<server:port>/IDMProv/makeRequestDetail.do?requestId=<PRD ID>&requestType=<request type>
```

The *<PRD ID>* must specify a DN for a provisioning request definition or a unique ID for a role or resource. The *<request type>* must be PROV.

Here's an example that shows what the URL one might use to deep link to a provisioning request definition:

```
http://testserver:8080/IDMProv/makeRequestDetail.do?requestId=cn=EmailChange,cn=RequestDefs,cn=AppConfig,cn=PicasoDriver,cn=TestDrivers,o=novell&requestType=PROV
```

# 14 Launching the Identity Reporting Module

This section provides instructions for launching the Identity Reporting Module from the User Application. Topics include:

- ♦ [Section 14.1, “About the Identity Reporting Module,” on page 215](#)
- ♦ [Section 14.2, “Accessing the Reporting Module,” on page 215](#)

## 14.1 About the Identity Reporting Module

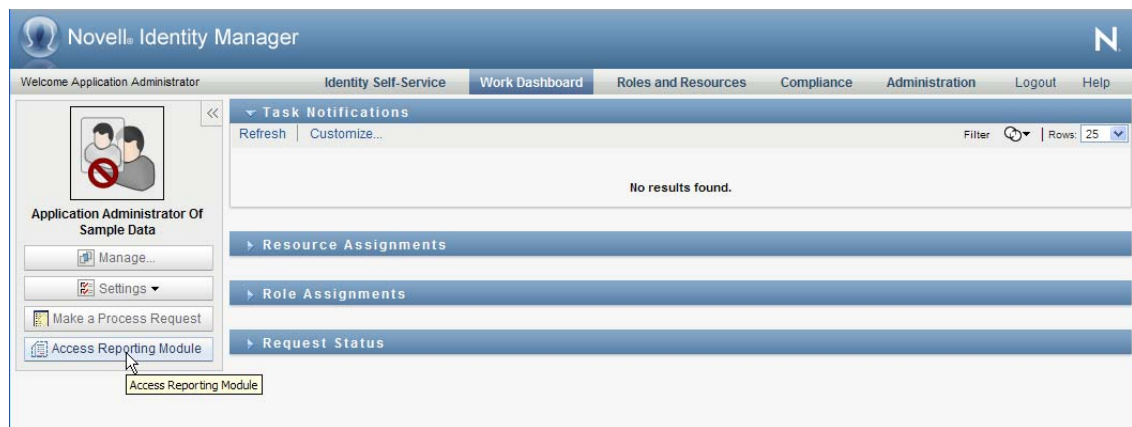
The Identity Reporting Module gives you the ability to generate reports that show information about various aspects of your Identity Manager configuration, including information collected from one or more Identity Vaults or Managed Systems. The reporting module provides a set of predefined report definitions you can use to generate reports. In addition, it gives the option to import custom reports defined in a third-party tool.

You can access the reporting module directly or launch it from the *Work Dashboard* within the User Application. If you want to be able to launch it from the *Work Dashboard*, you need to have your Configuration Administrator specify the URL for the reporting module on the *Administration* tab. The Configuration Administrator needs to specify the URL in the *Novell Identity Manager Reporting Module URL* field within the *Provisioning UI Display Settings* page. In addition, you need to have the *Access Reporting Module* navigation permission. The Report Administrator is given this permission by default.

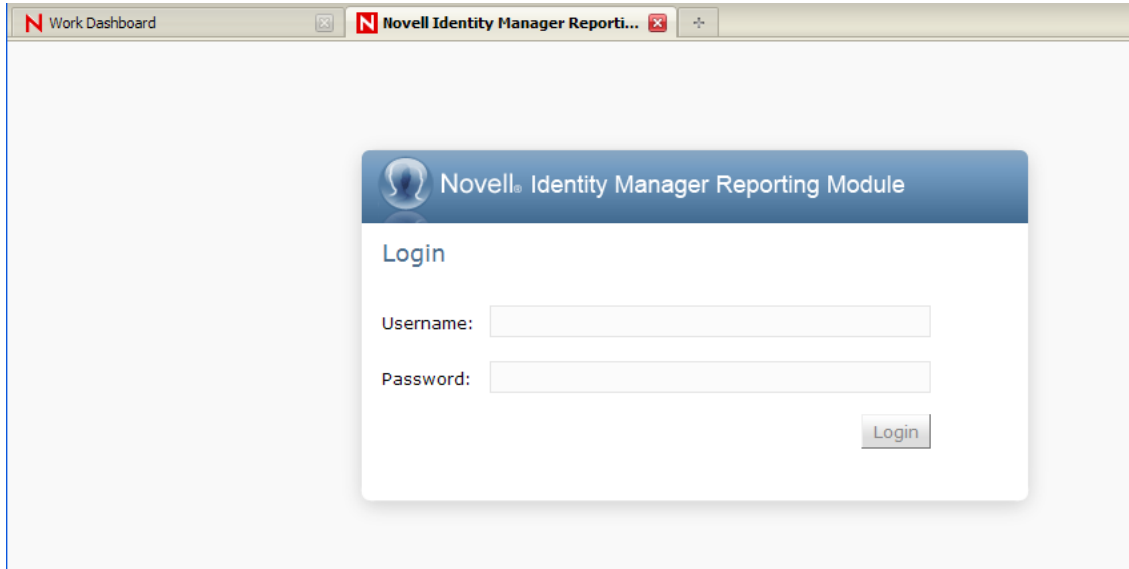
## 14.2 Accessing the Reporting Module

To access the Identity Reporting Module from the User Application:

- 1 Log into the User Application as a Report Administrator.
- 2 Click *Access Reporting Module* in the User Profile section of the Work Dashboard:



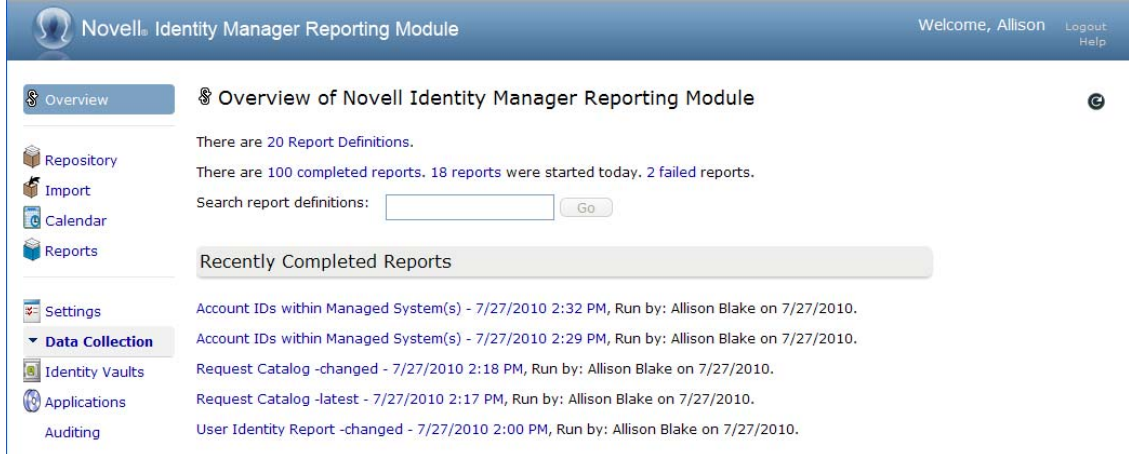
When you click this button, the login window for the reporting module opens in a new window:



**Single Sign-On (SSO) Behavior** When Single Sign-On (SSO) is enabled for the Roles Based Provisioning Module, you do not see the Login page. Instead, you are logged into the reporting module automatically.

- 3 If SSO has not been enabled, login as a Report Administrator or other user that has the *Access Reporting Module* navigation permission.

The reporting module displays the *Overview* page:





---

# IV Using the Roles and Resources Tab

These sections tell you how to use the *Roles and Resources* tab of the Identity Manager User Application.

- ♦ [Chapter 15, “Introducing Roles and Resources,” on page 219](#)
- ♦ [Chapter 16, “Managing Roles in the User Application,” on page 233](#)
- ♦ [Chapter 17, “Managing Resources in the User Application,” on page 251](#)
- ♦ [Chapter 18, “Managing Separation of Duties in the User Application,” on page 271](#)
- ♦ [Chapter 19, “Creating and Viewing Reports,” on page 275](#)
- ♦ [Chapter 20, “Configuring the Role and Resource Settings,” on page 287](#)



---

# 15 Introducing Roles and Resources

This chapter provides an overview of the *Roles and Resources* tab. Topics include:

- ♦ [Section 15.1, “About the Roles and Resources Tab,” on page 219](#)
- ♦ [Section 15.2, “Accessing the Roles and Resources Tab,” on page 227](#)
- ♦ [Section 15.3, “Exploring the Tab’s Features,” on page 227](#)
- ♦ [Section 15.4, “Roles and Resources Actions You Can Perform,” on page 228](#)
- ♦ [Section 15.5, “Understanding the Icons Used on the Roles and Resources Tab,” on page 229](#)

## 15.1 About the Roles and Resources Tab

The purpose of the *Roles and Resources* tab is to give you a convenient way to perform roles-based provisioning actions. These actions allow you to manage role definitions and role assignments within your organization, as well as resource definitions and resource assignments. Role assignments can be mapped to resources within a company, such as user accounts, computers, and databases. Alternatively, resources may be assigned directly to users. For example, you might use the *Roles and Resources* tab to:

- ♦ Make role and resource requests for yourself or other users within your organization
- ♦ Create roles and role relationships within the roles hierarchy
- ♦ Create separation of duties (SoD) constraints to manage potential conflicts between role assignments
- ♦ Look at reports that provide details about the current state of the Role Catalog and the roles currently assigned to users, groups, and containers

When a role or resource assignment request requires permission from one or more individuals in an organization, the request starts a workflow. The workflow coordinates the approvals needed to fulfill the request. Some assignment requests require approval from a single individual; others require approval from several individuals. In some instances, a request can be fulfilled without any approvals.

---

**NOTE:** Role approvals are triggered for explicit role-to-user assignments only.

---

When a role assignment request results in a potential separation of duties conflict, the initiator has the option to override the separation of duties constraint, and provide a justification for making an exception to the constraint. In some cases, a separation of duties conflict can cause a workflow to start. The workflow coordinates the approvals needed to allow the separation of duties exception to take effect.

Your workflow designer and system administrator are responsible for setting up the contents of the *Roles and Resources* tab for you and the others in your organization. The flow of control for a workflow, as well as the appearance of forms, can vary depending on how the approval definition for the workflow was defined in the Designer for Identity Manager. In addition, what you can see and do is typically determined by your job requirements and your level of authority.

---

**NOTE:** The *Roles and Resources* tab is available only with Identity Manager 4.0.2 Advanced Edition. Standard Edition does not support this feature.

---

## 15.1.1 About Roles

This section provides an overview of terms and concepts used in the *Roles and Resources* tab:

- ♦ [“Roles and Role Assignments” on page 220](#)
- ♦ [“Roles Catalog and Role Hierarchy” on page 221](#)
- ♦ [“Separation of Duties” on page 223](#)
- ♦ [“Roles Reporting and Auditing” on page 223](#)
- ♦ [“Roles Security” on page 224](#)
- ♦ [“Role and Resource Service Driver” on page 225](#)

### Roles and Role Assignments

A *role* defines a set of permissions related to one or more target systems or applications. The *Roles and Resources* tab allows users to request *role assignments*, which are associations between a role and a user, group, or container. The *Roles and Resources* tab also allows you to define *role relationships*, which establish associations between roles in the roles hierarchy.

You can assign roles directly to a user, in which case these *direct assignments* give a user explicit access to the permissions associated with the role. You can also define *indirect assignments*, which allow users to acquire roles through membership in a group, container, or related role in the role hierarchy.

---

**NOTE:** Role approvals are triggered for explicit role to user assignments only.

---

When you request a role assignment, you have the option to define a *role assignment effective date*, which specifies the date and time when the assignment takes effect. If you leave this blank, it means the assignment is immediate.

You can also define a *role assignment expiration date*, which specifies the date and time when the assignment will automatically be removed.

When a user requests a role assignment, the Role and Resource Subsystem manages the life cycle of the role request. To see which actions have been taken on the request by users or by the subsystem itself, you can check the status of the request on the *Request Status* tab in the *Role Catalog*.

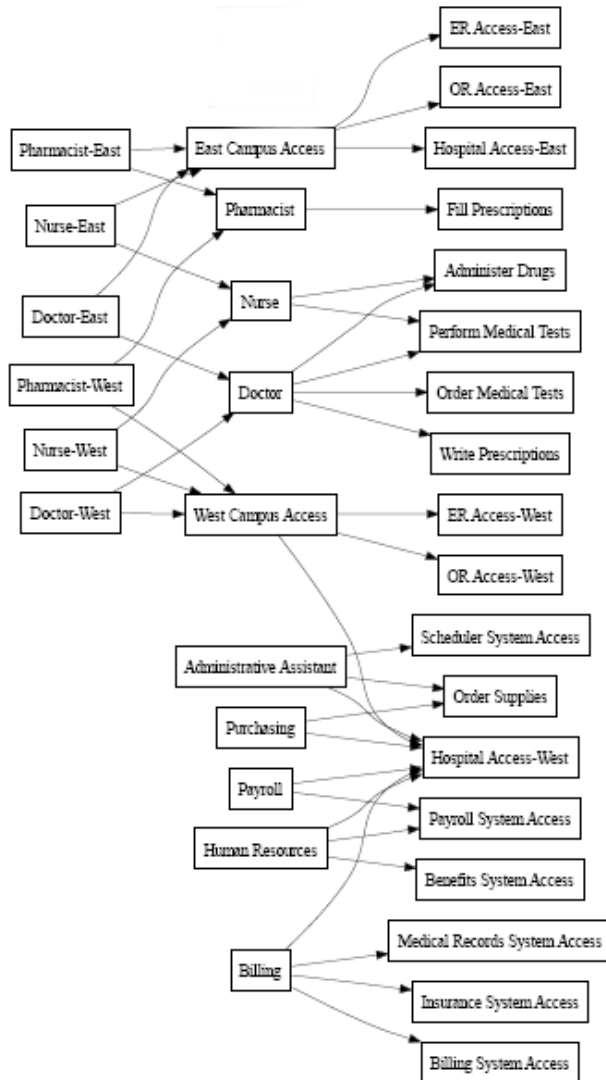
## Roles Catalog and Role Hierarchy

Before users can begin assigning roles, these roles must be defined in the *Role Catalog*. The *Role Catalog* is the storage repository for all role definitions and supporting data needed by the Role and Resource Subsystem. To set up the *Role Catalog*, a Role Module Administrator (or Role Manager) defines the roles and the roles hierarchy.

The *roles hierarchy* establishes relationships between roles in the catalog. By defining role relationships, you can simplify the task of granting permissions through role assignments. For example, instead of assigning 50 separate medical roles each time a doctor joins your organization, you can define a Doctor role and specify a role relationship between the Doctor role and each of the medical roles. By assigning users to the Doctor role, you can give these users the permissions defined for each of the related medical roles.

The roles hierarchy supports three levels. Roles defined at the highest level (called Business Roles) define operations that have business meaning within the organization. Mid-level roles (called IT Roles) supports technology functions. Roles defined at the lowest level of the hierarchy (called Permission Roles) define lower-level privileges. The following example shows a sample role hierarchy with three levels for a medical organization. The highest level of the hierarchy is on the left and the lowest level is on the right:

**Figure 15-1** Sample Roles Hierarchy



A higher-level role automatically includes privileges from the lower-level roles that it contains. For example, a Business Role automatically includes privileges from the IT Roles that it contains. Similarly, an IT Role automatically includes privileges from the Permission Roles that it contains.

Role relationships are not permitted between peer roles within the hierarchy. In addition, lower-level roles cannot contain higher-level roles.

When you define a role, you can optionally designate one or more owners for that role. A *role owner* is a user who is designated as the owner of the role definition. When you generate reports against the Role Catalog, you can filter these reports based on the role owner. The role owner does not automatically have the authorization to administer changes to a role definition. In some cases, the owner must ask a role administrator to perform any administration actions on the role.

When you define a role, you can optionally associate the role with one or more role categories. A *role category* allows you to categorize roles for the purpose of organizing the roles system. After a role has been associated with a category, you can use this category as a filter when browsing the Role Catalog.

If a role assignment request requires approval, the role definition specifies details about the workflow process used to coordinate approvals, as well as the list of approvers. The approvers are those individuals who can approve or deny a role assignment request.

## Separation of Duties

A key feature of the Role and Resource Subsystem is the ability to define *separation of duties (SoD) constraints*. A separation of duties (SoD) constraint is a rule that defines two roles that are considered to be in conflict. The Security Officers create the separation of duties constraints for an organization. By defining SoD constraints, these officers can prevent users from being assigned to conflicting roles, or maintain an audit trail to keep track of situations where violations have been allowed. In a separation of duties constraint, the conflicting roles must be at the same level in the roles hierarchy.

Some separation of duties constraints can be overridden without approval, whereas others require approval. Conflicts that are permitted without approval are referred to as *separation of duties violations*. Conflicts that have been approved are referred to as *separation of duties approved exceptions*. The Role and Resource Subsystem does not require approvals for SoD violations that result from indirect assignments, such as membership in a group or container, or role relationships.

If a separation of duties conflict requires approval, the constraint definition specifies details about the workflow process used to coordinate approvals, as well as the list of approvers. The approvers are those individuals that can approve or deny an SoD exception. A default list is defined as part of the Role and Resource Subsystem configuration. However, this list can be overridden in the definition of an SoD constraint.

## Roles Reporting and Auditing

The Role and Resource Subsystem provides a rich reporting facility to help auditors analyze the Role Catalog, as well as the current state of role assignments and SoD constraints, violations, and exceptions. The roles reporting facility allows Roles Auditors and Roles Module Administrators to display the following types of reports in PDF format:

- ◆ Role List Report
- ◆ Role Detail Report
- ◆ Role Assignment Report
- ◆ SoD Constraint Report
- ◆ SoD Violation and Exception Report
- ◆ User Roles Report
- ◆ User Entitlements Report

In addition to providing information through the reporting facility, the Role and Resource Subsystem can be configured to log events to Novell or OpenXDAS auditing clients.

## Roles Security

The Role and Resource Subsystem uses a set of system roles to secure access to functions within the *Roles and Resources* tab. Each menu action in the *Roles and Resources* tab is mapped to one or more of the system roles. If a user is not a member of one of the roles associated with an action, the corresponding menu item is not displayed on the *Roles and Resources* tab.

The *system roles* are administrative roles automatically defined by the system at install time for the purpose of delegated administration. These include the following:

- ◆ Roles Administrator
- ◆ Roles Manager

The system roles are described in detail below:

**Table 15-1** *System Roles*

| <b>Role</b>         | <b>Description</b>  |
|---------------------|---|
| Roles Administrator | <p>A system role that allows members to create, remove, or modify all roles, and grant or revoke any role assignment to any user, group, or container. This role also allows members to run any report for any user. A person in this role can perform the following functions in the User Application with unlimited scope:</p> <ul style="list-style-type: none"><li>◆ Create, remove, and modify roles.</li><li>◆ Modify role relationships for roles.</li><li>◆ Request assignment of users, groups or containers to roles.</li><li>◆ Create, remove, and modify SoD constraints.</li><li>◆ Browse the Role Catalog.</li><li>◆ Configure the Role and Resource Subsystem.</li><li>◆ View the status of all requests.</li><li>◆ Retract role assignment requests.</li><li>◆ Run any and all reports.</li></ul>   |
| Roles Manager       | <p>A system role that allows members to modify roles and role relationships, and grant or revoke role assignments for users. A person in this role is able to perform the following functions in the User Application and is limited in scope by directory browse rights to the role objects:</p> <ul style="list-style-type: none"><li>◆ Create new roles and modify existing roles to which the user has browse rights.</li><li>◆ Modify role relationships for roles to which the user has browse rights.</li><li>◆ Request assignment of users, groups, or containers to roles to which the user has browse rights.</li><li>◆ Browse the Role Catalog (limited in scope by browse rights).</li><li>◆ Browse role assignment requests for users, groups, and containers (limited in scope by directory browse rights to role, user, group, and container objects).</li><li>◆ Retract role assignment requests for users, groups, and containers (limited in scope by directory browse rights to role, user, group, and container objects).</li></ul> |



## Authenticated user

In addition to supporting the system roles, the Role and Resource Subsystem also allows access by authenticated users. An authenticated user is a user logged in to the User Application who does not have any special privileges through membership in a system role. A typical authenticated user can perform any of the following functions:

- ♦ View all roles that have been assigned to the user.
- ♦ Request assignment (for himself or herself only) to roles to which he or she has browse rights.
- ♦ View request status for those requests for which he or she is either a requester or recipient.
- ♦ Retract role assignment requests for those requests for which he or she is both requester and recipient.

## Role and Resource Service Driver

The Role and Resource Subsystem uses the Role and Resource Service driver to manage back-end processing of roles. For example, it manages all role assignments, starts workflows for role assignment requests and SoD conflicts that require approvals, and maintains indirect role assignments according to group and container membership, as well as membership in related roles. The driver also grants and revokes entitlements for users based on their role memberships, and performs cleanup procedures for requests that have been completed.

**What happens when entitlements change for a resource** If you change the entitlement for an existing resource, the driver does not grant the new entitlement for users who are currently assigned the resource. To grant the new entitlement, you need to remove and reassign the resource to the users who need the entitlement.

For details on the Role and Resource Service driver, see the *Identity Manager User Application: Administration Guide* (<http://www.netiq.com/documentation/idm402/index.html>).

## 15.1.2 About Resources

This section provides an overview of resource management terms and concepts used in the User Application.

### About Resource-Based Provisioning

The purpose of the resource functionality within the User Application is to give you a convenient way to perform resource-based provisioning actions. These actions allow you to manage resource definitions and resource assignments within your organization. Resource assignments can be mapped to users or to roles within a company. For example, you might use resources to:

- ♦ Make resource requests for yourself or other users within your organization
- ♦ Create resources and map them to entitlements

When a resource assignment request requires permission from one or more individuals in an organization, the request starts a workflow. The workflow coordinates the approvals needed to fulfill the request. Some resource assignment requests require approval from a single individual; others require approval from several individuals. In some instances, a request can be fulfilled without any approvals.

The following business rules govern the behavior of resources within the User Application:

- ◆ Resources can only be assigned to a user. This does not preclude a resource being granted to users in a container or group based on implicit role assignment. However, the resource assignment will only be associated with a user.
- ◆ Resources can be assigned in any of the following ways:
  - ◆ Directly by a user through UI mechanisms
  - ◆ Through a provisioning request
  - ◆ Through a role request assignment
  - ◆ Through a Rest or SOAP interface
- ◆ The same resource can be granted to a user multiple times (if this capability has been enabled in the resource definition).
- ◆ A resource definition can have no more than one entitlement bound to it.
- ◆ A resource definition can have one or more same-entitlement references bound to it. This capability provides support for entitlements where the entitlement parameters represent provisionable accounts or permissions on the connected system.
- ◆ Entitlement and decision support parameters can be specified at design time (static) or at request time (dynamic).

Your workflow designer and system administrator are responsible for setting up the User Application for you and the others in your organization. The flow of control for a resource-based workflow, as well as the appearance of forms, can vary depending on how the approval definition for the workflow was defined in the Designer for Identity Manager. In addition, what you can see and do is typically determined by your job requirements and your level of authority.

## Resources

A *resource* is any digital entity such as a user account, computer, or database that a business user needs to be able to access. The User Application provides a convenient way for end users to request the resources they need. In addition, it provides tools that administrators can use to define resources.

Each resource is mapped to an entitlement. A resource definition can have no more than one entitlement bound to it. A resource definition can be bound to the same entitlement more than once, with different entitlement parameters for each resource.

## Resource Requests

Resources can be assigned to users only. They cannot be assigned to groups or containers. However, if a role is assigned to a group or container, the users in the group or container may automatically be granted access to the resources associated with the role.

Resource requests may require approvals. The approval process for a resource may be handled by a provisioning request definition, or by an external system by setting the status code on the resource request.

If a resource grant request is initiated by a role assignment then it is possible that the resource will not be granted, even though the role is provisioned. The most likely reason for this would be that the necessary approvals were not provided.

A resource request can grant a resource to a user or revoke a resource from a user.

## Role and Resource Service Driver

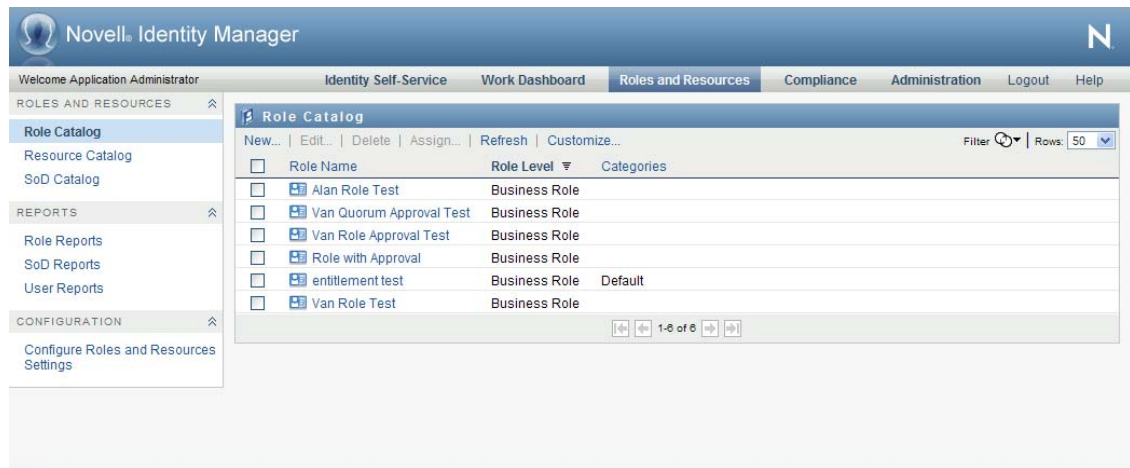
The User Application uses the Role and Resource Service Driver to manage back-end processing of resources. For example, it manages all resource requests, starts workflows for resource requests, and initiates the provisioning process for resource requests.

## 15.2 Accessing the Roles and Resources Tab

To access the *Roles and Resources* tab:

- 1 Click *Roles and Resources* in the User Application.

By default, the *Roles and Resources* tab displays the *Role Catalog* page.



If you go to another tab in the user interface but then want to return, you just need to click the *Roles and Resources* tab to open it again.

## 15.3 Exploring the Tab's Features

This section describes the default features of the *Roles and Resources* tab. (Your tab might look different because of customizations made for your organization; consult your system administrator or workflow designer.)

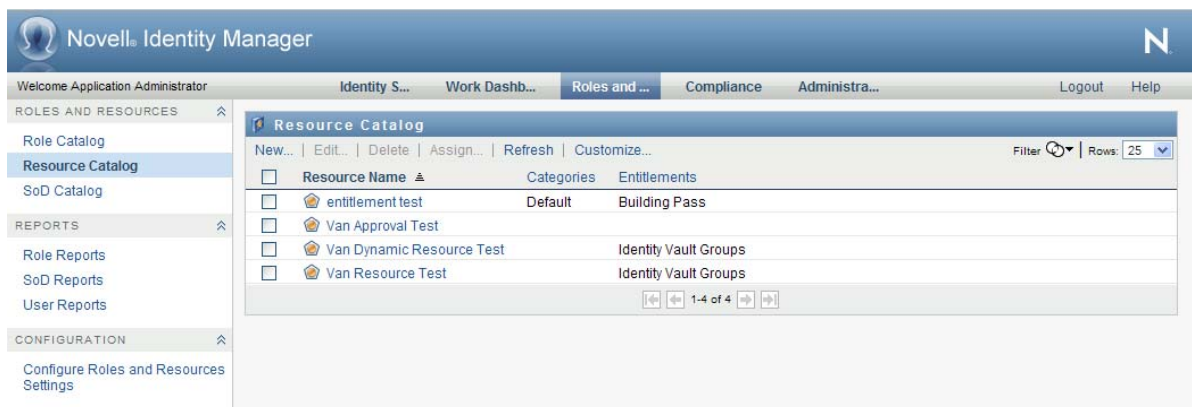
The left side of the *Roles and Resources* tab displays a menu of actions you can perform. The actions are listed by category (*Roles and Resources*, *Reports*, and *Configuration*):



Some of the menus on the *Roles and Resources* tab may not be available if you have not given navigation access.

When you click an action, it displays a corresponding page on the right. The page typically contains a window that shows the details for that action. For example, it might display a list or a form where you can enter data or make a selection, as shown below:

**Figure 15-2** Page Displayed for an Action



## 15.4 Roles and Resources Actions You Can Perform

Here's a summary of the actions that are available to you by default on the *Roles and Resources* tab:

**Table 15-2** Roles and Resources Actions

| Category            | Action       | Description   |
|---------------------|--------------|---|
| Roles and Resources | Role Catalog | Allows you to create, modify, and delete roles. Also lets you define role relationships, associate resources with roles, and assign roles to users, groups, and containers. |

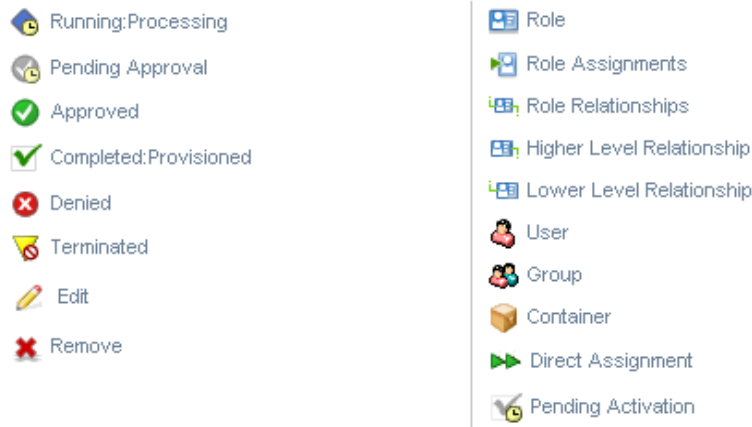
For details, see [Chapter 16, "Managing Roles in the User Application,"](#) on page 233.

| Category       | Action                                 | Description   |
|----------------|--|---|
|                | Resource Catalog                       | <p>Allows you to create, modify, and delete resources. Also lets you assign resources to users.</p> <p>For details, see <a href="#">Chapter 17, “Managing Resources in the User Application,”</a> on page 251.</p>  |
|                | SoD Catalog                            | <p>Allows you to define Separation of Duties (SoD) constraints. An SoD constraint represents a rule that makes two roles mutually exclusive. If a user is in one role, they cannot be in the second role, unless there is an exception allowed for that constraint. You can define whether exceptions to the constraint are always allowed or are only allowed through an approval flow.</p> <p>For details, see <a href="#">“Managing Separation of Duties in the User Application”</a> on page 271.</p> |
| Role Reporting | Role Reports                           | <p>Enables you to create and view reports that describe the current state of roles and role assignments.</p> <p>For details, see <a href="#">Section 19.2, “Role Reports,”</a> on page 275.</p>   |
|                | SoD Reports                            | <p>Enables you to create and view reports that describe the current state of Separation of Duties constraints, violations, and approved exceptions.</p> <p>For details, see <a href="#">Section 19.3, “SoD Reports,”</a> on page 279.</p>   |
|                | User Reports                           | <p>Enables you to create and view reports that describe the current state of role memberships and entitlements for users.</p> <p>For details, see <a href="#">Section 19.4, “User Reports,”</a> on page 281.</p>  |
| Configuration  | Configure Roles and Resources Settings | <p>Allows you to specify administrative settings for the Role and Resource Subsystem.</p> <p>For details, see <a href="#">“Configuring the Role and Resource Settings”</a> on page 287.</p>   |

## 15.5 Understanding the Icons Used on the Roles and Resources Tab

When you use the *Roles and Resources* tab, you see icons in many places that convey important information. These are the icons you see:

**Figure 15-3** Icons Used on the Roles and Resources Tab



The table below provides detailed descriptions of the icons used on the *Roles and Resources* tab:

**Table 15-3** Icons Used on the Roles and Resources Tab

| Icon                          | Description   |
|-------------------------------|---|
| <i>Running: Processing</i>    | Indicates that a role request is still in process.<br><br>Appears on the Request Status page.   |
| <i>Pending Approval</i>       | Indicates that a role request is awaiting approval, either for a separation of duties exception or for the role assignment itself.<br><br>Appears on the Request Status page.   |
| <i>Approved</i>               | Indicates that a role request has been approved. If a separation of duties exception was detected, this status can also be used to indicate that the exception was approved.<br><br>Appears on the Request Status page. |
| <i>Completed: Provisioned</i> | Indicates that a role request has been approved and the role has been assigned to the recipient (user, group, or container).<br><br>Appears on the Request Status page.   |
| <i>Denied</i>                 | Indicates that a role request has been denied. If a separation of duties exception was detected, this status may also be used to indicate that the exception was denied.<br><br>Appears on the Request Status page.     |
| <i>Terminated</i>             | Indicates that a role request terminated before completion, either because the user cancelled the request or because an error occurred during the course of processing.<br><br>Appears on the Request Status pages.     |
| <i>Role</i>                   | Indicates that an object is a role.<br><br>Appears on the Request Status page.  |

| <b>Icon</b>                      | <b>Description</b>   |
|----------------------------------|--|
| <i>Higher Level Relationship</i> | <p>Indicates that a role has a higher-level relationship to the currently selected role, which means that it contains the currently selected role.</p> <p>Appears on the Role Relationships page.</p>    |
| <i>Lower Level Relationship</i>  | <p>Indicates that a role has a lower-level relationship to the currently selected role, which means that is contained by the currently selected role.</p> <p>Appears on the Role Relationships page.</p> |
| <i>User</i>                      | <p>Indicates that an object is a user.</p> <p>Appears on the Role Assignments page.</p>  |
| <i>Group</i>                     | <p>Indicates that an object is a group.</p> <p>Appears on the Role Assignments page.</p>   |
| <i>Container</i>                 | <p>Indicates that an object is a container.</p> <p>Appears on the Role Assignments page.</p>   |
| <i>Direct Assignment</i>         | <p>Indicates that a role was assigned directly to the currently selected user, group, or container.</p> <p>Appears on the Roles Assignments page.</p>  |
| <i>Pending Activation</i>        | <p>Indicates that a role request has completed its processing and has been approved, but has an activation date that is in the future.</p> <p>Appears on the Request Status page.</p>                    |





# 16 Managing Roles in the User Application

This section describes the role management capabilities of the User Application. Topics include:

- ♦ [Section 16.1, “Browsing the Role Catalog,” on page 233](#)

## 16.1 Browsing the Role Catalog

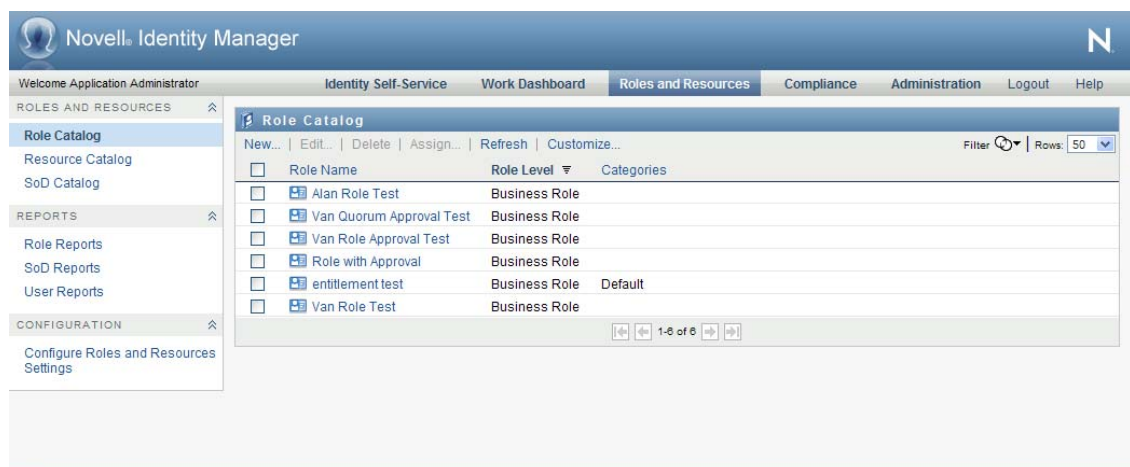
The *Role Catalog* action on the *Roles and Resources* tab of the Identity Manager user interface allows you to view roles that have been previously defined in the catalog. It also lets you create new roles and modify, delete, and assign existing roles.

- ♦ [Section 16.1.1, “Viewing Roles,” on page 233](#)
- ♦ [Section 16.1.2, “Creating New Roles,” on page 235](#)
- ♦ [Section 16.1.3, “Editing an Existing Role,” on page 244](#)
- ♦ [Section 16.1.4, “Deleting Roles,” on page 245](#)
- ♦ [Section 16.1.5, “Assigning Roles,” on page 246](#)
- ♦ [Section 16.1.6, “Refreshing the Role List,” on page 249](#)
- ♦ [Section 16.1.7, “Customizing the Role List Display,” on page 249](#)

### 16.1.1 Viewing Roles

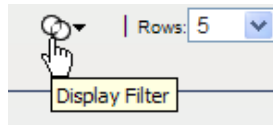
- 1 Click *Role Catalog* in the list of *Roles and Resources* actions.

The User Application displays a list of roles currently defined in the catalog.

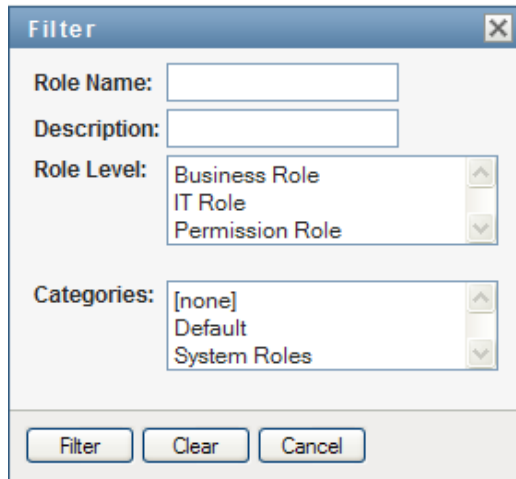


## Filtering the Role List

- 1 Click the *Display Filter* button in the upper right corner of the *Role Catalog* display.



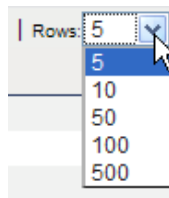
- 2 Specify a filter string for the role name or description, or select one or more role levels or categories in the *Filter* dialog.



- 3 Click *Filter* to apply your selection criteria.
- 4 To remove the current filter, click *Reset*.

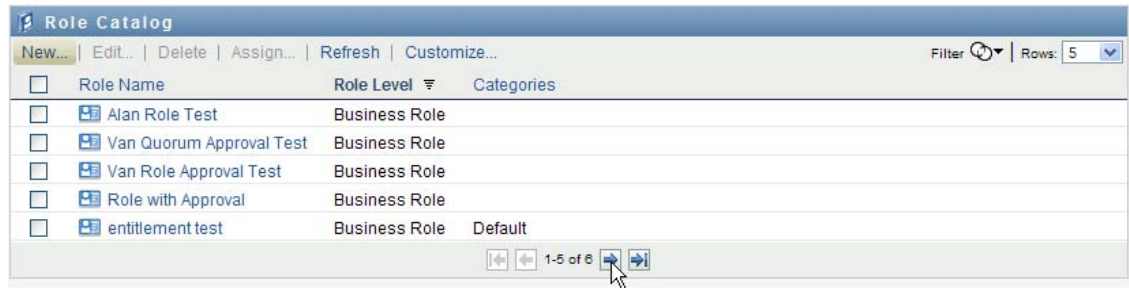
## Setting the Maximum Number of Roles on a Page

- 1 Click on the *Rows* dropdown list and select the number of rows you want to be displayed on each page:



## Scrolling within the Role List

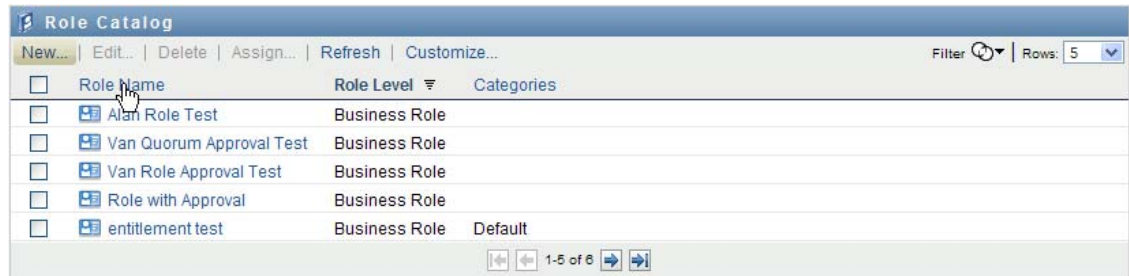
- 1 To scroll to another page in the role list, click on the Next, Previous, First or Last button at the bottom of the list:



## Sorting the Role List

To sort the role list:

- 1 Click the header for the column you want to sort on.



The pyramid-shaped sort indicator shows you which column is the new sort column. When the sort is ascending, the sort indicator is shown in its normal, upright position.

When the sort is descending, the sort indicator is upside down.

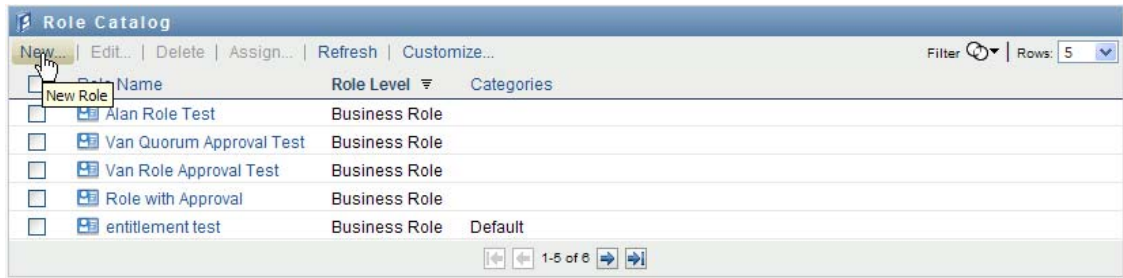
The initial sort column is determined by the administrator.

If you override the initial sort column, your sort column is added to the list of required columns. Required columns are indicated with an asterisk (\*).

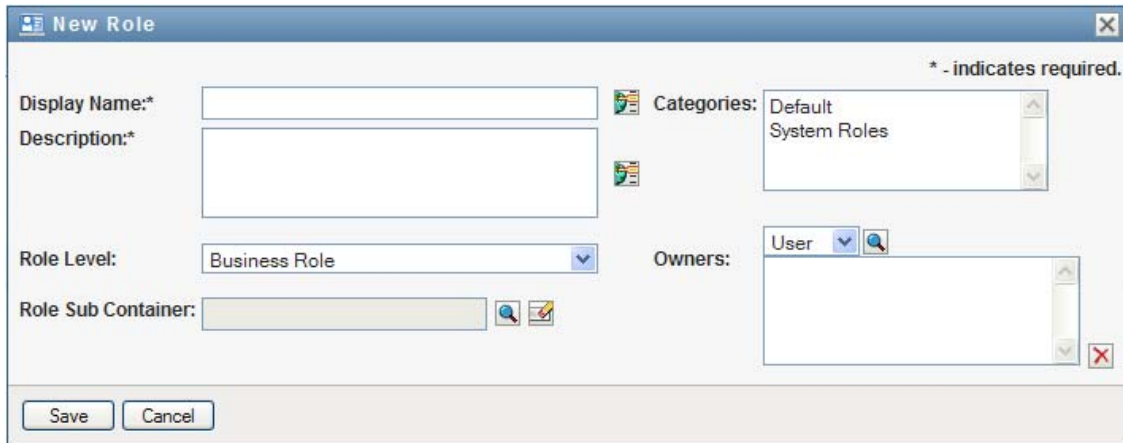
When you modify the sort order for the task list, your preference is saved in the Identity Vault along with your other user preferences.

## 16.1.2 Creating New Roles

- 1 Click the *New* button at the top of the *Role Catalog* display:



The User Application displays the New Role dialog:



2 Provide details for the role definition, as described below:

**Table 16-1** Role Details

| Field                     | Description   |
|---------------------------|---|
| <i>Display Name</i>       | <p>The text used when the role name displays in the User Application. You cannot include the following characters in the <i>Display Name</i> when you create a role:</p> <p>&lt; &gt; , ; \ " + # = /   &amp; *</p> <p>You can translate this name in any of the User Application's supported languages. For more information, see <a href="#">Table 1-1, "Common Buttons," on page 25</a>.</p> |
| <i>Description</i>        | <p>The text used when the role description displays in the User Application. Like the Display Name, you can translate it to any of the User Application's supported languages. For more information, see <a href="#">Table 1-1, "Common Buttons," on page 25</a>.</p>   |
| <i>Role Level</i>         | <p>(Read-only when modifying a role.) Choose a role level from the drop-down list.</p> <p>Role levels are defined using the Designer for Identity Manager Role Configuration editor.</p>  |
| <i>Role Sub Container</i> | <p>(Read-only when modifying a role.) The location for the role objects in the driver. Role containers reside under role levels. The User Application shows only the role containers that reside under the role level that you choose. You can create a role either directly in a role level, or in a container within the role level. Specifying the role container is optional.</p>           |

| Field      | Description  |
|------------|--|
| Categories | Allow you to categorize roles for role organization. Categories are used for filtering lists of roles. Categories are multi-select.  |
| Owners     | Users who are designated as the owners of the role definition. When you generate reports against the Role Catalog, you can filter the report based on the role owner. The role owner does not automatically have the authorization to administer changes to a role definition. |

3 Click *Save* to save the role definition.

The User Application displays several additional tabs at the bottom of the window to allow to complete the role definition.

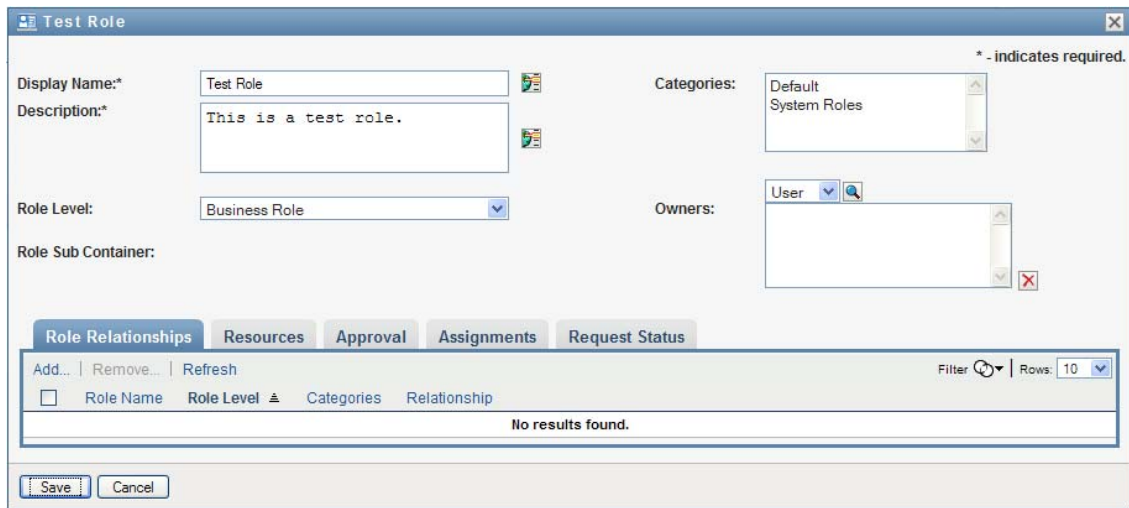
## Defining the Role Relationships

The *Role Relationships* tab allows you to define how roles are related in a higher and lower role containment hierarchy. This hierarchy enables you to group permissions or resources contained by lower-level roles into a higher-level role that makes assignment of permissions easier. The allowed relationships are:

- ♦ Top-level roles (business roles) can contain lower-level roles. They cannot be contained by other roles. If you select a top-level role, the Role Relationships page allows you to add a lower-level (child) role relationship only.
- ♦ Mid-level roles (IT roles) can contain lower-level roles, and they can be contained by higher-level roles. The Role Relationship page allows you to add either lower-level (child) role or higher-level (parent) role.
- ♦ Bottom-level roles (permission roles) can be contained by higher-level roles, but they cannot contain other bottom-level roles. The Role Relationship page allows you to add only a higher-level role.

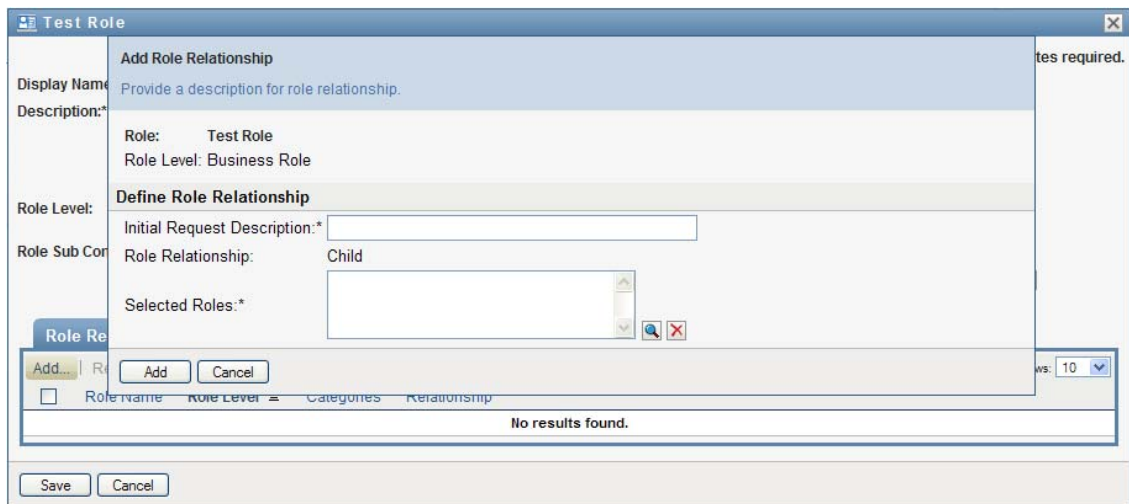
To define a role relationship:

- 1 Click the *Role Relationships* tab.



2 Click *Add*.

The *Add Role Relationship* dialog is displayed.



3 Provide text describing the relationship in the *Initial Request Description* field.

4 Specify the type of relationship you want to define by selecting the type in the *Role Relationship* dropdown.

If the new role is an IT role, the *Role Relationship* dropdown lets you define a *Child* or *Parent* relationship. If the new role is a business role, the *Role Relationship* dropdown displays read-only text indicating that this is a *Child* relationship, since only lower-level roles can be related to a business role. If the new role is a permission role, the *Role Relationship* dropdown displays read-only text indicating that this is a *Parent* relationship, since only higher-level roles can be related to a permission role.

The list of roles available for selection is filtered according to the type you selected.

5 Use the Object Selector to the right of the *Selected Roles* field to select the role(s) you want to associate with the new role.

6 Click *Add*.

## Associating Resources with the Role

To associate a resource with a role:

- 1 Click the *Resources* tab.
- 2 Click *Add*.

The screenshot shows the 'Test Role' dialog box. The 'Resources' tab is selected, and the 'Add' button is highlighted. The table below the tabs is empty and shows 'No results found.'

The User Application displays the *Add Resource Association* dialog.

The 'Add Resource Association' dialog box is shown. It contains two input fields: 'Select Resource:\*' and 'Association Description:\*'. The 'Add' button is highlighted.

- 3 Use the Object Selector to select the resource you want and provide text that explains the reason for the association.

The wizard displays a page that provides information about the selected resource, such as the name of the resource categories, owner, entitlement, and entitlement values.

**Add Resource Association**  
 Select a resource and specify a description for the resource association.

Resource:\*

Association Description:\*

**Resource Information**

Categories: Default

Resource Description: entitlement test

Entitlement: Building Pass

Entitlement Values: Cambridge Office

For entitlements that take static parameter values, which provide additional attributes or detailed information for the entitlement, the wizard displays the static values next to the *Entitlement Value* label. For entitlements that take dynamic parameters, the wizard displays the resource request form, which includes fields for the dynamic parameters, as well as any decision support fields defined for the form.

**Step 2 of 2: Define the Resource Parameters.**  
 The Association Description helps describe the binding of this resource to the role.

Resource Name: **Parking Pass**

Association Description\*:

**Resource Information**

Category: -

Resource Description: Parking Pass

Owner: -

Entitlement: Parking Permission

Entitlement Value: [ Value is set in Request Form below... ]

**Resource Request Information**

Parking Garage:\*

VIP Parking:\*  true  false

Valid for # of Days:\*

Note: Only visitors are allowed VIP parking



- 4 In the *Association Description* field, type text that explains why the resource is associated with the role.
- 5 Click *Add* to associate the resource with the role.

The *Resource Associations* list shows the resource you added to the role definition:

**What happens to existing role assignments** When you add a new resource association to a role that already has identities assigned to it, the system initiates a new request to grant the resource to each of the identities.

**NOTE:** In RBPM releases prior to the Public Patch 401C, you would see different results if a resource with parameters were granted to a user through a role association rather than through direct assignment to the user. This was the case in the following situations:

- ◆ A resource that has an entitlement parameter, as well as a field parameter defined on the Request Form tab, is associated with a role. If a user were assigned to the role directly, by group membership, or by being in a container, this user would be assigned the resource as well. However, the resource assignment would only have the entitlement parameter value.

This issue has been resolved in Public Patch 401c and in release 4.0.2. However, if your assignments were created in a prior release (370, 400, or before Public 401C), and you want all of the resource parameters to appear, you need to revoke the user from the role and then reassign the user.

- ◆ A resource that has two or more fields defined on the Request Form tab only is associated with a role. If a user were assigned the role directly, by group membership, or by being in a container, this user would be assigned the resource the same number of times as the number of field parameters. In other words, the user would have one resource assignment for each field parameter. If the resource were assigned directly, the user would only have one assignment with all of the parameters listed.

This issue has been resolved in Public Patch 401C and in release 4.0.2. However, if your resource associations were created in a prior release (370, 400, or before Public Patch 401C), you will still see this behavior. To take advantage of the fix, you must delete the resource association and recreate it.

To delete a resource association for a role:

- 1 Select the resource association in the *Resource Associations* list.

- 2 Click *Remove*.

**What happens to existing role assignments** When you remove a resource association from a role that already has identities assigned to it, the system initiates a new request to revoke the resource from each of the identities.

## Defining the Approval Process for a Role

To define the approval process for a role:

- 1 Click the *Approval* tab.
- 2 Provide details for the approval process, as described below:

**Table 16-2** *Approval Details*

| Field                    | Description  |
|--------------------------|--|
| <i>Approval Required</i> | <p>Select this checkbox if the role requires approval when requested, and you want the approval process to execute the standard role assignment approval definition.</p> <p>Deselect this checkbox if the role does not require approval when requested.</p> <p><b>NOTE:</b> Role approvals are triggered for explicit role-to-user assignments only.</p>  |
| <i>Custom Approval</i>   | <p>Select this radio button if you want to use a custom approval definition (provisioning request definition). Use the <i>Object Selector</i> to select the approval definition.</p>   |
| <i>Standard Approval</i> | <p>Select this radio button if this role uses the standard role assignment approval definition specified in the Role and Resource Subsystem configuration. The name of the approval definition displays as read-only in the <i>Role Assignment Approval Definition</i> below.</p> <p>You must select the type of approval (<i>Serial</i> or <i>Quorum</i>) and the valid approvers.</p>  |
| <i>Approval Type</i>     | <p>Select <i>Serial</i> if you want the role to be approved by all of the users in the <i>Approvers</i> list. The approvers are processed sequentially in the order they appear in the list.</p> <p>Select <i>Quorum</i> if you want the role to be approved by a percentage of the users in the <i>Approvers</i> list. The approval is complete when the percentage of users specified is reached.</p> <p>For example, if you want one of four users in the list to approve the condition, you would specify Quorum and a percentage of 25. Alternatively, you can specify 100% if all four approvers must approve in parallel. The value must be an integer between 1 and 100.</p> <p><b>TIP:</b> The Serial and Quorum fields have hover text that explains their behavior.</p> |

| Field   | Description   |
|---|---|
| <i>Approvers</i>  | <p>Select <i>User</i> if the role approval task should be assigned to one or more users. Select <i>Group</i> if the role approval task should be assigned to a group. Select <i>Container</i> if the role approval task should be assigned to a container. Select <i>Role</i> if the role approval task should be assigned to a role.</p> <p>To locate a specific user, group, container, or role, use the <i>Object Selector</i>. To change the order of the approvers in the list, or to remove an approver, see <a href="#">Section 1.4.4, “Common User Actions,” on page 24</a>.</p>  |
| <i>Revoke Approval Required (Same as Grant Configuration)</i> | <p>Select this checkbox if the role requires approval when revoked.</p> <p>The approval process used for role revocation requests, as well as the list of approvers, is the same as for role grant requests. If you have indicated that you want the approval process to execute the standard role assignment approval definition, this process will be used. Alternatively, you can specify a custom approval process for both role grant requests and role revocation requests. Within a custom provisioning request definition, you can identify whether the action is a grant or revoke and customize the approval process accordingly.</p> <p>Deselect this checkbox if the role does not require approval when revoked.</p> |

## Making Role Assignments

For details on making role assignments, see [Section 16.1.5, “Assigning Roles,” on page 246](#).

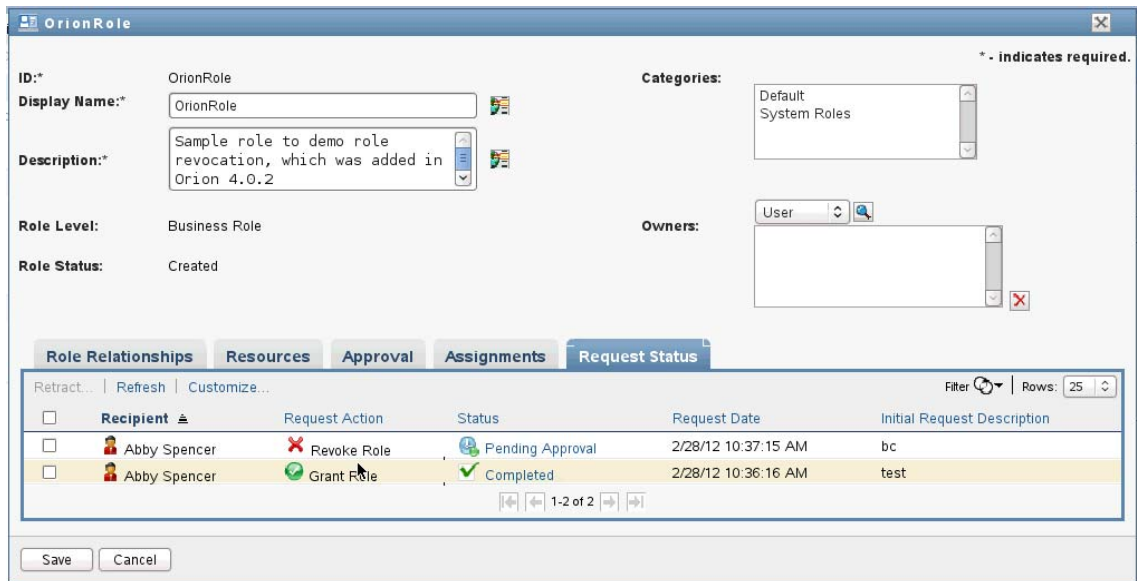
## Checking the Status of Requests

The *Request Status* action allows you to see the status of your role assignment requests, including requests you’ve made directly as well as role assignment requests for groups or containers to which you belong. It lets you see the current state of each request. In addition, it gives you the option to retract a request that has not been completed or terminated if you have changed your mind and do not need to have the request fulfilled.

The *Request Status* action shows all role assignment requests, including those that are running, pending approval, approved, completed, denied, or terminated.

To view the status of role assignment requests:

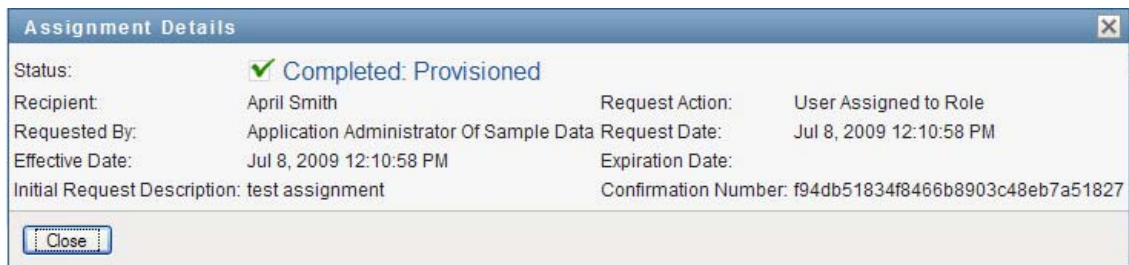
- 1 Click the *Request Status* tab.



The *Request Action* shows whether the action was a grant or revoke. If an approval was required, and the approval process has not completed, the status shows *Pending Approval*.

- 2 To see the detailed status information for a request, click the status.

The Assignment Details window is displayed:



For details on what the status values mean, see [Section 10.4, “Viewing Your Request Status,” on page 159](#).

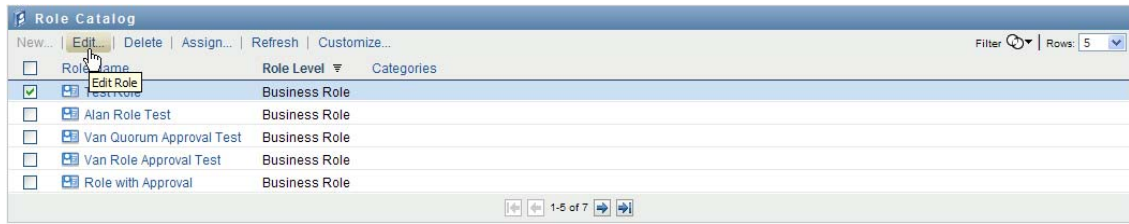
- 3 To retract a request, select the request and click *Retract*.

You need to have permission to retract a request.

If the request has been completed or terminated, you will see an error message if you try to retract the request.

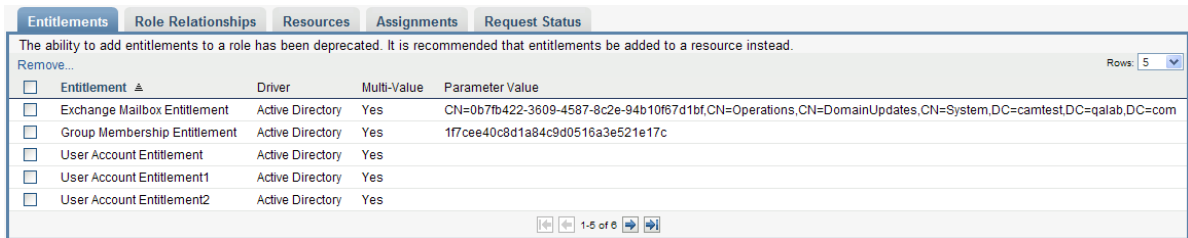
## 16.1.3 Editing an Existing Role

- 1 Select a previously defined role and click *Edit*.



2 Make your changes to the role settings and click *Save*.

**Entitlements associated with existing roles** Roles defined in earlier releases of the Roles Based Provisioning Module may have associated entitlements. If a role has an entitlement associated with it, the user interface displays the *Entitlements* tab, which allows you to see the entitlement mapping, and optionally remove it. Entitlement mappings for roles will continue to work in this release, but Novell now recommends that you associate entitlements with resources, rather than with roles.



## 16.1.4 Deleting Roles

1 Select a previously defined role and click *Delete*.

When you instruct the User Application to delete a role, it first sets the role status to *Pending Delete*. The Role and Resource Service driver then notes the change of status and performs these steps:

- ◆ Removes the resource assignments for the role
- ◆ Deletes the role itself

The Role and Resource Service driver optimizes this process. However, the process may take some time, depending on the number of users assigned to the role, because the Role and Resource driver must ensure that it does not remove a resource from a user if they have this resource by other means. If the role remains in the *Pending Delete* state for an inordinate amount of time, double check your driver to ensure that it is current and running.

When a role has the status of *Pending Delete*, you are unable to edit, delete, or assign the role.

---

**NOTE:** For version 4.0.2, a new attribute called `nrfStatus` has been added to the `nrfRole` object to manage the role status. This attribute has two states, *Created* and *Pending Delete*.

---

**What happens to existing role assignments** If you delete a role that has an associated resource as well as one or more identities assigned to it, the system removes the resource assignment from each identity that has the associated resource.

---

**NOTE:** If you delete a role that has a resource assigned to it (or remove a user from the role), the system removes resource assignments for users in that role, even if those resources were first assigned directly. The reason for this is that the system assumes that the last authoritative source for a resource assignment is the controller of that resource, as illustrated by the following scenario:

1. A resource is created and mapped to an entitlement.
2. A user is assigned to the resource created above.
3. A role is created that is bound to the resource created in the first step above.
4. The same user is then assigned to the role created above.
5. The user is removed from the role.

In this situation, the user gets removed from the resource even though they had the resource assigned directly. Initially, the resource assignment is considered the authoritative source. However, when the user is assigned to a role that is associated with the same resource, the role becomes the authoritative source.

---

**Deleting Roles in SoD Constraints** When a conflicting role of an SoD constraint is deleted, the SoD constraint will appear with the word *Invalid* in brackets after the name, such as *Doctor Pharmacists SoD [Invalid]*, in the SoD Catalog list.

---

**WARNING:** A Role Manager who has been given the Delete Role permission for the system roles (or the container that contains these roles) can delete system roles. The system roles should not be deleted. If any of the system roles is deleted, the User Application will malfunction.

---

## 16.1.5 Assigning Roles

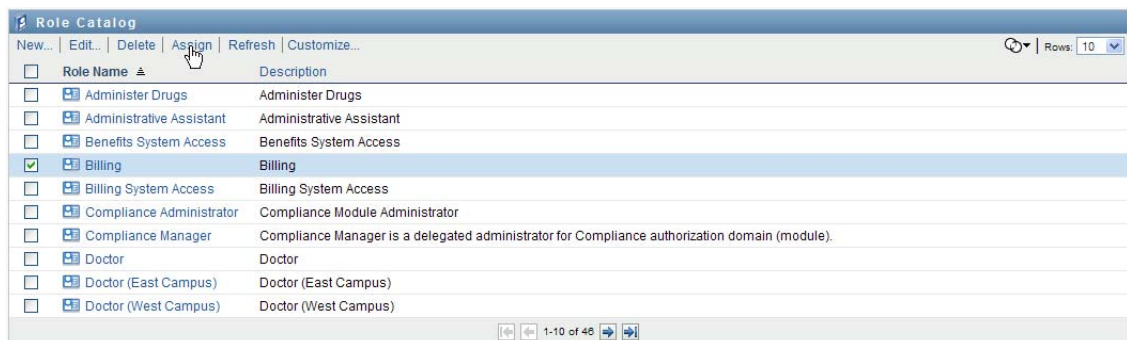
You can assign a role in either of two ways:

- ♦ From the *Role Catalog*
- ♦ From the *Edit Role* dialog

Both of these methods are described below.

### Assigning a Role From the Catalog

- 1 Select a previously defined role in the *Role Catalog* and click *Assign*.



The User Application displays the *Assign Role* dialog box:

**2** Fill in the fields on the *Add Role Assignment* dialog:

- 2a** Provide text describing the reason for the request in the *Initial Request Description* field.
- 2b** In the *Type of Assignment* field, select *User*, *Group*, or *Container* to indicate what type of identities the role will be assigned to.
- 2c** In the *Object Selector*, enter a search string and click *Search*.

Select the users, groups, or containers you want to assign.

**Assigning a role to multiple identities** You can select one or more users (or groups or containers) for the role assignment. If you select multiple identities, all of the selected identities receive the same role assignment values.

**2d** Specify the start date for the role assignment in the *Effective Date* field.

You can type in a date using the format *mm/dd/yyyy hh:mm:ss a* (where *a* specifies AM or PM). Alternatively, you can click the *Calendar* icon and select the date from the *Calendar* pop-up window:

| «  | Jun 2009 |    |    |    |    |    | » |
|----|----------|----|----|----|----|----|---|
| S  | M        | T  | W  | T  | F  | S  |   |
| 31 | 1        | 2  | 3  | 4  | 5  | 6  |   |
| 7  | 8        | 9  | 10 | 11 | 12 | 13 |   |
| 14 | 15       | 16 | 17 | 18 | 19 | 20 |   |
| 21 | 22       | 23 | 24 | 25 | 26 | 27 |   |
| 28 | 29       | 30 | 1  | 2  | 3  | 4  |   |
| 5  | 6        | 7  | 8  | 9  | 10 | 11 |   |

**2e** Specify the expiration date for the role assignment in the *Expiration Date* field.

---

**NOTE:** The expiration date only applies to user assignments. For groups and containers, the *Expiration Date* field is not available.

---

To specify an expiration, click *Specify Expiration*. You can type in a date using the format mm/dd/yyyy hh:mm:ss a (where *a* specifies AM or PM). Alternatively, you can click the Calendar icon and select the date from the Calendar pop-up window.

By default, the expiration date is set to *No Expiration*, which indicates that this role assignment will remain in effect indefinitely.

- 3 Click *Submit*.

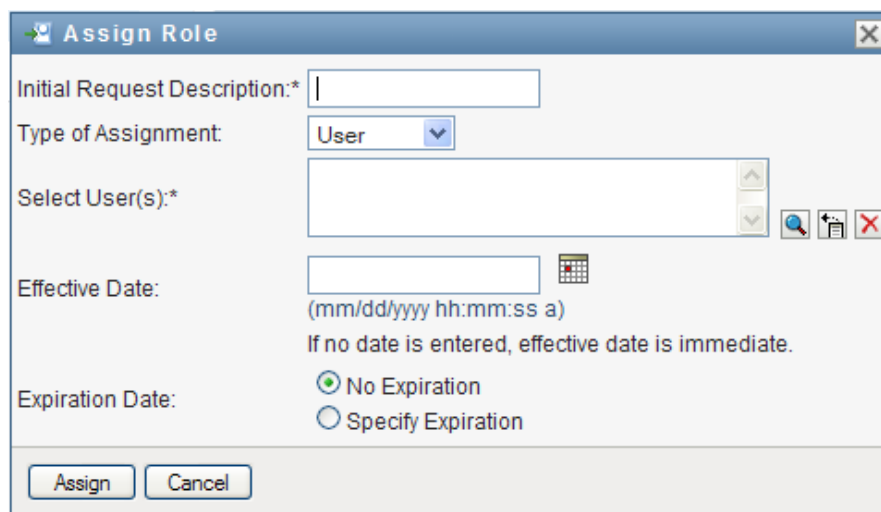
## Assigning a Role From the Edit Role Dialog

- 1 In the *Role Catalog*, select a role and click *Edit* to open the *Edit Role* dialog.
- 2 Click the *Assignments* tab.

The *Assignments* tab displays a list of assignments that have been granted for the selected role.

- 3 To add a new assignment, click *Assign*.

The User Application displays the *Assign Role* dialog box:



For details on working with the role assignment request form, see [“Assigning a Role From the Catalog” on page 246](#).

## Resolving Separation of Duties Conflicts

If a separation of duties conflict will occur if a role is assigned to one or more users, the user interface displays the Separation of Duties Conflicts box at the bottom of the page. In this case, you need to provide a business justification for the role assignment. For more information about Separation of Duties constraints, see [“Browsing the SoD Catalog” on page 271](#).

---

**NOTE:** You do not need to provide a justification in cases where the new role assignment conflicts with an existing assignment that the user acquired indirectly, either through a role relationship, or by membership in a group or container.

If a user is added to a role indirectly, and a potential separation of duties conflict is detected, the User Application allows the new assignment to be added and records the violation for reporting and audit purposes. If necessary, role administrators can correct the violation by redefining roles.

---



## 16.1.6 Refreshing the Role List

To refresh the roles list, click *Refresh*.

---

**NOTE:** If you create a role assignment, and then remove it, you see a message indicating that the assignment has been removed, but the assignment may still be listed. If you refresh the page, you should see that the assignment has been removed.

---

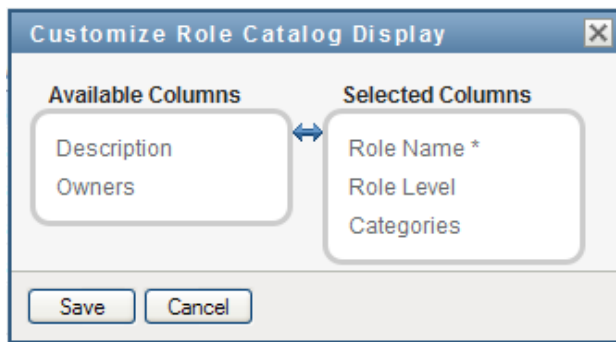
## 16.1.7 Customizing the Role List Display

The *Role Catalog* allows you to select and deselect columns, and also reorder columns within the task list display. This behavior is controlled by a setting within the *Customize Role Catalog Display* dialog. When you modify the column list or reorder the columns, your customizations are saved in the Identity Vault along with your other user preferences.

To customize the display of columns:

- 1 Click *Customize* in the *Role Catalog*:

The User Application displays the list of columns currently selected for the display, and a list of additional columns that are available for selection.



- 2 To include an additional column in the display, select the column in the *Available Columns* list box, and drag it to the *Selected Columns* list box.

To select multiple columns in the list, hold down the Ctrl key and select the columns. To select a range of columns that appear together in the list, hold down the Shift key and select the columns.

You can reorder the columns in the display by moving them up or down in the *Selected Columns* list box.

- 3 To remove a column from the display, select the column in the *Selected Columns* list box, and drag it to the *Available Columns* list box.

The *Role Name* column is a mandatory column and cannot be removed from the role list display.

- 4 To save your changes, click *Save*.



# 17 Managing Resources in the User Application

This section describes the resource management capabilities of the User Application. Topics include:

- ♦ [Section 17.1, “Browsing the Resource Catalog,” on page 251](#)

## 17.1 Browsing the Resource Catalog

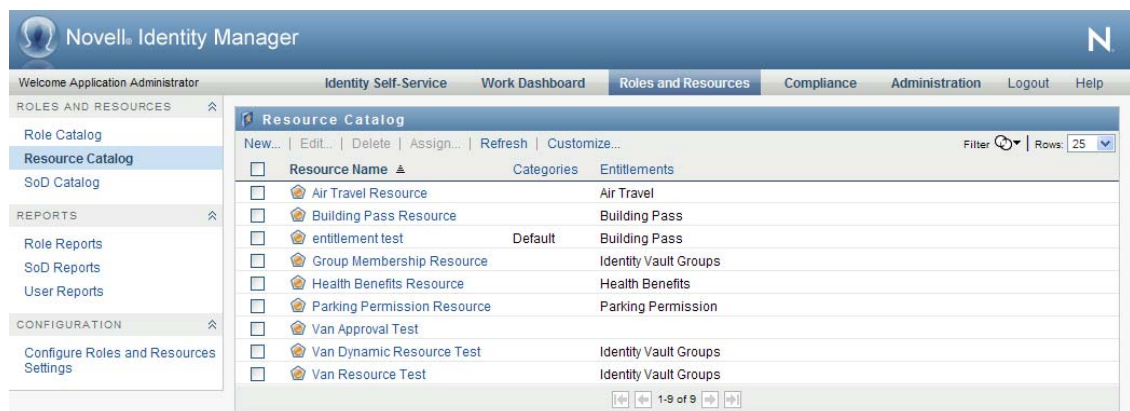
The *Resource Catalog* action on the *Roles and Resources* tab of the Identity Manager user interface allows you to view resources that have been previously defined in the catalog. It also lets you create new resources and modify, delete, and assign existing resources.

- ♦ [Section 17.1.1, “Viewing Resources,” on page 251](#)
- ♦ [Section 17.1.2, “Creating New Resources,” on page 253](#)
- ♦ [Section 17.1.3, “Editing an Existing Resource,” on page 266](#)
- ♦ [Section 17.1.4, “Deleting Resources,” on page 267](#)
- ♦ [Section 17.1.5, “Assigning Resources,” on page 267](#)
- ♦ [Section 17.1.6, “Refreshing the Resource List,” on page 269](#)
- ♦ [Section 17.1.7, “Customizing the Resource List Display,” on page 269](#)

### 17.1.1 Viewing Resources

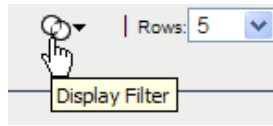
- 1 Click *Resource Catalog* in the list of *Roles and Resources* actions.

The User Application displays a list of resources currently defined in the catalog.

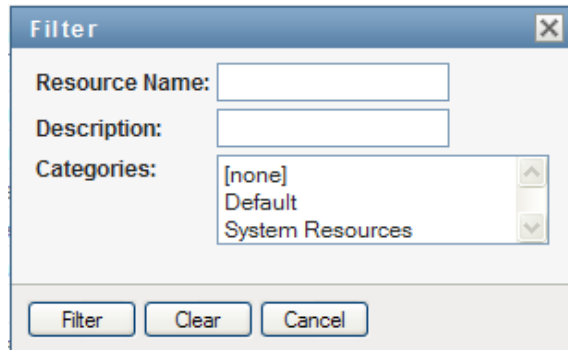


## Filtering the Resource List

- 1 Click the *Display Filter* button in the upper right corner of the *Resource Catalog* display.



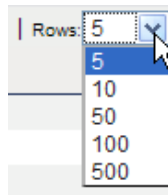
- 2 In the *Filter* dialog, specify a filter string for the resource name or description, or select one or more categories for which you want to see resources. Click *Filter*:



- 3 To remove the current filter, click *Clear*.

## Setting the Maximum Number of Resources on a Page

- 1 Click on the *Rows* dropdown list and select the number of rows you want to be displayed on each page:



## Scrolling within the Resource List

- 1 To scroll to another page in the resource list, click on the Next, Previous, First or Last button at the bottom of the list.

## Sorting the Resource List

To sort the resource list:

- 1 Click the header for the column you want to sort on.

The pyramid-shaped sort indicator shows you which column is the new sort column. When the sort is ascending, the sort indicator is shown in its normal, upright position.

When the sort is descending, the sort indicator is upside down.

The initial sort column is determined by the administrator.

If you override the initial sort column, your sort column is added to the list of required columns. Required columns are indicated with an asterisk (\*).

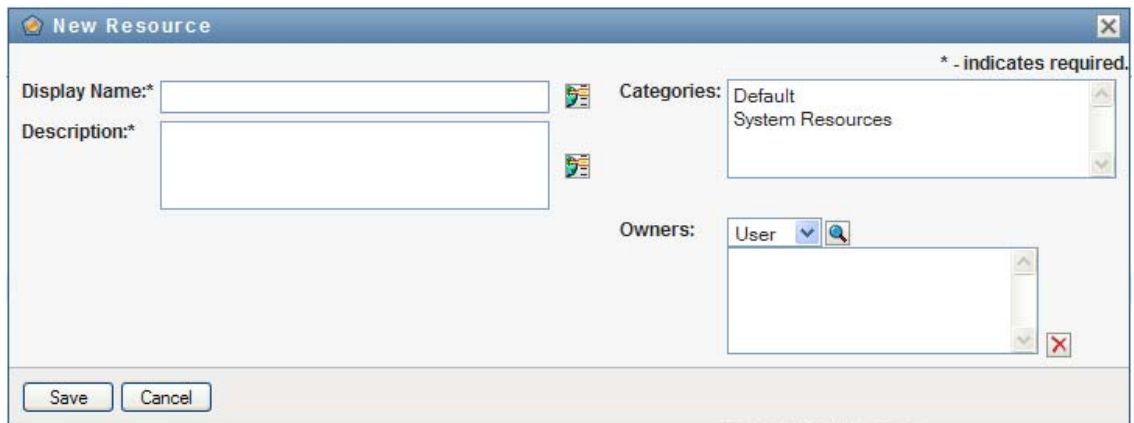
When you modify the sort order for the task list, your preference is saved in the Identity Vault along with your other user preferences.

## 17.1.2 Creating New Resources

- 1 Click the *New* button at the top of the *Resource Catalog* display:



The User Application displays the New Resource dialog:



- 2 Provide details for the resource definition, as described below:

| Field               | Description   |
|---------------------|---|
| <i>Display Name</i> | <p>The text used when the resource name displays in the User Application. You cannot include the following characters in the <i>Display Name</i> when you create a resource:</p> <p>&lt; &gt; , ; \ " + # = /   &amp; *</p> <p>You can translate this name in any of the User Application's supported languages. For more information, see <a href="#">Table 1-1, "Common Buttons," on page 25.</a></p> |

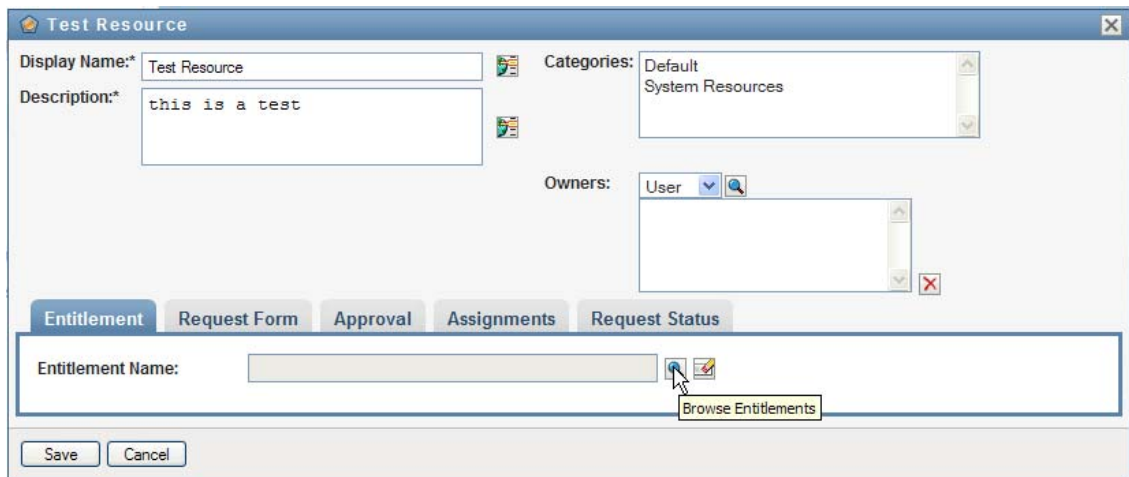
| Field              | Description  |
|--------------------|--|
| <i>Description</i> | The text used when the role description displays in the User Application. Like the Display Name, you can translate it to any of the User Application's supported languages. For more information, see <a href="#">Table 1-1, "Common Buttons,"</a> on page 25. |
| <i>Categories</i>  | Allow you to categorize resources for resource organization. Categories are used for filtering lists of resources. Categories are multi-select.  |
| <i>Owners</i>      | Users who are designated as the owners of the resource definition. The resource owner does not automatically have the authorization to administer changes to a resource definition.  |

- 3 Click *Save* to save the role definition.

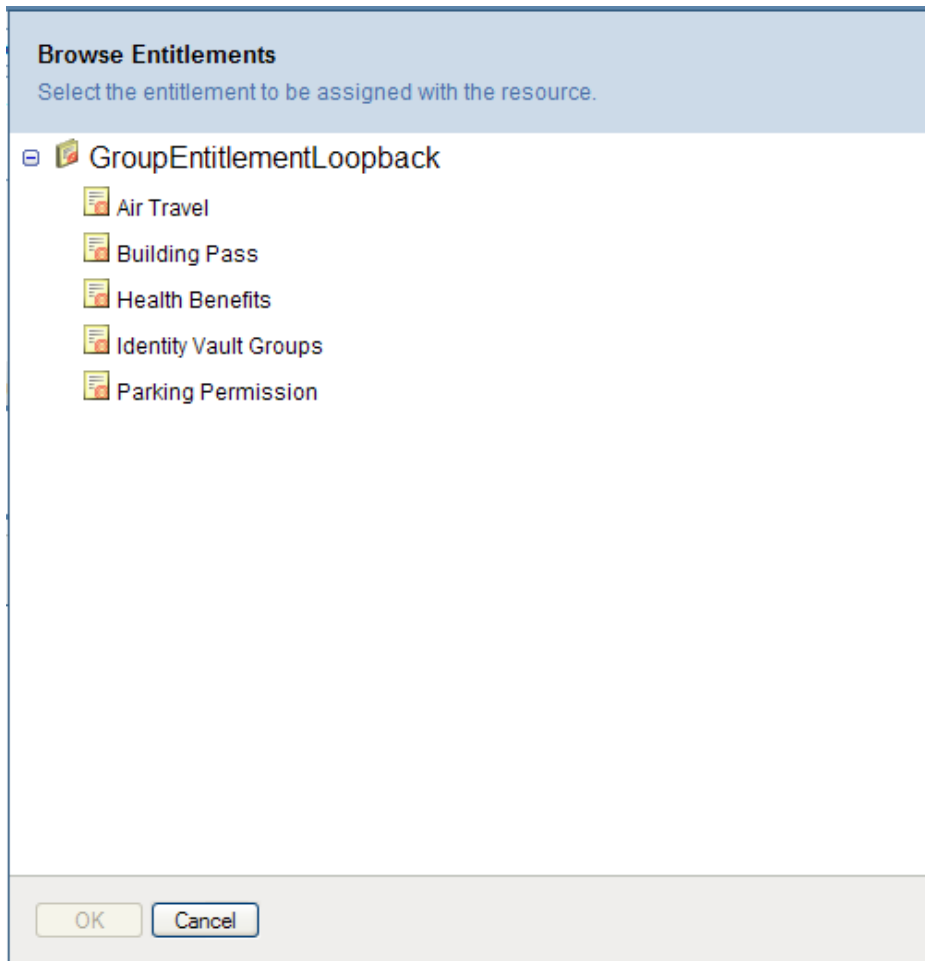
The User Application displays several additional tabs at the bottom of the window to allow you to complete the resource definition.

## Defining the Entitlement for a Resource Assignment

- 1 Click the *Entitlement* tab.
- 2 Click *Browse Entitlements* to select the entitlement:



The User Application displays a tree-view list of available entitlements:



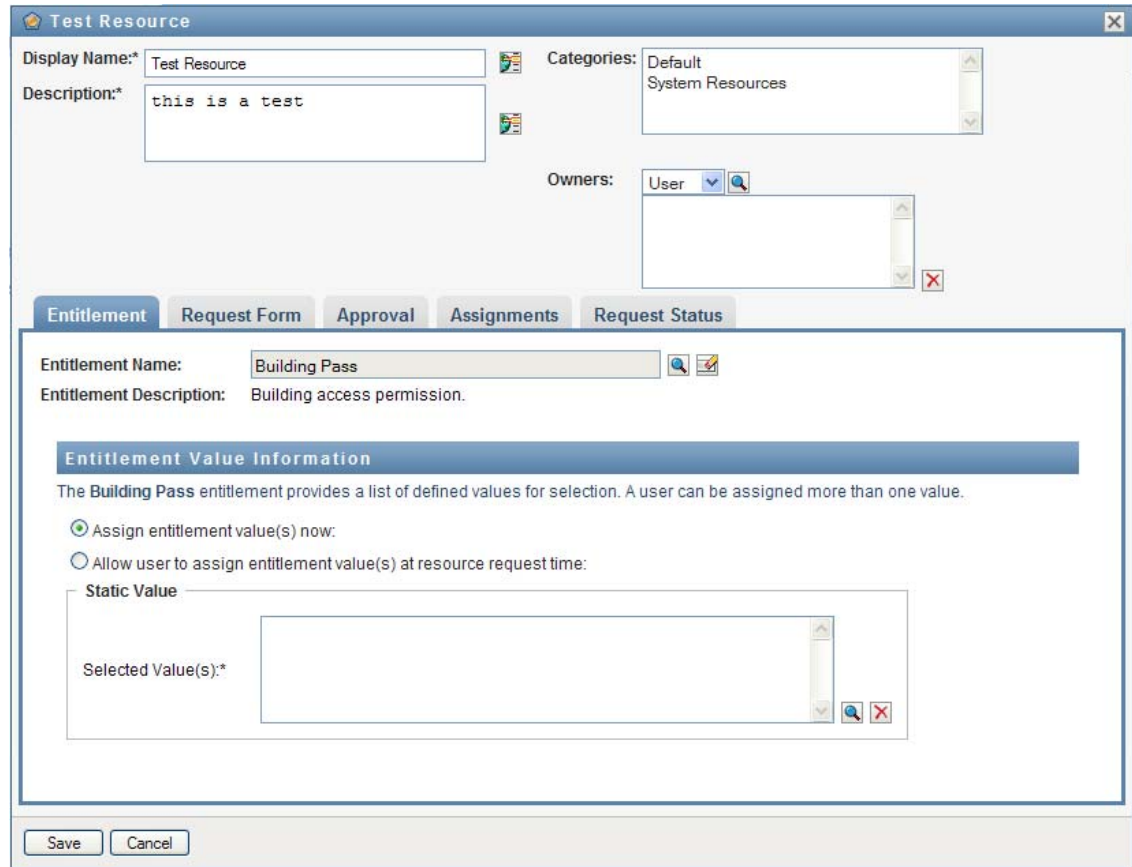
The list shows all drivers and entitlements found in the User Application driver set.

**NOTE:** If you have not configured the resource correctly, when you access the *Browse Entitlements* page to select an Entitlement, you will see a message indicating that you have not configured your entitlements for resource mapping.

For information about configuring your drivers and entitlements for resource mapping, see [“Enabling Drivers for Resource Mappings,”](#) in the *NetIQ Identity Manager User Application: Administration Guide*.

- 3 Select the entitlement you want to use and click *OK*.

The *Entitlement* tab shows information about any values that might be required for the entitlement:



- 4 Specify the details of the entitlement binding. The details vary depending on the type of entitlement you are associating with the resource:

| Type of Entitlement   | Description   |
|-----------------------|---|
| Valueless entitlement | <p>The entitlement accepts no parameter values. For example, a resource might be bound to an entitlement called Health Benefits that simply makes the recipient eligible for health care benefits. This type of entitlement has a fixed behavior and thereby requires no further information from the requester.</p> <p>When you bind to a valueless entitlement, no further configuration is required.</p> |



| Type of Entitlement          | Description   |
|------------------------------|---|
| Free-form valued entitlement | <p>The entitlement that requires a parameter value specified as a free-form string at request time. For example, a resource might be bound to an entitlement called Clothing that allows the requester to specify a value that represents their favorite color.</p> <p>You can assign a value at design time when you're defining the resource, or allow the user to assign a value at request time.</p> <p>For more information, see <a href="#">"Binding to a Free-Form Valued Entitlement" on page 257</a>.</p>  |
| Single-valued entitlement    | <p>The entitlement that requires a single parameter value. For example, a resource might be bound to an entitlement called Parking Permission that allows the requester to select a parking location. The allowable values are provided by an entitlement list, which can include a static list of values defined by an administrator or a dynamic list of values generated from an LDAP query.</p> <p>You can assign a value at design time when you're defining the resource, or allow the user to assign a value at request time.</p> <p>For more information, see <a href="#">"Binding to a Single-Valued Entitlement" on page 259</a>.</p> |
| Multi-valued entitlement     | <p>The entitlement that accepts one or more parameter values. For example, a resource might be bound to an entitlement called Building Pass that allows the requester to select one or more buildings. The allowable values are provided by an entitlement list, which can include a static list of values defined by an administrator or a dynamic list of values generated from an LDAP query.</p> <p>You can assign a value at design time when you're defining the resource, or allow the user to assign a value at request time.</p> <p>For more information, see <a href="#">"Binding to a Multi-Valued Entitlement" on page 259</a>.</p> |

## Binding to a Free-Form Valued Entitlement

- 1 To assign a static value at design time, select *Assign entitlement value(s) now*.  
Type a free-form value for the resource:

Entitlement Request Form Approval Assignments Request Status

Entitlement Name: Air Travel

Entitlement Description: Air Travel (include reason your are requesting)

**Entitlement Value Information**

The Air Travel entitlement allows the user to type in any value.

Assign entitlement value(s) now:  
 Allow user to assign entitlement value(s) at resource request time:

**Static Value**

Selected Value(s):\* Air travel is essential for your work.

2 To assign a dynamic value at request time, select *Allow user to assign entitlement value(s) at resource request time*.

2a Specify a label that the user will see when requesting the resource:

Entitlement Request Form Approval Assignments Request Status

Entitlement Name: Air Travel

Entitlement Description: Air Travel (include reason your are requesting)

**Entitlement Value Information**

The Air Travel entitlement allows the user to type in any value.

Assign entitlement value(s) now:  
 Allow user to assign entitlement value(s) at resource request time:

**Dynamic Value**

Label for value field:\* Justification:

2b To localize the label, click the *Add language display value* button and specify the foreign language text for the label:

Entitlement Request Form Approval Assignments Request Status

Entitlement Name: Air Travel

Entitlement Description: Air Travel (include reason your are requesting)

**Entitlement Value Information**

The Air Travel entitlement allows the user to type in any value.

Assign entitlement value(s) now:  
 Allow user to assign entitlement value(s) at resource request time:

**Dynamic Value**

Label for value field:\* Justification: Add language display value.

## Binding to a Single-Valued Entitlement

- 1 To assign a static value at design time, select *Assign entitlement value(s) now*.  
Select a single value from the default entitlement list:
- 2 To assign a dynamic value at request time, select *Allow user to assign entitlement value(s) at resource request time*.
  - 2a Specify a label that the user will see when requesting the resource.
  - 2b To localize the label, click the *Add language display value* button and specify the foreign language text for the label.
  - 2c In the *Display values from Entitlement List* dropdown, select the list you want to use to display the allowable values.

For an administrator-defined or query entitlement, the allowable values are provided by a list defined in the entitlement. The values are first loaded into code map database tables to allow you to provide user-friendly labels and localized strings. Once loaded, these tables can be used as a source for creating additional entitlement lists.

By default, the User Application creates an entitlement list that includes all rows in the list. You can create more entitlement lists if you want to show selected rows only.

## Binding to a Multi-Valued Entitlement

- 1 To assign a static value at design time, select *Assign an entitlement value at this time*.  
Use the Object Selector to pick the entitlement values:

The screenshot shows a web-based configuration interface for an entitlement. At the top, there are tabs for 'Entitlement', 'Request Form', 'Approval', 'Assignments', and 'Request Status'. The 'Entitlement' tab is active. Below the tabs, there are fields for 'Entitlement Name' (Building Pass) and 'Entitlement Description' (Building access permission). A section titled 'Entitlement Value Information' contains the text: 'The Building Pass entitlement provides a list of defined values for selection. A user can be assigned more than one value.' Below this, there are two radio button options: 'Assign entitlement value(s) now' (which is selected) and 'Allow user to assign entitlement value(s) at resource request time:'. Under the selected option, there is a 'Static Value' section with a 'Selected Value(s):\*' label and a large empty text area. To the right of the text area are two small icons: a blue circle with a magnifying glass and a red 'X'. A tooltip box with the text 'Click to open object selector.' is positioned over the magnifying glass icon.

- 2 Select one or more values from the default entitlement list:

**Entitlement Values**  
Select the entitlement parameter(s) from the table.

| <input type="checkbox"/> | Name             | Description |
|--------------------------|------------------|-------------|
| <input type="checkbox"/> | Cambridge Office |             |
| <input type="checkbox"/> | Waltham Office   |             |

Filter | Rows: 10

Selected Value(s):

Add Cancel

- 3 To assign a dynamic value at request time, select *Allow user to assign entitlement value(s) at resource request time*.
  - 3a Specify a label that the user will see when requesting the resource:
  - 3b To localize the label, click the *Add language display value* button and specify the foreign language text for the label:
  - 3c In the *Display values from Entitlement List* dropdown, select the list you want to use to display the allowable values.
  - 3d Specify whether the user can select multiple values by selecting the *Allow user to request multiple assignments by selecting more than one value* checkbox.

**Entitlement** Request Form Approval Assignments Request Status

Entitlement Name: Building Pass

Entitlement Description: Building access permission.

**Entitlement Value Information**

The **Building Pass** entitlement provides a list of defined values for selection. A user can be assigned more than one value.

Assign entitlement value(s) now.  
 Allow user to assign entitlement value(s) at resource request time:

**Dynamic Value**

Label for value field\*: Building(s):

Display values from Entitlement List\*: Building access permission

Allow user to request multiple assignments by selecting more than one value.

Since the entitlement definition allows multiple assignments, you can specify whether you want the resource to also allow multiple assignments.

## Defining the Request Form

The request form for a resource displays two different types of fields:

- ◆ Entitlement parameter fields, which map to entitlement parameters for which the user can provide values at request time.
- ◆ Decision support fields, which allow the requester to provide additional information that may help the approver make a decision about whether to approve or deny the request.

The *Request Form* tab shows both types of fields, and provides a user interface for creating and editing decision support fields.

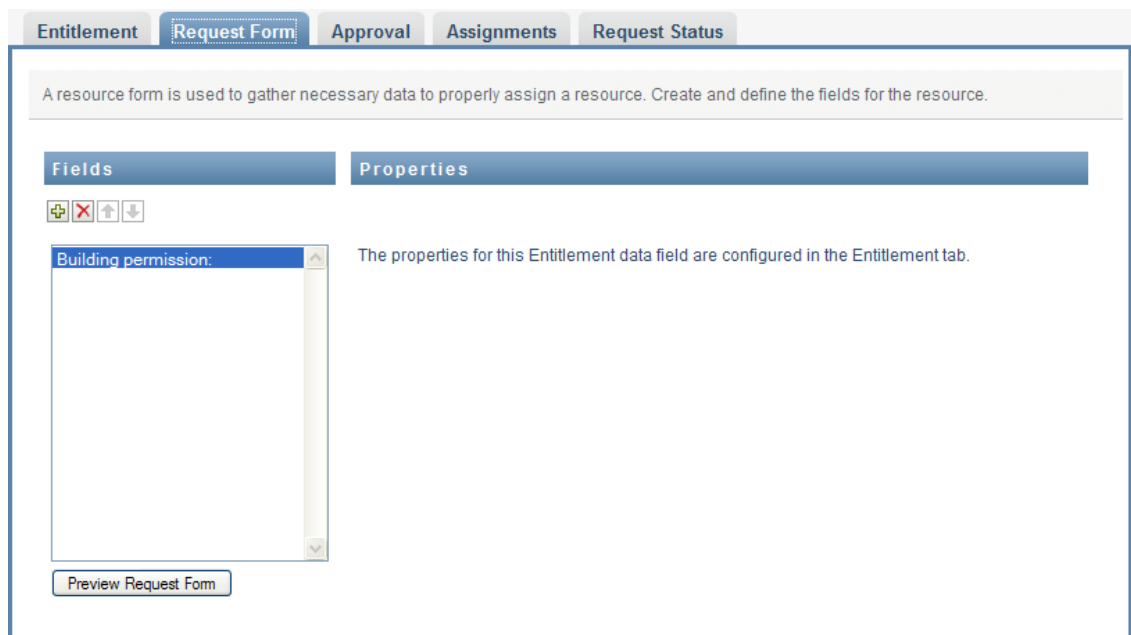
In addition to the fields shown on the *Request Form* tab, the request form always includes the following required fields:

- ◆ *User*
- ◆ *Reason*

All of the fields on the request form are shown on the approval form as read-only values.

To define the request form:

- 1 Click the *Request Form* tab.



The *Request Form* tab shows a list of fields that correspond to entitlement parameters for which values will be specified at request time. The properties for entitlement parameter fields are configured on the Action tab. You cannot change the behavior of fields that map to entitlement parameters.

- 2 To add a decision support data field:
  - 2a Click the plus sign (+) to add a new field:



- 2b** The *Request Form* tab adds a new field (with the default label *Field Label 1*) to the list of fields, and displays the Properties panel to allow you to define the characteristics of the field:

The screenshot shows a software interface with a top navigation bar containing tabs: Entitlement, Request Form, Approval, Assignments, and Request Status. The 'Request Form' tab is active. Below the tabs is a descriptive text: 'A resource form is used to gather necessary data to properly assign a resource. Create and define the fields for the resource.' The main area is divided into two panels: 'Fields' and 'Properties'. The 'Fields' panel contains a list with one item: 'Building permission: Field Label 1'. Below the list is a 'Preview Request Form' button. The 'Properties' panel contains the following settings: 'Assign Value:' with radio buttons for 'Now' and 'At resource request time' (selected); 'Display Label:\*' with a text input field containing 'Field Label 1'; 'Data Value:\*' with radio buttons for 'Value must be of type:' (selected) and 'Value must come from list'; a dropdown menu for 'String'; and another dropdown menu for '<No Lists Found>'. There are also icons for adding, deleting, and moving fields at the top of the Fields panel.

- 2c** To assign the decision support value right away, click *Now*.

This is a close-up of the 'Properties' panel. It features a blue header with the word 'Properties'. Below the header, the 'Assign Value:' section has two radio buttons: 'Now' (selected) and 'At resource request time'. The 'Display Label:\*' section has a text input field with 'Field Label 1'. The 'Data Type:\*' section has a dropdown menu showing 'String'. The 'Data Value:\*' section has an empty text input field. At the bottom, there is a checkbox labeled 'Hide' which is currently unchecked.

Provide a display label for the field, as well as the data type and value. The following data types are supported:

| Data type | Description   |
|-----------|---|
| Boolean   | A logical data type having one of two possible values: true or false. |
| Integer   | A sequence of natural numbers.  |
| List      | A set of predetermined values from which a value is selected.         |
| String    | A sequence of values representing text.                               |

To hide the value on the request form, click *Hide*. A field that is hidden on the request form is still visible on the approval form.

- 2d** To allow the user to assign the value at request time, click *At resource request time*.

Properties

Assign Value:  Now  
 At resource request time

Display Label:\*

Data Value:\*  Value must be of type:   
 Value must come from list:

Provide a display label for the field, and specify whether the value must be of a particular data type or come from a list.

## Defining the Approval Flow Settings

To define the approval process:

- 1 Click the *Approval* tab.

Entitlement
Request Form
Approval
Assignments
Request Status

Allow role approval process to override resource approval process

Grant Approval  Required

Revoke Approval  Required  Same as Grant Configuration

- 2 Specify whether the approval process for the resource can be overridden by the approval process for a role by selecting or deselecting the *Allow role approval process to override resource approval process* checkbox.

If the *Allow role approval process to override resource approval process* checkbox is selected, the role approval process will always override the resource approval process whenever the resource is associated with a role. Once the associated role has been approved, the resource is automatically provisioned, without any need for approval.

**3** Define the approval process for a grant operation, as follows:

- 3a** Open the *Grant Approval* section of the *Approval* tab.
- 3b** Specify the approval details, as described below:

| Field                    | Description   |
|--------------------------|---|
| <i>Required</i>          | <p>Select this box if the resource requires approval when requested.</p> <p>Deselect this box if the resource does not require approval when requested.</p>   |
| <i>Custom Approval</i>   | <p>When you select <i>Custom Approval</i>, you need to select a custom Resource Assignment Approval Definition. This is the name of the provisioning request definition executed when the resource is requested.</p>  |
| <i>Standard Approval</i> | <p>When you select <i>Standard Approval</i>, the resource uses the standard resource assignment approval definition specified in the Resource Subsystem configuration settings.</p>   |
| <i>Approval Type</i>     | <p>Select <i>Serial</i> if you want the role to be approved by all of the users in the <i>Approvers</i> list. The approvers are processed sequentially in the order they appear in the list.</p> <p>Select <i>Quorum</i> if you want the role to be approved by a percentage of the users in the <i>Approvers</i> list. The approval is complete when the percentage of users specified is reached.</p> <p>For example, if you want one of four users in the list to approve the condition, you would specify Quorum and a percentage of 25. Alternatively, you can specify 100% if all four approvers must approve in parallel. The value must be an integer between 1 and 100.</p> <p><b>TIP:</b> The Info button displays text that explains the approval types.</p> |
| <i>Approvers</i>         | <p>Select <i>User</i> if the role approval task should be assigned to one or more users. Select <i>Group</i> if the role approval task should be assigned to a group. Select <i>Role</i> if the role approval task should be assigned to a role.</p> <p>To locate a specific user, group, or role, use the <i>Object Selector</i> or <i>History</i> buttons. To change the order of the approvers in the list, or to remove an approver, see <a href="#">Section 1.4.4, “Common User Actions,” on page 24.</a></p>  |



4 Define the approval details for a revoke operation, as follows:

4a Open the *Revoke Approval* section of the Approval tab.

4b Specify the approval details, as described below:

| Field                              | Description  |
|------------------------------------|--|
| <i>Required</i>                    | Select this box if the resource requires approval when requested.<br><br>Deselect this box if the resource does not require approval when requested. |
| <i>Same as Grant Configuration</i> | Select this box to copy the settings you used for the grant operation to the settings for the revoke operation.                                      |

For all other approval details, see the field descriptions for the grant operation, which are presented in [Step 3b on page 264](#).

## Assigning a Resource

For details, see [“Assigning a Resource From the Edit Resource Dialog” on page 268](#).

## Checking the Status of Requests

The *Request Status* action allows you to see the status of your resource assignment requests, including requests you’ve made directly as well as resources assigned through roles. It lets you see the current state of each request. In addition, it gives you the option to retract a request that has not been completed or terminated if you have changed your mind and do not need to have the request fulfilled.

The *Request Status* action shows all resource assignment requests, including those that are running, pending approval, approved, completed, denied, or terminated.

- 1 Click the *Request Status* tab.

| <input type="checkbox"/> | Recipient     | Request Date      | Status      | Initial Request Description | Request Action    | Comments |
|--------------------------|---------------|-------------------|-------------|-----------------------------|-------------------|----------|
| <input type="checkbox"/> | Abby Spencer  | 7/7/09 9:33:31 AM | ✓ Completed | Created by the Role Driver  | ✓ Grant Resource  |          |
| <input type="checkbox"/> | Alan Delegate | 7/7/09 9:33:26 AM | ✓ Completed | Created by the Role Driver  | ✓ Grant Resource  |          |
| <input type="checkbox"/> | Alan User     | 7/7/09 9:33:27 AM | ✓ Completed | Created by the Role Driver  | ✓ Grant Resource  |          |
| <input type="checkbox"/> | Allison Blake | 7/3/09 3:16:25 PM | ✓ Completed | Created by the Role Driver  | ✗ Revoke Resource |          |
| <input type="checkbox"/> | Allison Blake | 7/3/09 6:56:57 AM | ✓ Completed | Created by the Role Driver  | ✓ Grant Resource  |          |

For each field on the request form, the Request Status display shows a separate column in the list. For example, the Parking Garage column is added to the request list to show entitlement values specified for the resource assignment:

| Entitlement                         |               | Request Form       |          | Approval                    |                | Assignments           |          | Request Status     |  |
|-------------------------------------|---------------|--------------------|----------|-----------------------------|----------------|-----------------------|----------|--------------------|--|
| Retract...   Refresh   Customize... |               |                    |          |                             |                |                       |          | Filter    Rows: 25 |  |
| <input type="checkbox"/>            | Recipient ▲   | Request Date       | Status   | Initial Request Description | Request Action | Parking Garage        | Comments |                    |  |
| <input type="checkbox"/>            | Allison Blake | 7/31/09 7:13:39 PM | Approved | test assignment             | Grant Resource | Cambridge:Ames Street |          |                    |  |
| 1-1 of 1                            |               |                    |          |                             |                |                       |          |                    |  |

2 To see the detailed status information for a request, click the status:

| Entitlement                         |               | Request Form      |           | Approval                    |                 | Assignments |  | Request Status    |  |
|-------------------------------------|---------------|-------------------|-----------|-----------------------------|-----------------|-------------|--|-------------------|--|
| Retract...   Refresh   Customize... |               |                   |           |                             |                 |             |  | Filter    Rows: 5 |  |
| <input type="checkbox"/>            | Recipient ▲   | Request Date      | Status    | Initial Request Description | Request Action  | Comments    |  |                   |  |
| <input type="checkbox"/>            | Abby Spencer  | 7/7/09 9:33:31 AM | Completed | Created by the Role Driver  | Grant Resource  |             |  |                   |  |
| <input type="checkbox"/>            | Alan Delegate | 7/7/09 9:33:26 AM | Completed | Created by the Role Driver  | Grant Resource  |             |  |                   |  |
| <input type="checkbox"/>            | Alan User     | 7/7/09 9:33:27 AM | Completed | Created by the Role Driver  | Grant Resource  |             |  |                   |  |
| <input type="checkbox"/>            | Allison Blake | 7/3/09 3:16:25 PM | Completed | Created by the Role Driver  | Revoke Resource |             |  |                   |  |
| <input type="checkbox"/>            | Allison Blake | 7/3/09 6:56:57 AM | Completed | Created by the Role Driver  | Grant Resource  |             |  |                   |  |
| 1-5 of 42                           |               |                   |           |                             |                 |             |  |                   |  |

The Assignment Details window is displayed:

**Assignment Details** X

Status: **Completed**

Recipient: Abby Spencer      Request Action: Grant Resource

Requested By: Application Administrator Of Sample Data      Request Date: 7/7/09 9:33:31 AM

Initial Request Description: Created by the Role Driver      Confirmation Number: 0564d3d0a5884cddae23a6678c3a466d

For details on what the status values mean, see [Section 10.4, “Viewing Your Request Status,” on page 159.](#)

3 To retract a request, select the request and click *Retract*.

If the request has been completed or terminated, you will see an error message if you try to retract the request.

## 17.1.3 Editing an Existing Resource

1 Select a previously defined resource and click *Edit*.

| Resource Catalog   |                             |                       |
|--|-----------------------------|-----------------------|
| New...   Edit...   Delete   Assign...   Refresh   Customize... |                             |                       |
| Filter    Rows: 25   |                             |                       |
| <input type="checkbox"/>                                       | Resource Name ▲             | Entitlements          |
| <input type="checkbox"/>                                       | Air Travel Resource         | Air Travel            |
| <input type="checkbox"/>                                       | Building Pass Resource      | Building Pass         |
| <input type="checkbox"/>                                       | entitlement test            | Building Pass         |
| <input type="checkbox"/>                                       | Group Membership Resource   | Identity Vault Groups |
| <input type="checkbox"/>                                       | Health Benefits Resource    | Health Benefits       |
| <input type="checkbox"/>                                       | Parking Permission Resource | Parking Permission    |
| <input checked="" type="checkbox"/>                            | Test Resource               | Building Pass         |
| <input type="checkbox"/>                                       | Van Approval Test           |                       |
| <input type="checkbox"/>                                       | Van Dynamic Resource Test   | Identity Vault Groups |
| <input type="checkbox"/>                                       | Van Resource Test           | Identity Vault Groups |
| 1-10 of 10   |                             |                       |

2 Make your changes to the resource settings and click *Save*.

## 17.1.4 Deleting Resources

- 1 Select a previously defined resource and click *Delete*.

**What happens to existing resource assignments** When you delete a resource that already has one or more identities assigned to it, the system removes the resource from those identities. If the resource has been associated with a role, the system also removes all role associations that pertain to the deleted resource.

## 17.1.5 Assigning Resources

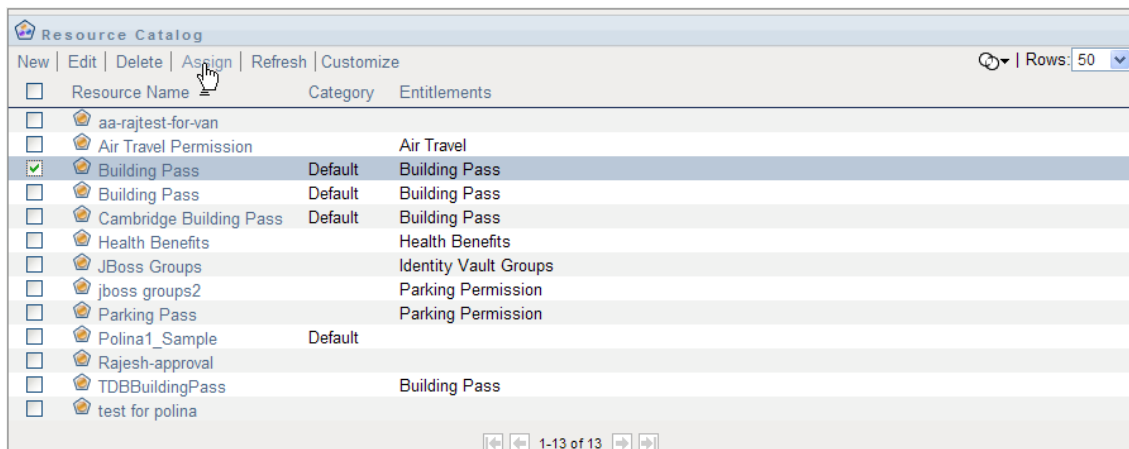
You can assign a resource in either of two ways:

- ♦ From the *Resource Catalog*
- ♦ From the *Edit Resource* dialog

Both of these methods are described below.

### Assigning a Resource From the Catalog

- 1 Select a previously defined resource in the *Resource Catalog* and click *Assign*.



The User Application displays the resource request form:



The screenshot shows the 'Assign Resource' dialog box. It has a title bar with a close button. The dialog contains two required fields: 'Initial Request Description:\*' and 'User:\*'. The 'User:\*' field includes an Object Selector icon (a magnifying glass over a document) and a red 'X' icon. At the bottom of the dialog are 'Assign' and 'Cancel' buttons.

The *Initial Request Description* and *User* fields are required fields that are present in all resource request forms. You can use the Object Selector to select the users for the resource assignment.

**Assigning a resource to multiple users** You can select one or more users for the resource assignment. If you select multiple users, all of the users receive the same resource assignment parameter values.

The request form may include additional fields to accept values for dynamic parameter values or decision-support values, as shown below:

In the example shown above, the *Building permission* field is used to accept an entitlement parameter value, whereas the *Company Name* and *Require parking?* fields are decision-support fields. These fields are not part of the entitlement definition. Instead, these have been added to the resource definition.

- 2 Fill in the fields on the request form.
- 3 Click *Submit*.

## Assigning a Resource From the Edit Resource Dialog

- 1 In the *Resource Catalog*, select a resource and click *Edit* to open the *Edit Resource* dialog.

- 2 Click the *Assignments* tab.

The *Assignments* tab displays a list of assignments that have been granted for the selected resource.

- 3 To add a new assignment, click *Assign*.

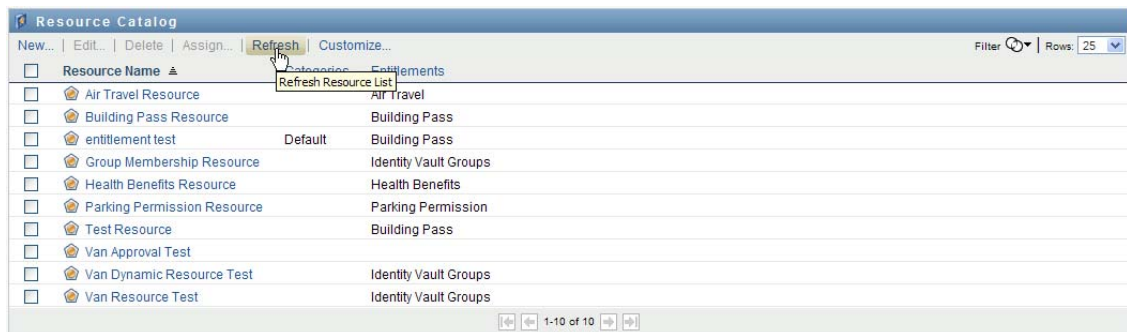
The User Application displays the resource request form:



For details on working with the request form, see [“Assigning a Resource From the Catalog”](#) on page 267.

## 17.1.6 Refreshing the Resource List

- 1 Click *Refresh*.




---

**NOTE:** If you create a resource assignment, and then remove it, you see a message indicating that the assignment has been removed, but the assignment may still be listed. If you refresh the page, you should see that the assignment has been removed.

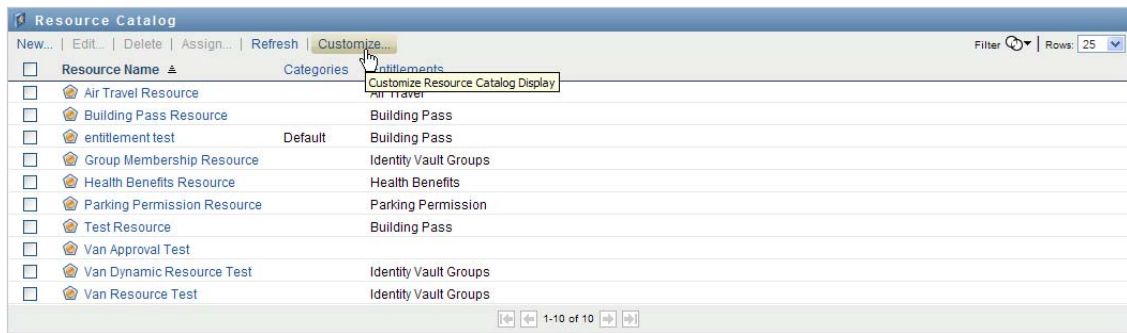
---

## 17.1.7 Customizing the Resource List Display

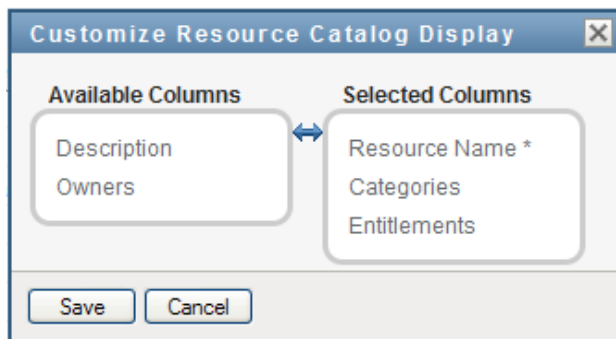
The *Resource Catalog* allows you to select and deselect columns, and also reorder columns within the task list display. The column selection and order are controlled by settings within the *Customize Resource Catalog Display* dialog. When you modify the column list or reorder the columns, your customizations are saved in the Identity Vault along with your other user preferences.

To customize the display of columns:

- 1 Click *Customize* in the *Resource Catalog*:



The User Application displays the list of columns currently selected for the display, and a list of additional columns that are available for selection.



- To include an additional column in the display, select the column in the *Available Columns* list box, and drag it to the *Selected Columns* list box.

To select multiple columns in the list, hold down the Ctrl key and select the columns. To select a range of columns that appear together in the list, hold down the Shift key and select the columns.

You can reorder the columns in the display by moving them up or down in the *Selected Columns* list box.

- To remove a column from the display, select the column in the *Selected Columns* list box, and drag it to the *Available Columns* list box.

The *Resource Name* column is a mandatory column and cannot be removed from the task list display.

- To save your changes, click *Save*.

# 18 Managing Separation of Duties in the User Application

This section describes the separation of duties (SoD) management capabilities of the User Application. Topics include:

- ◆ [Section 18.1, “Browsing the SoD Catalog,” on page 271](#)

## 18.1 Browsing the SoD Catalog

The *SoD Catalog* action on the *Roles and Resources* tab of the Identity Manager user interface allows you to:

- ◆ Define a Separation of Duties (SoD) constraint (or rule).
- ◆ Define how to process requests for exceptions to the constraint.

An SoD constraint represents a rule that makes two roles, of the same level, mutually exclusive. If a user is in one role, they cannot be in the second role, unless there is an exception allowed for that constraint. You can define whether exceptions to the constraint are always allowed or are only allowed through an approval flow.

- ◆ [Section 18.1.1, “Viewing Separation of Duties Constraints,” on page 271](#)
- ◆ [Section 18.1.2, “Creating New Separation of Duties Constraints,” on page 273](#)
- ◆ [Section 18.1.3, “Editing an Existing Separation of Duties Constraint,” on page 274](#)
- ◆ [Section 18.1.4, “Deleting Separation of Duties Constraints,” on page 274](#)
- ◆ [Section 18.1.5, “Refreshing the Separation of Duties Constraint List,” on page 274](#)

### 18.1.1 Viewing Separation of Duties Constraints

- 1 Click *SoD Catalog* in the list of *Roles and Resources* actions.

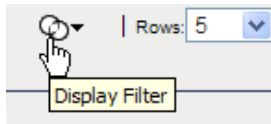
The User Application displays a list of separation of duties constraints currently defined in the catalog.



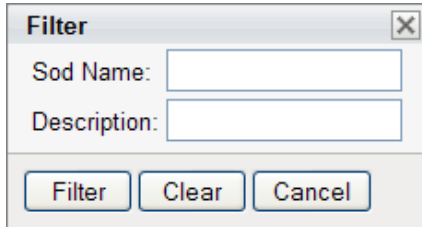
| <input type="checkbox"/> | SoD Name     | Conflicting Roles              | Role Level ▲ | Description  |
|--------------------------|--------------|--------------------------------|--------------|--------------|
| <input type="checkbox"/> | Van SoD Test | reportAdmin<br>complianceAdmin |              | Van SoD Test |

### Filtering the Separation of Duties List

- 1 Click the *Display Filter* button in the upper right corner of the *Separation of Duties Constraints* display.



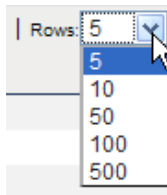
- 2 Specify a filter string for the constraint name or description in the *Filter* dialog.



- 3 Click *Filter* to apply your selection criteria.
- 4 To remove the current filter, click *Reset*.

## Setting the Maximum Number of Rows on a Page

- 1 Click on the Rows dropdown list and select the number of rows you want to be displayed on each page:



## Scrolling within the Separation of Duties List

- 1 To scroll to another page in the constraint list, click on the Next, Previous, First or Last button at the bottom of the list.

## Sorting the Separation of Duties List

To sort the constraint list:

- 1 Click the header for the column you want to sort on.

The pyramid-shaped sort indicator shows you which column is the new sort column. When the sort is ascending, the sort indicator is shown in its normal, upright position.

When the sort is descending, the sort indicator is upside down.

The initial sort column is determined by the administrator.

If you override the initial sort column, your sort column is added to the list of required columns. Required columns are indicated with an asterisk (\*).

When you modify the sort order for the constraint list, your preference is saved in the Identity Vault along with your other user preferences.

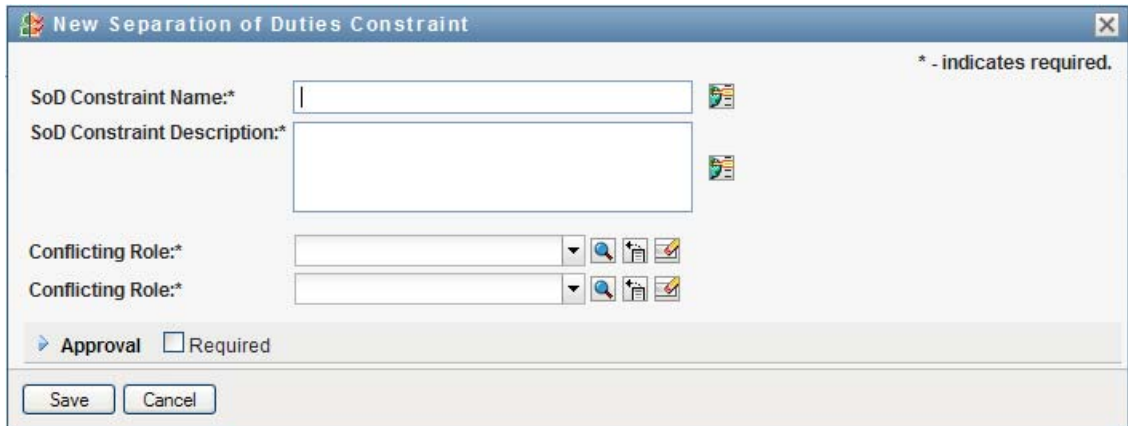


## 18.1.2 Creating New Separation of Duties Constraints

- 1 Click the *New* button at the top of the *Separation of Duties Constraints* display:



The User Application displays the *New Separate of Duties Constraint* dialog:

A screenshot of a dialog box titled "New Separation of Duties Constraint". The dialog has a close button in the top right corner. It contains several fields: "SoD Constraint Name:\*" (text input), "SoD Constraint Description:\*" (text area), "Conflicting Role:\*" (dropdown menu), and another "Conflicting Role:\*" (dropdown menu). Below these fields is a section for "Approval" with a checkbox for "Required". At the bottom are "Save" and "Cancel" buttons. A note in the top right corner says "\* - indicates required.".

- 2 Provide a name for the constraint in the *SoD Constraint Name* field, and type a description in the *SoD Constraint Description* field.
- 3 Select each of the conflicting roles in the two conflicting roles fields. The order of the roles selected is not important.
- 4 Define the approval details, as described under [“Defining the Approval Flow Settings” on page 273](#).

### Defining the Approval Flow Settings

- 1 Open the *Approval* section of the page.
- 2 Specify the approval details, as described below:

| Field           | Description  |
|-----------------|--|
| <i>Required</i> | Select this box if the SoD constraint requires approval for exceptions.<br><br>Deselect this box if the SoD constraint does not require approval for exceptions. |

| Field                        | Description  |
|------------------------------|--|
| <i>Use Default Approvers</i> | <p>Select <i>Yes</i> if you want to use the default list of approvers defined in the SoD approval definition. If you select <i>Yes</i>, the page displays the list of approvers specified in the approval definition. You cannot edit this list.</p> <p>Select <i>No</i> if you want to specify a different list as part of the SoD constraint definition. If you select <i>No</i>, you need to use the <i>Approvers</i> control to specify the users who will be responsible for approving SoD exceptions.</p>  |
| <i>Default Approvers</i>     | Displays a read-only list of the approvers specified on the <i>Configure Roles and Resources Settings</i> page.  |
| <i>Approvers</i>             | <p>Allows you to specify a list of approvers as part of the constraint definition.</p> <p>Select <i>User</i> if the approval task should be assigned to one or more users. Select <i>Group</i> if the approval task should be assigned to a group. Select <i>Container</i> if the approval task should be assigned to one or more containers. Select <i>Role</i> if the approval task should be assigned to a role.</p> <p>To locate a specific user, group, or role, use the <i>Object Selector</i> button. To change the order of the approvers in the list, or to remove an approver, see <a href="#">Section 1.4.4, "Common User Actions," on page 24.</a></p> |

### 18.1.3 Editing an Existing Separation of Duties Constraint

- 1 Select a previously defined role and click *Edit*.
- 2 Make your changes to the role settings and click *Save*.

### 18.1.4 Deleting Separation of Duties Constraints

- 1 Select a previously defined role and click *Delete*.

### 18.1.5 Refreshing the Separation of Duties Constraint List

- 1 Click *Refresh*.

---

# 19 Creating and Viewing Reports

This section describes the reports you can create and view from the *Roles and Resources* tab. Each report is a read-only PDF display of data about the current state of the Role Catalog at the time the report is generated. A single report does not reflect changes in data over a period of time. To track roles information for compliance, please use your audit logs.

---

**IMPORTANT:** The reports you can create and view from the *Roles and Resources* tab have been deprecated and will not be supported in a future release. Novell now recommends that you use the Identity Reporting Module to generate reports.

---

Topics in this section include:

- ♦ [Section 19.1, "About the Role Reporting Actions," on page 275](#)
- ♦ [Section 19.2, "Role Reports," on page 275](#)
- ♦ [Section 19.3, "SoD Reports," on page 279](#)
- ♦ [Section 19.4, "User Reports," on page 281](#)

## 19.1 About the Role Reporting Actions

The *Roles and Resources* tab enables you to create and view reports that describe the current state of roles. These reports can help you to monitor, add, modify, and delete roles or separations of duties.

You must be a Role Administrator or Role Auditor to create and view the role reports. The User Application Administrator has Role Administrator rights by default.

## 19.2 Role Reports

Two role reports are available:

- ♦ Role List Report
- ♦ Role Assignment Report

### 19.2.1 The Role List Report

The Role List Report shows:

- ♦ All roles, grouped by role level
- ♦ The business name of each role
- ♦ The container and description for each role
- ♦ Optionally, Quorum percentages, contained roles, containing roles, groups and containers the role is indirectly assigned to, and entitlements that are bound to each role

To create and view the Role List Report:

- 1 Open the User Application and choose *Reports > Role Reports*.
- 2 Choose *Role List Report* in the *Select a Report* drop-down menu and click *Select*. The Role Reports page prompts you to select the parameters to include in the report.

Role Reports

Select a Role report, specify report details and run the report. Each report will be generated in PDF format and will open in a new window.

\* -indicates required.

Select a Report: Role List Report [v] [Select]

Report Details

**Report Name:** Role List Report  
**Description:** Shows administrative attributes of roles in the role vault.

Select from the options below to filter the results that will appear in the generated report.

Show all administrative details for each role.

Show roles owned by:  All Roles  Select a Role Owner: [ ]

Show Role Levels for:  All Levels  Select Levels: [Permission to connected systems  
IT Role  
Business Role]

Show Role Categories for:  All Categories  Select Categories: [Building Access  
Doctor  
Pharmacist  
System Access]

[Run Report]

- 3 Select *Show all administrative details for each role* to see the following information if applicable and available:
  - ♦ Quorum percentage
  - ♦ Contained roles
  - ♦ Containing roles
  - ♦ Groups that this role is indirectly assigned to
  - ♦ Containers that this role is indirectly assigned to
  - ♦ Entitlements that are bound to the role
- 4 Choose whether to show all roles or roles owned by a selected owner. When you choose *Select Role Owners*, the owner selection box activates. Use this icon to make your selection:
  - ☒ Open the object selection dialog.
    - To select a user, choose First or Last name and type one or more characters of the name to retrieve a selection list. Choose from the selection list.
    - To select a group of users, choose from the Description list of groups, or type characters in the Description box to select a shorter list of groups. Choose from the selection list.
    - To select a container of users, click a container in the directory tree.
- 5 Choose whether to show roles at all security levels, or select one or more levels to show. To select a level, click it in the selection pull-down box. To select more than one level, hold down the Shift key or Ctrl key as you click.

- 6 Choose whether to show roles in all categories, or select one or more categories to show. To select a category, click it in the selection pull-down box. To select more than one category, hold down the Shift key or Ctrl key as you click.
- 7 Click *Run Report* to create and view a PDF report similar to the sample in [Figure 19-1](#).

**Figure 19-1** Sample Role List Report

**Novell** Report Date: Fri Nov 16 15:24:30 EST

| Role List Report                  |  |
|-----------------------------------|--|
| <b>Business Role (Total: 2)</b>   |  |
| <b>Role Name:</b>                 | <b>Doctor (East Campus) (Business Role)</b>  |
| Container                         | Doctor (East Campus).Level30.RoleDefs        |
| Description                       | Doctor (East Campus)                         |
| <b>Role Name:</b>                 | <b>Doctor (West Campus) (Business Role)</b>  |
| Container                         | Doctor (West Campus).Level30.RoleDefs        |
| Description                       | Doctor (West Campus)                         |
| <b>IT Role (Total: 1)</b>         |  |
| <b>Role Name:</b>                 | <b>Doctor (IT Role)</b>                      |
| Container                         | Doctor.Level20.RoleDefs                      |
| Description                       | Doctor                                       |
| <b>Permission Role (Total: 4)</b> |  |
| <b>Role Name:</b>                 | <b>Administer Drugs (Permission Role)</b>    |
| Container                         | Administer Drugs.Level10.RoleDefs            |
| Description                       | Administer Drugs                             |
| <b>Role Name:</b>                 | <b>Order Medical Tests (Permission Role)</b> |

- 8 To save the report, choose *File > Save A Copy* in the Adobe Reader window. Specify a directory to save the file in and specify a filename for the report.

## 19.2.2 The Role Assignment Report

The Role Assignment Report shows:

- ♦ Roles grouped by role level
- ♦ Each role's business name, container, category, and description
- ♦ Users assigned to the role and names of people who approved the assignments

To create and view the Role Assignment Report:

- 1 Open the User Application and choose *Reports > Role Reports*.
- 2 Choose *Role Assignment Report* in the *Select a Report* drop-down menu and click *Select*. The Role Reports page prompts you to select the parameters to include in the report.

**Role Reports**

Select a Role report, specify report details and run the report. Each report will be generated in PDF format and will open in a new window.

\* -indicates required.

Select a Report: Role Assignment Report Select

**Report Details**

**Report Name:** **Role Assignment Report**  
**Description:** Show all assignments for a specific role or group of roles.

Select from the options below to filter the results that will appear in the generated report.

Show assignments for:  All Roles  Select a Role:

Show roles owned by:  All Role Owners  Select a Role Owner:

Show Role Levels for:  All Levels  Select Levels:

Show Role Categories for:  All Categories  Select Categories:

Only show roles that have assignments.

**Sort Order and Grouping**

Role Name List roles by name

Role Category List roles by category

Run Report

- 3 Choose to show all role assignments or to show assignments for selected roles. If you choose *Select Roles*, the selection box activates and presents the selection icons described in [Step 4 on page 276](#).
- 4 Choose to show roles owned by all role owners or by a selected role owner. If you choose *Select a Role Owner*, the selection box activates and presents the selection icons described in [Step 4 on page 276](#).
- 5 Choose to show roles for all role levels or to select one or more role levels. To select a level, click it in the selection pull-down box. To select more than one level, hold down the Shift key or Ctrl key as you click each level.
- 6 Choose to show roles for all role categories or to select one or more role categories. To select a category, click it in the selection pull-down box. To select more than one category, hold down the Shift key or Ctrl key as you click each category.
- 7 Click *Only show roles that have assignments* to filter the report to include only roles that have been assigned.
- 8 If you are choosing to show assignments for all roles rather than just one role, under *Sort Order and Grouping* choose to group roles by either name or category.
- 9 Click *Run Report* to create and view a PDF report similar to the sample in [Figure 19-2](#).

Figure 19-2 Sample Role Assignment Report

Novell. Report Date: Fri Nov 16 15:32:44 EST

| Role Assignment Report          |                         |
|---------------------------------|-------------------------|
| <b>IT Role (Total: 4)</b>       |                         |
| <b>Role Name:</b>               | <b>Doctor (IT Role)</b> |
| Container                       | Doctor.Level20.RoleDefs |
| Role Categories                 |                         |
| Description                     | Doctor                  |
| <b>Assignments to this Role</b> | <b>Approver(s)</b>      |
| Bill Bender (User)              |                         |
| Kate Smith (User)               |                         |
| Chip Nano (User)                |                         |
| <b>Role Name:</b>               | <b>Nurse (IT Role)</b>  |
| Container                       | Nurse.Level20.RoleDefs  |

- 10 To save the report, choose *File > Save A Copy* in the Adobe Reader window. Specify a directory to save the file in and specify a filename for the report.

## 19.3 SoD Reports

Two reports describe the current state of separation of duties:

- ♦ SoD Constraint Report
- ♦ SoD Violations and Exceptions Report

### 19.3.1 SoD Constraint Report

The SoD Constraint Report shows:

- ♦ Currently defined separation of duties constraints by name
- ♦ The description of the separation of duties
- ♦ The list of the conflicting roles
- ♦ The list of people with permission to approve an exception to a violation of separation of duties

To create and view the SoD Constraint Report:

- 1 Open the User Application and choose *Reports > SoD Reports*.
- 2 Choose *SoD Constraint Report* in the *Select a Report* drop-down menu and click *Select*. The Role Reports page prompts you to select the parameters to include in the report.

- 3 Choose to list all SoD Constraints, or select one SoD Constraint. If you choose *Select an SoD Constraint*, the selection box activates. See the description of selection box icons at [Step 4 on page 276](#).
- 4 Choose to list all roles or select a role. If you choose *Select a Role*, the selection box activates. See the description of selection box icons at [Step 4 on page 276](#).
- 5 Click *Run Report* to create and view a PDF report similar to the one in [Figure 19-3](#).

**Figure 19-3** Sample SoD Constraint Report

|   |   |
|---|---|
| Novell.                                       | Report Date: Fri Nov 16 15:23:08 EST              |
| <b>Sod Constraint Report</b>                  |   |
| <b>SoD Constraint Name: Doctor-Nurse</b>      |   |
| SoD Constraint Description                    | Doctor-Nurse                                      |
| Conflicting Roles                             | Doctor, Nurse                                     |
| Approver(s)                                   | Ned North, Sally South                            |
| <hr/>   |   |
| <b>SoD Constraint Name: Doctor-Pharmacist</b> |   |
| SoD Constraint Description                    | Doctor-Pharmacist                                 |
| Conflicting Roles                             | Doctor, Pharmacist                                |
| Approver(s)                                   | Anthony Palani, Chip Nano, Ned North, Sally South |

- 6 To save the report, choose *File > Save A Copy* in the Adobe Reader window. Specify a directory to save the file in and specify a filename for the report.

## 19.3.2 SoD Violations and Exceptions Report

The SoD Violations and Exceptions Report shows:

- ◆ The name of each separation of duties constraint, its description, and the conflicting roles
- ◆ The users in violation of the constraint, including both approved exceptions and unapproved violations. Users can be in violation by being members of a group or container that grants them a conflicting role.
- ◆ Approved exceptions. These are violations that have been approved as exceptions to the separation of duties.
- ◆ The names of those who approved or denied the exceptions and the date and time of the approval or denial.



To create and view the SoD Violations and Exceptions Report:

- 1 Open the User Application and choose *Reports > SoD Reports*.
- 2 Choose *SoD Violations and Exceptions Report* in the *Select a Report* drop-down menu and click *Select*. The Role Reports page prompts you to select the parameters to include in the report.

- 3 Choose *All SoD Constraints* to show any violations and exceptions outstanding across all SoD constraints. Or, choose *Select an SoD Constraint* to focus the report on violations of a single SoD constraint.
- 4 Click *Run Report* to create and view a PDF report similar to the sample shown below.

**Novell.**

Report Date: **Fri Nov 16 15:23:52 EST**

### **Sod Violations and Exceptions Report**

**SoD Constraint Name:** Doctor-Nurse  
**SoD Constraint Description:** Doctor-Nurse  
**Conflicting Roles:** Doctor, Nurse  
**List of all users in violation:**  
Bill Bender, Kate Smith  
**Approved Exception(s)**  
Bill Bender  
Bill Bender

**Approver(s)**  
Ned North (Denied, 11/16/07 11:45 AM)  
Sally South (Approved, 11/16/07 11:46 AM)  
Ned North (Denied, 11/16/07 11:46 AM)  
Sally South (Approved, 11/16/07 11:47 AM)

- 5 To save the report, choose *File > Save A Copy* in the Adobe Reader window. Specify a directory to save the file in and specify a filename for the report.

## 19.4 User Reports

Two user reports are available:

- ♦ User Roles Report
- ♦ User Entitlement Report

### 19.4.1 User Roles Report

The User Roles Report shows:

- ♦ Selected users, groups of users, or containers of users

- ♦ The Roles in which each user holds membership
- ♦ The date at which membership in the role became or becomes effective
- ♦ The expiration date of the role membership
- ♦ Optionally, the source of the membership in the role

To create and view a User Roles Report:

- 1 Open the User Application and choose *Reports > User Reports*.
- 2 Choose *User Roles Report* in the *Select a Report* drop-down menu and click *Select*.

- 3 In the *User* pane, choose either a user, group, or container for whom or which you want to view roles. See the description of selection box functions at [Step 4 on page 276](#).
- 4 In the *Report Details* pane, choose one or more types of detail to report:

| Detail   | Meaning  |
|--|--|
| <i>Only show directly assigned roles.</i>                        | The User Roles Report shows any roles that are directly assigned to the selected user, if any. The report does not show roles inherited from membership in a group or container. |
| <i>Include approval information for directly assigned roles.</i> | The User Roles Report shows who approved each directly assigned role for each user.  |
| <i>Only show users with role(s) assigned.</i>                    | The User Roles Report shows selected users who have assigned roles. The report does not show users who do not have directly or indirectly assigned roles.                        |

- 5 In the *Sort Order and Grouping* pane, choose to sort users by first name or last name.

6 In the *Sort Order and Grouping* pane, choose to sort each user's roles by level or name.

7 Click *Run Report* to create and view a report similar to the sample shown below.

**Novell.** Report Date: **Fri Nov 16 15:22:32 EST**

| User Roles Report          |  |                   |                   |
|----------------------------|--|-------------------|-------------------|
| <b>User: Allison Blake</b> |  |                   |                   |
| Role                       | Source                                     | Effective Date    | Expiration Date   |
| Order Medical Tests        | Direct Assignment                          | 11/16/07 11:41 AM |                   |
| <b>User: Bill Bender</b>   |  |                   |                   |
| Role                       | Source                                     | Effective Date    | Expiration Date   |
| Nurse                      | Direct Assignment                          | 11/16/07 11:46 AM | 12/29/07 12:00 AM |
| Doctor                     | Direct Assignment                          | 11/16/07 11:47 AM | 12/29/07 12:00 AM |
| Pharmacist                 | Membership in Group Pharmacy               | 11/16/07 11:50 AM |                   |
| Order Medical Tests        | Membership in Role Relationship Doctor     | 11/16/07 11:47 AM |                   |
| Write Prescriptions        | Membership in Role Relationship Doctor     | 11/16/07 11:47 AM |                   |
| Administer Drugs           | Membership in Role Relationship Doctor     | 11/16/07 11:46 AM |                   |
| Fill Prescriptions         | Membership in Role Relationship Pharmacist | 11/16/07 11:50 AM |                   |
| Perform Medical Tests      | Membership in Role Relationship Doctor     | 11/16/07 11:46 AM |                   |

8 To save the report, choose *File > Save A Copy* in the Adobe Reader window. Specify a directory to save the file in and specify a filename for the report.

## 19.4.2 User Entitlements Report

The User Entitlements Report shows:

- ♦ All entitlements by their distinguished names
- ♦ Users that hold each entitlement
- ♦ The date at which the user's entitlement becomes effective
- ♦ The date at which the user's entitlement expires
- ♦ The role the user holds that grants the entitlement

To create and view a User Entitlements Report:

- 1 Open the User Application and choose *Reports > User Reports*.
- 2 Choose *User Entitlements Report* in the *Select a Report* drop-down menu and click *Select*.

**User Reports**

Select a Role report, specify report details and run the report. Each report will be generated in PDF format and will open in a new window.

\* -indicates required.

Select a Report:

**User Selection**

**Report Name:** User Entitlements Report  
**Description:** Show list of Entitlements.

Select from the options below to filter the results that will appear in the generated report.

Select User:

Select Group:

Select Container:

**Sort Order and Grouping**

List entitlement details for each user  
 List user details for each entitlement

- 3 In the *User Selection* pane, select the kind of user: an individual user, group, or container. Descriptions of the selection icons are at [Step 4 on page 276](#).
- 4 In the *Sort Order and Grouping* pane, choose one of the following:
  - ◆ *List entitlement details for each user*
  - ◆ *List user details for each entitlement*
- 5 Choose *Run Report* to see a PDF report similar to one of the samples in [Figure 19-4](#) and [Figure 19-5](#).

**Figure 19-4** Sample User Entitlements Report: Entitlement Details for Each User

**Novell** Report Date: Fri Nov 16 15:35:58 EST

---

**User Entitlements Report**

| Entitlement   | Source (Membership in Role) | Effective Date | Expiration Date |
|---|-----------------------------|----------------|-----------------|
| <b>User: Bill Bender</b>                                  |                             |                |                 |
| cn=MedSecureAccess,cn=HajenDriver,cn=TestDrivers,o=novell | Doctor                      | 11/16/2007     | 12/29/2007      |
| <b>User: Kate Smith</b>                                   |                             |                |                 |
| cn=MedSecureAccess,cn=HajenDriver,cn=TestDrivers,o=novell | Doctor                      | 11/16/2007     | 12/30/2007      |
| <b>User: Chip Nano</b>                                    |                             |                |                 |
| cn=MedSecureAccess,cn=HajenDriver,cn=TestDrivers,o=novell | Doctor                      | 11/16/2007     | 11/25/2007      |

**Figure 19-5** Sample User Entitlements Report: User Details for Each Entitlement

**Novell.** Report Date: Fri Nov 16 15:36:25 EST

---

**User Entitlements Report**

Entitlement: cn=MedSecureAccess,cn=HajenDriver,cn=TestDrivers,o=novell

| User        | Source (Membership in Role) | Effective Date | Expiration Date |
|-------------|-----------------------------|----------------|-----------------|
| Bill Bender | Doctor                      | 11/16/2007     | 12/29/2007      |
| Kate Smith  | Doctor                      | 11/16/2007     | 12/30/2007      |
| Chip Nano   | Doctor                      | 11/16/2007     | 11/25/2007      |

---

- 6 To save the report, choose *File > Save A Copy* in the Adobe Reader window. Specify a directory to save the file in and specify a filename for the report.



---

# 20 Configuring the Role and Resource Settings

This section describes the user interface for configuring role and resource settings. It includes the following topics:

- ◆ [Section 20.1, “About the Configure Roles and Resources Settings Action,” on page 287](#)
- ◆ [Section 20.2, “Configuring the Roles Settings,” on page 288](#)
- ◆ [Section 20.3, “Configuring the Resources Settings,” on page 288](#)
- ◆ [Section 20.4, “Configuring the Entitlement Query Settings,” on page 289](#)
- ◆ [Section 20.5, “Configuring the Separation of Duties Settings,” on page 289](#)
- ◆ [Section 20.6, “Configuring the Report Settings,” on page 290](#)

## 20.1 About the Configure Roles and Resources Settings Action

The *Configure Roles and Resources Settings* action allows you to define the basic configuration of the role and resource system. The page has the following sections:

- ◆ Role Settings
- ◆ Resource Settings
- ◆ Entitlement Query Settings
- ◆ Separation of Duties (SoD) Settings
- ◆ Report Settings

To modify the *Configure Roles and Resources Settings* in edit mode, you must have *both* of the following assignments:

- ◆ Role Administrator (or Role Manager with the *Configure Roles Settings* permission)
- ◆ Resource Administrator (or Resource Manager with the *Configure Resources Settings* permission)

To view settings on the *Configure Roles and Resources Settings* page in read-only mode, you only need to have *one* of the permissions listed above.

When you are in edit mode, only some of the settings on the *Configure Roles and Resources Settings* page are editable. Some of the settings show read-only values that are set at installation time and cannot be modified.

## 20.2 Configuring the Roles Settings

To configure the roles settings:

- 1 Click *Configure Roles and Resources Settings* in the *Configuration* group of actions.
- 2 Scroll to the *Roles Settings* section of the page.

Role Settings

These settings control the behavior of the role management components of the User Application. You can define a removal grace period for the time between removal of a role assignment and the initiation of related entitlement removal processes. You can also set the display strings for business levels. The remaining settings are read-only.

Role Container: cn=RoleDefs,cn=RoleConfig,cn=AppConfig,cn=Jboss5Picasso,cn=TestDrivers,o=novell

Role Request Container: cn=Requests,cn=RoleConfig,cn=AppConfig,cn=Jboss5Picasso,cn=TestDrivers,o=novell

Default Role Approval Definition: Role Approval

Role Assignment Grace Period:\* 0 seconds (0=immediate)

Role Level Display Names:\*

Level 30:\* Business Role

Level 20:\* IT Role

Level 10:\* Permission Role

The following settings are read-only settings that are fixed at installation time:

- ◆ Roles Container
  - ◆ Role Request Container
  - ◆ Default Role Approval Definition
- 3 Specify (in seconds) a *Role Assignment Grace Period*.

This value specifies the amount of time, in seconds, before a role assignment is removed from the *Role Catalog* (0 by default). A grace period of zero means that when someone is removed from a role assignment, the removal happens immediately and the subsequent revocation of entitlements is initiated immediately. You might use the grace period to delay the removal of an account that would subsequently be re-added (for example if a person was being moved between containers). An entitlement can disable an account (this is the default) rather than removing it.

---

**NOTE:** The *Role Assignment Grace Period* is a legacy setting that affects only Role to Entitlement assignments; it does not affect Role to Resource to Entitlement mappings. It has no impact on roles created or assigned with the new resource model provided in this release.

---

- 4 Define the display name for the role levels. Each level has a separate display name that can be translated into several languages. To provide foreign-language strings, click *Add language display value*.
- 5 Click *Save* to make your settings permanent.

## 20.3 Configuring the Resources Settings

To view the resource settings:

- 1 Click *Configure Roles and Resources Settings* in the *Configuration* group of actions.
- 2 Scroll to the *Resources Settings* section of the page.



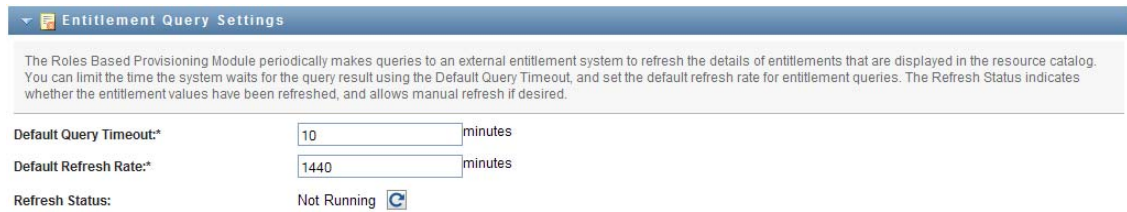


These settings control the behavior of the resource management components of the User Application. All of the resource settings are read-only.

## 20.4 Configuring the Entitlement Query Settings

To configure the entitlement query settings:

- 1 Click *Configure Roles and Resources Settings* in the *Configuration* group of actions.
- 2 Scroll to the *Entitlement Query Settings* section of the page.

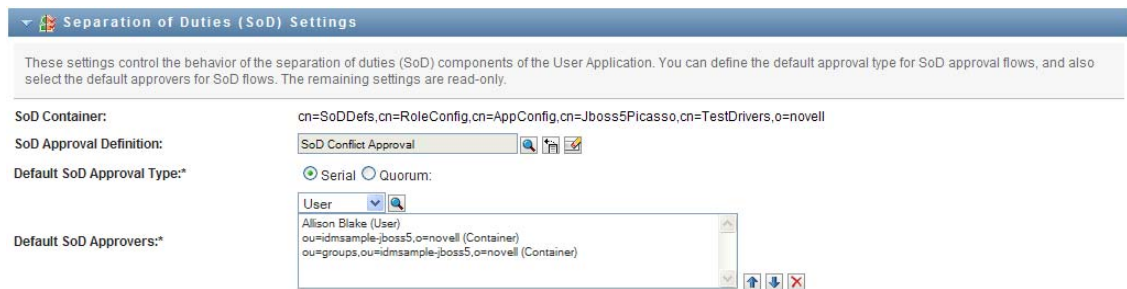


These settings control the behavior of entitlement queries performed by the User Application. You can define a timeout interval and a refresh rate for entitlement queries. In addition, you can see whether the entitlement values have been refreshed, and begin a manual refresh, if necessary.

## 20.5 Configuring the Separation of Duties Settings

To configure the separation of duties (SoD) settings:

- 1 Click *Configure Roles and Resources Settings* in the *Configuration* group of actions.
- 2 Scroll to the *Separation of Duties (SoD) Settings* section of the page.



The SoD Container setting is a read-only setting that is fixed at installation time.

- ◆ SoD Container
- ◆ Default SoD Approval Definition

- 3 In the *SoD Approval Definition* field, choose the provisioning request definition that you will use to handle SoD approvals.
- 4 Choose a *Default SoD Approval Type* of *Serial* or *Quorum*.

| Field         | Description   |
|---------------|---|
| <i>Serial</i> | Select <i>Serial</i> if you want the role to be approved by all of the users in the <i>Approvers</i> list. The approvers are processed sequentially in the order they appear in the list.   |
| <i>Quorum</i> | Select <i>Quorum</i> if you want the role to be approved by a percentage of the users in the <i>Approvers</i> list. The approval is complete when the percentage of users specified is reached.<br><br>For example, if you want one of four users in the list to approve the condition, you would specify <i>Quorum</i> and a percentage of 25. Alternatively, you can specify 100% if all four approvers must approve in parallel. The value must be an integer between 1 and 100. |

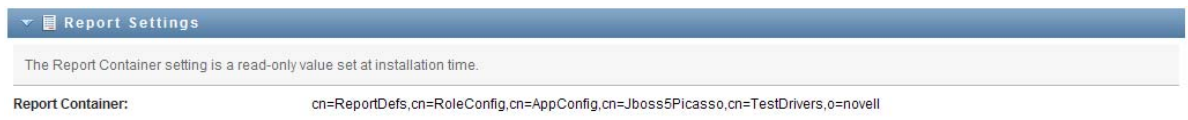
- 5 Modify the *Default SoD Approvers*.

| Field                        | Description   |
|------------------------------|---|
| <i>Default SoD Approvers</i> | Select <i>User</i> if the role approval task should be assigned to one or more users. Select <i>Group</i> if the role approval task should be assigned to a group. Only one member of the group needs to approve. Select <i>Role</i> if the role approval task should be assigned to a role. Like groups, only one member of the role needs to approve.<br><br>To locate a specific user, group, or role, use the Object Selector or History buttons. To change the order of the approvers in the list or to remove an approver, see <a href="#">Section 1.4.4, "Common User Actions," on page 24</a> |

- 6 Click *Save* to make your settings permanent.

## 20.6 Configuring the Report Settings

The *Report Container* value is a read-only setting that is fixed at installation time.



---

# V Using the Compliance Tab

These sections tell you how to use the *Compliance* tab of the Identity Manager User Application:

- ♦ [Chapter 21, “Introducing the Compliance Tab,” on page 293](#)
- ♦ [Chapter 22, “Making Attestation Requests,” on page 307](#)



---

# 21 Introducing the Compliance Tab

This section provides an overview of the Compliance tab. Topics include:

- ♦ [Section 21.1, “About the Compliance Tab,” on page 293](#)
- ♦ [Section 21.2, “Accessing the Tab,” on page 296](#)
- ♦ [Section 21.3, “Exploring the Tab’s Features,” on page 296](#)
- ♦ [Section 21.4, “Compliance Actions You Can Perform,” on page 297](#)
- ♦ [Section 21.5, “Understanding the Attestation Requests Legend,” on page 298](#)
- ♦ [Section 21.6, “Common Compliance Actions,” on page 300](#)

For more general information about accessing and working with the Identity Manager user interface, see [Chapter 1, “Getting Started,” on page 15](#).

## 21.1 About the Compliance Tab

The *Compliance* tab provides a convenient way to perform compliance-based actions.

The *Compliance* tab allows you to initiate attestation processes and check the status of these processes. You can use the *Compliance* tab to:

- ♦ Initiate an attestation process to allow users to confirm that their user profiles contain accurate information
- ♦ Initiate an attestation process to verify the violations and approved exceptions for a set of separation of duties (SoD) constraints
- ♦ Initiate an attestation process to verify the assignments for a set of roles
- ♦ Initiate an attestation process to verify the assignments for a set of users
- ♦ View the status of your attestation requests to analyze the results for each process

---

**NOTE:** The *Compliance* tab is available only with Identity Manager 4.0.2 Advanced Edition. Standard Edition does not support this feature.

---

### Compliance and Proxy mode

Proxy mode works only on the *Work Dashboard* tab and is not supported on the *Compliance* tab. If you enter proxy mode on the *Work Dashboard* tab, and then switch to the *Compliance* tab, proxy mode is turned off for both tabs.

## 21.1.1 About Compliance and Attestation

*Compliance* is the process of ensuring that an organization conforms to relevant business laws and regulations. One of the key elements of compliance is attestation. *Attestation* gives an organization a method for verifying that personnel are fully aware of organizational policies and are taking steps to comply with these policies. By requesting that employees or administrators regularly attest to the accuracy of data, management ensures that personnel information such as user profiles, role assignments, and approved separation of duties (SoD) exceptions are up-to-date and in compliance.

### Attestation Requests and Processes

To allow individuals within an organization to verify the accuracy of corporate data, a user makes an *attestation request*. This request in turn initiates one or more workflow processes. The *workflow processes* give the *attesters* an opportunity to attest to the correctness of the data. A separate workflow process is initiated for each attester. An attester is assigned a workflow task in the *Task Notifications* list on the *Work Dashboard* tab. To complete the workflow process, the attester opens the task, reviews the data, and attests that it is correct or incorrect.

The Roles Based Provisioning Module supports four types of attestation:

- ◆ User profile
- ◆ SoD violations
- ◆ Role assignment
- ◆ User assignment

In the case of a user profile attestation process, each user must be the attester for his/her own profile; no other individual can be the attester. In the case of SoD violation, role assignment, and user assignment attestation, the attester may be any user, group, or role. The initiator for the attestation request specifies whether every member or only a single member must attest for a group or role. In the case of a user attestation process, every member must attest for a selected group or role.

To simplify the process of making attestation requests, the Roles Based Provisioning Module installs a set of default request definitions, one for each attestation type:

- ◆ User Profile - Default
- ◆ SoD Violation - Default
- ◆ Role Assignment - Default
- ◆ User Assignment - Default

You can use these request definitions as the basis for making your own requests. Once you've provided the details for a new request, you can save these details for future use.

### Attestation Forms

Each workflow has an *attestation form* associated with it. The attester must review the form and fill it in to affirm the correctness of the data. The form is usually defined by the Compliance Administrator.

Each attestation form contains a required *attestation question* along with a set of optional *survey questions*. The attestation question is a yes or no question attesting to or denying the overall data. Survey questions can be set up to gather additional data or ask qualifying questions.

The user profile attestation form also include a set of *user attributes* with values that the attester must review. The attestation form for an SoD violation, role assignment, or user assignment process includes an *attestation report*.

## Attestation Reports

The attestation report for an SoD violation, role assignment, or a user assignment process provides detailed information that the attester is expected to review. The report is generated at the time the attestation process is initiated to ensure that all users are reviewing the same information. The report may be generated in several languages, depending on the report languages settings specified for the attestation process.

## Attestation Request Status

Once an attestation request has been initiated, it can be easily tracked throughout its lifecycle. The User Application provides a convenient way to look at the status of the request as a whole, as well as the detailed status for each individual workflow process associated with the request. The high-level status for a request gives the user a way to see whether the request is running, completed, initializing, or in error. The detailed status provides information about the number of workflow processes, and the status for each workflow. In addition, it shows the *attestation results*, which indicate how many answers to the attestation question were affirmative and how many were negative. The attestation results also show which attesters have not taken any action on their assigned workflow tasks.

## Compliance Security

The Compliance tab recognizes a single administrator role called the Compliance Administrator. A Compliance Administrator is designated at installation time. After installation, additional users can be assigned to the Compliance Administrator role. To make additional assignments, you need to use the *RBPM Provisioning and Security > Administrator Assignments* page in the User Application.

The Compliance Administrator role is described in detail below:

**Table 21-1** System Role for Compliance Functions

| Role                     | Description   |
|--------------------------|---|
| Compliance Administrator | <p>An administrator who has the full range of capabilities within the Compliance domain. The Compliance Administrator can perform all possible actions for all objects within the Compliance domain.</p> <p>These actions include the ability to:</p> <ul style="list-style-type: none"><li>◆ Request user profile attestation processes.</li><li>◆ Request SoD violation attestation processes.</li><li>◆ Request role assignment attestation processes.</li><li>◆ Request user assignment attestation processes.</li><li>◆ View the status for all attestation requests that have been submitted.</li></ul> <p><b>NOTE:</b> Any user can be defined as an attester for an attestation process. An attester does not need to belong to either the Compliance Administrator role.</p> |

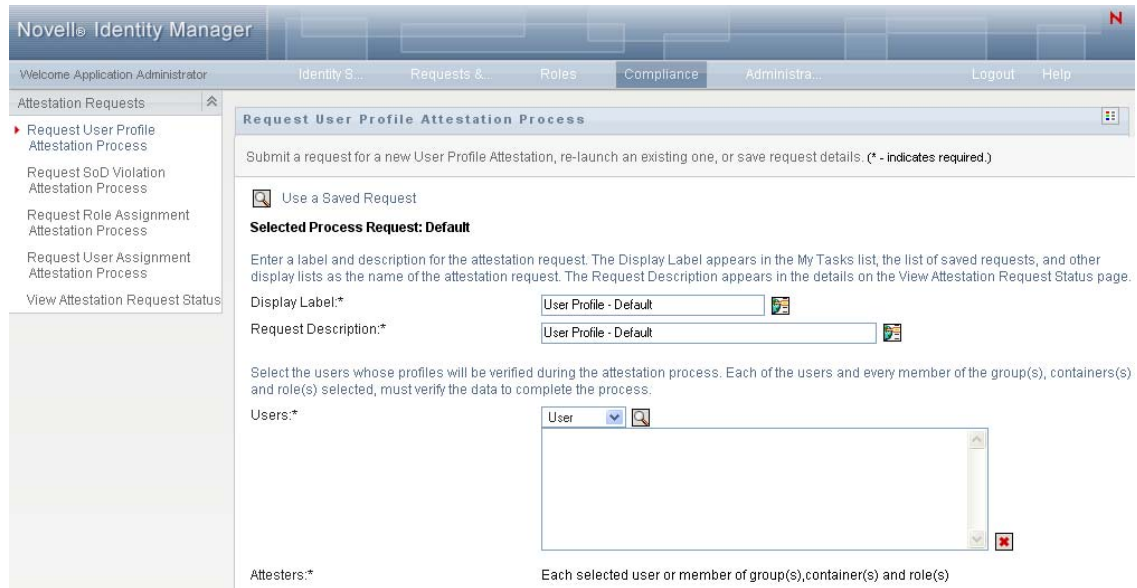
The *Compliance* tab does not allow access by authenticated users that do not have membership in the Compliance Administrator role listed above.

## 21.2 Accessing the Tab

To access the *Compliance* tab:

- 1 Click *Compliance* in the User Application.

By default, the *Compliance* tab displays the Request User Profile Attestation Process page.



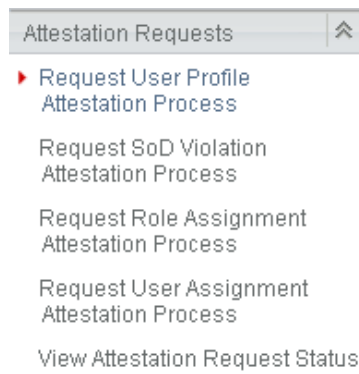
If you go to another tab in the user interface but then want to return, you just need to click the *Compliance* tab to open it again.

## 21.3 Exploring the Tab's Features

This section describes the default features of the *Compliance* tab. (Your tab might look different because of customizations made for your organization; consult your system administrator.)

The left side of the *Compliance* tab displays a menu of actions you can perform. The actions are listed within the *Attestation Requests* category:

**Figure 21-1** *Compliance Tab Menu*

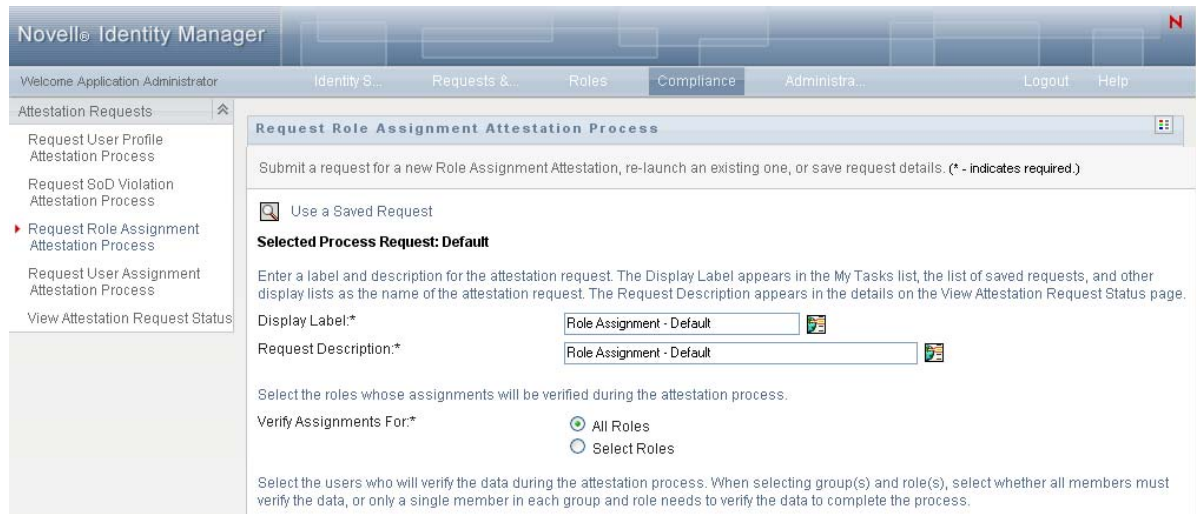


The *Attestation Requests* actions are only displayed if you are a Compliance Administrator.



When you click an action, it displays a corresponding page on the right. The page typically contains a window that shows the details for that action. For example, it might display a list or a form where you can enter data or make a selection, as shown below:

**Figure 21-2** Page Displayed for an Action



Most pages you work with on the *Compliance* tab include a button in the upper right corner that lets you display the *Compliance* legend:



For details on the *Compliance* legend, see [Section 21.5, “Understanding the Attestation Requests Legend,”](#) on page 298.

## 21.4 Compliance Actions You Can Perform

Here’s a summary of the actions that are available to you by default on the *Compliance* tab:

**Table 21-2** *Compliance Actions*

| Category             | Action                                      | Description  |
|----------------------|---|--|
| Attestation Requests | Request User Profile Attestation Process    | Submits a request for an attestation process to verify user profile information.<br><br>For details, see <a href="#">Section 22.2, “Requesting User Profile Attestation Processes,”</a> on page 307.   |
|                      | Request SoD Violation Attestation Process   | Submits a request for an attestation process to verify the violations and exceptions for a set of SoD constraints.<br><br>For details, see <a href="#">Section 22.3, “Requesting SoD Violation Attestation Processes,”</a> on page 309.  |
|                      | Request Role Assignment Attestation Process | Submits a request for an attestation process to verify assignments for selected roles.<br><br>For details, see <a href="#">Section 22.4, “Requesting Role Assignment Attestation Processes,”</a> on page 311.  |
|                      | Request User Assignment Attestation Process | Submits a request for an attestation process to verify assignments for selected users.<br><br>For details, see <a href="#">Section 22.5, “Requesting User Assignment Attestation Process,”</a> on page 313.  |
|                      | View Attestation Request Status             | Allows you to see the status of your attestation requests. In addition, it gives you the option to see the detailed status for each workflow started for a request and optionally retract a workflow.<br><br>For details, see <a href="#">Section 22.6, “Checking the Status of Your Attestation Requests,”</a> on page 315. |

## 21.5 Understanding the Attestation Requests Legend

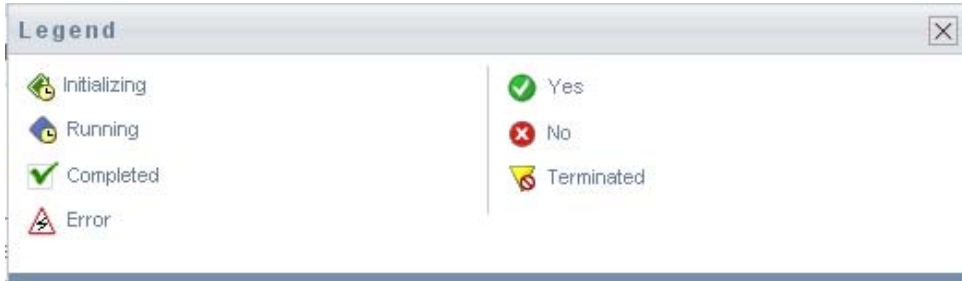
Most pages you work with on the *Compliance* tab include a button in the upper right corner that lets you display the *Compliance* legend. To display the legend, click the *Legend* button, shown in [Figure 21-3](#) on page 298:

**Figure 21-3** *The Legend Button*



The legend provides a brief description of the icons used throughout the *Compliance* tab. The figure below shows the legend.

**Figure 21-4** Compliance Legend



The table below provides detailed descriptions of the icons in the legend:

**Table 21-3** Legend Icons

| Icon                | Description  |
|---------------------|--|
| <i>Initializing</i> | Indicates that an attestation request has started.<br><br>Appears on the View Attestation Request Status page. Note that you are not able to view the details of an initializing request on the View Attestation Request Status page.                |
| <i>Running</i>      | Indicates that an attestation request is still in process.<br><br>Appears on the View Attestation Request Status page.   |
| <i>Completed</i>    | Indicates that an attestation request has completed processing.<br><br>Appears on the View Attestation Request Status page.  |
| <i>Error</i>        | Indicates that an error occurred during the course of processing.<br><br>Appears on the View Attestation Request Status page.  |
| <i>Yes</i>          | Indicates that an attester verified that the information for an attestation process is correct.<br><br>Appears on the View Attestation Request Status page.  |
| <i>No</i>           | Indicates that an attester has invalidated the information for an attestation process.<br><br>Appears on the View Attestation Request Status page.   |
| <i>Terminated</i>   | Indicates that a workflow for an attestation request terminated before completion, because the user retracted the workflow or because an error occurred during the course of processing.<br><br>Appears on the View Attestation Request Status page. |

## 21.6 Common Compliance Actions

The Compliance tab provides a consistent user interface with common tools for accessing and displaying data. This section describes several of the common user interface elements and includes instructions for:

- ♦ [Section 21.6.1, “Specifying the Label and Description for a Request,” on page 300](#)
- ♦ [Section 21.6.2, “Defining the Attesters,” on page 300](#)
- ♦ [Section 21.6.3, “Specifying the Deadline,” on page 301](#)
- ♦ [Section 21.6.4, “Defining the Attestation Form,” on page 302](#)
- ♦ [Section 21.6.5, “Submitting an Attestation Request,” on page 303](#)
- ♦ [Section 21.6.6, “Saving Request Details,” on page 304](#)
- ♦ [Section 21.6.7, “Using a Saved Request,” on page 305](#)

### 21.6.1 Specifying the Label and Description for a Request

You need to define a display label and description for all attestation request types. The *Compliance* tab provides a consistent interface for doing this.

To define the display label and request description:

- 1 In the left-navigation menu on the *Compliance* tab, select the action you want to perform under *Attestation Requests*.
- 2 Type a label in the *Display Label* field.  
The Display Label appears in the My Tasks list, the list of saved requests, and other display lists as the name of the attestation process.  
To provide localized text for the label, click the *Add Language* button. Then, type the localized text to the right of the target language, and click *OK*.
- 3 Type a description in the *Request Description* field.  
When you review the request status on the View Attestation Request Status page, the Request Description appears in the details for the request.  
To provide localized text for the description, click the *Add Language* button. Then, type the localized text to the right of the target language, and click *OK*.

### 21.6.2 Defining the Attesters

The *Request SoD Violation Attestation Process*, *Request Role Assignment Attestation Process*, and *Request User Assignment Attestation Process* actions provide a consistent interface for defining attesters.

To define the attesters for an SoD, role assignment, or user assignment attestation process:

- 1 In the left-navigation menu on the *Compliance* tab, select the action you want to perform under *Attestation Requests*.
- 2 In the *Attesters* field, specify which users, groups, and roles will be attesters for the attestation process:
  - 2a To add one or more users to the list, select *User* in the drop-down list.

Select the users who will verify the data during the attestation process. When selecting group(s) and role(s), select whether all members must verify the data, or only a single member in each group and role needs to verify the data to complete the process.

Attesters:\*

The screenshot shows a web interface for selecting attesters. It features a dropdown menu with three options: 'User', 'Group', and 'Role'. Below the dropdown is a large, empty list area with a search icon and a delete icon. At the bottom, there are two radio buttons: 'Every member of the group(s) and role(s) selected must attest to the data.' and 'A single member of each group and role selected must attest to the data.'

Use the *Object Selector* to select the users. In the *Object Selector*, you can include multiple users by clicking the checkbox for each item, and clicking *Select*.

For details on using the *Object Selector*, see [Section 1.4.4, “Common User Actions,”](#) on page 24.

**2b** To add one or more groups to the list, select *Group* in the drop-down list.

Use the *Object Selector* to select the groups. In the *Object Selector*, you can include multiple users by clicking the checkbox for each item, and clicking *Select*.

**2c** To add one or more roles to the list, select *Role* in the drop-down list.

Use the *Object Selector* to select the roles. In the *Object Selector*, you can include multiple roles by clicking the checkbox for each item, and clicking *Select*.

**2d** To delete an item, select it and click the *Delete* button. You can select multiple items before clicking the *Delete* button.

**2e** For group(s) and role(s) attesters, specify whether all members must attest to the data or only a single member in each group and role by selecting one of the following buttons:

- ◆ *Every member of the group(s) and role(s) selected must attest to the data.*
- ◆ *A single member of each group and role selected must attest to the data.*

In the case of a user profile attestation process, every member of a selected group or role must attest.

## 21.6.3 Specifying the Deadline

Each attestation process has a deadline associated with it. The deadline indicates how long you want the process to continue running.

The deadline is required to launch an attestation process, but is not required for a saved request.

To specify the deadline for an attestation process:

- 1** In the left-navigation menu on the *Compliance* tab, select the action you want to perform under *Attestation Requests*.
- 2** In the *Deadline* field, indicate how long you want the attestation process to continue running. If you want to specify the duration for the process in weeks, days, or hours, type a number in the *Duration* field, and select *Weeks*, *Days*, or *Hours* as the unit of measure. If you would prefer to define an expiration date, select *Specify End Date* and use the Calendar control to select the date and time. If the process will run indefinitely, select *No Expiration*.

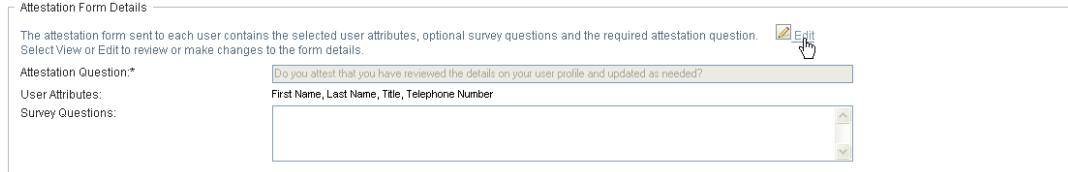
The value specified in the *Deadline* field is not stored with the details for a saved request.

## 21.6.4 Defining the Attestation Form

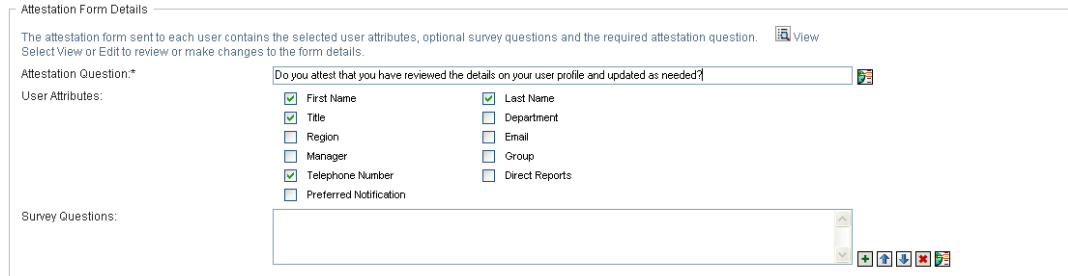
You need to define an attestation form for all attestation types. The *Compliance* tab provides a consistent interface for doing this.

To define the form for an attestation process:

- 1 In the left-navigation menu on the *Compliance* tab, select the action you want to perform under *Attestation Requests*.
- 2 Define the details of the attestation form, as follows:
  - 2a Click the *Edit* button.



- 2b Type the attestation question in the *Attestation Question* field.



The attestation question is a required question for any attestation process. This question gives the attester an opportunity to attest to or invalidate the data. The question must have a simple yes or no answer. You must define an attestation question when initiating an attestation process, and each attester must answer this question to complete their response.

To provide localized text for the attestation question, click the *Add Language* button. Then, type the localized text to the right of the target language, and click *OK*.

- 2c For a user profile attestation process, you need to indicate which user attributes you want to verify. In the *User Attributes* field, select each attribute you want to include.

The list of attributes to choose from includes all attributes marked as viewable in the directory abstraction layer, except for those that are binary or calculated.

- 2d In the *Survey Questions* field, you can optionally include one or more questions that an attester can answer during the execution of an attestation process. An attestation process is not required to include survey questions. However, if they are included, they may optionally be answered by the attester.

Follow these steps to define and organize the list of survey questions:

- 2d1 Click the *Add Item* button to add a survey question.



Type the localized text for the question to the right of the target language, and click *OK*.

**2d2** To move a question up in the list, select the question and click the *Move Up* button.

**2d3** To move a question down in the list, select the question and click the *Move Down* button.

**2d4** To delete a question, select it and click the *Delete* button.

**2d5** To edit the localized text for an existing question, select the question and click the *Add Language* button. Then, type the localized text to the right of the target language, and click *OK*.

**2e** When you have finished making changes to the form, click the *View* button.

You can switch back and forth between the read only and editable views by clicking the *View* or *Edit* button.

## 21.6.5 Submitting an Attestation Request

After you have defined the details for an attestation request, you need to submit the request to initiate the process. When you submit a request, the User Application displays a confirmation number for your request. This number is also known as a correlation ID, since it correlates a set of workflows associated with a single request.

The following fields are required to launch a request:

**Table 21-4** Fields Required to Launch a Request

| Attestation Type | Required Fields  |
|------------------|--|
| User Profile     | Display Label, Request Description, Users, Deadline, Attestation Question  |
| SoD Violation    | Display Label, Request Description, SoD Constraints, Attesters, Deadline, Report Locale, Attestation Question          |
| Role Assignment  | Display Label, Request Description, Verify Assignments For, Attesters, Deadline, Report Locale, Attestation Question   |
| User Assignment  | Display Label, Request Description, Verify Roles Assigned To, Attesters, Deadline, Report Locale, Attestation Question |

To submit an attestation request:

- 1 In the left-navigation menu on the *Compliance* tab, select the action you want to perform under *Attestation Requests*.
- 2 Click *Submit* to initiate the attestation process.

The *confirmation number* for your request is displayed at the top of the page. Record this number so you can easily track the progress of your request on the View Attestation Request Status page. If you do not record this number, you can always track the request by using the Display Label.

## 21.6.6 Saving Request Details

When you're defining the details for an attestation request, you have the option to save these details for later use. For example, you might want to save the parameter and form values you specify so you can use them again in a future request.

When you click *Use a Saved Request*, the name you specify for the saved request appears in the list of saved requests, along with the display label.

The following fields are required for a saved request:

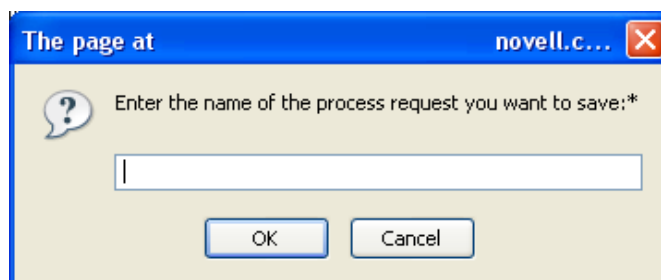
**Table 21-5** Fields Required for a Saved Request

| Attestation Type | Required Fields  |
|------------------|--|
| User Profile     | Display Label, Request Description, Attestation Question                                 |
| SoD Violation    | Display Label, Request Description, SoD Constraints, Report Locale, Attestation Question |
| Role Assignment  | Display Label, Request Description, Roles, Report Locale, Attestation Question           |
| User Assignment  | Display Label, Request Description, Report Locale, Attestation Question                  |

To save request details:

- 1 In the left-navigation menu on the *Compliance* tab, select the action you want to perform under *Attestation Requests*.
- 2 Click *Save Request Details*.

Type the name you would like to use to identify the saved process request and click *OK*.



The following characters are not allowed in the name for a saved request: <> , ; \ " + # = / | & \*  
Spaces at the beginning or the end of the name are automatically stripped out.

If the process request already exists, the User Application prompts you to overwrite the existing definition.



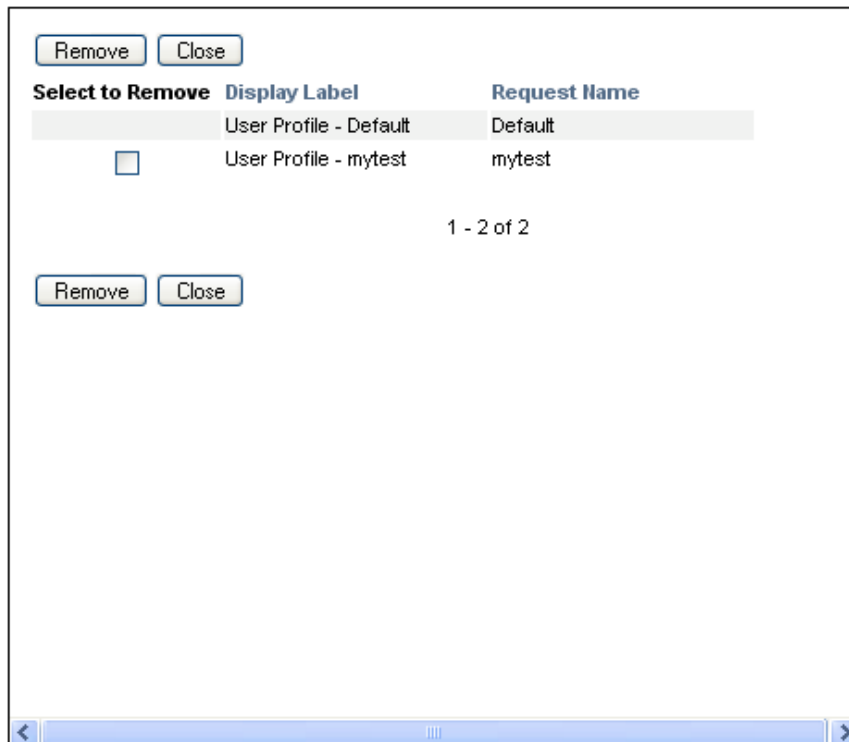
## 21.6.7 Using a Saved Request

When you're making an attestation request, you have the option to use details from a previously saved request as the basis for the new request. The saved requests that are available for selection vary depending on the type of attestation process you are requesting. For example, if you are making a user profile attestation request (as shown below), you will see only those saved requests that apply to user profile attestation processes.

To use a saved request:

- 1 In the left-navigation menu on the *Compliance* tab, select the action you want to perform under *Attestation Requests*.
- 2 Click *Use a Saved Request*.

The User Application displays a pop-in window to allow you to select the saved request.



- 2a To select a request, click the display label or the request name. The request name is the common name (CN) for the saved request definition.
- 2b To remove a saved request, click the checkbox to the left of the display label, and click *Remove*. You can remove multiple saved requests with a single click.

You cannot remove any of the default request definitions that are installed with the product. Therefore, the default request definitions do not show a checkbox.

When you click the *Remove* button, the User Application displays a confirmation window before removing the saved request.



---

# 22 Making Attestation Requests

This section provides instructions for making attestation requests. Topics include:

- ♦ [Section 22.1, “About the Attestation Requests Actions,” on page 307](#)
- ♦ [Section 22.2, “Requesting User Profile Attestation Processes,” on page 307](#)
- ♦ [Section 22.3, “Requesting SoD Violation Attestation Processes,” on page 309](#)
- ♦ [Section 22.4, “Requesting Role Assignment Attestation Processes,” on page 311](#)
- ♦ [Section 22.5, “Requesting User Assignment Attestation Process,” on page 313](#)
- ♦ [Section 22.6, “Checking the Status of Your Attestation Requests,” on page 315](#)

## 22.1 About the Attestation Requests Actions

The *Compliance* tab in the Identity Manager User Application includes a group of actions called *Attestation Requests*. The *Attestation Requests* actions give you the ability to make attestation process requests and check the status of requests you’ve made.

## 22.2 Requesting User Profile Attestation Processes

The *Request User Profile Attestation Process* action lets you initiate an attestation process to verify one or more user profiles. It also gives you the option to save the details associated with an attestation request (such as parameter and form values) as a pre-filled form for later requests.

To initiate a user profile attestation process:

- 1 Click *Request User Profile Attestation Process* in the list of *Attestation Requests* actions.  
The User Application displays a page that lets you specify details about the attestation process.

**Request User Profile Attestation Process**

Submit a request for a new User Profile Attestation, re-launch an existing one, or save request details. (\* - indicates required.)

Use a Saved Request

**Selected Process Request: Default**

Enter a label and description for the attestation request. The Display Label appears in the My Tasks list, the list of saved requests, and other display lists as the name of the attestation request. The Request Description appears in the details on the View Attestation Request Status page.

Display Label:\*

Request Description:\*

Select the users whose profiles will be verified during the attestation process. Each of the users and every member of the group(s), container(s) and role(s) selected, must verify the data to complete the process.

Users:\*

Attesters:\*

Each selected user or member of group(s), container(s) and role(s)

- 2 If you want to use the details from a previously saved request as the basis for this request, click *Use a Saved Request*. For more information, see [Section 21.6.7, "Using a Saved Request,"](#) on page 305.
- 3 Specify the display label and description for the request. For more information, see [Section 21.6.1, "Specifying the Label and Description for a Request,"](#) on page 300.
- 4 In the *Users* box, select the users whose profiles will be verified:
  - 4a To include one or more users explicitly, select *User* in the drop-down list.

Select the users whose profiles will be verified during the attestation process. Each of the users and every member of the group(s), container(s) and role(s) selected, must verify the data to complete the process.

Users:\*

User

Group

Role

Container

Use the *Object Selector* to select the users. In the *Object Selector*, you can include multiple users by clicking the checkbox for each item, and clicking *Select*.

For details on using the *Object Selector*, see [Section 1.4.4, "Common User Actions,"](#) on page 24.

- 4b To include the users in one or more groups, select *Group* in the drop-down list.
 

Use the *Object Selector* to select the groups. In the *Object Selector*, you can include multiple groups by clicking the checkbox for each item, and clicking *Select*.
- 4c To include the users in one or more roles, click *Role* in the drop-down list.
 

Use the *Object Selector* to select the roles. In the *Object Selector*, you can include multiple roles by clicking the checkbox for each item, and clicking *Select*.
- 4d To include the users in a container, click *Container* in the drop-down list.
 

Use the *Object Selector* to drill down to the desired container, then click on the container to select it.

If you want the user assignment report to include all users in the selected sub-containers, you need to check the *Include all users of sub-containers* checkbox at the bottom of the list of selected items. The *Include all users of sub-containers* checkbox is displayed only when *Container* is selected in the drop-down list. However, you can change the *Include all users of sub-containers* setting without having to remove and add any of your previously selected containers.

You must select at least one user, group, role, or container to launch an attestation process. However, you are not required to select a user, group, role, or container to save a request.

- 5 In the *Attesters* field, note that the text is read-only. In a user profile attestation process, the attesters are the users selected in the *Users* field, along with all of the members of any groups, roles, and containers you added in the *Users* field. This is because each user must be the attester for his/her own profile; no other user can be the attester.
- 6 Specify the deadline for the attestation process. For more information, see [Section 21.6.3, “Specifying the Deadline,”](#) on page 301.
- 7 Define the details of the attestation form. For more information, see [Section 21.6.4, “Defining the Attestation Form,”](#) on page 302.
- 8 Submit the request. For more information, see [Section 21.6.5, “Submitting an Attestation Request,”](#) on page 303.
- 9 Optionally click *Save Request Details* to save the details associated with an attestation process request (such as parameter and form values) for later use. For more information, see [Section 21.6.6, “Saving Request Details,”](#) on page 304.

## 22.3 Requesting SoD Violation Attestation Processes

The *Request SoD Violation Attestation Process* action lets you initiate an attestation process to verify the violations and exceptions for one or more SoD constraints. It also gives you the option to save the details associated with an attestation request (such as parameter and form values) as a pre-filled form for later requests.

When you initiate an SoD attestation process, the User Application generates a set of localized reports for the attesters to review.

The attesters do not need to have rights for the selected constraints to review the reports. If an attester selected for an SoD attestation process does not have rights to view an SoD constraint, the User Application still allows the attester to view the report showing the violations and exceptions for the constraint.

To initiate an SoD violation attestation process:

- 1 Click *Request SoD Violation Attestation Process* in the list of *Attestation Requests* actions.  
The User Application displays a page that lets you specify details about the attestation process.

- 2 If you want to use the details from a previously saved request as the basis for this request, click *Use a Saved Request*. For more information, see [Section 21.6.7, “Using a Saved Request,” on page 305](#).
- 3 Specify the display label and description for the request. For more information, see [Section 21.6.1, “Specifying the Label and Description for a Request,” on page 300](#).
- 4 Select the SoD constraints whose violations and exceptions will be verified, as follows:
  - 4a To include all existing constraints, select the *All SoD Constraints* button.

Select the SoD Constraints whose violations and exceptions will be verified during the attainment process.

SoD Constraints:\*  All SoD Constraints  Select SoD Constraints

- 4b To choose the constraints individually, select the *Select SoD Constraints* button.

Use the *Object Selector* to select each constraint. In the *Object Selector*, you can include multiple constraints by clicking the checkbox for each item, and clicking *Select*.

For details on using the *Object Selector* and *Show History* tools, see [Section 1.4.4, “Common User Actions,” on page 24](#).

You must select at least one SoD constraint to launch an attainment process. However, you are not required to select an SoD constraint to save a request.

- 5 In the *Attesters* field, specify which users, groups, and roles will be attesters for the attainment process. For details, see [Section 21.6.2, “Defining the Attesters,” on page 300](#).  
You must select at least one user, group, or role as an attester to launch an attainment process. However, you are not required to select an attester to save a request.
- 6 Specify the deadline for the attainment process. For more information, see [Section 21.6.3, “Specifying the Deadline,” on page 301](#).
- 7 In the *Report Languages* field, click the *Add Language* button to specify which language locales you would like to use for the reports generated for the attainment process. Select the default locale in the *Default Locale* dropdown list. Then, pick the languages you want to include and click *OK*.

When you initiate an SoD attestation process, the User Application generates a set of localized reports for the attesters to review. These reports provide the same data in one or more languages. They are generated at the time the request is submitted to ensure all of the attesters are reviewing the same set of data. You can specify the set of report languages that will be generated and stored for the attestation process. When an attester selects an attestation task for review, the system displays the localized report that matches the attester's preferred locale (or browser locale, if the user does not have a preferred locale). If no report exists for that locale, the User Application displays the report that uses the default locale.

- 8 Define the details of the attestation form. For more information, see [Section 21.6.4, “Defining the Attestation Form,”](#) on page 302.
- 9 Submit the request. For more information, see [Section 21.6.5, “Submitting an Attestation Request,”](#) on page 303.
- 10 Optionally click *Save Request Details* to save the details associated with an attestation process request (such as parameter and form values) for later use. For more information, see [Section 21.6.6, “Saving Request Details,”](#) on page 304.

## 22.4 Requesting Role Assignment Attestation Processes

The *Request Role Assignment Attestation Process* action lets you initiate an attestation process to verify the accuracy of assignments for selected roles. It also gives you the option to save the details associated with an attestation request (such as parameter and form values) as a pre-filled form for later requests.

When you initiate a role assignment attestation process, the User Application generates a set of localized reports for the attesters to review.

The attesters do not need to have rights for the selected roles to review the reports. If an attester selected for a role assignment attestation process does not have rights to view a particular role, the User Application still allows the attester to view the report showing the role assignments.

The report generated for a role assignment attestation process shows the users assigned to the selected roles. Only roles that have assignments are included in the report.

To initiate a role assignment attestation process:

- 1 Click *Request Role Assignment Attestation Process* in the list of *Attestation Requests* actions.  
The User Application displays a page that lets you specify details about the attestation process.

**Request Role Assignment Attestation Process**

Submit a request for a new Role Assignment Attestation, re-launch an existing one, or save request details. (\* - indicates required.)

Use a Saved Request

**Selected Process Request: Default**

Enter a label and description for the attestation request. The Display Label appears in the My Tasks list, the list of saved requests, and other display lists as the name of the attestation request. The Request Description appears in the details on the View Attestation Request Status page.

Display Label:\*

Request Description:\*

Select the roles whose assignments will be verified during the attestation process.

Verify Assignments For:\*  All Roles  Select Roles

Select the users who will verify the data during the attestation process. When selecting group(s) and role(s), select whether all members must verify the data, or only a single member in each group and role needs to verify the data to complete the process.

Attesters:\*

Every member of the group(s) and role(s) selected must attest to the data.  
 A single member of each group and role selected must attest to the data.

- 2 If you want to use the details from a previously saved request as the basis for this request, click *Use a Saved Request*. For more information, see [Section 21.6.7, "Using a Saved Request," on page 305](#).
- 3 Specify the display label and description for the request. For more information, see [Section 21.6.1, "Specifying the Label and Description for a Request," on page 300](#).
- 4 In the *Verify Assignments For* box, select the roles whose assignments will be verified, as follows:
  - 4a To include all existing roles, select the *All Roles* button.

Select the roles whose assignments will be verified during the attestation process.

Verify Assignments For:\*  All Roles  Select Roles

- 4b To choose the roles individually, select the *Select Roles* button.

Use the *Object Selector* or the *Show History* tool to select each role. In the *Object Selector*, you can include multiple roles by clicking the checkbox for each item, and clicking *Select*.

For details on using the *Object Selector* and *Show History* tools, see [Section 1.4.4, "Common User Actions," on page 24](#).

You must select at least one role to launch an attestation process. However, you are not required to select a role to save a request.

- 5 In the *Attesters* field, specify which users, groups, and roles will be attesters for the attestation process. For details, see [Section 21.6.2, "Defining the Attesters," on page 300](#).  
 You must select at least one user, group, or role as an attester to launch an attestation process. However, you are not required to select an attester to save a request.
- 6 Specify the deadline for the attestation process. For more information, see [Section 21.6.3, "Specifying the Deadline," on page 301](#).



- 7 In the *Report Languages* field, click the *Add Language* button to specify which languages you would like to use for the reports generated for the attestation process. Select the default locale in the *Default Locale* dropdown list. Then, pick the languages you want to include and click *OK*.

When you initiate a role assignment attestation process, the User Application generates a set of localized reports for the attesters to review. These reports provide the same data in one or more languages. They are generated at the time the request is submitted to ensure all of the attesters are reviewing the same set of data. You can specify the set of report languages that will be generated and stored for the attestation process. When an attester selects an attestation task for review, the system displays the localized report that matches the attester's preferred locale (or browser locale, if the user does not have a preferred locale). If no report exists for that locale, the User Application displays the report that uses the default locale.

- 8 Define the details of the attestation form. For more information, see [Section 21.6.4, "Defining the Attestation Form,"](#) on page 302.
- 9 Submit the request. For more information, see [Section 21.6.5, "Submitting an Attestation Request,"](#) on page 303.
- 10 Optionally click *Save Request Details* to save the details associated with an attestation process request (such as parameter and form values) for later use. For more information, see [Section 21.6.6, "Saving Request Details,"](#) on page 304.

## 22.5 Requesting User Assignment Attestation Process

The *Request User Assignment Attestation Process* action lets you initiate an attestation process to verify the accuracy of role assignments for selected users. It also gives you the option to save the details associated with an attestation request (such as parameter and form values) as a pre-filled form for later requests.

When you initiate a user assignment attestation process, the User Application generates a set of localized reports for the attesters to review.

The attesters do not need to have rights for the roles associated with the selected users to review the reports. If an attester selected for a user assignment attestation process does not have rights to view a particular role, the User Application still allows the attester to view the report showing the user assignments.

The report shows the role assignments for the selected users. If you choose a container, group, or role, the report shows the role assignments for users within the selected container, group, or role.

To initiate a role assignment attestation process:

- 1 Click *Request User Assignment Attestation Process* in the list of *Attestation Requests* actions.  
The User Application displays a page that lets you specify details about the attestation process.

**Request User Assignment Attestation Process**

Submit a request for a new User Assignment Attestation, re-launch an existing one, or save request details. (\* - indicates required.)

Use a Saved Request

**Selected Process Request: Default**

Enter a label and description for the attestation request. The Display Label appears in the My Tasks list, the list of saved requests, and other display lists as the name of the attestation request. The Request Description appears in the details on the View Attestation Request Status page.

Display Label:\*

Request Description:\*

Select the users whose role assignments will be verified during the attestation process. A report will be generated containing associated role assignments for each of the users and every member of the group(s), containers(s) and role(s) selected.

Verify Roles Assigned To:\*

Select the users who will verify the data during the attestation process. When selecting group(s) and role(s), select whether all members must verify the data, or only a single member in each group and role needs to verify the data to complete the process.

Attesters:\*

- 2 If you want to use the details from a previously saved request as the basis for this request, click *Use a Saved Request*. For more information, see [Section 21.6.7, “Using a Saved Request,” on page 305](#).
- 3 Specify the display label and description for the request. For more information, see [Section 21.6.1, “Specifying the Label and Description for a Request,” on page 300](#).
- 4 In the *Verify Roles Assigned To* box, select the users whose assignments will be verified:
  - 4a To include one or more users explicitly, select *User* in the drop-down list.

Select the users whose role assignments will be verified during the attestation process. A report will be generated containing associated role assignments for each of the users and every member of the group(s), containers(s) and role(s) selected.

Verify Roles Assigned To:\*

User  
 Group  
 Role  
 Container

Use the *Object Selector* to select the users. In the *Object Selector*, you can include multiple users by clicking the checkbox for each item, and clicking *Select*.

For details on using the *Object Selector*, see [Section 1.4.4, “Common User Actions,” on page 24](#).

- 4b To include the users in one or more groups, select *Group* in the drop-down list.
 

Use the *Object Selector* to select the groups. In the *Object Selector*, you can include multiple users by clicking the checkbox for each item, and clicking *Select*.
- 4c To include the users in one or more roles, click *Role* in the drop-down list.
 

Use the *Object Selector* to select the roles. In the *Object Selector*, you can include multiple roles by clicking the checkbox for each item, and clicking *Select*.
- 4d To include the users in a container, click *Container* in the drop-down list.

Use the *Object Selector* to drill down to the desired container, then click on the container to select it.

If you want the user assignment report to include all users in the selected sub-containers, you need to check the *Include all users of sub-containers* checkbox at the bottom of the list of selected items. The *Include all users of sub-containers* checkbox is displayed only when *Container* is selected in the drop-down list. However, you can change the *Include all users of sub-containers* setting without having to remove and add any of your previously selected containers.

You must select at least one user, group, role, or container to launch an attestation process. However, you are not required to select a user, group, role, or container to save a request.

- 5 In the *Attesters* field, specify which users, groups, and roles will be attesters for the attestation process. For details, see [Section 21.6.2, “Defining the Attesters,” on page 300](#).

You must select at least one user, group, or role as an attester to launch an attestation process. However, you are not required to select an attester to save a request.

- 6 Specify the deadline for the attestation process. For more information, see [Section 21.6.3, “Specifying the Deadline,” on page 301](#).

- 7 In the *Report Languages* field, click the *Add Language* button to specify which languages you would like to use for the reports generated for the attestation process. Select the default locale in the *Default Locale* dropdown list. Then, pick the languages you want to include and click *OK*.

When you initiate a user assignment attestation process, the User Application generates a set of localized reports for the attesters to review. These reports provide the same data in one or more languages. They are generated at the time the request is submitted to ensure all of the attesters are reviewing the same set of data. You can specify the set of report languages that will be generated and stored for the attestation process. When an attester selects an attestation task for review, the system displays the localized report that matches the attester's preferred locale (or browser locale, if the user does not have a preferred locale). If no report exists for that locale, the User Application displays the report that uses the default locale.

- 8 Define the details of the attestation form. For more information, see [Section 21.6.4, “Defining the Attestation Form,” on page 302](#).
- 9 Submit the request. For more information, see [Section 21.6.5, “Submitting an Attestation Request,” on page 303](#).
- 10 Optionally click *Save Request Details* to save the details associated with an attestation process request (such as parameter and form values) for later use. For more information, see [Section 21.6.6, “Saving Request Details,” on page 304](#).

## 22.6 Checking the Status of Your Attestation Requests

The *View Attestation Request Status* action lets you see the status of your attestation requests. In addition, it gives you the option to see the detailed status for each workflow process started for a request and optionally retract one or more running processes.

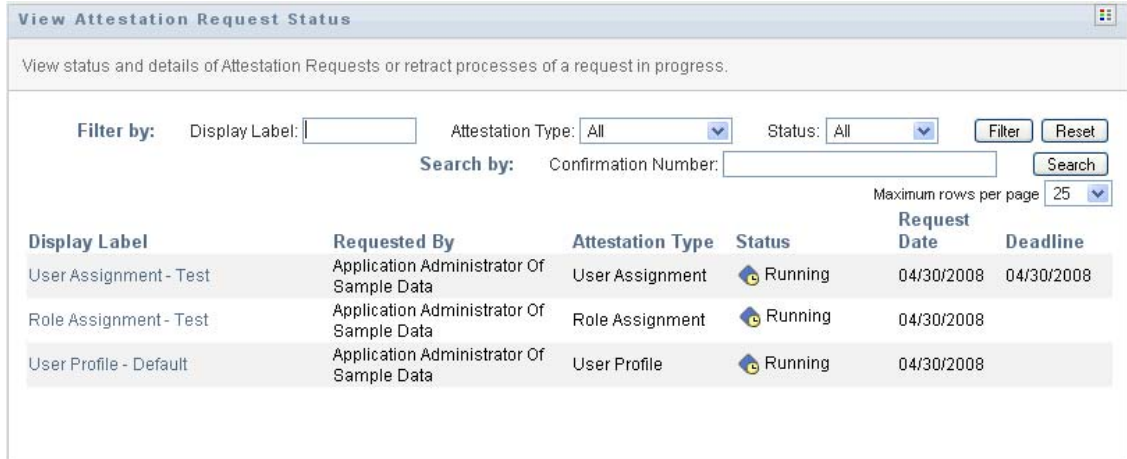
The *View Attestation Request Status* action shows all attestation requests, including those that are initializing, running, completed, or in error.

The User Application does not place any restrictions on what the Compliance Administrator can see on the View Attestation Request Status page. This role permits access to status information about all attestation requests.

To look at your attestation requests:

- 1 Click *View Attestation Request Status* in the list of *Attestation Requests* actions.

The User Application displays the current status of all attestation requests.



The columns in the attestation request list are described below:

- ◆ The *Display Label* column provides the name of the attestation process specified for the request. You can see the detailed status information for the request by clicking on the process display name.
- ◆ The *Requested By* column identifies the user who made the request.
- ◆ The *Attestation Type* column indicates what the type of attestation process this is. The type determines what kinds of information the process is intended to certify, as follows:

| Attestation Type | Description  |
|------------------|--|
| User Profile     | Indicates that this process is intended to ensure the accuracy of user profile information. To initiate this type of process, a Compliance Administrator needs to use the <i>Request User Profile Attestation Process</i> action.  |
| SoD Violation    | Indicates that this process is intended to ensure the accuracy of separation of duties violations and exceptions. To initiate this type of process, a Compliance Administrator needs to use the <i>Request SoD Violation Attestation Process</i> action.   |
| Role Assignment  | Indicates that this process is intended to ensure that users have the correct access to resources, information, or systems by verifying that each selected role has the correct user assignments. To initiate this type of process, the Compliance Administrator needs to use the <i>Request Role Assignment Attestation Process</i> action. |
| User Assignment  | Indicates that this process is intended to ensure that users have the correct access to resources, information, or systems by verifying that each selected user has the correct role assignments. To initiate this type of process, the Compliance Administrator needs to use the <i>Request User Assignment Attestation Process</i> action. |

- ◆ The *Status* column shows the status for the request as well as an icon that provides a visual indicator for the status. You can select the status from the *Status* dropdown and click *Filter* to narrow the results when searching for requests with a particular status:

| Status       | Description   |
|--------------|---|
| Initializing | Indicates that this is a new request that has just been started.  |
| Running      | Indicates that the request is still in process.   |
| Completed    | Indicates that the all attesters have responded (or the individual processes have been retracted by a Compliance Administrator) and the request has finished processing.  |
| Error        | Indicates that an error occurred during the course of processing.<br><br>The precise error message for the error is written to the trace or audit log, if either is active. If an error occurs, check your trace or audit log to see if the error message indicates a serious problem that must be fixed. |

- ◆ The *Request Date* column shows the date when the request was made.
- ◆ The *Deadline* column shows the date by which all of the processes associated with this request must be completed. If the column is blank, the request has no deadline.

2 You can filter the list of requests, as follows:

- 2a To view only those requests that start with a particular string of characters, see “[Filtering Data](#)” on page 27 for information about what to type in the *Display Label* box.
- 2b To view only those requests that have a particular type, select the type in the *Attestation Type* dropdown.
- 2c To view those role requests that have a particular status, select the status in the *Status* dropdown list.

| Status       | Description  |
|--------------|--|
| All          | Includes all requests.   |
| Initializing | Includes requests that have just started.  |
| Running      | Includes requests that have been started and are currently being processed.  |
| Completed    | Includes requests for which all attesters have responded (or the individual processes have been retracted by a Compliance Administrator) and processing has completed. |
| Error        | Includes requests that have resulted in errors.  |

- 2d To apply the filter criteria you’ve specified to the display, click *Filter*.
  - 2e To clear the currently specified filter criteria, click *Reset*.
- 3 To search by the confirmation number that was generated when the request was first submitted, type the number in the *Confirmation Number* field, and click *Search*.

The *Confirmation Number* field supports the maximum length possible for a confirmation number, which is 255 characters.

- 4 To set the maximum number of requests displayed on each page, select a number in the *Maximum rows per page* drop-down list.
- 5 To sort the list of requests, click on the column heading that contains the data you want to sort.
- 6 To see the details for a particular request, click on the name in the *Display Label* column and scroll down until you see the *Request Details* group box.

---

**NOTE:** If the status is *Initializing*, the *Display Label* is not clickable, because you are not able to view the details of an initializing request.

---

**Request Details**

**Selected Process Request: User Profile - Default**  
 Process Request Description: User Profile - Default  
 Confirmation Number: 402a097fa0ae4e3c91b0bf6e850ce003

Status: ▶ Running      Deadline: No Expiration  
 Request Date: 09/01/2009 10:11:53 AM      Requested By: Application Administrator Of Sample Data

**Number of Related Processes: 1**  
 Running Processes: 3      Completed Processes: 0      Terminated Processes: 0

**Attestation Results**  
✔ 'Yes' Responses: 0      ✘ 'No' Responses: 0      No Action Taken: 3  
[View Attestation Form Details](#)

Filter by: Attestation Result: All      Process Status: All             Rows: 25

Select: All or None     

| Attester  | Completed Date | Process Status                              | Attestation Result |
|---|----------------|---|--------------------|
| <input type="checkbox"/> Bin Liu                  |                | <span style="color: blue;">▶</span> Running | No Action Taken    |
| <input type="checkbox"/> Compliance Administrator |                | <span style="color: blue;">▶</span> Running | No Action Taken    |
| <input type="checkbox"/> Human Resources          |                | <span style="color: blue;">▶</span> Running | No Action Taken    |

1 - 3 of 3

The *Attester* column in the *Request Details* group box shows an icon next to each attester that indicates whether the attester is a user, group, or role. In addition to showing information already displayed in the summary, the *Request Details* group box shows status information for all processes related to the request.

- ◆ The *Number of Related Processes* section gives the total number of processes, as well as the number of running, completed, and terminated processes.

- ◆ The *Attestation Results* section provides data on how the attesters responded:

| Data            | Description   |
|-----------------|---|
| 'Yes' Responses | Provides the total number of attesters who gave an affirmative answer to the attestation question.<br><br><b>NOTE:</b> The default text for an affirmative answer is <i>Yes</i> . However, this text can be modified. If the text is modified, the field label changes accordingly. |
| 'No' Responses  | Provides the total number of attesters who gave a negative answer to the attestation question.<br><br><b>NOTE:</b> The default text for a negative answer is <i>No</i> . However, this text can be modified. If the text is modified, the field label changes accordingly.          |
| No Action Taken | Provides the total number of attesters who have not yet responded to the attestation process. The No Action Taken total also includes each attester who never responded and the process completed because it timed out, or was retracted by a Compliance Administrator.             |

**6a** To view details for a particular attestation form, click *View Attestation Form Details*.

Request Details

**Selected Process Request: User Assignment - Test**  
 Process Request Description: User Assignment - Test  
 Confirmation Number: d5d8a0f8ef784050823307d52eb4fe2a

Status: Running      Deadline: 05/07/2008 02:19:59 PM  
 Request Date: 04/30/2008 02:19:59 PM      Requested By: Application Administrator Of Sample Data

**Number of Related Processes: 3**  
 Running Processes: 1      Completed Processes: 2      Terminated Processes: 0

**Attestation Results**  
 'Yes' Responses: 1      'No' Responses: 1      No Action Taken: 1

[View Attestation Form Details](#)

Filter by:    Attestation Result:     Process Status:        

Select: All or None    Maximum rows per page:

| Attester                                 | Completed Date | Process Status | Attestation Result |
|--|----------------|----------------|--------------------|
| <input type="checkbox"/> Jack Miller     | 04/30/2008     | Completed      | Yes                |
| <input type="checkbox"/> Jay West        |                | Running        | No Action Taken    |
| <input type="checkbox"/> Margo MacKenzie | 04/30/2008     | Completed      | No                 |

   Select: All or None

The form details for an attestation process show the kind of information the attesters are expected to review. The form details vary depending on whether the attestation type is User Profile, SoD Violations, or Role Assignment.

To hide the form details, click *Attestation Form Details* at the top of the form details group box.

For information on the form details that attesters must review when they claim a workflow task, see [Section 10.1.4, “Claiming a Task,” on page 132](#).

**6b** You can filter the list of processes, as follows:

**6b1** To view only those processes that have a particular result, select the result in the *Attestation Result* dropdown.

| Result  | Description  |
|---------|--|
| All     | Includes all processes.  |
| Yes     | Includes only those processes for which the attester responded affirmatively.  |
| No      | Includes only those processes for which the attester responded negatively.   |
| Unknown | Includes only those processes for which no action was taken. The Unknown filter also includes each process for which an attester never responded and the process completed because it timed out, or was retracted by a Compliance Administrator. |

**6b2** To view those processes that have a particular status, select the status in the *Process Status* drop-down list.

| Status     | Description  |
|------------|--|
| All        | Includes all processes.  |
| Running    | Includes processes that have been started and are currently being processed.                           |
| Terminated | Includes processes that have been retracted or terminated.   |
| Completed  | Includes processes for which the attester has responded or the process completed because it timed out. |

**6b3** To apply the filter criteria you’ve specified to the display, click *Filter*.

**6b4** To clear the currently specified filter criteria, click *Reset*.

**6c** To set the maximum number of processes displayed on each page, select a number in the *Maximum rows per page* drop-down list.

**6d** To check the status for a particular attester, look at the *Process Status* column for the attester. The *Process Status* field shows the status for the process, along with the status icon. The icon provides a convenient way to see the status at a glance. The table below describes the status codes:



| Status     | Description   |
|------------|---|
| Running    | The process has been started and is currently being processed.  |
| Terminated | The process has been retracted on the View Attestation Request Status page, or terminated within iManager.  |
| Completed  | All attesters have responded and processing has completed for each workflow process assigned to an attester.<br><br>The Completed status includes processes for which the attester has responded, as well as processes that completed because they timed out. |

- 6e** To retract one or more processes, select the attesters and click *Retract Selected Processes*. If you want to retract all processes, click *All*. To clear your selection, click *None*.

The *Retract Selected Processes* checkbox is disabled if the process has been completed or terminated. The *Retract Selected Processes* button does not appear if the high-level request status is Completed or Error.



---

# VI Appendixes

The following appendix provide additional reference information and advanced topics for the Identity Manager User Application.

- ♦ [Appendix A, “Using the Identity Manager Approvals App,”](#) on page 325



---

# A Using the Identity Manager Approvals App

In addition to the User Application user interface used by Identity Manager customers, you can now use a new iOS app that allows Identity Manager users to remotely approve or deny requests through the Roles Based Provisioning Module for Identity Manager.

Once you install and configure the Approvals app, you can see the same approval tasks in the app that you would normally see in the User Application interface. All changes are synchronized between the Approvals app and the User Application.

You can also work in offline mode when disconnected from the Identity Manager Roles Based Provisioning Module server, and the Approvals app will automatically synchronize any changes once connectivity is restored.

This appendix provides information about installing and using the new Approvals app. For information about how Identity Manager administrators can configure their environment to allow users to use the app, see [“Configuring the Identity Manager Approvals App”](#) in the *NetIQ Identity Manager User Application: Administration Guide*.

For more detailed information about the Approvals app, see the following sections:

- ◆ [Section A.1, “Product Requirements,”](#) on page 325
- ◆ [Section A.2, “Installing the Approvals App,”](#) on page 326
- ◆ [Section A.3, “Configuring the Approvals App,”](#) on page 326
- ◆ [Section A.4, “Overview of the Approvals App,”](#) on page 329
- ◆ [Section A.5, “Changing the Approvals App Display Language,”](#) on page 331

## A.1 Product Requirements

The Approvals app requires an Apple iPhone or iPad with Apple iOS 5, iOS 6, or iOS 7 installed.

---

**NOTE:** If your administrator has not enabled use of the Approvals app, you may not be able to configure the app after installation. For information on how administrators can configure the Identity Manager environment to enable use of the Approvals app, see [“Configuring the Identity Manager Approvals App”](#) in the *NetIQ Identity Manager User Application: Administration Guide*.

---

## A.2 Installing the Approvals App

You can install the NetIQ Identity Manager Approvals app from the [Approvals app page \(http://appstore.com/NetIQIdentityManagerApprovals\)](http://appstore.com/NetIQIdentityManagerApprovals) on the Apple App Store onto your device.

After you install the Approvals app, you must then configure the app to be able to connect with your Roles Based Provisioning Module server.

---

**NOTE:** If your User Application password has expired, we recommend change your password before installing and configuring the Approvals app. If the password policy in your environment allows a limited number of grace logins when a password expires, the Approvals app may use all of those logins in an attempt to sync your Identity Manager tasks to your device.

---

## A.3 Configuring the Approvals App

You can configure the NetIQ Identity Manager Approvals app in several ways, depending on the needs of your environment and the way in which your administrator has configured Identity Manager:

- ♦ Make a request in the User Application interface for access to the Approvals app, and then launch the app on your device from the email link provided by your Identity Manager administrator. The link includes all the required configuration information.
- ♦ Click a configuration link or scan a configuration QR code using your device, where link or QR code provides either all required configuration information or generalized configuration information for your company.
- ♦ Manually enter the configuration information for your environment in the app itself.

---

**IMPORTANT:** In order for users to be able to automatically configure the Approvals app using either a link or QR code, the administrator for the Identity Manager environment must first enable the link or QR code.

---

### A.3.1 Requesting Mobile Access Through the User Application

If configured by your administrator, you can request access to the Approvals app using the User Application. Identity Manager then sends an email that contains a customized link you can open on your device to automatically configure the app with your information.

To request mobile access through the User Application:

- 1 In a Web browser, log in to the Identity Manager User Application using the HTTPS (<https://>) protocol.

---

**NOTE:** To request access to the Approvals app, you must log in to the User Application using the HTTPS protocol.

---

- 2 Click *Make a Process Request*.
- 3 Click the Process Request Category drop-down menu and select *Accounts*.
- 4 Click *Continue*.
- 5 Click *Request Mobile Approval App*.

---

**NOTE:** The process request category and name may vary, depending on how your administrator has configured the Approvals app request process.

---


- 6 Provide the required information in process request form and click *Submit*.
- 7 When you receive an email from your Identity Manager administrator, open the email on your device and click the link provided to connect your device to the Roles Based Provisioning Module server.

---

**NOTE:** If you have previously installed the app, the app may display a warning message that existing settings will be overwritten. Ensure that the host name displayed in the warning message is the same host you accessed when you requested access to the app. If in doubt, do not click the link and contact your administrator.

If the host name is correct, click *Accept* to overwrite your existing settings.

---

- 8 When the app starts up, enter your password and click the Test Connection icon  to verify your settings.

## A.3.2 Using a Configuration Link or QR Code

Your Identity Manager administrator may provide a configuration link to configure your Approvals app. Open the link in a browser on your device to automatically configure the app.

However, this link can only provide some of the required settings. Typically, a link or code can only provide the Roles Based Provisioning Module server details necessary for the Approvals app to function. After you click the link, you must manually configure your `Username` and `Password` settings, as well as any other settings not automatically configured.

In some environments, you may not be able to access your email from your device. If you cannot receive email on your device, you can instead use your device to scan a personalized QR code provided by the Identity Manager administrator.

Display the provided QR code on your computer or on a printed page, if necessary, and scan the code using a QR code reader on your device. After the QR code automatically configures the Approvals app for your environment, manually configure your `Username` and `Password` settings.



## A.3.3 Manually Configuring the Approvals App

If the administrator of your Identity Manager environment does not provide a link or QR code to use when configuring the Approvals app, you can also configure the required configuration settings manually.

---

**WARNING:** Because manually configuring the app on your device requires in-depth knowledge of Identity Manager components, we recommend only advanced users knowledgeable about the Roles Based Provisioning Module and User Application environment in your enterprise manually configure app settings. Other users should contact their Identity Manager administrator for information about configuring the app.

---

In the app, click the Settings icon , specify the required settings, and then click the Test Connection icon  to verify your settings.

The Approvals app requires the following settings:

| Login Setting Name                                      | Login Setting Description   |
|---|---|
| Username  | Specifies the user name you use to access the Roles Based Provisioning Module server.   |
| Password  | Specifies the password you use to access the Roles Based Provisioning Module server.  |
| Data Sync   | Specifies if you want the app to actively sync data to the Roles Based Provisioning Module server.  |
| Advanced > Server Details > Server                      | Specifies the fully qualified domain name or IP address of the Roles Based Provisioning Module server.  |
| Advanced > Server Details > Secure Port                 | Specifies the HTTPS port the app uses to connect to the server.   |
| Advanced > Server Details > Context                     | Specifies the context used when installing the User Application WAR file. The default value is <code>IDMProv</code> .   |
| Advanced > Server Details > User Container              | Specifies the full DN of the Identity Vault container that stores user information.   |
| Advanced > Server Details > Timeout                     | Specifies the number of seconds the app waits when attempting to connect to the server before cancelling the connection. The default value is 5 seconds.  |
| Advanced > Data Definition Settings > User Entity       | Specifies the LDAP entity that represents a user in the Identity Vault. The default value is <code>user</code> .  |
| Advanced > Data Definition Settings > Name Format       | Specifies the DAL attribute representation the app uses to format a user's full name. The default value is <code>FirstName LastName</code> .  |
| Advanced > Data Definition Settings > First Name Attr   | Specifies the name of the DAL attribute that represents a user's first name. The default value is <code>FirstName</code> .  |
| Advanced > Data Definition Settings > Last Name Attr    | Specifies the name of the DAL attribute that represents a user's last name. The default value is <code>LastName</code> .  |
| Advanced > Data Definition Settings > User Photo Attr   | Specifies the name of the DAL attribute that contains a user's photo. The default value is <code>UserPhoto</code> .<br><br><b>NOTE:</b> If you do not have a picture configured in the Identity Manager or have configured your Identity Manager settings to not display a picture, the app displays a generic image instead. |
| Advanced > Data Definition Settings > Work Phone Attr   | Specifies the name of the DAL attribute that represents a user's work phone number. The default value is <code>TelephoneNumber</code> .   |
| Advanced > Data Definition Settings > Mobile Phone Attr | Specifies the name of the DAL attribute that represents a user's mobile phone number. The default value is <code>mobile</code> .  |
| Advanced > Data Definition Settings > Email Attr        | Specifies the name of the DAL attribute that represents a user's email address. The default value is <code>Email</code> .   |
| Advanced > Data Definition Settings > Photo LDAP Attr   | Specifies the name of the LDAP attribute that contains the photo of the user. The default value is <code>photo</code> .   |



| Login Setting Name                                       | Login Setting Description   |
|--|---|
| Advanced > Data Definition Settings > Naming Attribute   | Specifies the naming DAL attribute used in the Identity Vault to describe a name. The default value is <code>cn</code> .  |
| Advanced > Data Definition Settings > Provisioning Admin | Specifies whether you are a Provisioning Administrator on the Roles Based Provisioning Module server.   |
| Advanced > Accepted Certificates                         | <p>Specifies any invalid or self-signed certificates from the Roles Based Provisioning Module server that you allow the Approvals app to accept.</p> <p>When the Approvals app detects a self-signed or invalid certificate, the app asks you to accept or reject the certificate. If you accept the certificate, the app adds a certificate to the Accepted Certificates list. You can remove a certificate from the Accepted Certificates list by clicking the name of the certificate and restarting the app.</p> <p><b>NOTE:</b> If the Roles Based Provisioning Module server certificate is valid, the app does not add the certificate to the Accepted Certificates list. The app accepts valid certificates by default.</p> |
| Advanced > Rejected Certificates                         | <p>Specifies any invalid or self-signed certificates from the Roles Based Provisioning Module server that you do not want the Approvals app to accept.</p> <p>When the Approvals app detects a self-signed or invalid certificate, the app asks you to accept or reject the certificate. If you reject the certificate, the app adds a certificate to the Rejected Certificates list. If the server then presents a rejected certificate, the app cannot create a connection to the server.</p> <p>You can remove a certificate from the Rejected Certificates list by clicking the name of the certificate.</p>  |

## A.4 Overview of the Approvals App

This section provides an overview of the NetIQ Identity Manager Approvals app user interface. Topics include:

- ◆ [Section A.4.1, “Tasks View,” on page 330](#)
- ◆ [Section A.4.2, “Details View,” on page 330](#)
- ◆ [Section A.4.3, “Bulk Mode,” on page 330](#)
- ◆ [Section A.4.4, “Completed Tasks View,” on page 331](#)
- ◆ [Section A.4.5, “Login Settings View,” on page 331](#)
- ◆ [Section A.4.6, “Advanced Settings View,” on page 331](#)

## A.4.1 Tasks View

The default view of the Approvals app is the Tasks view. This view displays all of the tasks currently assigned to or claimed by you, with the title of the task and the name and picture of the task recipient. The view lists tasks by expiration date, displaying the tasks due soonest at the top and tasks with no expiration date below.

---

**NOTE:** If a user does not have a picture configured in the Identity Manager or has configured their Identity Manager settings to not display a picture, the app displays a generic image instead.

---

If you want to approve or deny a request, or if you want to view the details of a particular task, click the task or task recipient name. If you want to contact a task recipient, click the recipient's picture.

## A.4.2 Details View

The Details view displays details for a particular task assigned to you. The fields displayed vary depending upon the request.

To approve or deny a task, provide any necessary information, and click either *Approve* or *Deny*.

## A.4.3 Bulk Mode



If you need to approve or deny a large number of similar tasks, you can switch from the default single-task mode to bulk mode in the Tasks view.

---


**NOTE:** You cannot approve all tasks in bulk mode. For more complex tasks, like attestation tasks, you must approve each attestation task separately in single-task mode. When you click the Bulk Mode icon, the app displays only the tasks in your list that can be approved in bulk mode.


---

To approve or deny multiple tasks:

- 1 In the Tasks view, click the Bulk Mode icon .
- 2 Select the tasks you want to approve or deny. You cannot approve some tasks and deny other tasks at the same time.
- 3 (Optional) If you want to approve or deny all tasks, click *All*.
- 4 (Optional) If you change your mind and do not want to approve or deny any tasks, click the single-task mode icon .
- 5 Click *Approve* or *Deny*.
- 6 (Optional) Provide a comment regarding the bulk operation.
- 7 Click *Confirm*.

## A.4.4 Completed Tasks View

To view your completed tasks, click the Completed Tasks icon . The view displays the completed task, as well as the time the task was approved or denied. You can click a completed task to view the details of that particular task. For more complex requests, you can click *Form Values* to view specific information for the request.

If necessary, you can delete one or more of your completed tasks from the Completed Tasks view. To delete tasks, click the Bulk Mode icon , select the tasks you want to delete, and click *Delete*.

---

**NOTE:** The Completed Tasks view only displays tasks completed on your device. You cannot view tasks completed in the User Application or on another device with the Approvals app installed.

---

## A.4.5 Login Settings View

The Login Settings view allows you to view or modify your login settings.

---

**WARNING:** If your Identity Manager administrator provided a link or QR code to automatically configure your app settings, we recommend you do not modify those default settings unless your administrator instructs you to do so.

---

## A.4.6 Advanced Settings View

The Advanced Settings view allows you to view or modify advanced settings that determine how you receive data from the Roles Based Provisioning Module server.

---

**WARNING:** If your Identity Manager administrator provided a link or QR code to automatically configure your app settings, we recommend you do not modify those default settings unless your administrator instructs you to do so.

If you accidentally change the Data Definition Settings in the Advanced Settings view, click *Restore Defaults* to restore the default settings provided by Identity Manager. *Restore Defaults* does not change your user name, password, or any of the Server Details settings.

---

## A.5 Changing the Approvals App Display Language

The Approvals app includes localized text strings in multiple languages. To change the language the Approvals app uses, change the Language and Region Format settings on your iOS device. The Region Format settings configure how dates, times, and phone numbers are displayed on the device.

To modify language and region settings:

- 1 On your iOS device, click *Settings*.
- 2 Click *General*.
- 3 Click *International*.
- 4 (Optional) If you want to change the language your device uses, click *Language*, select the language you want to use, and then click *Done*.

- 5 (Optional) If you want to change the region format your device uses for dates and times, click *Region Format*, select the format you want to use and click *International*.
- 6 Go back to your device's home screen.