AUTHORIZED DOCUMENTATION

User Application: User Guide

Novell®
Identity Manager Roles Based Provisioning Module

3.6.1

November 10, 2010

www.novell.com

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/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Copyright © 1997-2007 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. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed on the Novell Legal Patents Web page (http://www.novell.com/company/legal/patents/) and one or more additional patents or pending patent applications in the U.S. and in other countries.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
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.novell.com/documentation).

Novell Trademarks

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

Third-Party Materials

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

Contents

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)
- Requests and approvals (for workflow-based provisioning)
- Roles (for roles-based provisioning actions)
- 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
Part I, "Welcome to Identity Manager," on page 13	Introduction to the Identity Manager user interface and how to begin using it
Part II, "Using the Identity Self-Service Tab," on page 31	How to use the *Identity Self-Service* tab of the Identity Manager user interface to display and work with identity information, including: ◆ Organization charts ◆ Profiles (your identity details) ◆ Directory searches ◆ Passwords ◆ User accounts (and more)
Part III, "Using the Requests & Approvals Tab," on page 107	How to use the *Requests & Approvals* tab of the Identity Manager user interface to: ◆ Manage provisioning work (tasks and resource requests) for yourself or your team ◆ Configure provisioning settings for yourself or your team

Part	Description
Part IV, “Using the Roles Tab,” on page 201	How to use the Roles tab of the Identity Manager user interface to: ◆ Make role 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
Part V, “Using the Compliance Tab,” on page 265	How to use the Compliance tab of the Identity Manager user interface to: ◆ Make requests for user profile attestation processes ◆ Make requests for separation of duties (SoD) attestation processes ◆ Make requests for role assignment attestation processes ◆ Make requests for user assignment attestation processes

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 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.novell.com/documentation/idmrbpm361/).

Documentation Conventions

In Novell documentation, a greater-than symbol (>) is used to separate actions within a step and items in a cross-reference path.

A trademark symbol (®, ™, etc.) denotes a Novell trademark. An asterisk (*) denotes a third-party trademark.

When a single pathname can be written with a backslash for some platforms or a forward slash for other platforms, the pathname is presented with a backslash. Users of platforms that require a forward slash, such as Linux* or UNIX*, should use forward slashes as required by your software.

I

Welcome to Identity Manager

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

Getting Started

1

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) 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, 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)

- Requests and approvals, which enable you to:
  - Request resources
  - Check the approval of your resource requests
  - Work on tasks assigned to you for approving other resource requests
  - Perform 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)
  - Optionally provide a digital signature for each request or approval

  NOTE: Requests and approvals require the Roles Based Provisioning Module for Identity Manager.

- 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: Roles require the Roles Based Provisioning Module for Identity Manager.

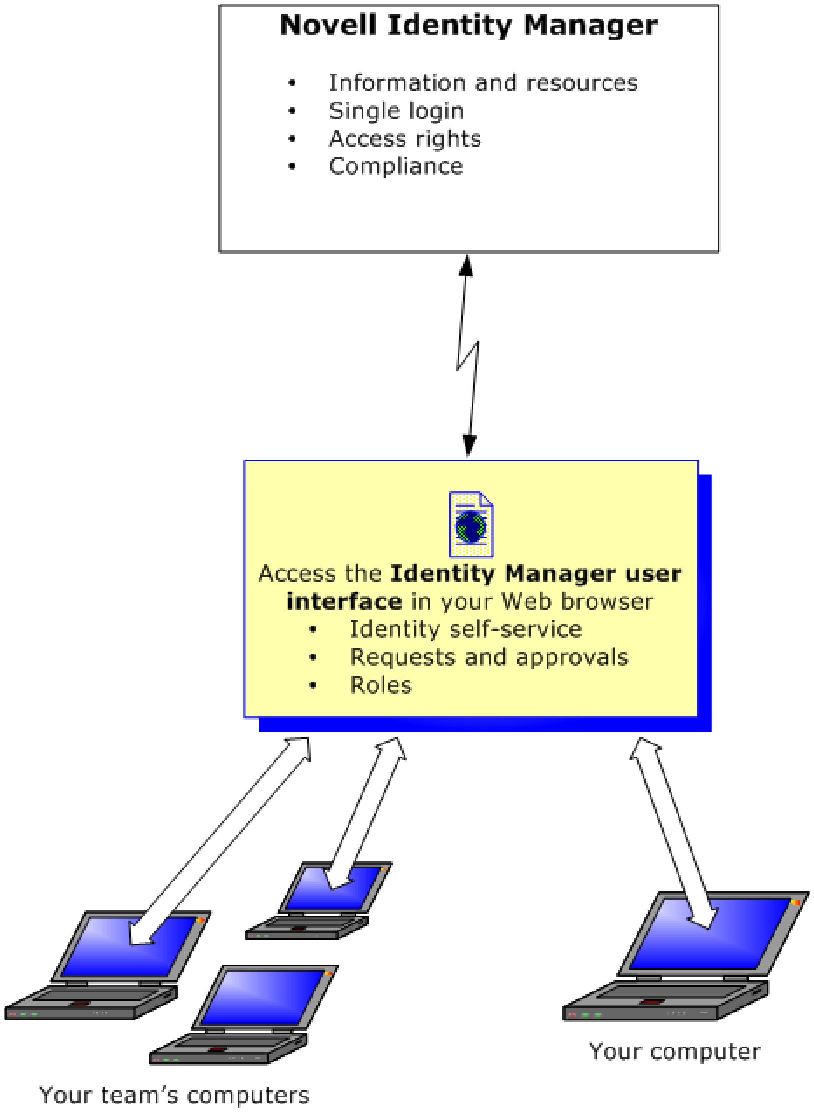
- Compliance, which enable you to:
  - Request user profile attestation processes
  - Request separation of duties (SoD) attestation processes
  - Request role assignment attestation processes
  - Request user assignment attestation processes

  NOTE: Compliance requires the Roles Based Provisioning Module for Identity Manager.

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 Requests and Approvals

- 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 Roles

- 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.
- 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.

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.

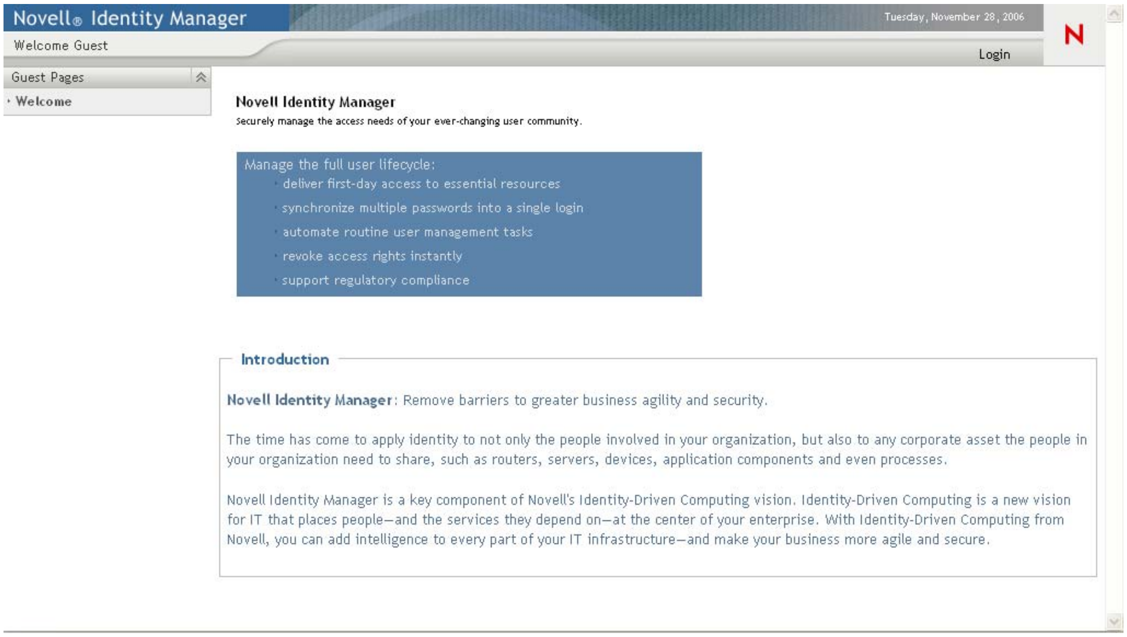
Because it works in a browser, the Identity Manager User Application is as easy to access as any Web page.

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/IDM.

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*



Novell Identity Manager

Securely manage the access needs of your ever-changing user community.

Manage the full user lifecycle:

- deliver first-day access to essential resources
- synchronize multiple passwords into a single login
- automate routine user management tasks
- revoke access rights instantly
- support regulatory compliance

Introduction

Novell Identity Manager: Remove barriers to greater business agility and security.

The time has come to apply identity to not only the people involved in your organization, but also to any corporate asset the people in your organization need to share, such as routers, servers, devices, application components and even processes.

Novell Identity Manager is a key component of Novell's Identity-Driven Computing vision. Identity-Driven Computing is a new vision for IT that places people—and the services they depend on—at the center of your enterprise. With Identity-Driven Computing from Novell, you can add intelligence to every part of your IT infrastructure—and make your business more agile and secure.

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.

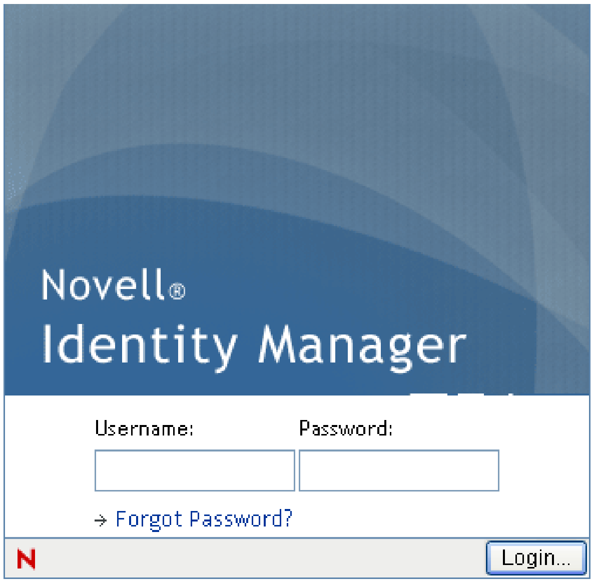
1.3 Logging In

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:



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

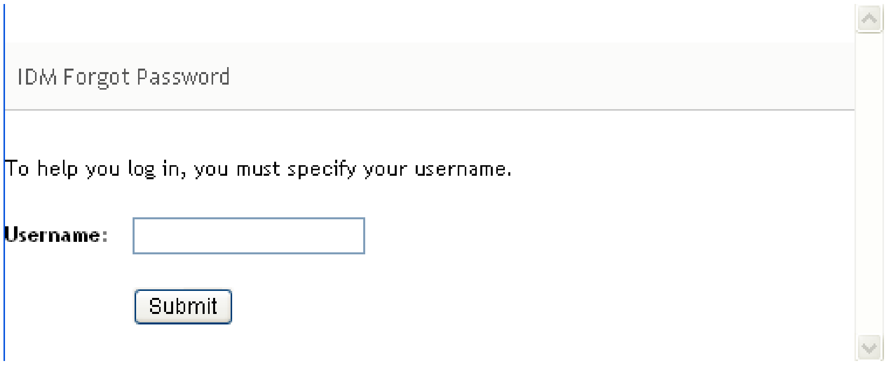
1.3.1 If You Forget Your Password

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:

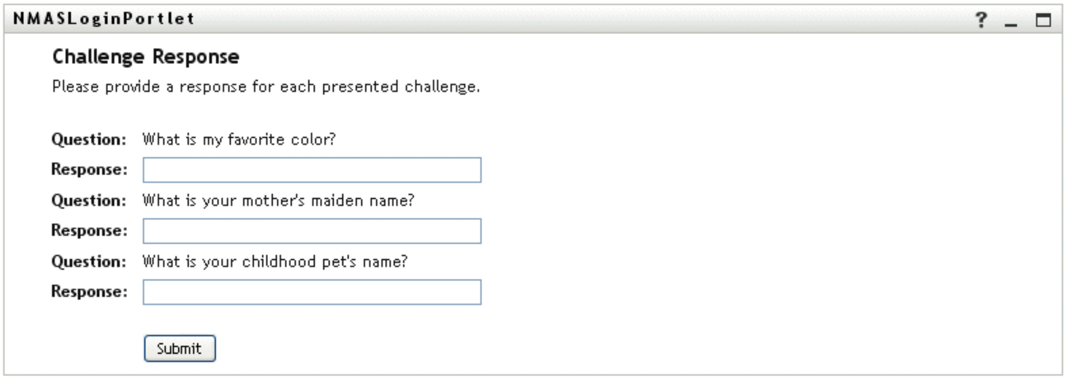

IDM Forgot Password

To help you log in, you must specify your username.

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:



NMASLoginPortlet

Challenge Response

Please provide a response for each presented challenge.

Question: What is my favorite color?

Response:

Question: What is your mother's maiden name?

Response:

Question: What is your childhood pet's name?

Response:

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

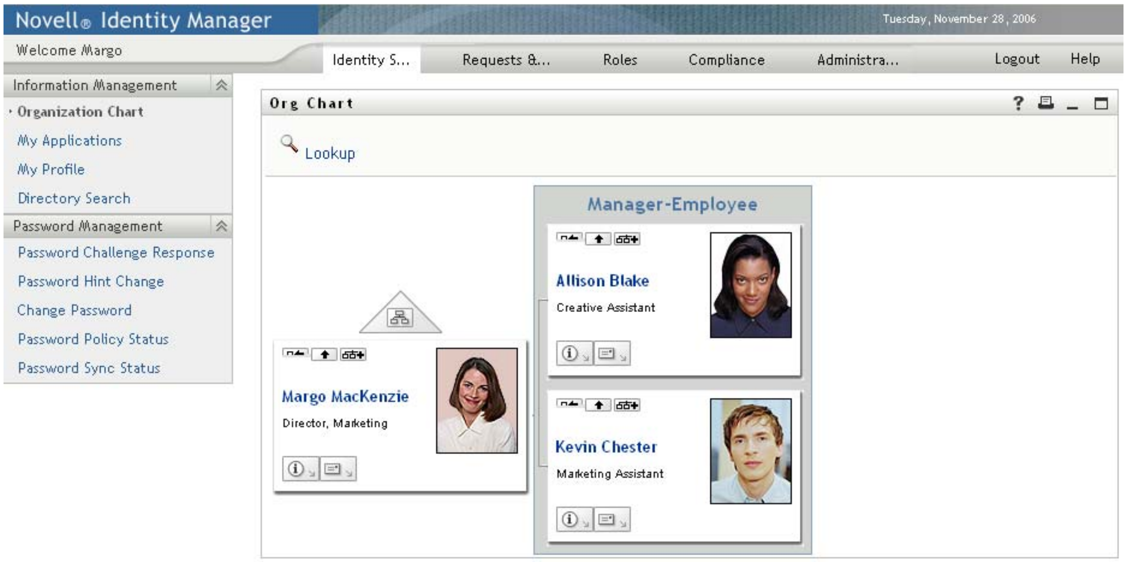
You might be prompted for other kinds of information as soon as you log in to the Identity Manager User Application. It all depends on how the system administrator has set up your password policy (if any). For example:

- 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 *On Login, You See Tabs and the Organization Chart*



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.

- *Requests & Approvals*

  To learn about this tab and how to work with it, see Part III, "Using the Requests & Approvals Tab," on page 107.

  NOTE: To enable the *Requests & Approval*s tab, your organization must have the Roles Based Provisioning Module for Identity Manager.

- *Roles*

  To learn about this tab and how to work with it, see Part IV, "Using the Roles Tab," on page 201.

  NOTE: To enable the *Roles* tab, your organization must have the Roles Based Provisioning Module for Identity Manager.

- *Compliance*

  To learn about this tab and how to work with it, see Part V, "Using the Compliance Tab," on page 265.

  NOTE: To enable the *Compliance* tab, your organization must have the Roles Based Provisioning Module for Identity Manager. The *Compliance* tab is not available unless you are a Compliance Module Administrator or Attestation Manager.

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* or *Compliance*).
2. Click the *Help* link (in the top right corner of the page).

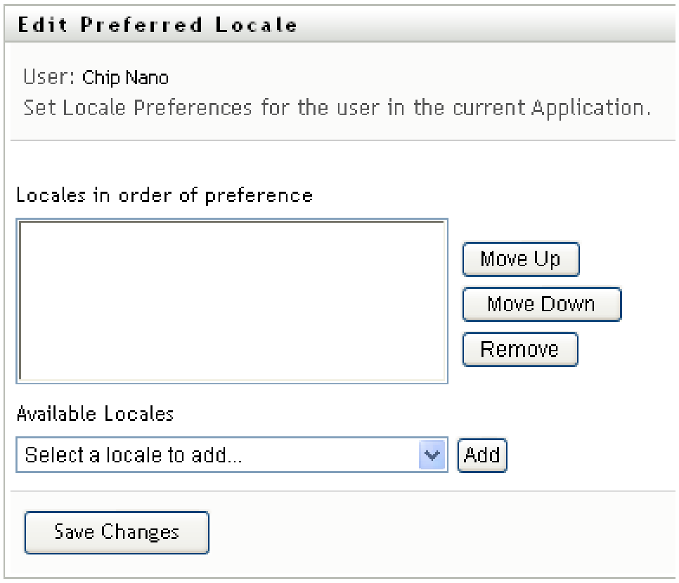
   The help page for the current tab displays.

1.4.2 Preferred Locale

If your administrator has not defined a preferred locale (language) for the User Application, 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.



Edit Preferred Locale

User: Chip Nano

Set Locale Preferences for the user in the current Application.

Locales in order of preference

Available Locales

Select a locale to add...

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).

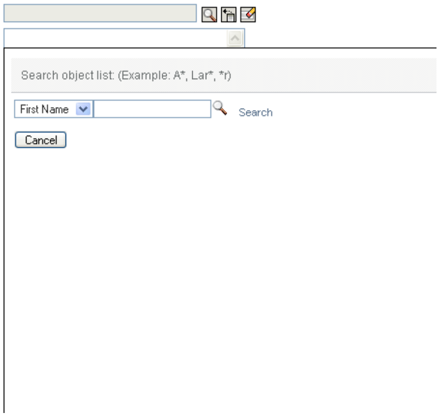
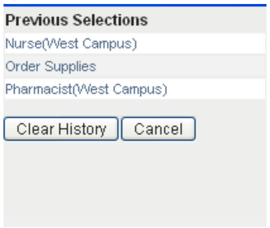
By default, the User Application thanks you for using Novell Identity Manager. Click the red link titled *Return to Novell Identity Manager Login* to return to a login prompt.

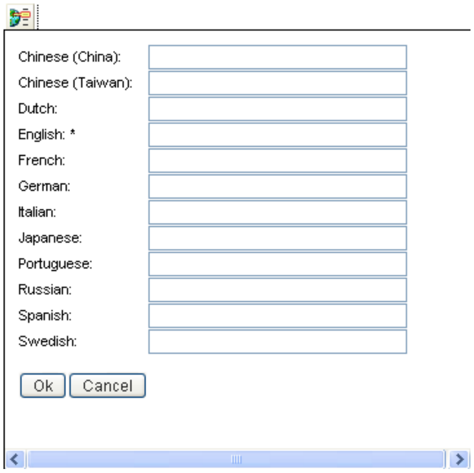
1.4.4 Common User Actions

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

***Table 1-1** Common Buttons*

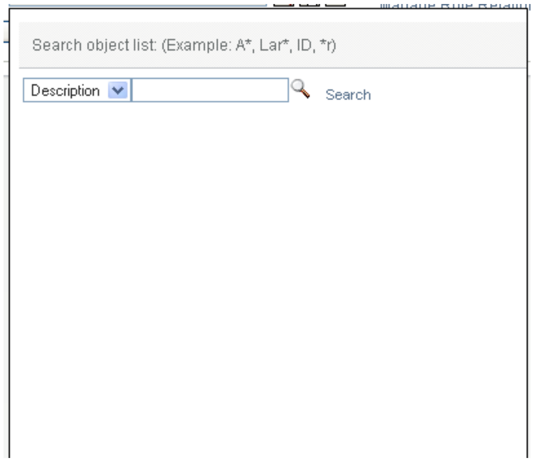
Button	Description
🔍	**Object Selector** Provides access to a Search dialog box or popin. You can enter search criteria for different types of objects based on your location within the User Application. For example, in the Identity Self-Service tab, you can search for users and groups while in the Roles tab, you can search for users, groups, and roles.  Search object list: (Example: A*, Lar*, *r) First Name Search Cancel See "Using the Object Selector Button for Searching" on page 26.
📋	**Show History** 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.  Previous Selections Nurse(West Campus) Order Supplies Pharmacist(West Campus)
📝	**Reset** Clears the current selection.

Button	Description
	Localize 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.  Chinese (China): Chinese (Taiwan): Dutch: English: * French: German: Italian: Japanese: Portuguese: Russian: Spanish: Swedish: Ok Cancel
✚	**Add** Adds a new item or object. You are prompted for additional information specific to the type of object you are adding.
✖	**Delete** Deletes the currently selected item.
↑ ↓	**Up or Down Arrow** Moves the currently selected object up or down on the list
	Legend Provides a description for the symbols used on the *Requests & Approvals* or *Roles* tabs.

Using the Object Selector Button for Searching

To use the Object Selector button:

1 Click 🔍. The Search dialog displays:



Search object list: (Example: A*, Lar*, ID, *r)

Description 🔍 Search

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*

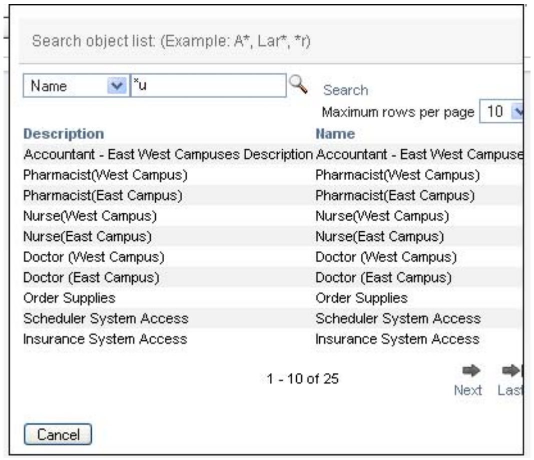
*u

*r

*e

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.



Search object list: (Example: A*, Lar*, *r)

Name ▾ *u Search

Maximum rows per page 10

Description	Name
Accountant - East West Campuses Description	Accountant - East West Campuse
Pharmacist(West Campus)	Pharmacist(West Campus)
Pharmacist(East Campus)	Pharmacist(East Campus)
Nurse(West Campus)	Nurse(West Campus)
Nurse(East Campus)	Nurse(East Campus)
Doctor (West Campus)	Doctor (West Campus)
Doctor (East Campus)	Doctor (East Campus)
Order Supplies	Order Supplies
Scheduler System Access	Scheduler System Access
Insurance System Access	Insurance System Access

1 - 10 of 25

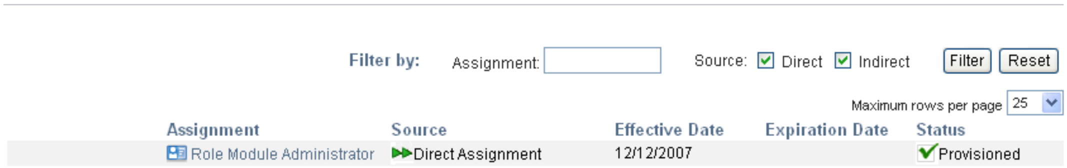
If you the result list includes the one you want, go to Step 4. Otherwise, go back to Step 2.

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 Roles 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 assignment and source (available in the My Roles action):

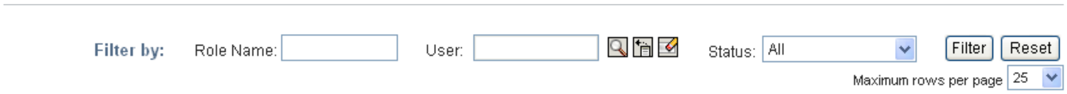


Filter by: Assignment: Source: ☑ Direct ☑ Indirect [Filter] [Reset]

Maximum rows per page 25

Assignment	Source	Effective Date	Expiration Date	Status
Role Module Administrator	Direct Assignment	12/12/2007		✓ Provisioned

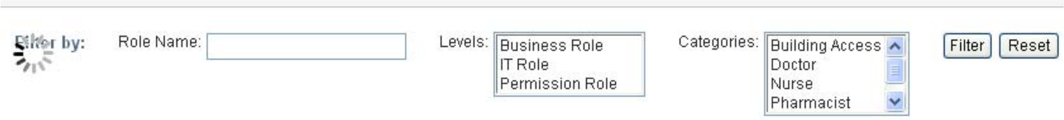
- Filtering by role name, user, and status (available in the View Request Status action):



Filter by: Role Name: User: Status: All [Filter] [Reset]

Maximum rows per page 25

- Filtering by role level and category (available in the Browse Role Catalog action):



Filter by: Role Name: Levels: Business Role, IT Role, Permission Role Categories: Building Access, Doctor, Nurse, Pharmacist [Filter] [Reset]

To use filtering:

1 Specify a value in the *Filter by* text field, 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 in the *Filter by* box. 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 assignment called Nurse:

nurse

n

n*

*u

*r

*e

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.

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 *Reset*.

2 To set the maximum number of items matching the filter by criteria that are displayed on each page, select a number in the *Maximum rows per page* dropdown list.

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.

To learn about	See
Doing identity self-service work	Part II, "Using the Identity Self-Service Tab," on page 31
Doing request and approval work	Part III, "Using the Requests & Approvals Tab," on page 107
Doing roles work	Part IV, "Using the Roles Tab," on page 201
Doing compliance work	Part V, "Using the Compliance Tab," on page 265

Using the Identity Self-Service Tab

II

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

Introducing the Identity Self-Service Tab

2

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:

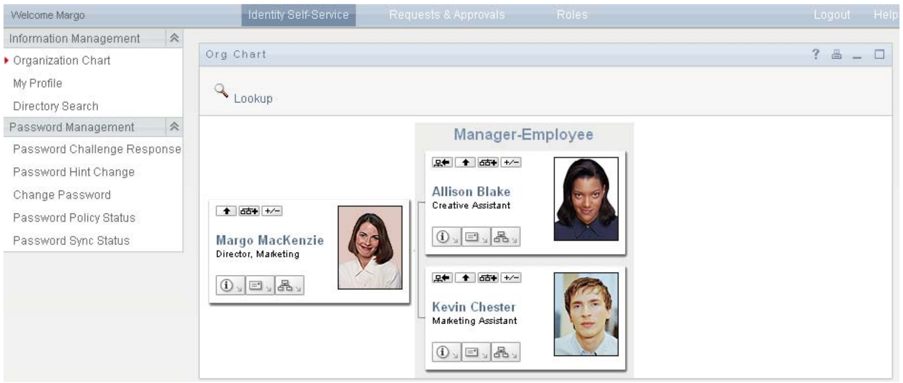
- Manage your own user account directly
- Look up other users and groups in the organization on demand
- Visualize how those users and groups are related
- List applications with which you are associated

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.

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*



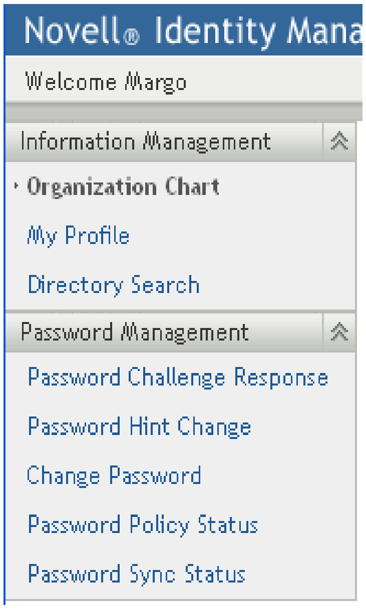
If you go to another tab in the Identity Manager User Application but then want to return, just click the *Identity Self-Service* tab to open it again.

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.)

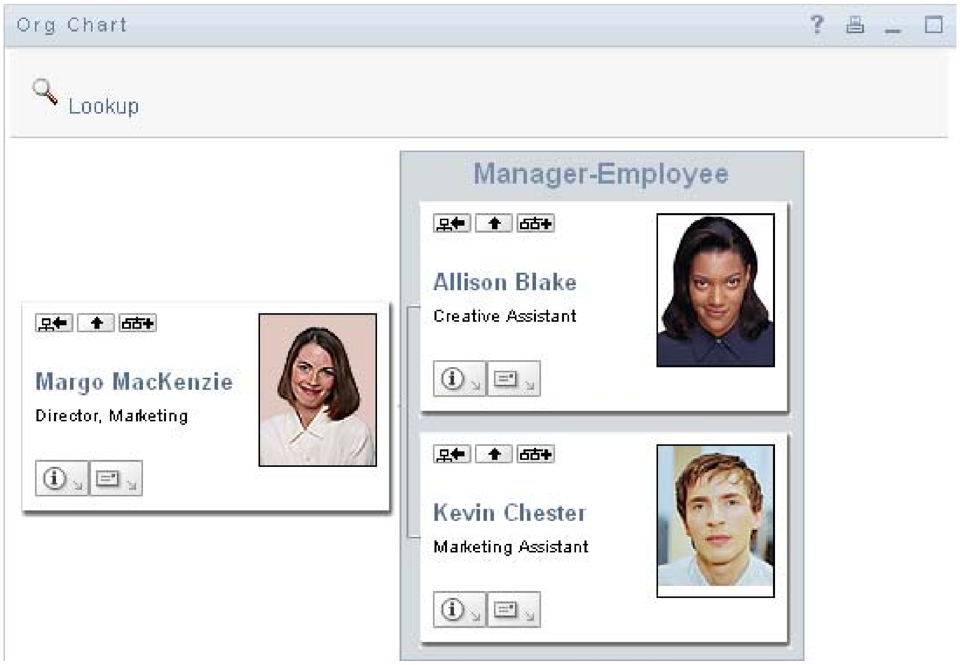
The left side of the *Identity Self-Service* tab displays a menu of actions you can perform. The actions are listed by category — *Information Management*, *Password Management*, and *Directory Management* (if authorized):

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	Displays the relationships among users and groups in the form of an interactive organizational chart. For details, see Chapter 3, "Using the Organization Chart," on page 39.
	Associations Report	Available to administrators. Displays applications with which a user is associated. For details, see Chapter 4, "Using the Associations Report," on page 53.
	My Profile	Displays the details for your user account and lets you work with that information. For details, see Chapter 5, "Using My Profile," on page 57.
	Directory Search	Lets you search for users or groups by entering search criteria or by using previously saved search criteria. For details, see Chapter 6, "Using Directory Search," on page 71.

Category	Action	Description
Password Management	Password Challenge Response	Lets you set or change your valid responses to administrator-defined challenge questions, and set or change user-defined challenge questions and responses. For details, see Chapter 7, “Performing Password Management,” on page 91.
	Password Hint Definition	Lets you set or change your password hint. For details, see Chapter 7, “Performing Password Management,” on page 91.
	Change Password	Lets you change (reset) your password, according to the rules established by your system administrator. For details, see Chapter 7, “Performing Password Management,” on page 91.
	Password Policy Status	Displays information about the effectiveness of your password management. For details, see Chapter 7, “Performing Password Management,” on page 91.
	Password Sync Status	Displays the status of password synchronization for your associated applications that synchronize with the Identity Vault. For details, see Chapter 7, “Performing Password Management,” on page 91.
Directory Management	Create User or Group	Available to administrators and authorized users. Lets you create a new user or group. For details, see Chapter 8, “Creating Users or Groups,” on page 97.

Using the Organization Chart

3

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:

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

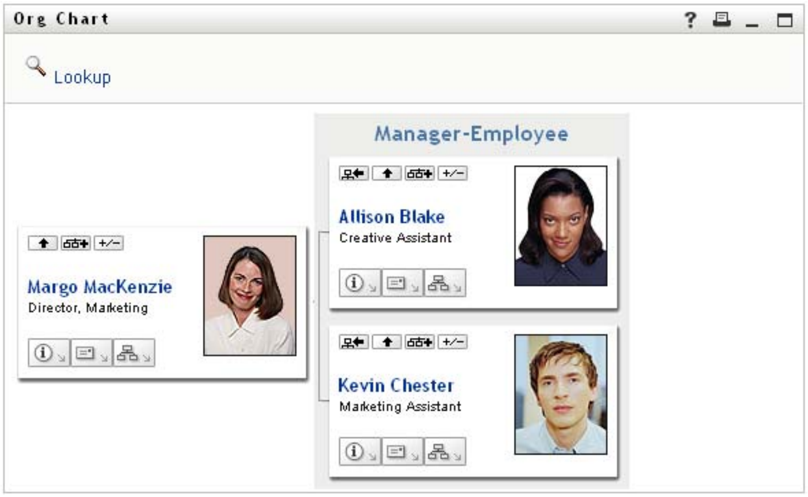
The Organization Chart page displays relationships. It can display relationships among managers, employees, and user groups in your business, and it can display other types of relationships that your administrator defines. The display is in the form of an organizational chart. In the chart, each person, 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.

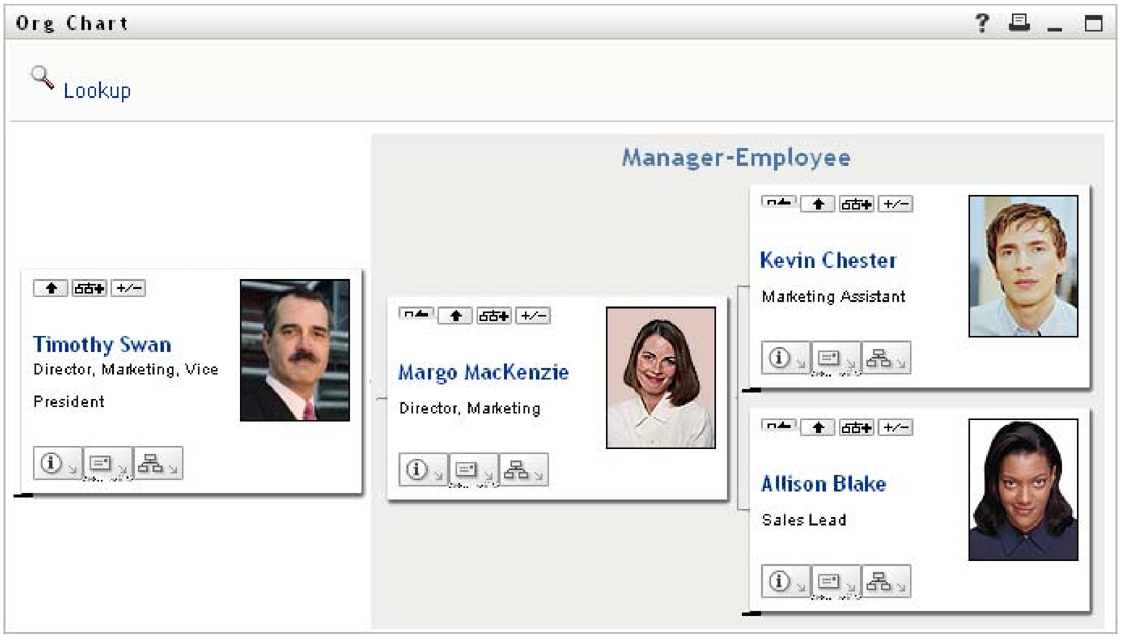
The following example introduces you to using Organization Chart. When you first display the Organization Chart page, it shows your own manager-employee relationships. For example, Margo MacKenzie (Marketing Director) logs in and sees the following default display of the Organization Chart page:

Figure 3-1 *Default View at Login*



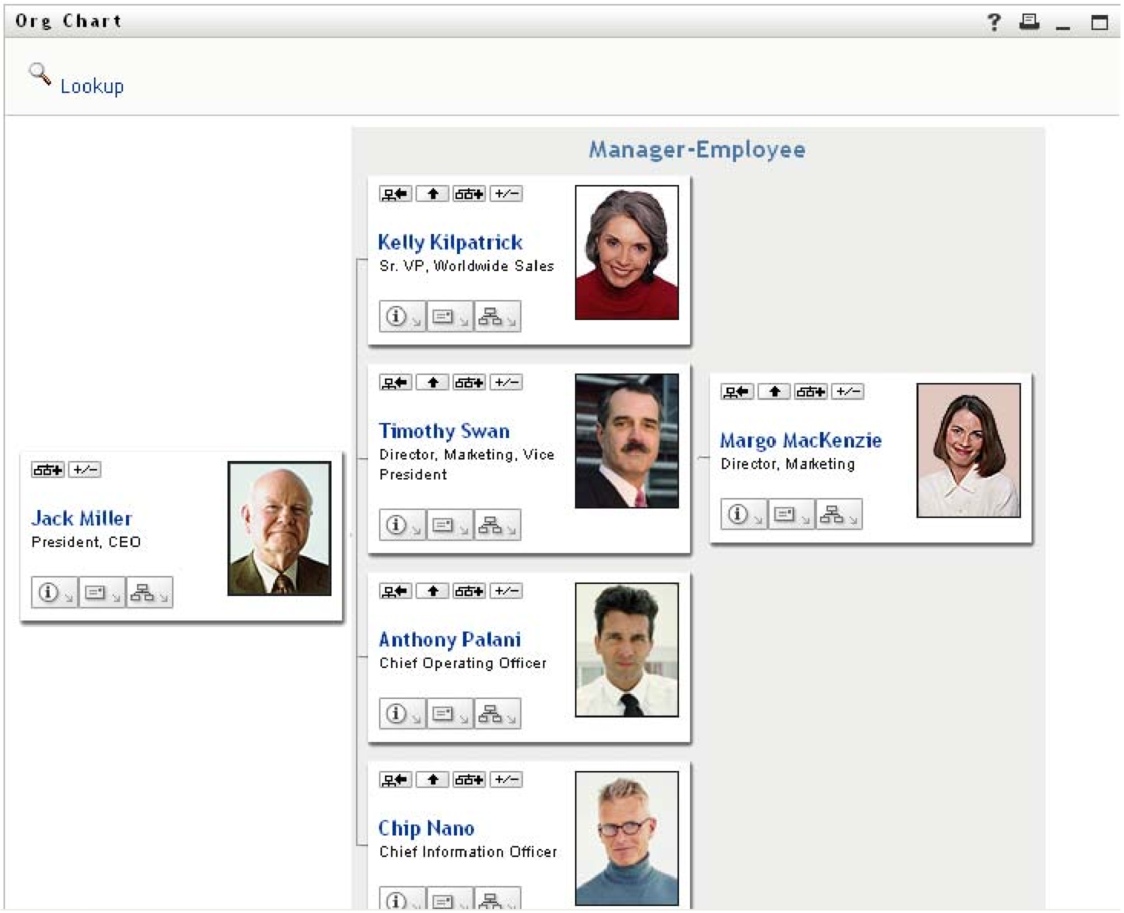
In her business card, Margo MacKenzie clicks *Go Up a Level* ⬆ to expand the chart to display her manager:

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



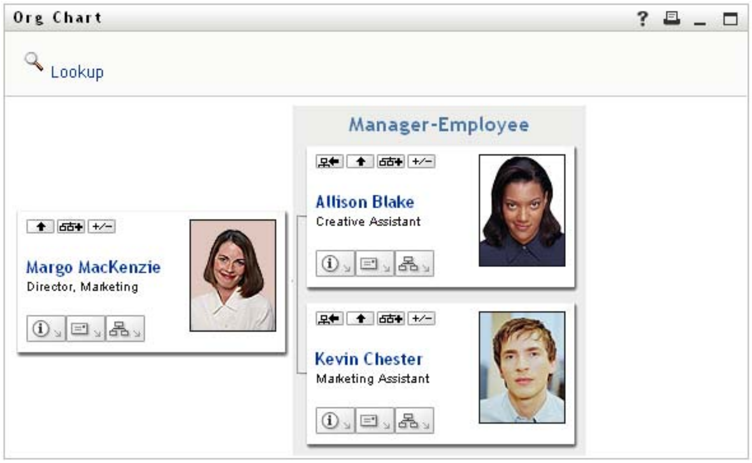
Margo then clicks *Go Up a Level* ⬆ in her manager's card, to show her manager's manager:

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:

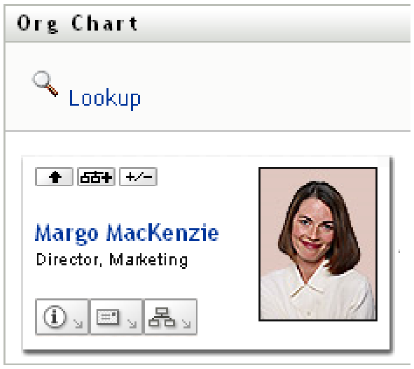
- Section 3.2.1, “Navigating to the Next Higher Level,” on page 42
- Section 3.2.2, “Resetting the Root of the Relationship,” on page 43
- Section 3.2.3, “Switching the Default Relationship,” on page 43
- Section 3.2.4, “Expanding or Collapsing the Default Chart,” on page 44
- Section 3.2.5, “Choosing 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

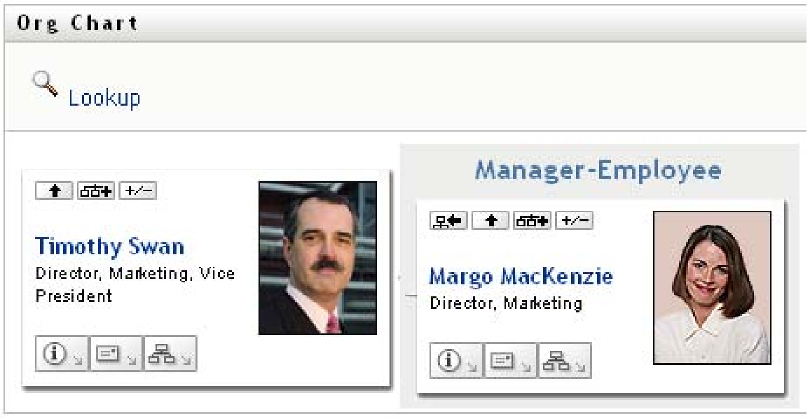
To navigate and expand to the next higher level in the relationship tree:

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.

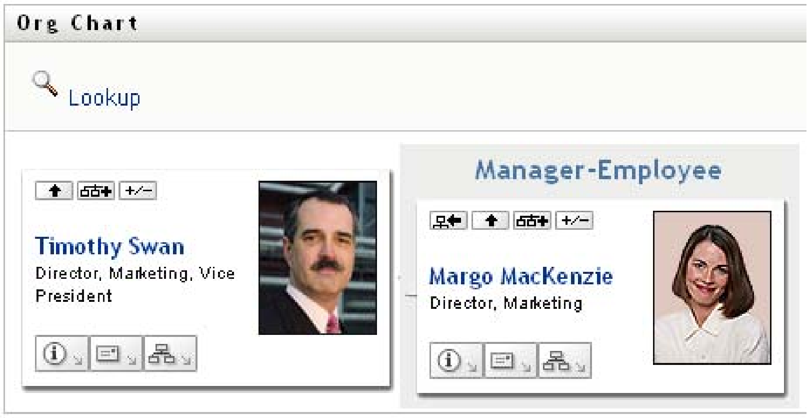
You can go up a level twice for a card.

3.2.2 Resetting the Root of the Relationship

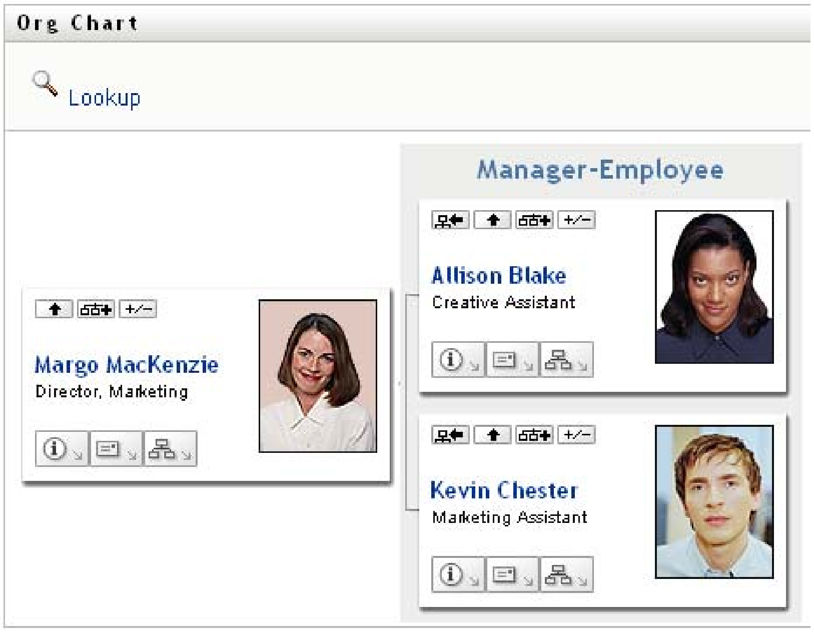
To reset the root of your view of the relationship chart:

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:



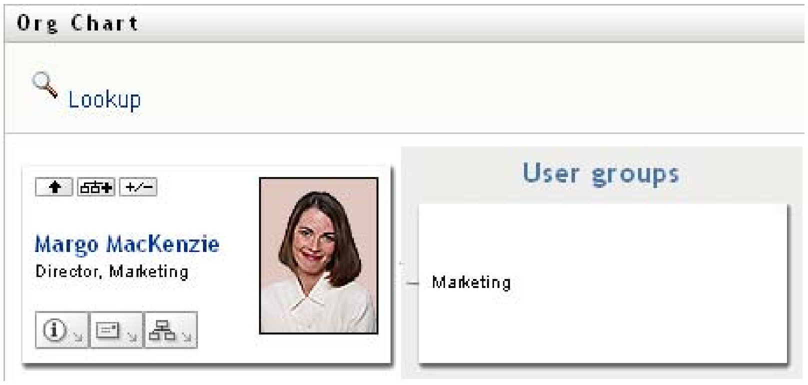
3.2.3 Switching the Default Relationship

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:



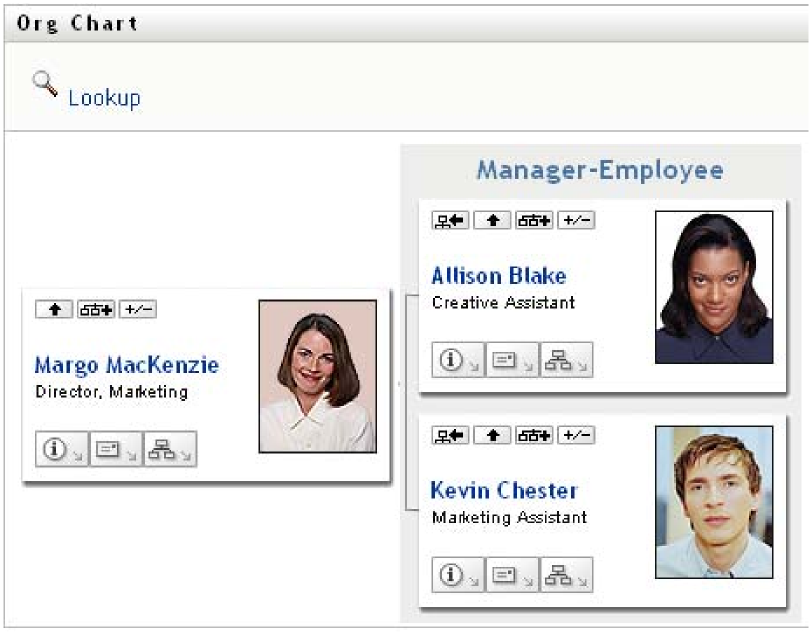
3.2.4 Expanding or Collapsing the Default Chart

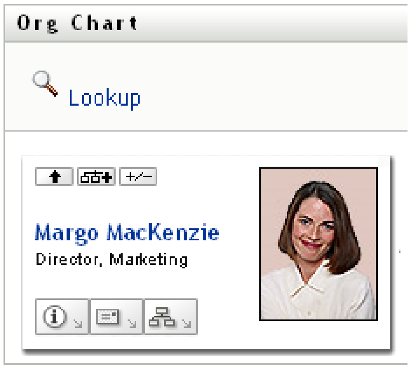
The default relationship chart is Manager-Employee, unless you or your administrator sets it to another type. To expand or collapse the default chart:

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.

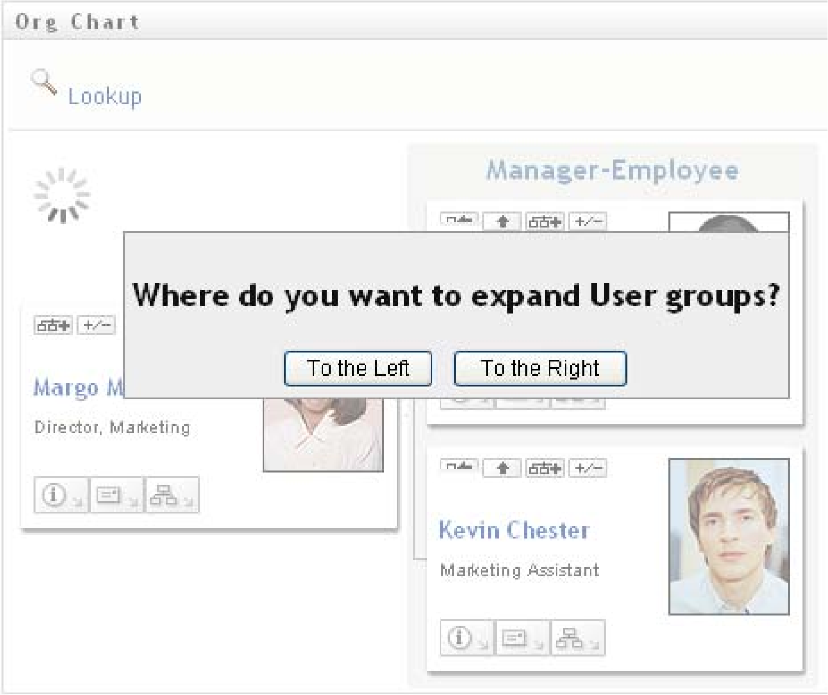
2 Click *Choose relationship to Expand/Collapse* in that card. A drop-down list opens.

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.

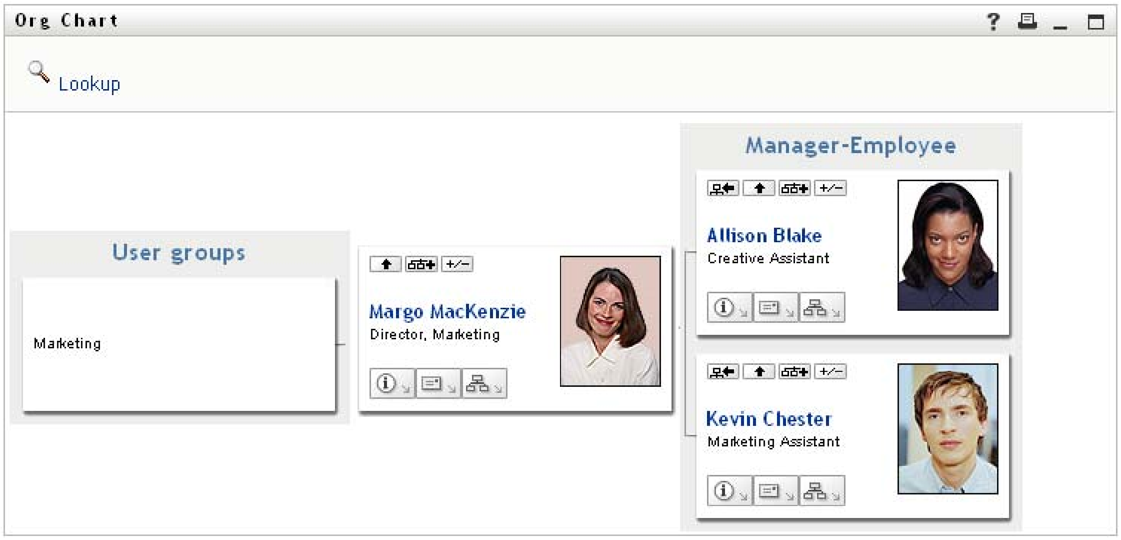
Additional relationships are available in the list if your administrator defines them.

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



Where do you want to expand User groups?

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

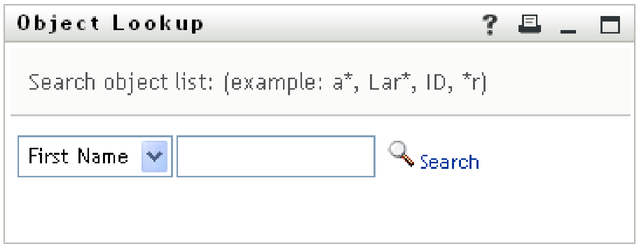


3.2.6 Looking Up a User in Organization Chart

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:



Object Lookup

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

First Name

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.

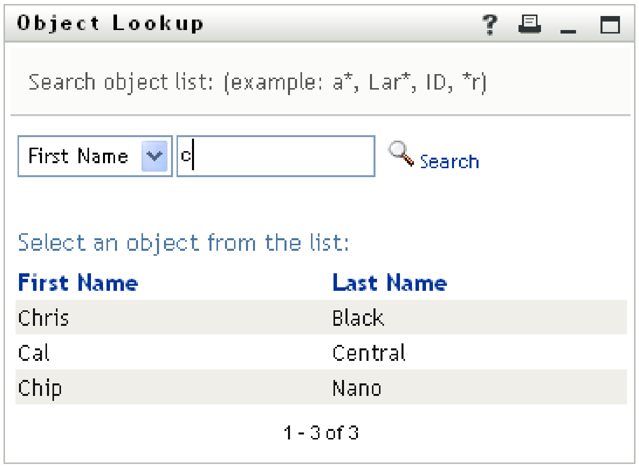
The search finds every name that begins with the text you type. It is not case sensitive. You can optionally use the asterisk (*) as a wildcard in your text to represent zero or more of any character.

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

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

3 Click *Search*.

The Lookup page displays your search results:



Object Lookup

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

First Name | c | Search

Select an object from the list:

First Name	Last Name
Chris	Black
Cal	Central
Chip	Nano

1 - 3 of 3

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:

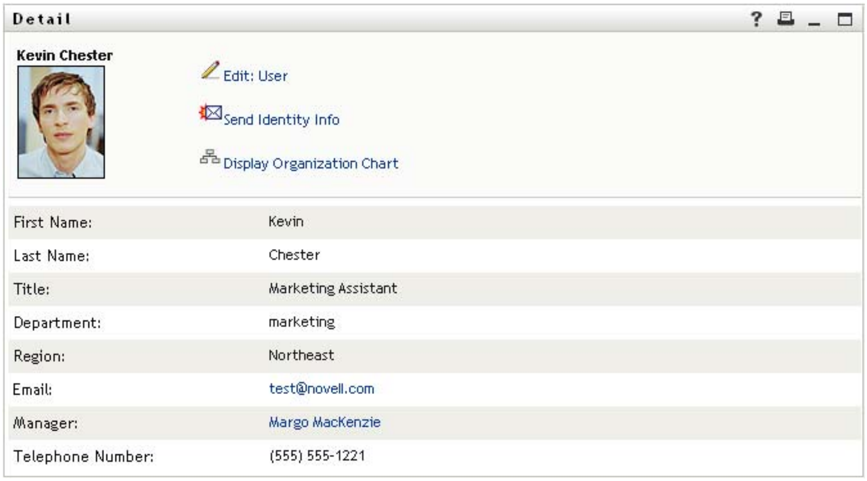
1 Find the card of a user whose details you want to display.

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:



Detail

Kevin Chester

Edit: User

Send Identity Info

Display Organization Chart

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

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.

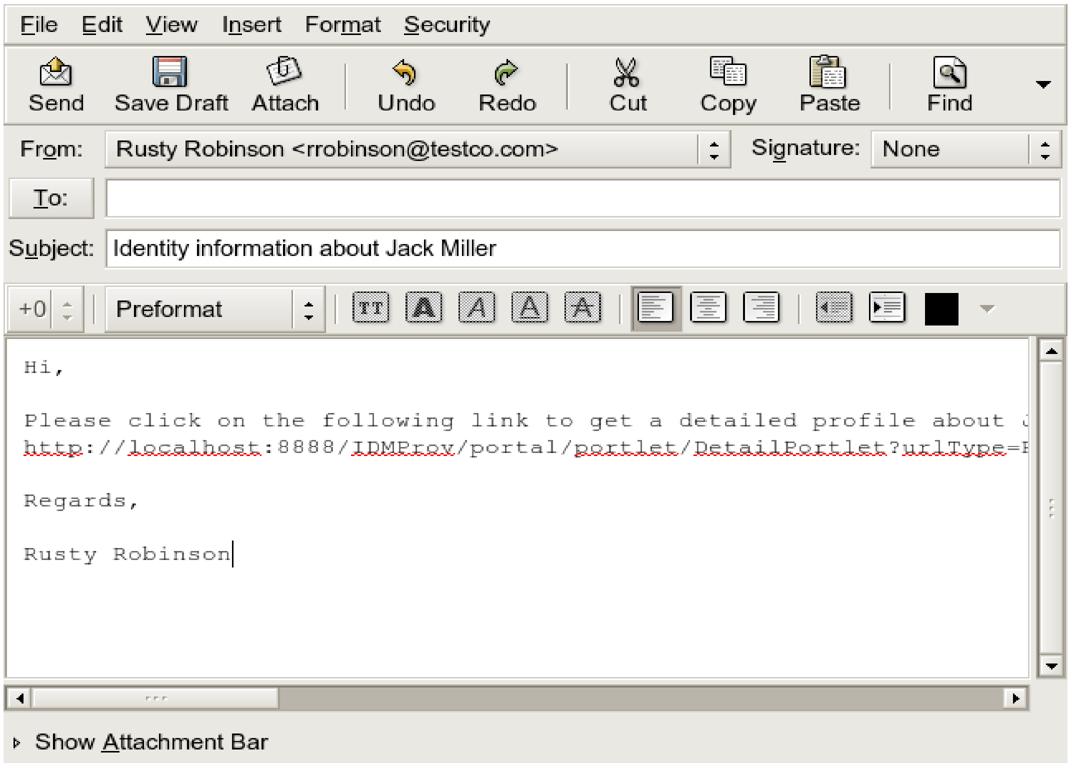
3 Select *Email Info*.

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: `Identity Information for` *`user-name`*

This part of the message	Contains
Body	Greeting, message, link, and sender’s name. The link (URL) is to the Profile page that displays detailed information about your chosen user. 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. To learn about using the features of the Profile page, see Chapter 5, “Using My Profile,” on page 57.

For example:



From: Rusty Robinson <rrobinson@testco.com>

Signature: None

To:

Subject: Identity information about Jack Miller

```
Hi,

Please click on the following link to get a detailed profile about
http://localhost:8888/IDMProv/portal/portlet/DetailPortlet?urlType=

Regards,

Rusty Robinson
```

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

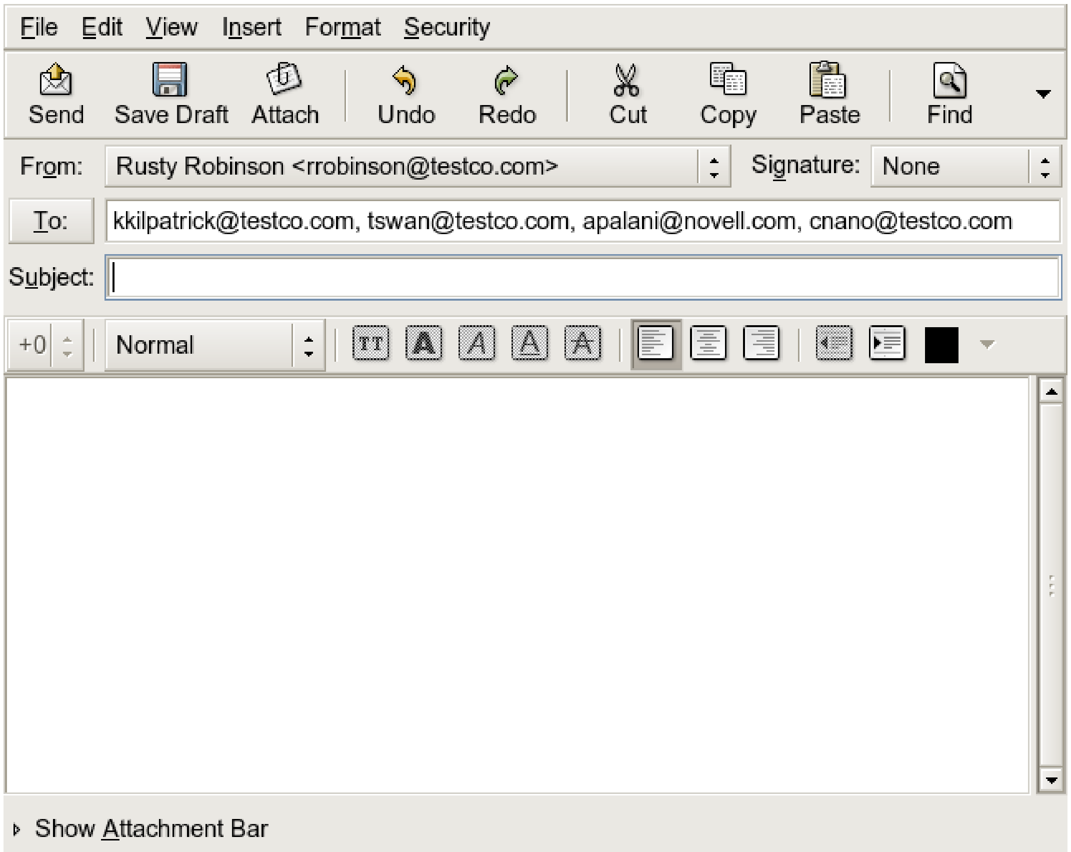
1 Find the card of a user who manages a team to whom you want to send e-mail.

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.



From: Rusty Robinson <rrobinson@testco.com>

Signature: None

To: kkilpatrick@testco.com, tswan@testco.com, apalani@novell.com, cnano@testco.com

Subject:

+0 Normal

4 Fill in the message contents.

5 Send the message.

Using the Associations Report 4

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.

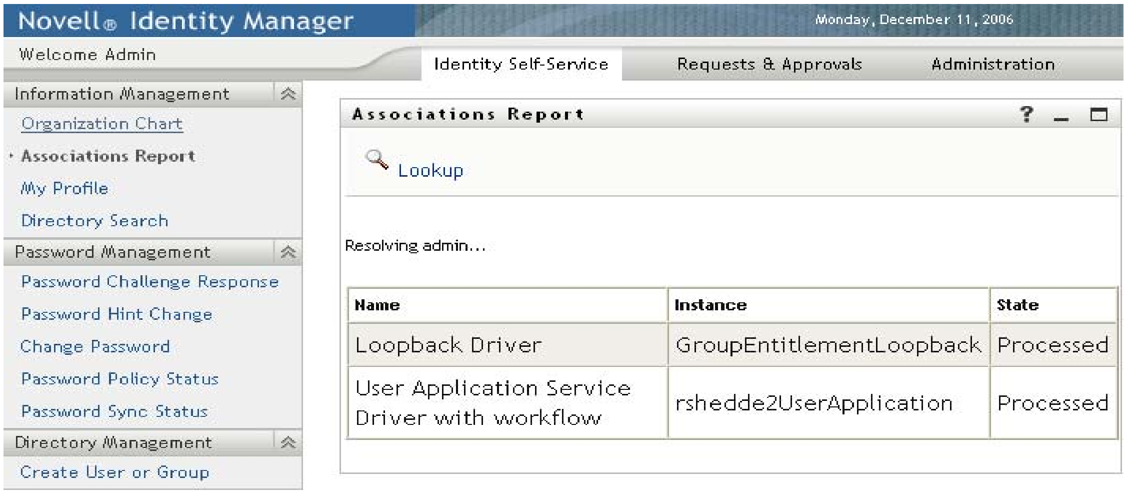
Table 4-1 *Association Status Table*

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



Resolving admin...

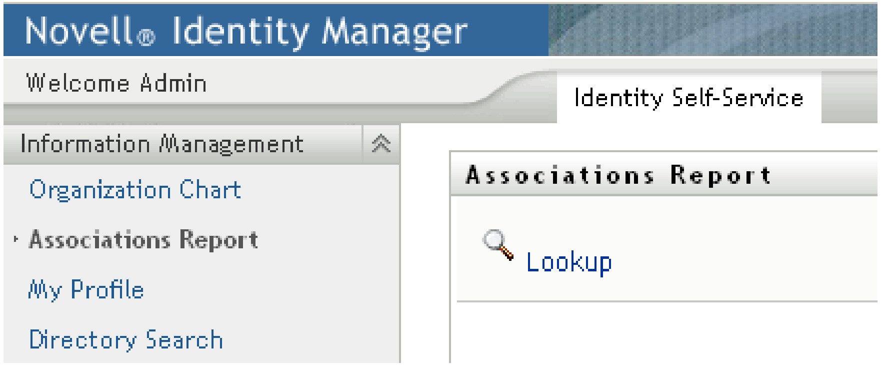
Name	Instance	State
Loopback Driver	GroupEntitlementLoopback	Processed
User Application Service Driver with workflow	rshedde2UserApplication	Processed

4.2 Displaying Associations

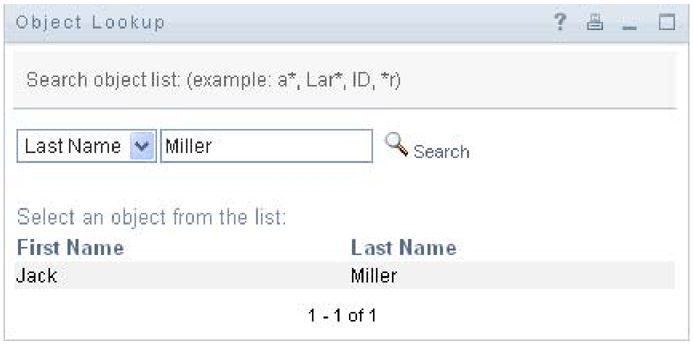
When you click *Associations Report*, the first associations shown are your own. To display another user's associations:

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*.



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

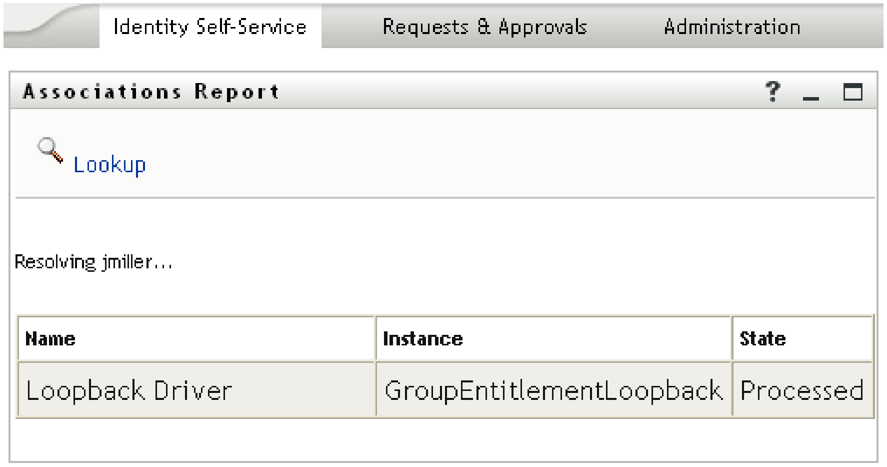
Last Name: Miller

Select an object from the list:

First Name	Last Name
Jack	Miller

1 - 1 of 1

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



Resolving jmiller...

Name	Instance	State
Loopback Driver	GroupEntitlementLoopback	Processed

Using My Profile

5

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

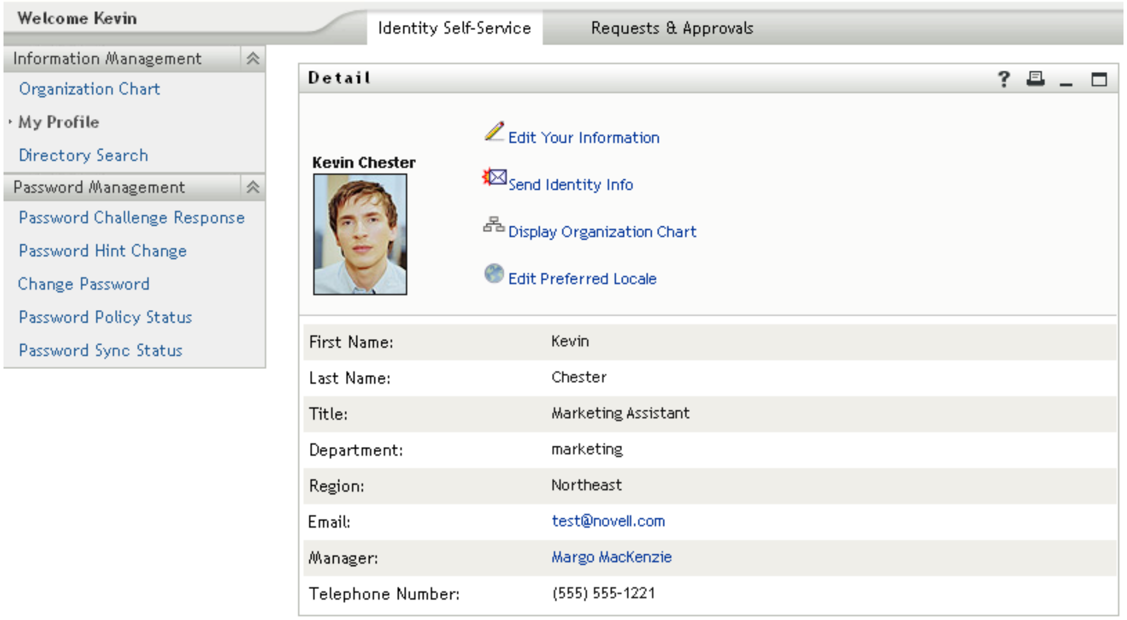
NOTE: This section describes the default features of the My Profile page. You might encounter some differences because of your job role, your level of authority, and customizations made for your organization; consult your system administrator for details.

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:

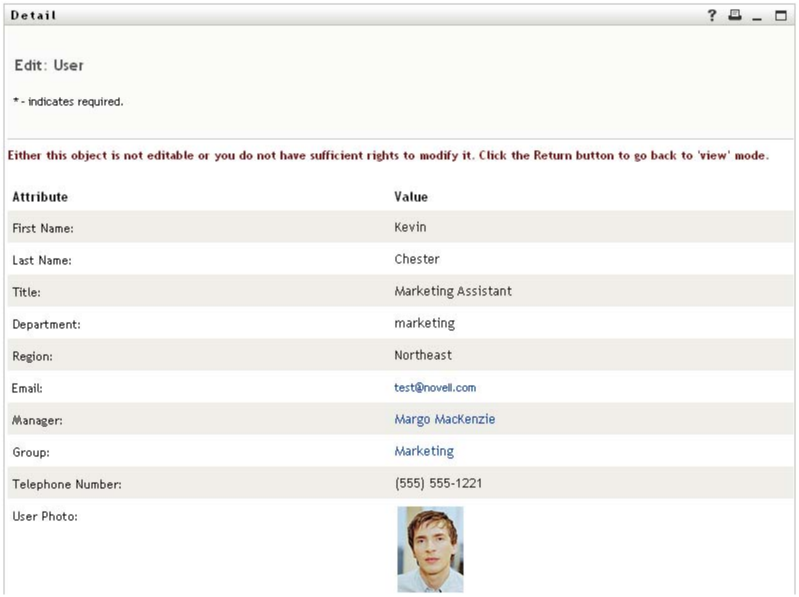
Figure 5-1 *My Profile Detail Page*



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

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*



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 *History* 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.

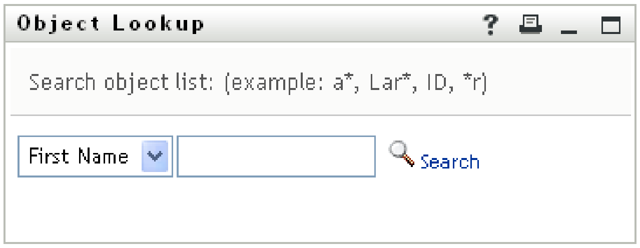
The following sections tell you more about using some of these editing buttons:

- "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:



Object Lookup

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

First Name

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.

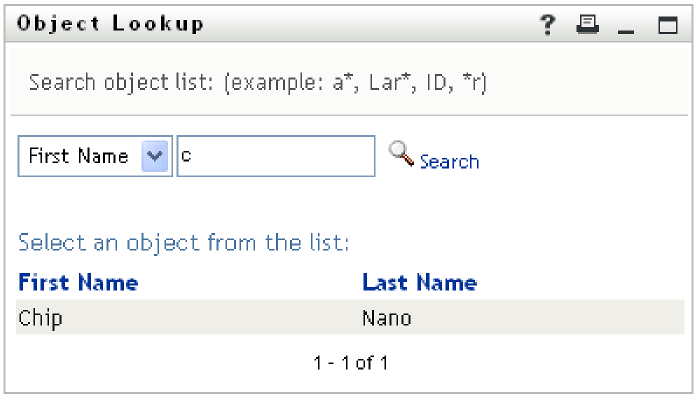
For instance, all of the following examples find the first name Chip:

```
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:



Object Lookup

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

First Name c

Select an object from the list:

First Name	Last Name
Chip	Nano

1 - 1 of 1

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.

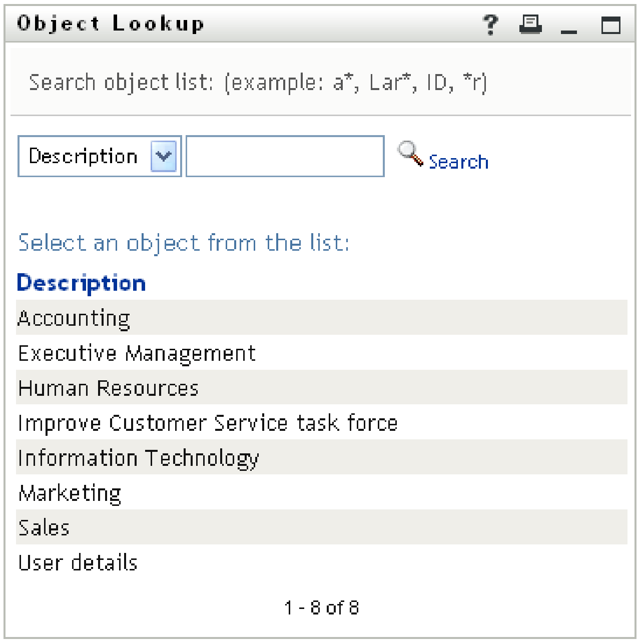
4 Select the user you want from the list.

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

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

Description

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.

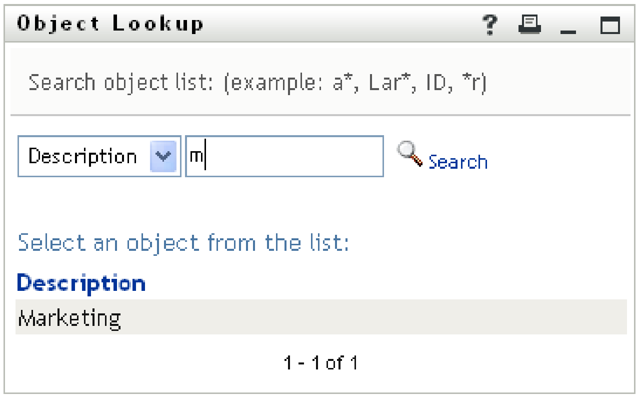
The search finds every description that begins with the text you type. It is not case sensitive. You can optionally use the asterisk (*) as a wildcard in your text to represent zero or more of any character.

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:



Object Lookup

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

Description: m

Select an object from the list:

Description
Marketing

1 - 1 of 1

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.

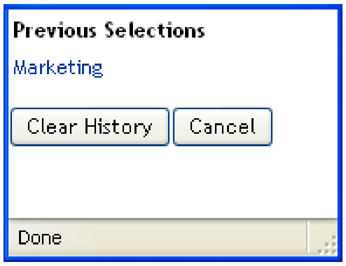
4 Select the group you want from the list.

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.



Previous Selections

Marketing

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 on the editing page.
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 on the editing page.

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 ✎ Replace or Delete Image to replace or remove it.

3 Click that button to display the File Upload page:

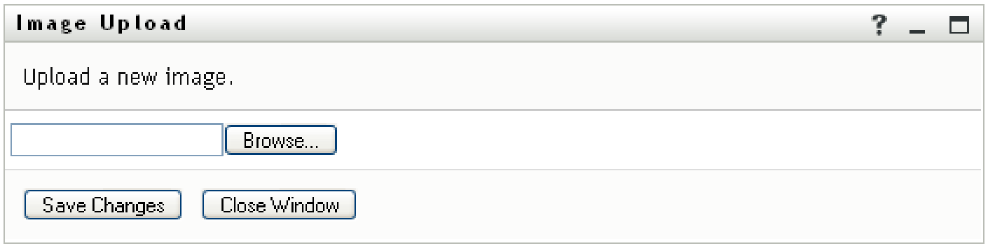


Image Upload

Upload a new image.

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

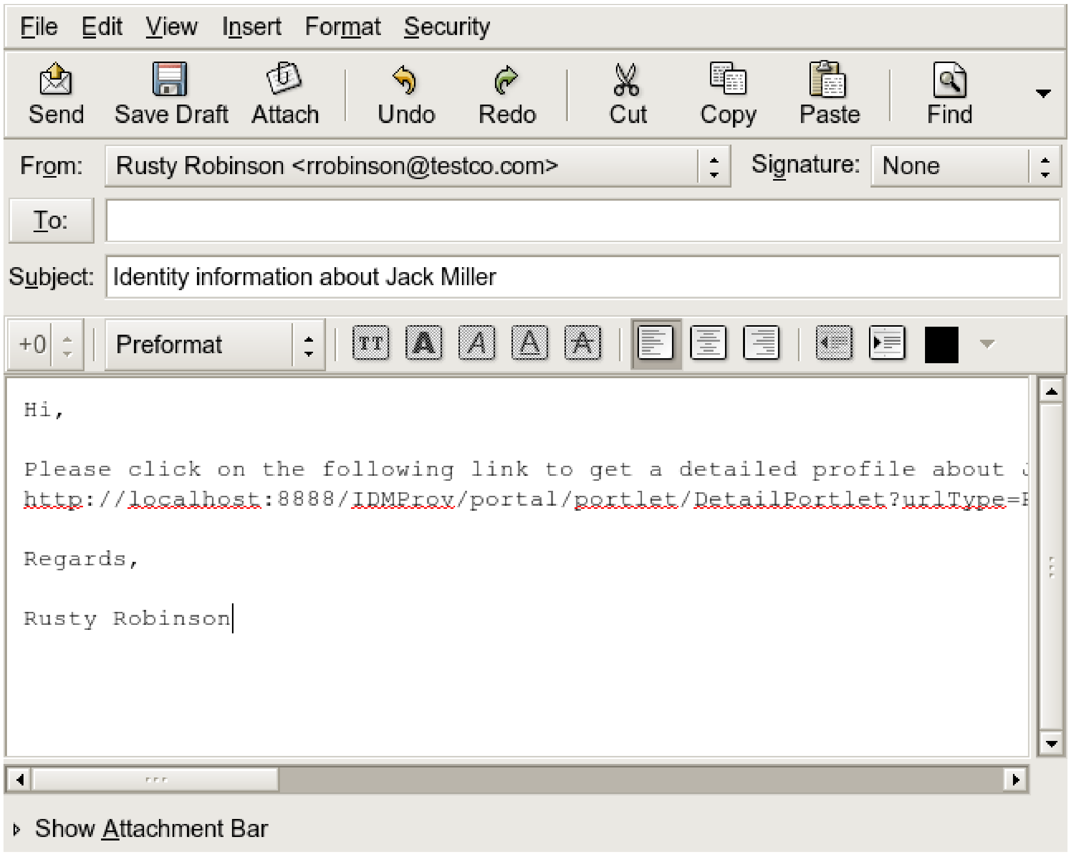
The My Profile page enables e-mailing details as links:

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: `Identity Information for` *`your-user-id`*
Body	A greeting, message, link, and your name. The link (URL) is to the Profile page that displays detailed information about you. 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:



From: Rusty Robinson <rrobinson@testco.com>

Signature: None

To:

Subject: Identity information about Jack Miller

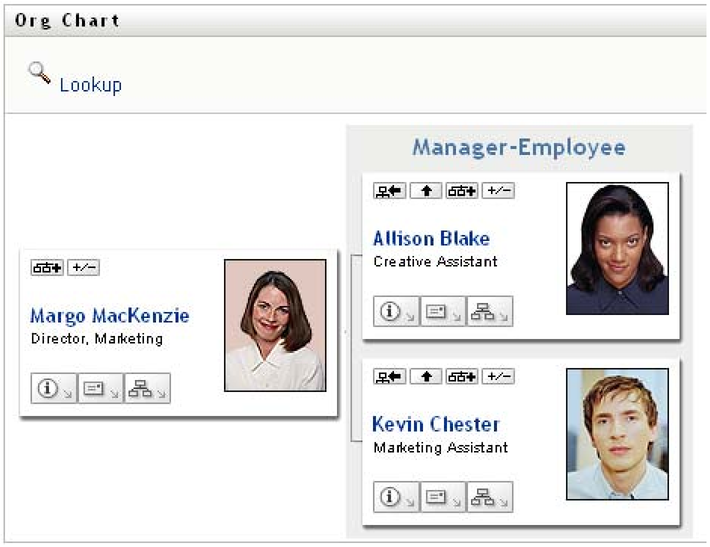
```
Hi,

Please click on the following link to get a detailed profile about J
http://localhost:8888/IDMProv/portal/portlet/DetailPortlet?urlType=F

Regards,

Rusty Robinson
```

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

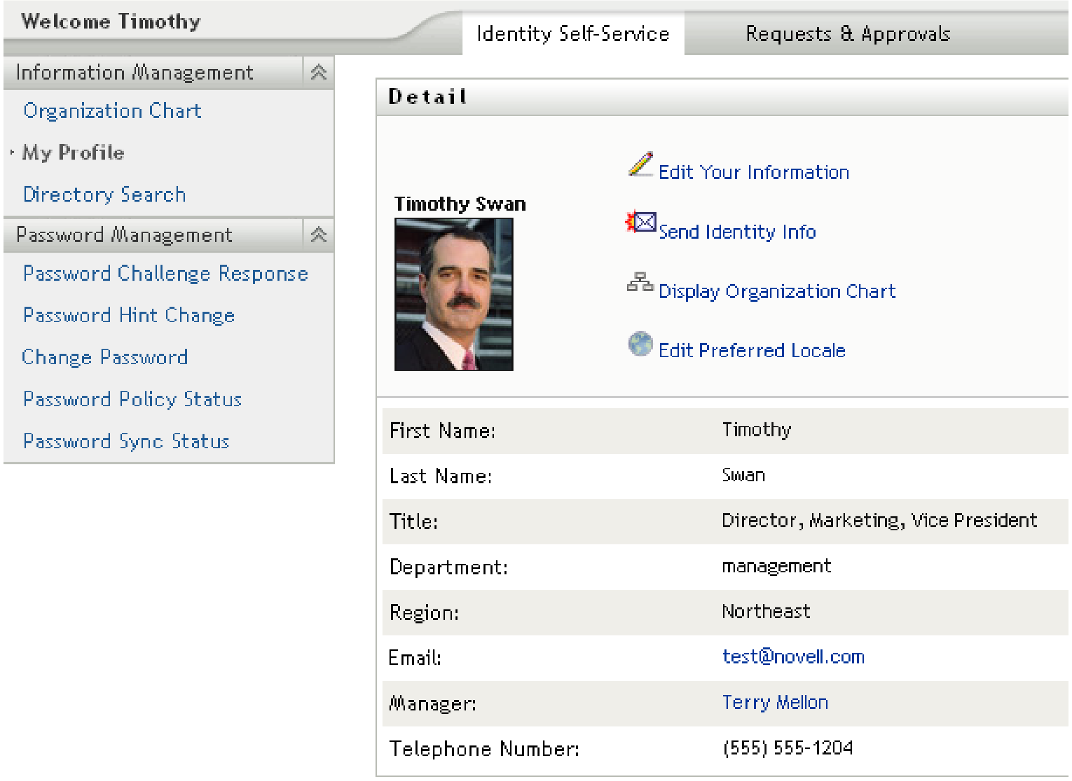
The Detail page of your profile can include links to other users or groups. You can display the details (Profile page) for any other user or group that is listed as a link in your details.

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*



Welcome Timothy

Identity Self-Service | Requests & Approvals

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

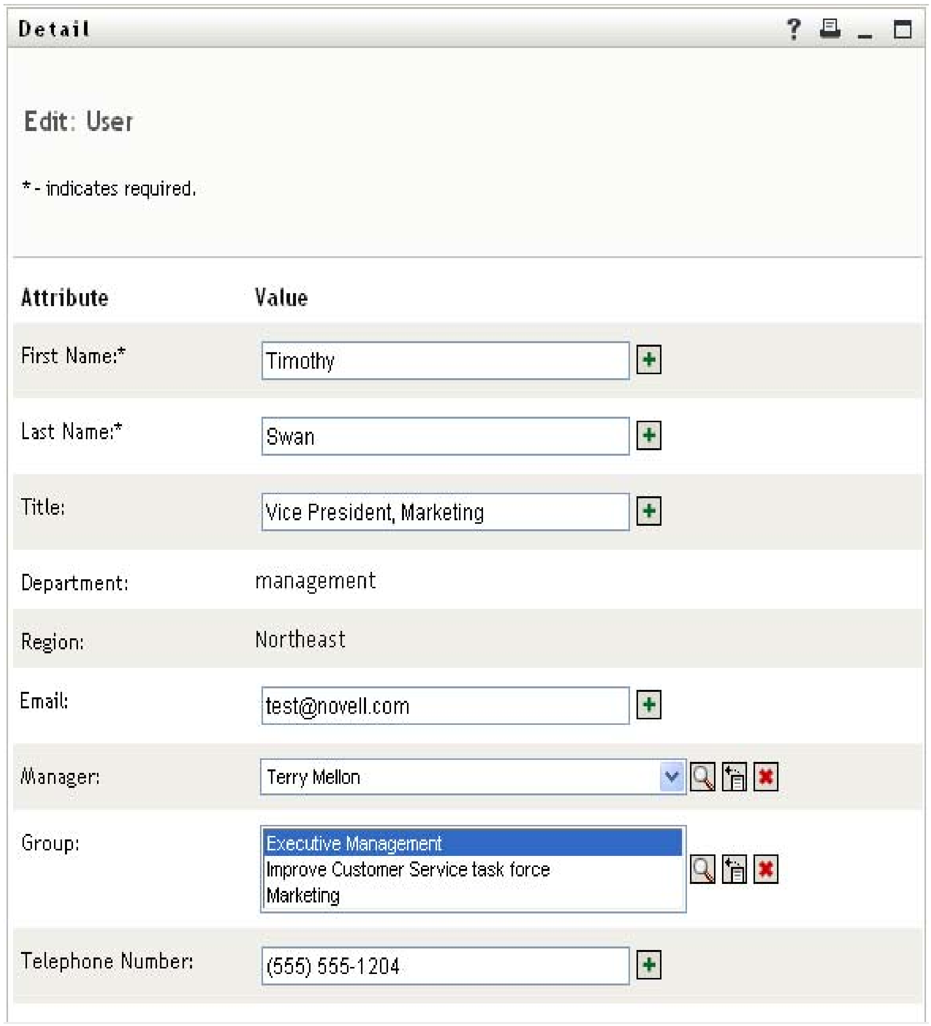
Timothy Swan

- 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



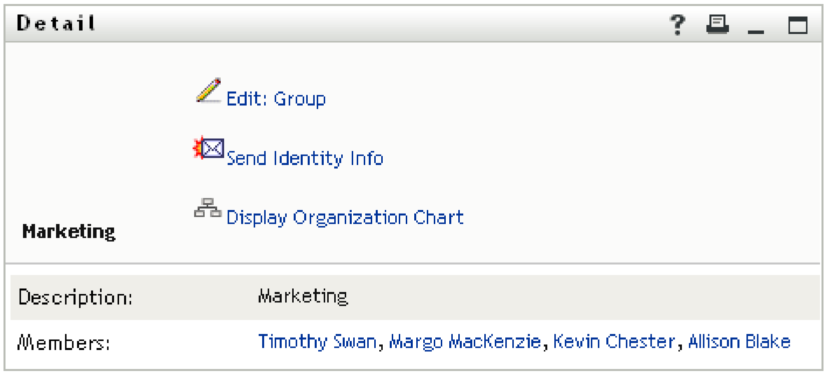
Edit: User

* - indicates required.

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 Improve Customer Service task force 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



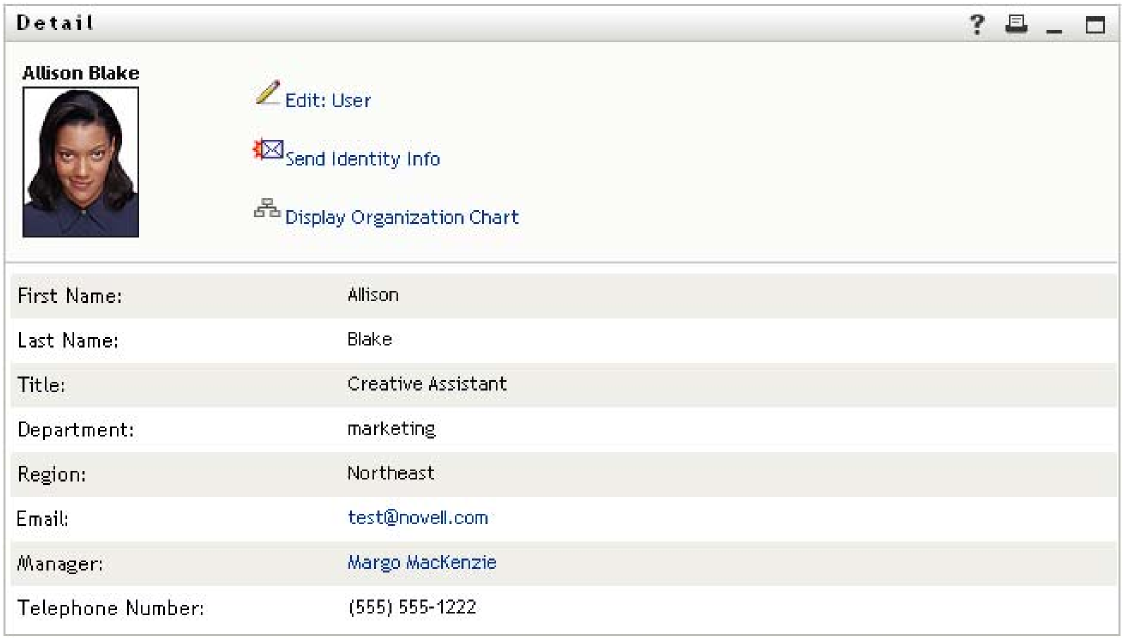
Marketing

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*



Allison Blake

Edit: User

Send Identity Info

Display Organization Chart

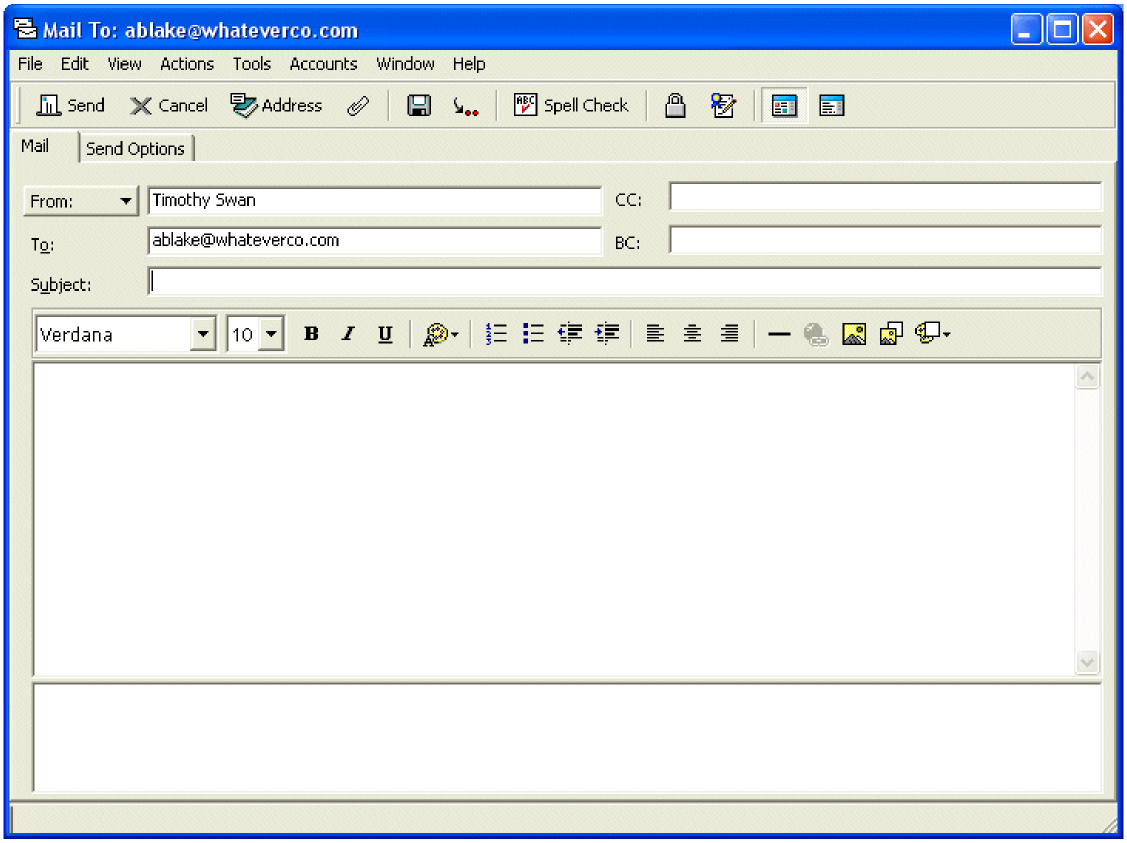
First Name:	Allison
Last Name:	Blake
Title:	Creative Assistant
Department:	marketing
Region:	Northeast
Email:	test@novell.com
Manager:	Margo MacKenzie
Telephone Number:	(555) 555-1222

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*


Mail To: ablake@whateverco.com
File Edit View Actions Tools Accounts Window Help
Send Cancel Address Spell Check
Mail Send Options

From: Timothy Swan

To: ablake@whateverco.com

CC:

BC:

Subject:

He can now type the message contents and send it.

5.6 Choosing a Preferred Language

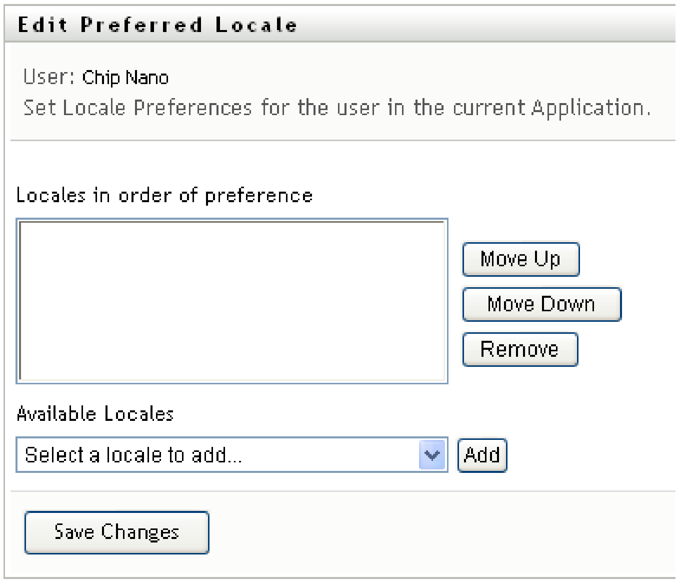
You can select the locale (language) that you prefer to use in the Identity Manager User Application. You can set the preferred locale at any time in *My Profile*.

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 Locale

User: Chip Nano

Set Locale Preferences for the user in the current Application.

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*.

Using Directory Search

6

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 88

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.

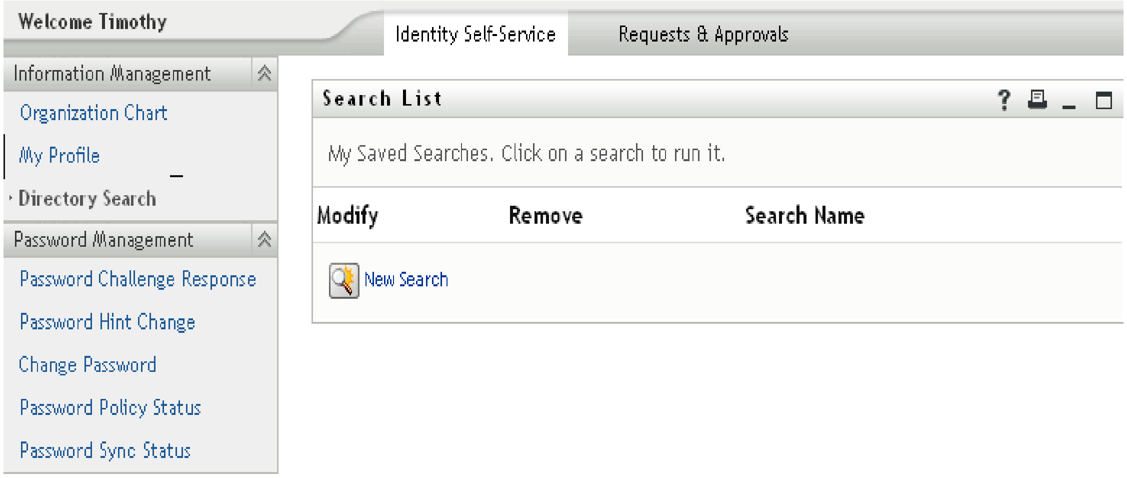
For more general information about accessing and working with the *Identity Self-Service* tab, see Chapter 2, "Introducing the Identity Self-Service Tab," on page 33.

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:

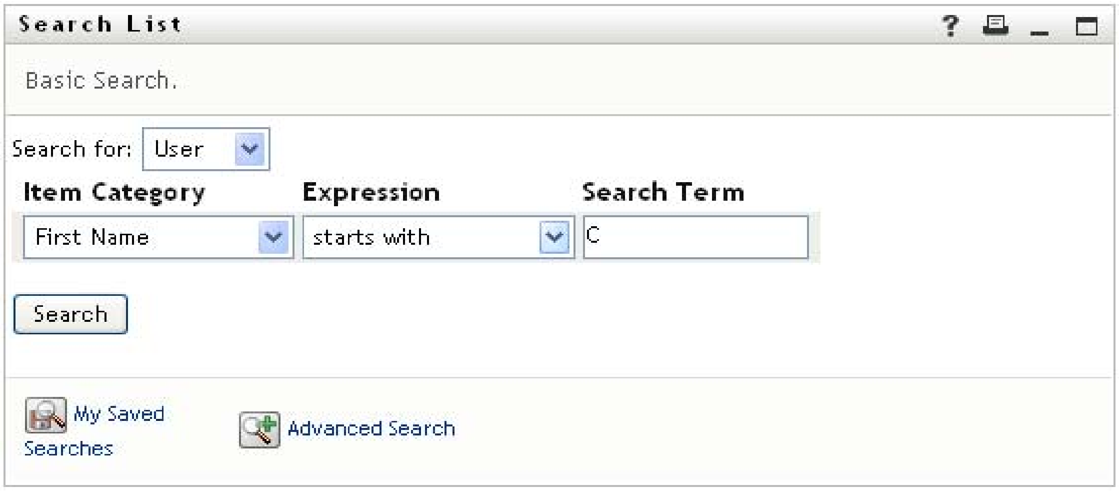
Figure 6-1 *Directory Search Page*



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

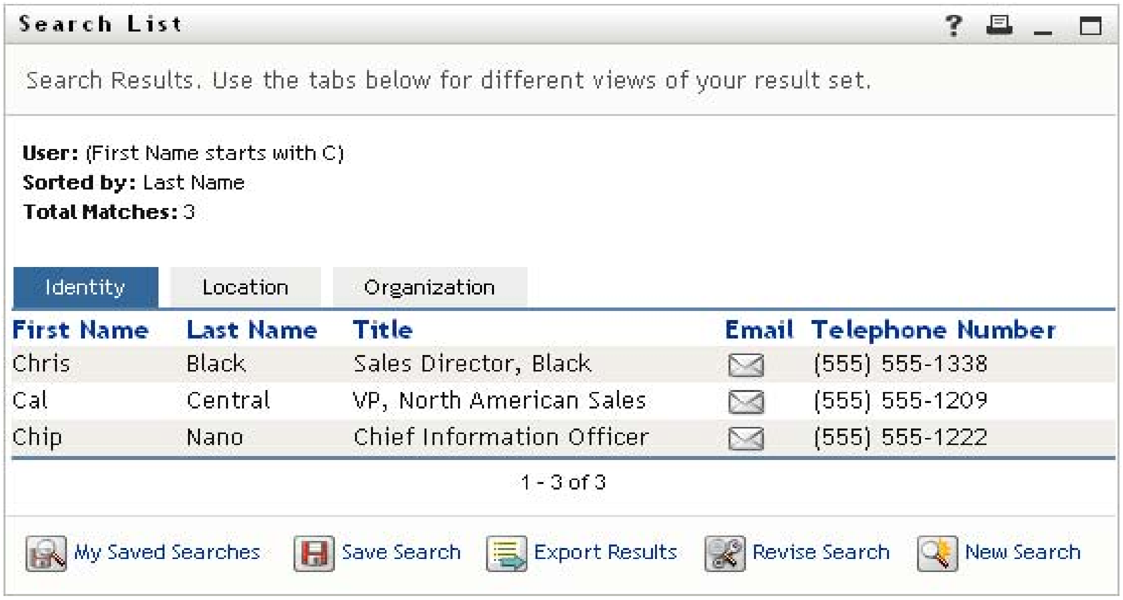
There's a user he wants to contact whose first name begins with the letter C, but he can't remember the full name. He just needs to specify a basic search with this criterion:

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



The 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



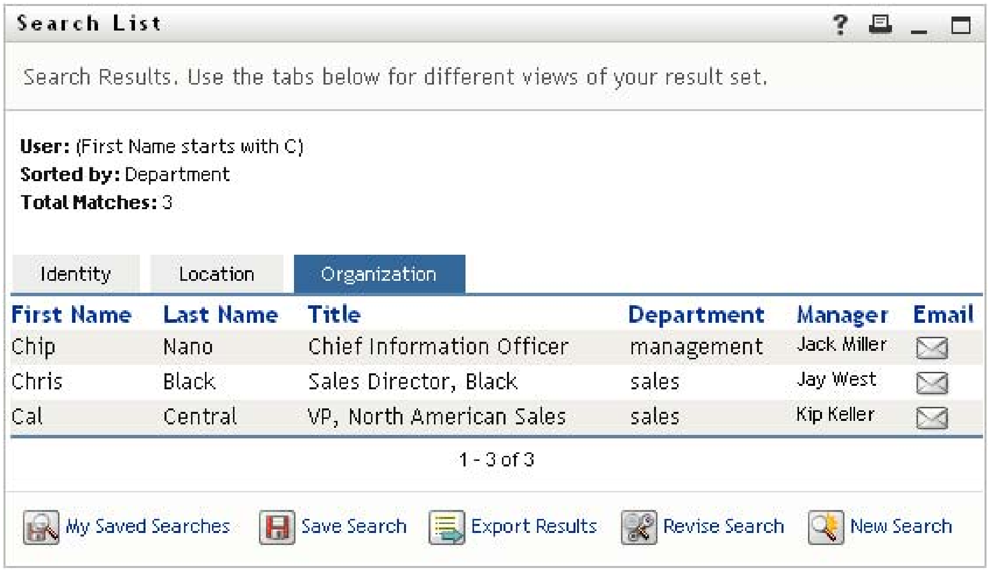
User: (First Name starts with C)
Sorted by: Last Name
Total Matches: 3

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

1 - 3 of 3

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



Search List

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

User: (First Name starts with C)
Sorted by: Department
Total Matches: 3

First Name	Last Name	Title	Department	Manager	Email
Chip	Nano	Chief Information Officer	management	Jack Miller	✉
Chris	Black	Sales Director, Black	sales	Jay West	✉
Cal	Central	VP, North American Sales	sales	Kip Keller	✉

1 - 3 of 3

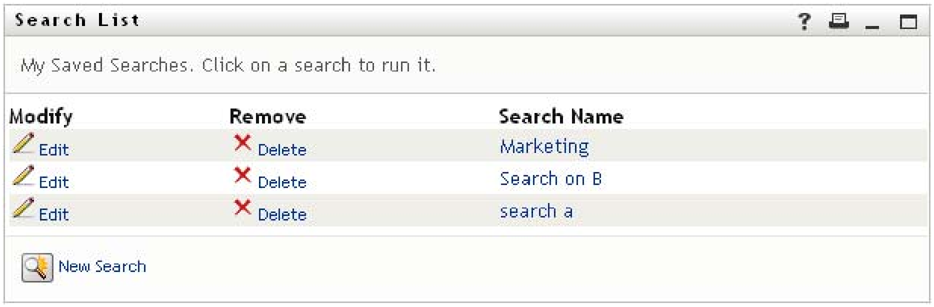
In addition to the tabs for different views, the search results page provides links and buttons for performing actions on its information. You can:

- 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



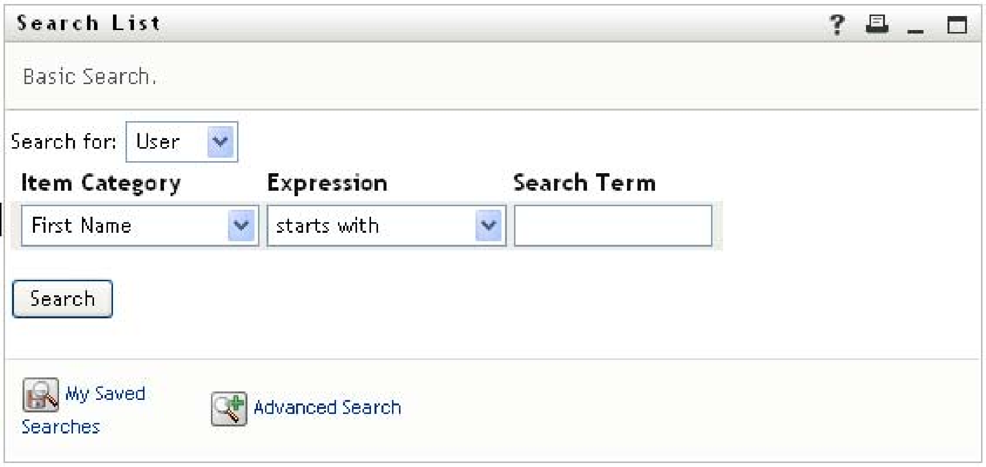
Search List

My Saved Searches. Click on a search to run it.

Modify	Remove	Search Name
Edit	✕ Delete	Marketing
Edit	✕ Delete	Search on B
Edit	✕ Delete	search a

6.2 Performing Basic Searches

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



Search List

Basic Search.

Search for: User

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 78.

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:

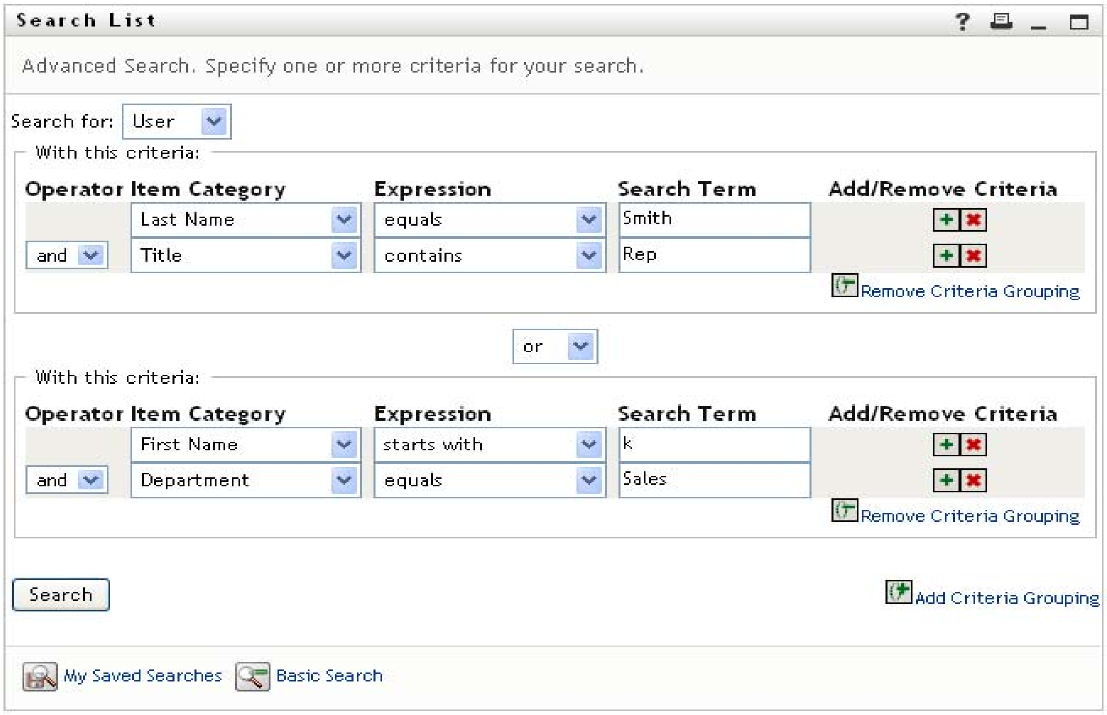
```
Last Name equals Smith AND Title contains Rep
```

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

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

Search for: User

With this criteria:

Operator	Item Category	Expression	Search Term	Add/Remove Criteria
	Last Name	equals	Smith	+ ✖
and	Title	contains	Rep	+ ✖

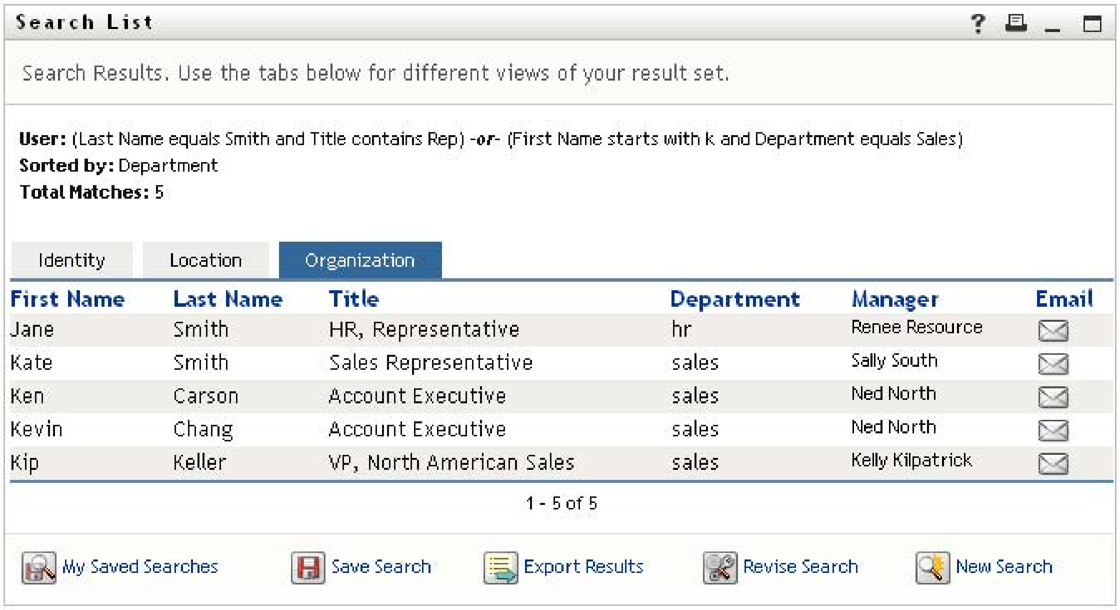
or

With this criteria:

Operator	Item Category	Expression	Search Term	Add/Remove Criteria
	First Name	starts with	k	+ ✖
and	Department	equals	Sales	+ ✖

The result of this search is shown in Figure 6-7 on page 75.

Figure 6-7 Result of Advanced Search



Search List

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

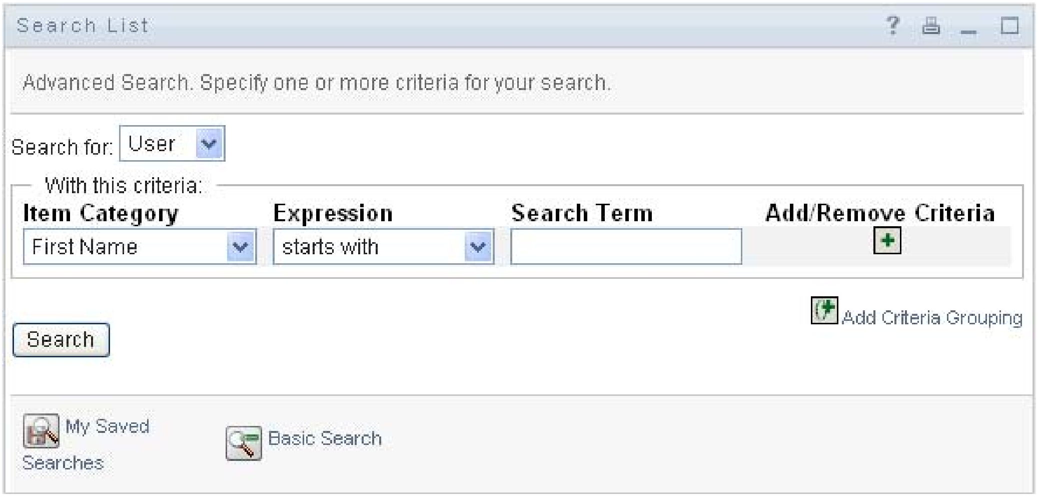
User: (Last Name equals Smith and Title contains Rep) *-or-* (First Name starts with k and Department equals Sales)
Sorted by: Department
Total Matches: 5

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

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:



Search List

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		⊞

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 78.
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:

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)	◆ starts with ◆ contains ◆ equals ◆ ends with ◆ is present ◆ does not start with ◆ does not contain ◆ does not equal ◆ does not end with ◆ is not present
String (text) with a predetermined list of choices User or group (or other object identified by DN) Boolean (true or false)	◆ equals ◆ is present ◆ does not equal ◆ is not present

If the attribute is a	You can select one of these comparison operations
User (item category: Manager, Group, or Direct Reports)	◆ equals ◆ is present ◆ does not equal ◆ is not present
Group (item category: Members)	◆ equals ◆ is present ◆ does not equal ◆ is not present
Time (in date-time or date-only format) Number (integer)	◆ equals ◆ greater than ◆ greater than or equal to ◆ less than ◆ less than or equal to ◆ is present ◆ does not equal ◆ not greater than ◆ not greater than or equal to ◆ not less than ◆ not less than or equal to ◆ is not present

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 *Lookup, History,* and *Reset* buttons that display on the right.
Time (in date-time or date-only format)	Use the *Calendar* and *Reset* buttons that display on the right.
Number (integer)	Type your number in the text box that displays on the right.

If the attribute is a	You do this to specify the value
Boolean (true or false)	Type `true` or `false` 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*

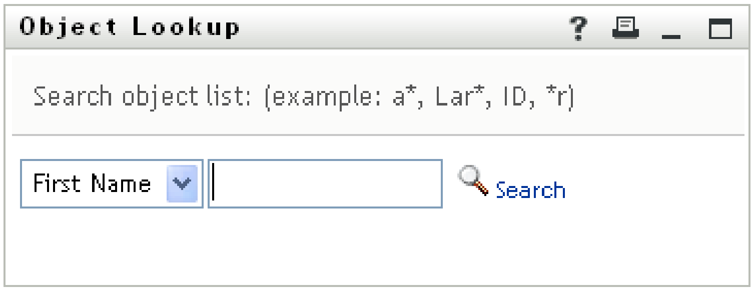
Button	What It Does
🔍	Looks up a value to use for a comparison
📋	Displays a *History* list of values used for a comparison
✎	Resets the value for a comparison

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:



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

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.

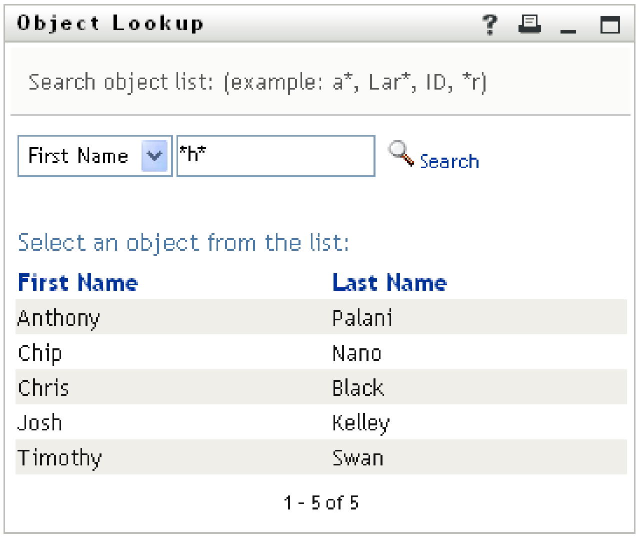
The search finds every name that begins with the text you type. It is not case sensitive. You can optionally use the asterisk (*) as a wildcard in your text to represent zero or more of any character.

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:



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

First Name *h*

Select an object from the list:

First Name	Last Name
Anthony	Palani
Chip	Nano
Chris	Black
Josh	Kelley
Timothy	Swan

1 - 5 of 5

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

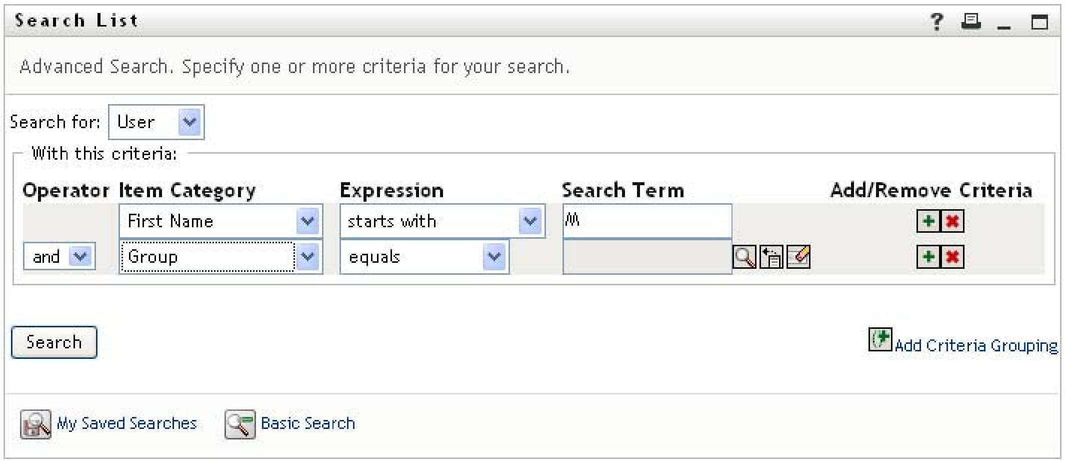
You can sort the search results in ascending or descending order by clicking the column headings.

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:



Search List

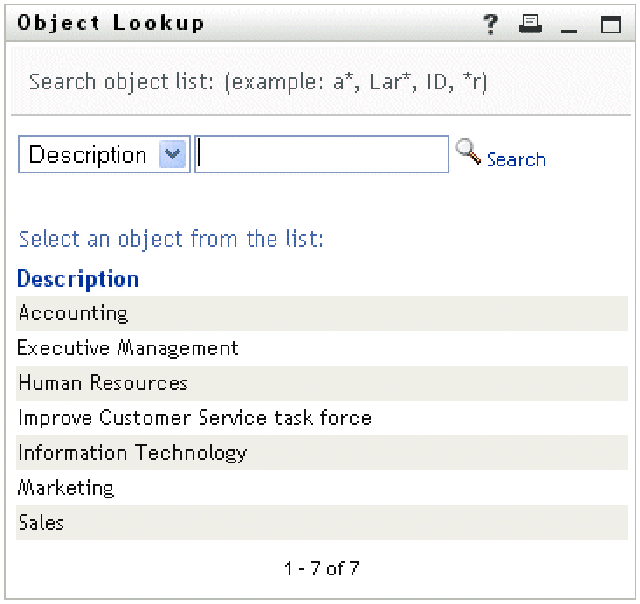
Advanced Search. Specify one or more criteria for your search.

Search for: User

With this criteria:

Operator	Item Category	Expression	Search Term	Add/Remove Criteria
	First Name	starts with	M	
and	Group	equals		

The Lookup page displays search results:



Object Lookup

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

Description

Select an object from the list:

Description
Accounting
Executive Management
Human Resources
Improve Customer Service task force
Information Technology
Marketing
Sales

1 - 7 of 7

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.

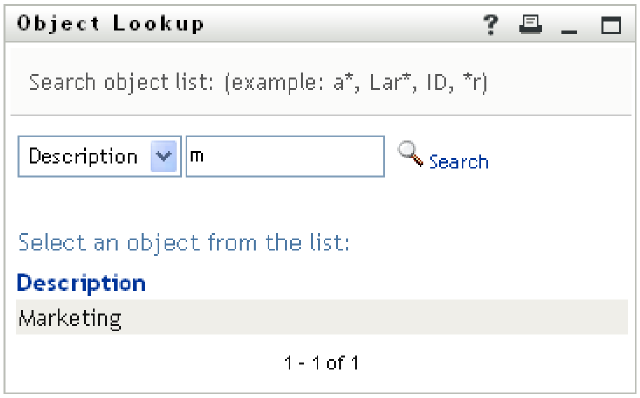
The search finds every description that begins with the text you type. It is not case sensitive. You can optionally use the asterisk (*) as a wildcard in your text to represent zero or more of any character.

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:


Object Lookup
Search object list: (example: a*, Lar*, ID, *r)
Description
Search
Select an object from the list:
Description
1 - 1 of 1

m

Marketing

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.

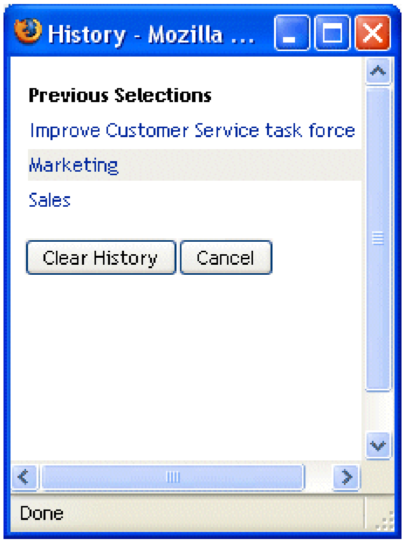
4 Select the group you want from the list.

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:



Previous Selections

Improve Customer Service task force

Marketing

Sales

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 as the value to use for your comparison.
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 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 83
- Section 6.4.2, "Using the Search List," on page 85
- Section 6.4.3, "Other Actions You Can Perform," on page 86

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 84

On any search results page, you can select

- View My Saved Searches
- Save Search

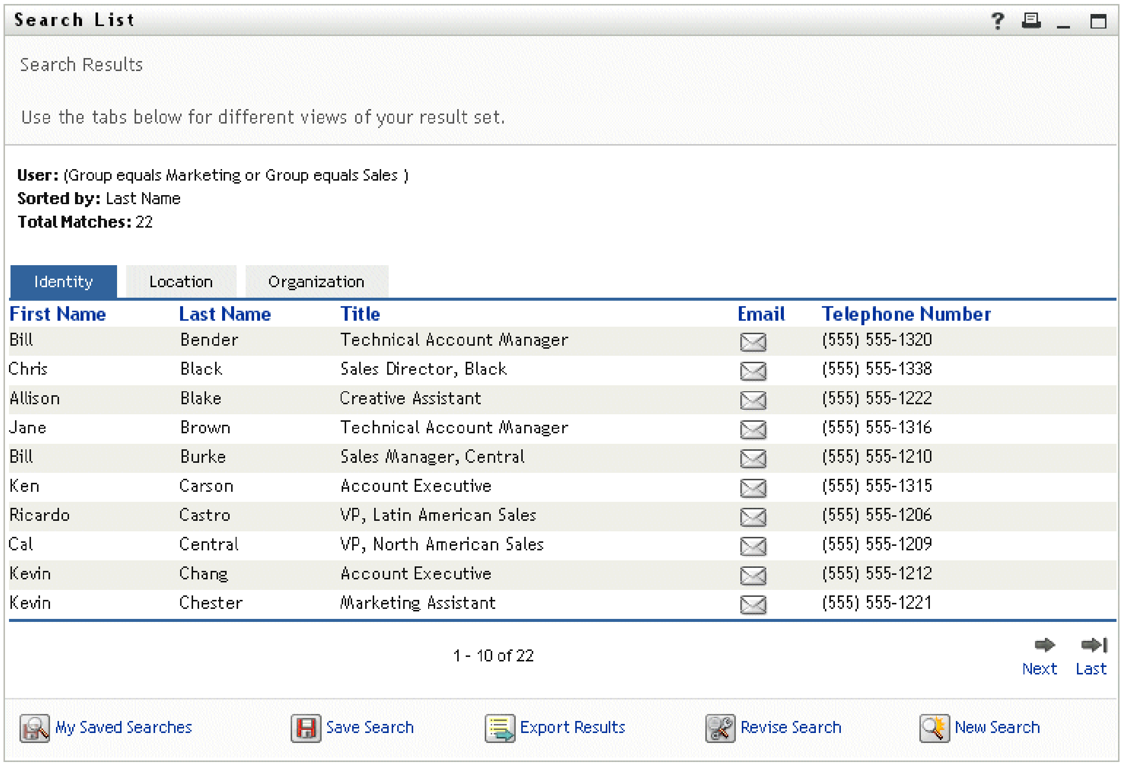
- Revise Search
- Export Results
- Start a New Search

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

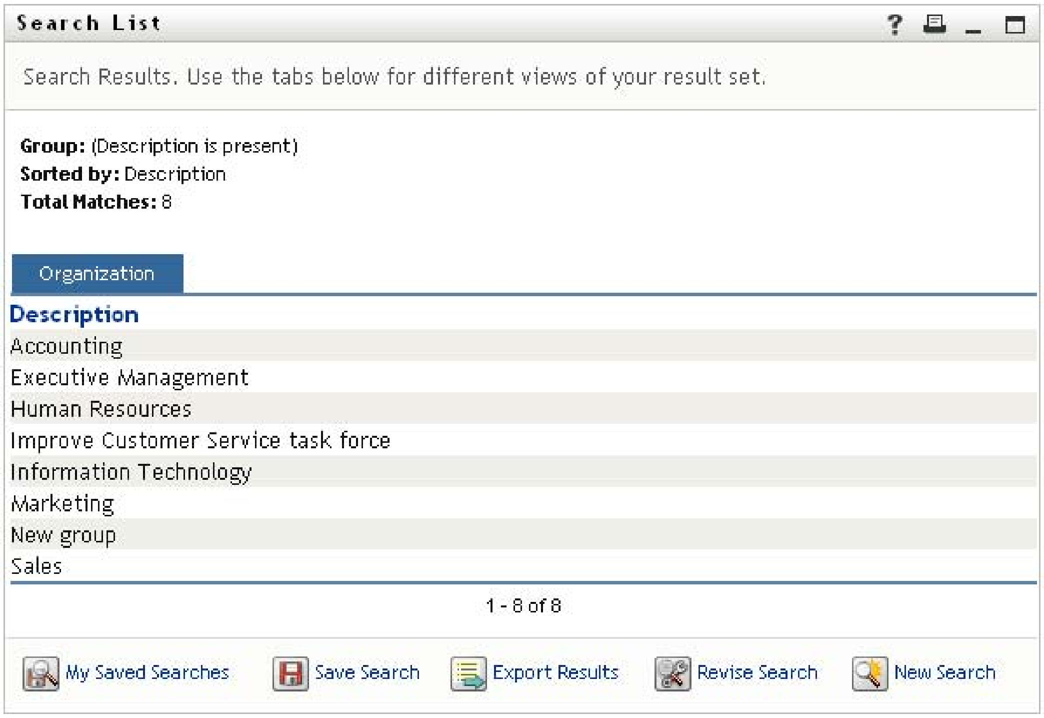
First Name	Last Name	Title	Email	Telephone Number
Bill	Bender	Technical Account Manager	✉	(555) 555-1320
Chris	Black	Sales Director, Black	✉	(555) 555-1338
Allison	Blake	Creative Assistant	✉	(555) 555-1222
Jane	Brown	Technical Account Manager	✉	(555) 555-1316
Bill	Burke	Sales Manager, Central	✉	(555) 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

For a Group Search

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

Figure 6-9 Group Search Results



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

Group: (Description is present)
Sorted by: Description
Total Matches: 8

Description
Accounting
Executive Management
Human Resources
Improve Customer Service task force
Information Technology
Marketing
New group
Sales

1 - 8 of 8

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 85
- "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.

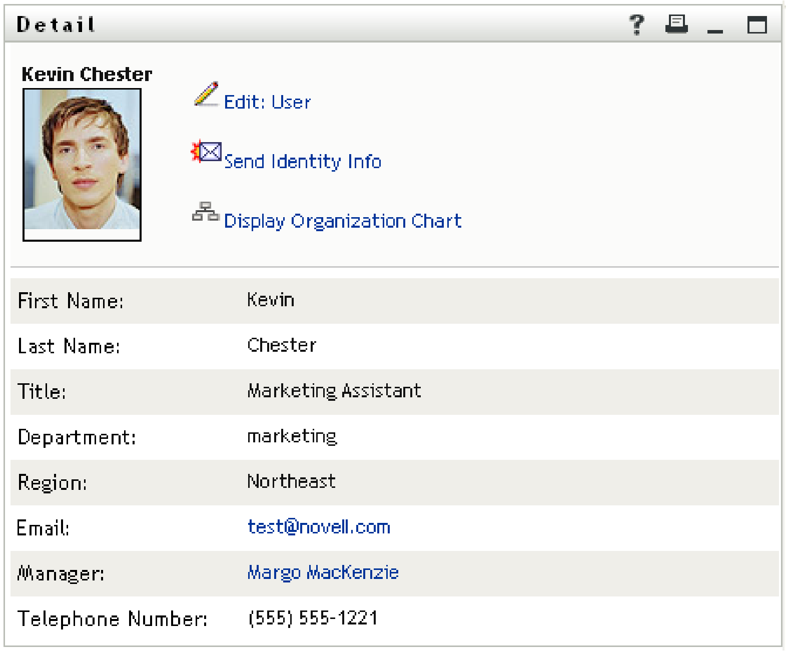
The initial sort is in ascending order.

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:



Detail

Kevin Chester

Edit: User

Send Identity Info

Display Organization Chart

First Name:	Kevin
Last Name:	Chester
Title:	Marketing Assistant
Department:	marketing
Region:	Northeast
Email:	test@novell.com
Manager:	Margo MacKenzie
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.

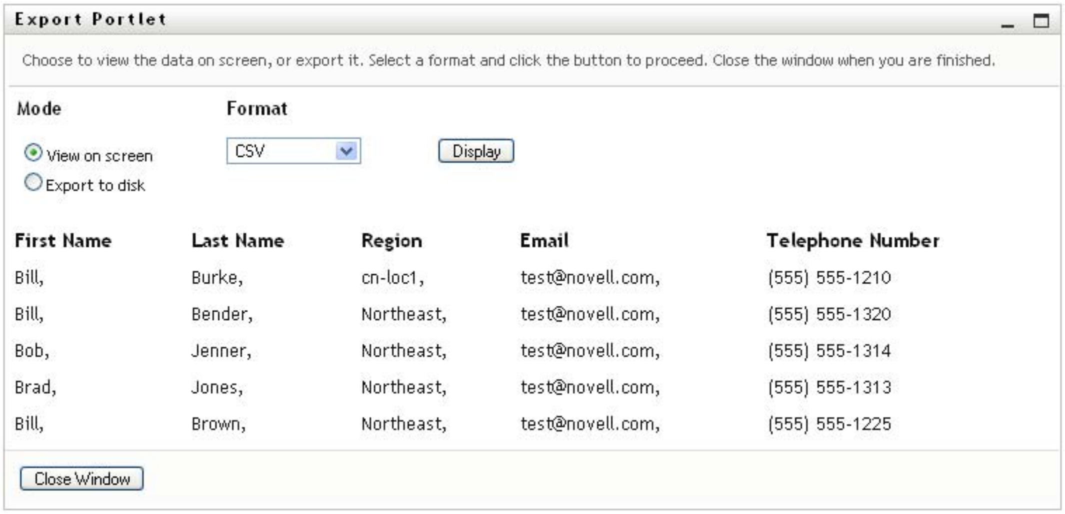
   To learn more about working with saved searches, see Section 6.5, "Using Saved Searches," on page 88.

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:



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.

Mode

● View on screen

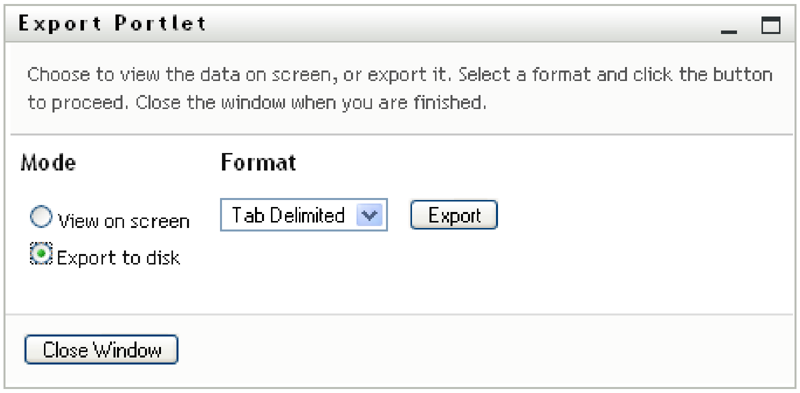
○ Export to disk

Format: CSV

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, check *Export to disk*.

   The Export page displays:



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.

Mode

○ View on screen
● Export to disk

Format

Tab Delimited

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.*date*.*time*.csv For example: `SearchListResult.27-Sep-05.11.21.47.csv`
Tab Delimited	SearchListResult.*date*.*time*.txt For example: `SearchListResult.27-Sep-05.11.20.51.txt`
XML (available if you are exporting to disk)	SearchListResult.*date*.*time*.xml For example: `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:

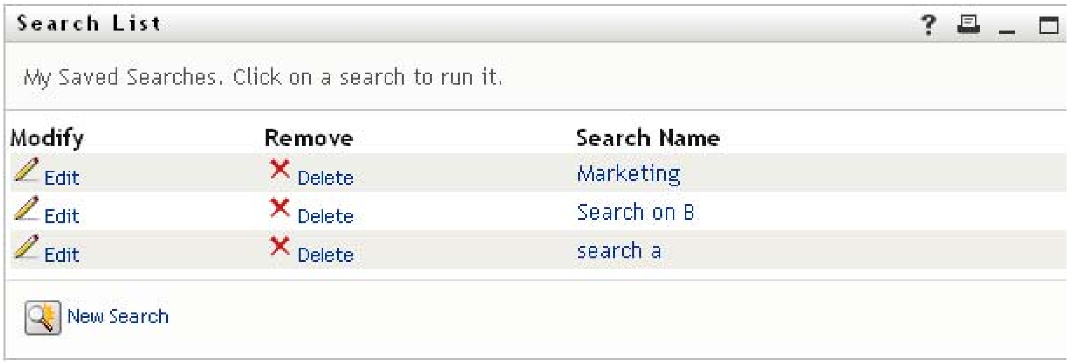
- Section 6.5.1, "To List Saved Searches," on page 89

- 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 89

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*



My Saved Searches. Click on a search to run it.

Modify	Remove	Search Name
Edit	✕ Delete	Marketing
Edit	✕ Delete	Search on B
Edit	✕ Delete	search a

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.

Performing Password Management

7

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:

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: ◆ Your valid responses to administrator-defined challenge questions ◆ User-defined challenge questions and responses
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. You can change requirements marked **Valid**
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

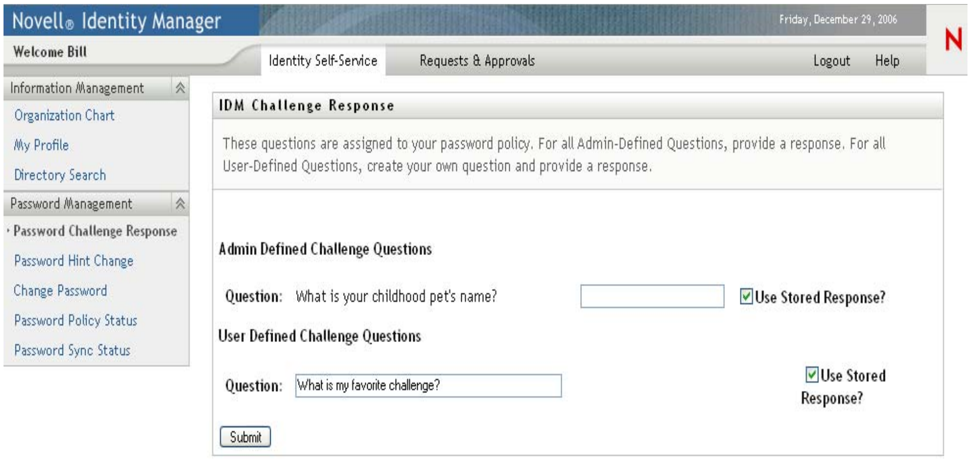
Challenge questions are used to verify your identity during login when you have forgotten your password. If the system administrator has set up a password policy that enables this feature for you, you can use the Password Challenge Response page to:

- 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:



IDM Challenge Response

These questions are assigned to your password policy. For all Admin-Defined Questions, provide a response. For all User-Defined Questions, create your own question and provide a response.

Admin Defined Challenge Questions

Question: What is your childhood pet's name? ☑ Use Stored Response?

User Defined Challenge Questions

Question: What is my favorite challenge? ☑ Use Stored Response?

The *Response* text boxes display as blank (even if you have previously defined responses).

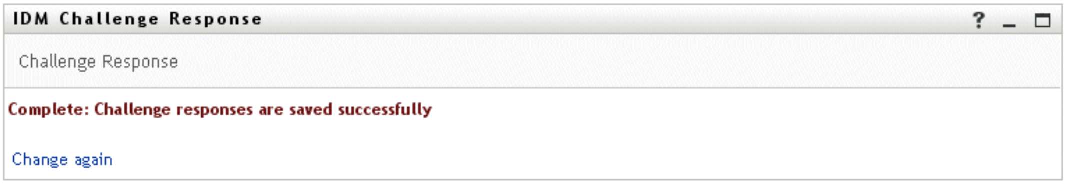
2 Type an appropriate response in each *Response* text box (they are all required), or use your previously stored response.

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*.

The status of your request displays. For example:



IDM Challenge Response

Challenge Response

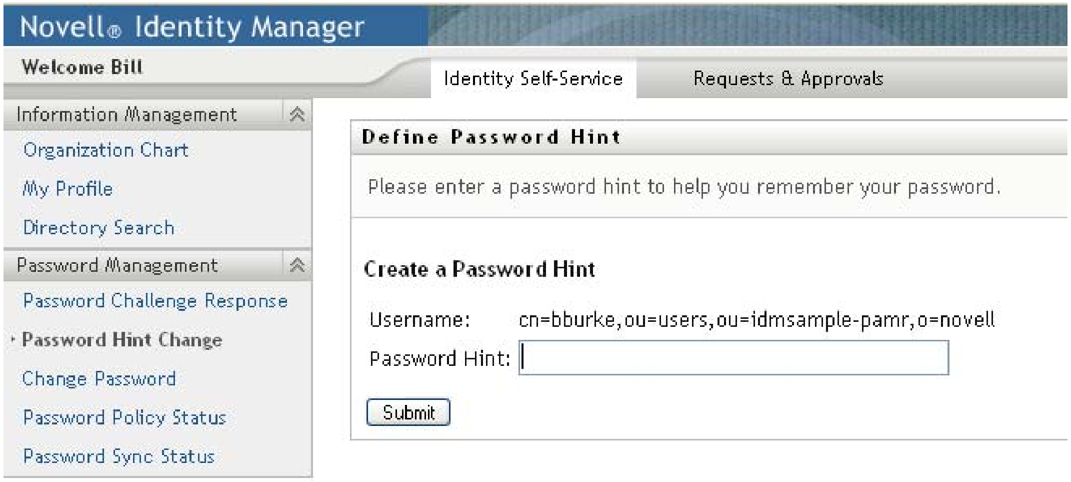
Complete: Challenge responses are saved successfully

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:



Define Password Hint

Please enter a password hint to help you remember your password.

Create a Password Hint

Username: cn=bburke,ou=users,ou=idmsample-pamr,o=novell

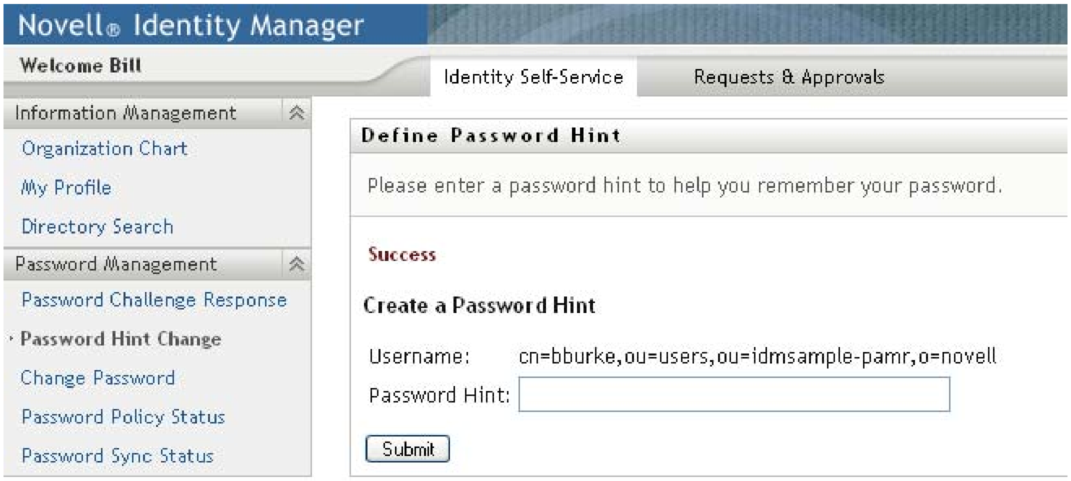
Password Hint:

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. For example:



Define Password Hint

Please enter a password hint to help you remember your password.

Success

Create a Password Hint

Username: cn=bburke,ou=users,ou=idmsample-pamr,o=novell

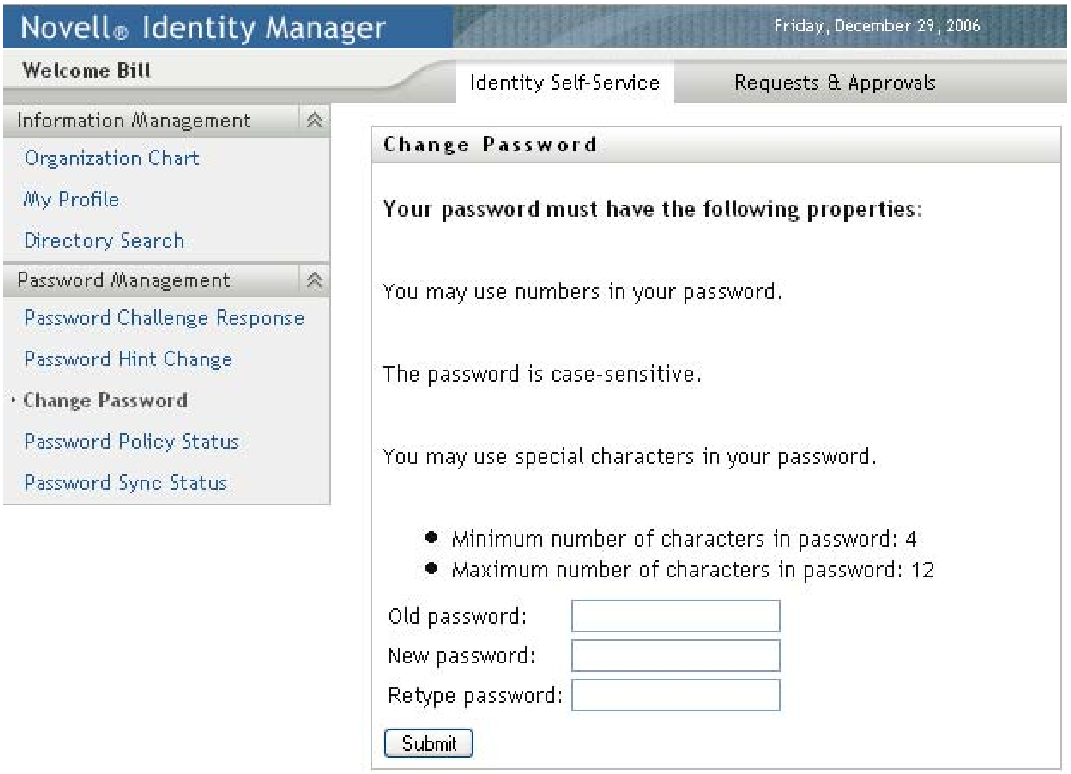
Password Hint:

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:



Change Password

Your password must have the following properties:

You may use numbers in your password.

The password is case-sensitive.

You may use special characters in your password.

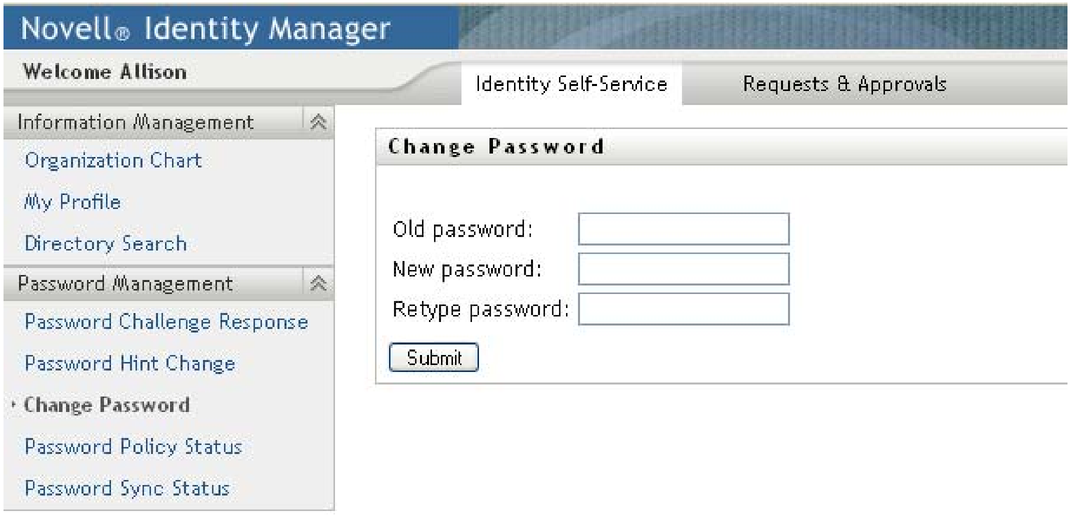
- Minimum number of characters in password: 4
- Maximum number of characters in password: 12

Old password:

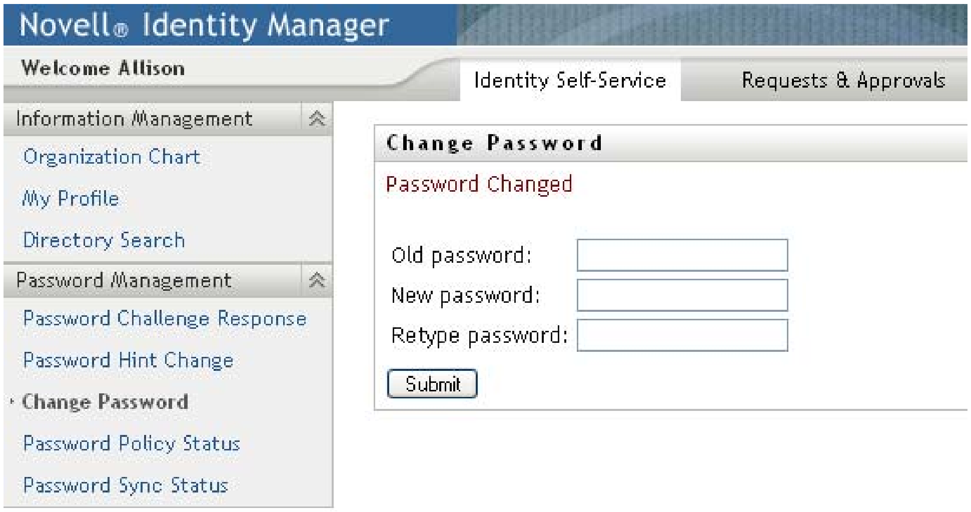
New password:

Retype password:

If no password policy applies, you'll see the basic Change Password page:



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*.
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 93.
7. The status of your request is displayed. For example:



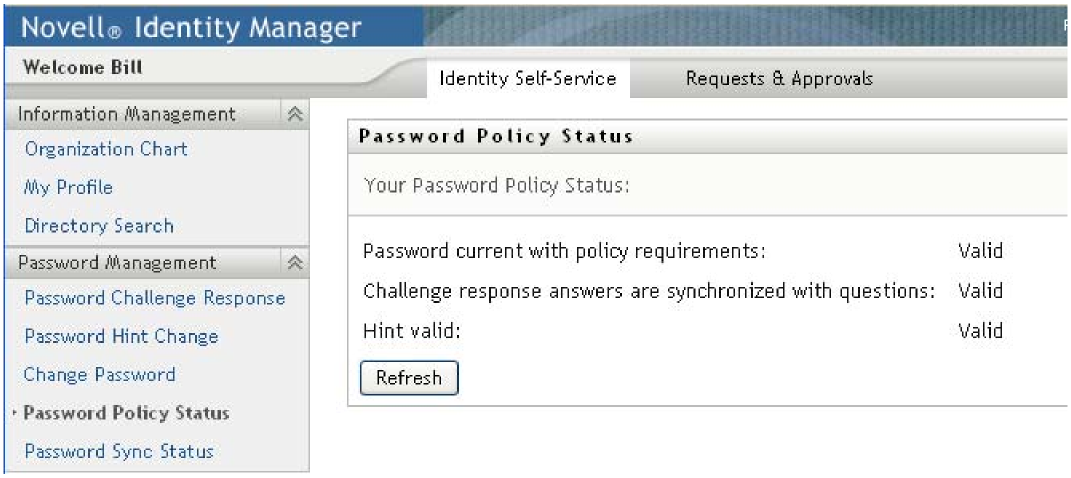
Password Changed

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:



Password Policy Status

Your Password Policy Status:

Password current with policy requirements: Valid

Challenge response answers are synchronized with questions: Valid

Hint valid: Valid

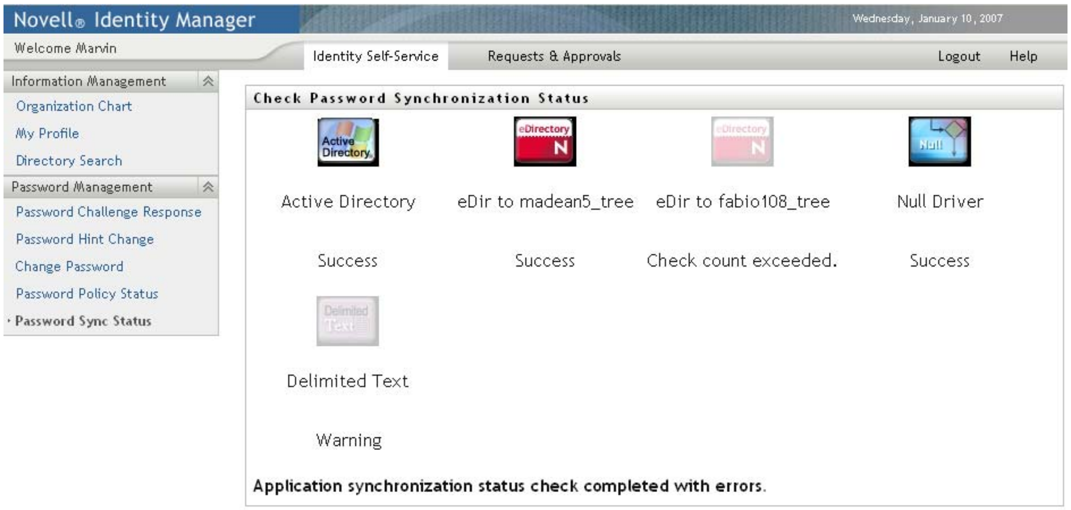
Items labeled invalid are items that you cannot change.

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:



Check Password Synchronization Status

Active Directory: Success

eDir to madean5_tree: Success

eDir to fabio108_tree: Check count exceeded.

Null Driver: Success

Delimited Text: Warning

Application synchronization status check completed with errors.

Creating Users or Groups

8

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 100
- 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.

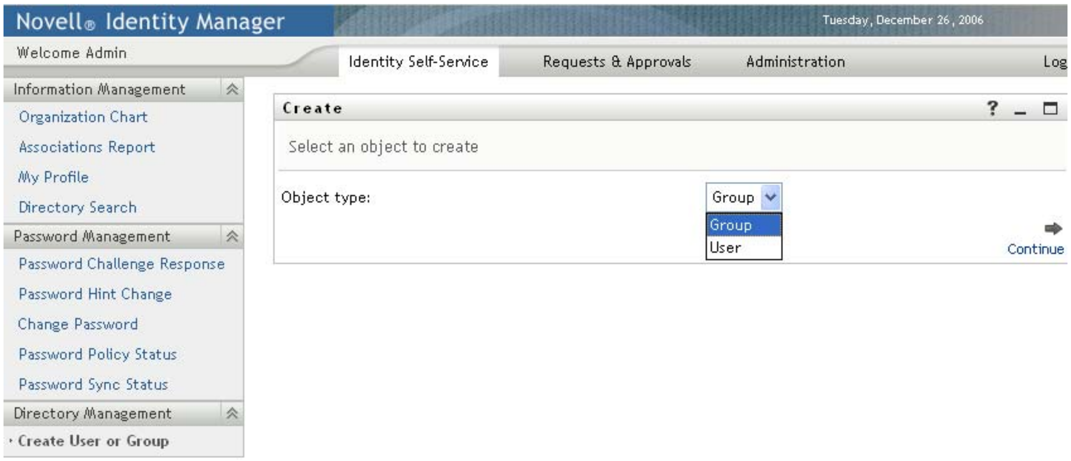
Details on enabling access to the Create User or Group page are in the "Page Administration" section of the *Identity Manager User Application: Administration Guide* (http://www.novell.com/documentation/idmrbpm361/index.html). To enable access, open iManager, add the user as a Trustee, and add the Assigned 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).

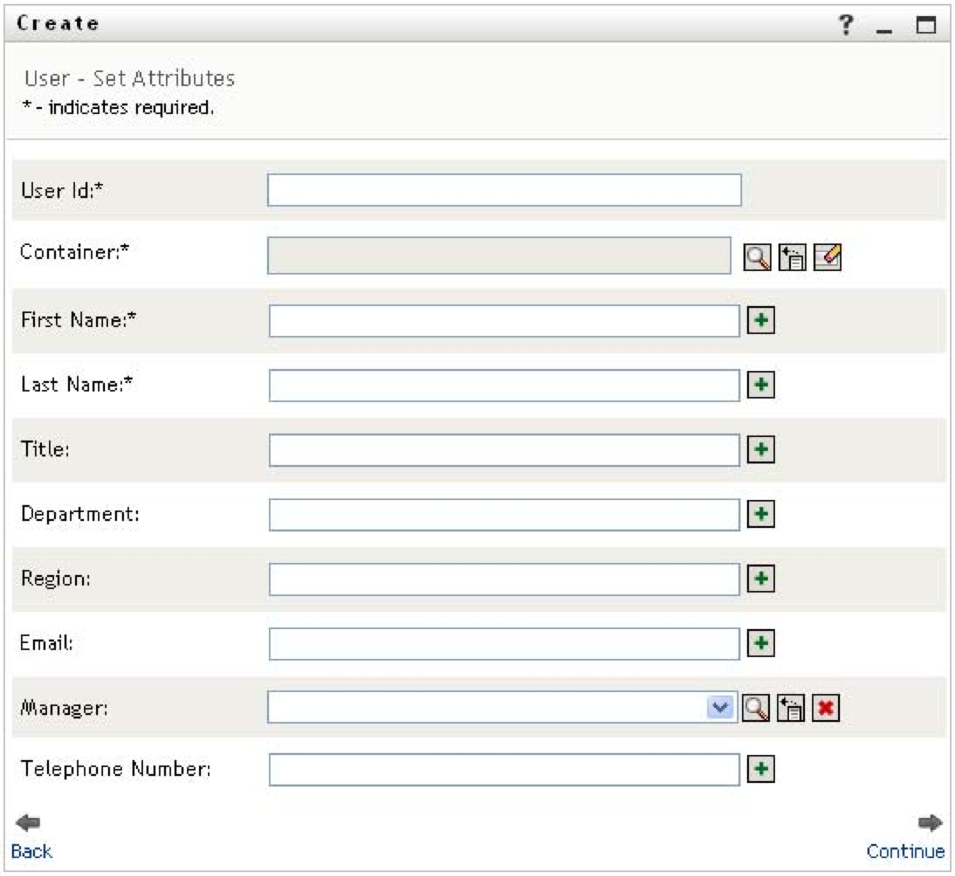
The *Select an object to create* panel displays.



Object type: Group

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

The *User - Set Attributes* panel displays:



3 Specify values for the following required attributes:

Attribute	What to Specify
User ID	The username for this new user.

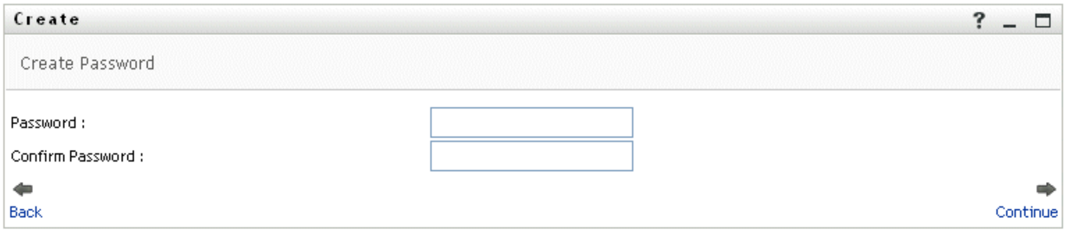
Attribute	What to Specify
Container	An organizational unit in the Identity Vault under which you want the new user stored (such as an OU named users). For example: `ou=users,ou=MyUnit,o=MyOrg` To learn about using the buttons provided to specify a container, see Section 8.4, "Using the Editing Buttons," on page 101. 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:



Password :

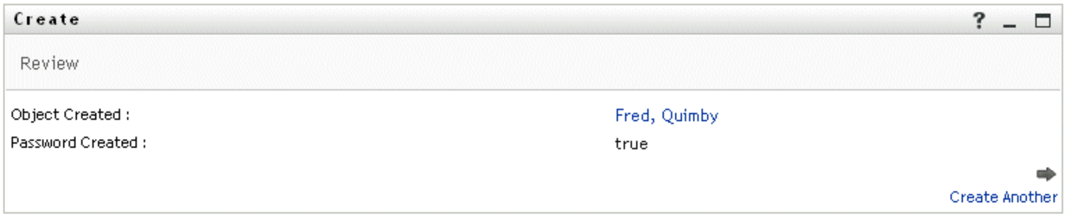
Confirm Password :

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:



Object Created : Fred, Quimby

Password Created : true

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

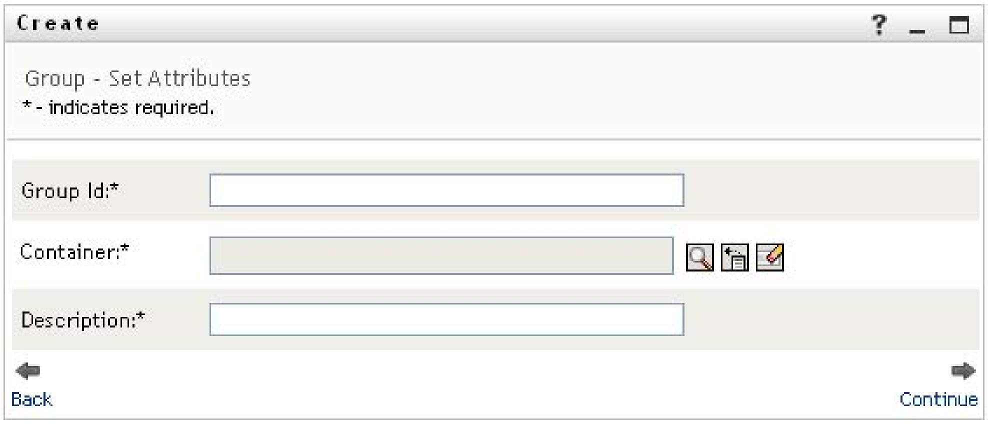
8.3 Creating a Group

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:



Group - Set Attributes

* - indicates required.

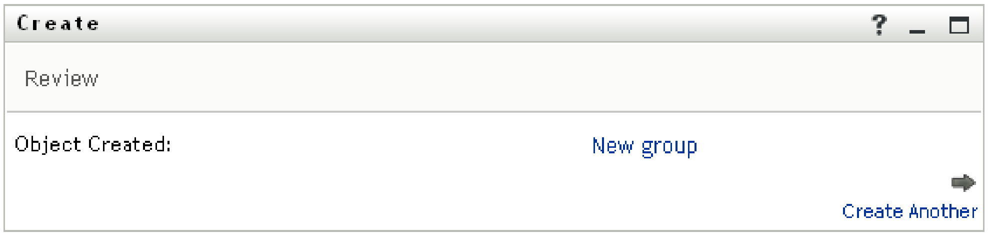
Group Id:*	
Container:*	
Description:*	

3 Specify values for the following required attributes:

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

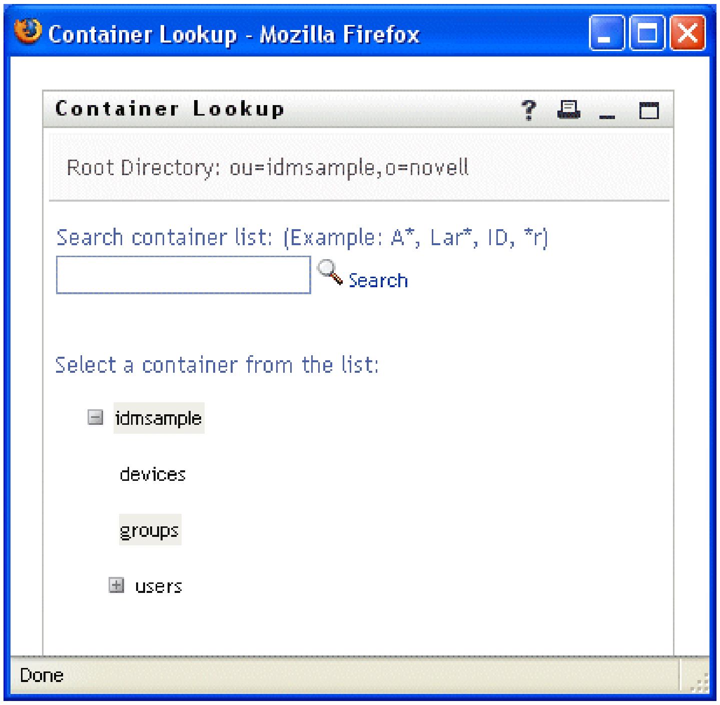
IMPORTANT: It is possible to use the Edit User page of the *Identity Self-Service* tab to break the hierarchical reporting structure. For example, you can add a direct report to a manager even if the direct report has another manager assigned, or you can have a manager report to a person in his or her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


Container Lookup - Mozilla Firefox
Container Lookup
Search
Select a container from the list:
idmsample
devices
groups
users
Done

Root Directory: ou=idmsample,o=novell

Search container list: (Example: A*, Lar*, ID, *r)

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.

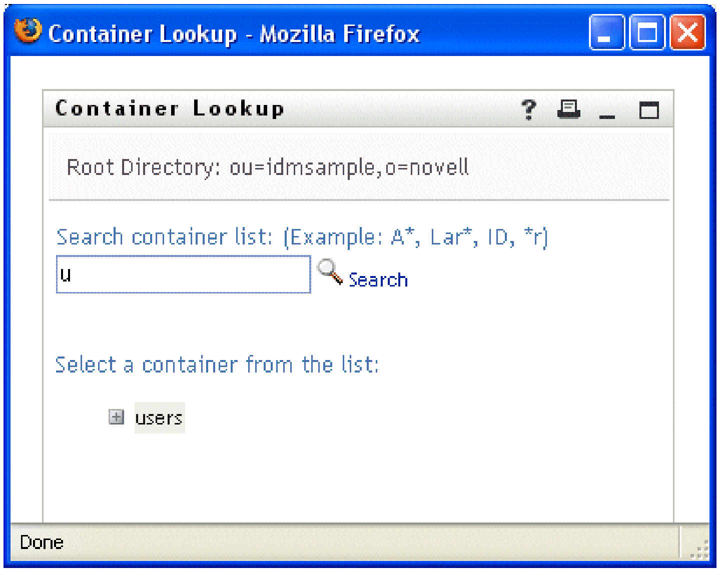
In the text box, type all or part of the container name to search for. The search finds every container name that begins with the text you type. It is not case sensitive. You can optionally use the asterisk (*) as a wildcard in your text to represent zero or more of any character.

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:



Root Directory: ou=idmsample,o=novell

Search container list: (Example: A*, Lar*, ID, *r)

u

Select a container from the list:

users

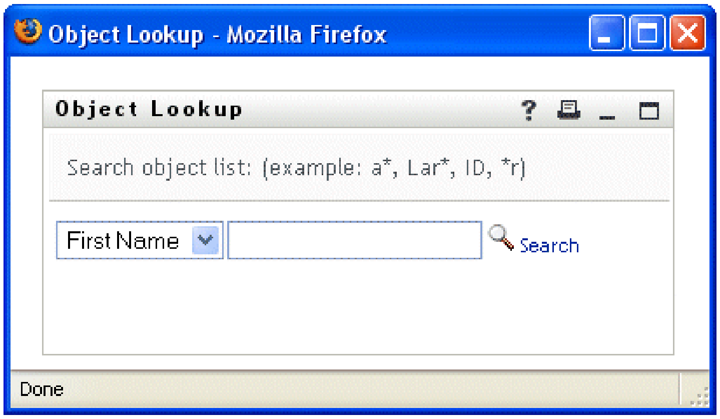
4 Select the container you want from the tree.

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:



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

First Name

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.

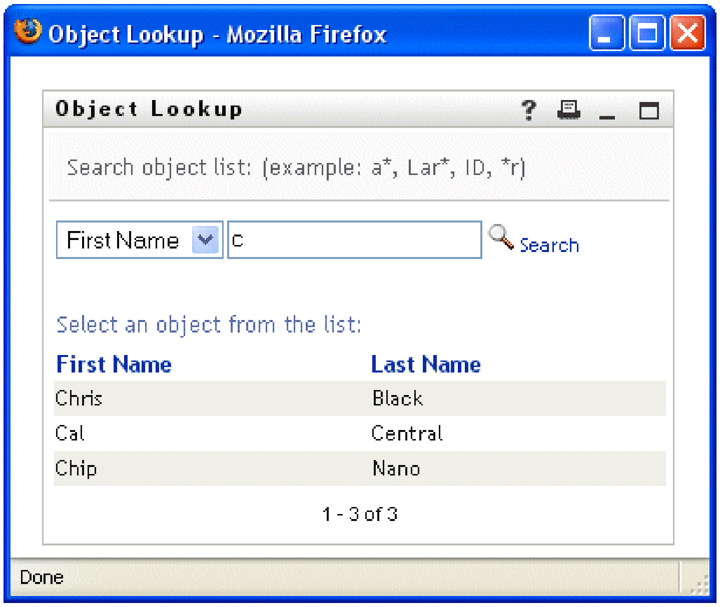
For instance, all of the following examples find the first name Chip:

```
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:



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

First Name: c

Select an object from the list:

First Name	Last Name
Chris	Black
Cal	Central
Chip	Nano

1 - 3 of 3

Done

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.

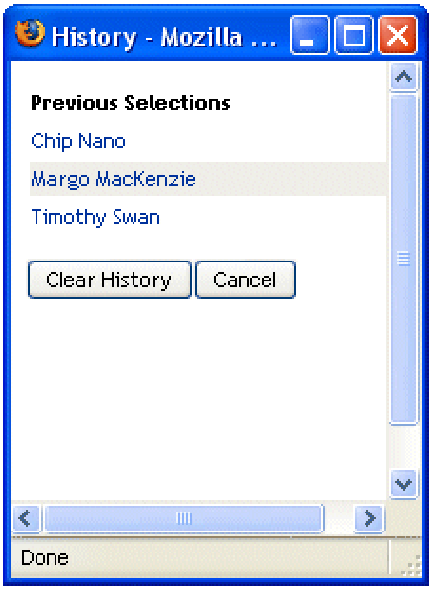
4 Select the user you want from the list.

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:



Previous Selections

Chip Nano

Margo MacKenzie

Timothy Swan

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 Requests & Approvals Tab

III

These sections tell you how to use the *Requests & Approvals* tab of the Identity Manager User Application.

Introducing the Requests & Approvals Tab

9

This section provides an overview of the *Requests & Approvals* tab. Topics include:

- Section 9.1, "About the Requests & Approvals Tab," on page 109
- Section 9.2, "Accessing the Requests & Approvals Tab," on page 110
- Section 9.3, "Exploring the Tab's Features," on page 110
- Section 9.4, "Requests & Approvals Actions You Can Perform," on page 112
- Section 9.5, "Understanding the Requests & Approvals Legend," on page 115

For more general information about accessing and working with the Identity Manager user interface, see Chapter 1, "Getting Started," on page 15.

9.1 About the Requests & Approvals Tab

The purpose of the *Requests & Approvals* tab is to give you a convenient way to perform workflow-based provisioning actions. These actions allow you to manage user access to secure resources in your organization. These resources can include digital entities such as user accounts, computers, and databases. For example, you might use the *Requests & Approvals* tab to:

- Make provisioning requests
- Manage provisioning work (workflow tasks associated with resource requests, as well as role and attestation requests)
- Configure provisioning settings for yourself or your team

When a provisioning 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.

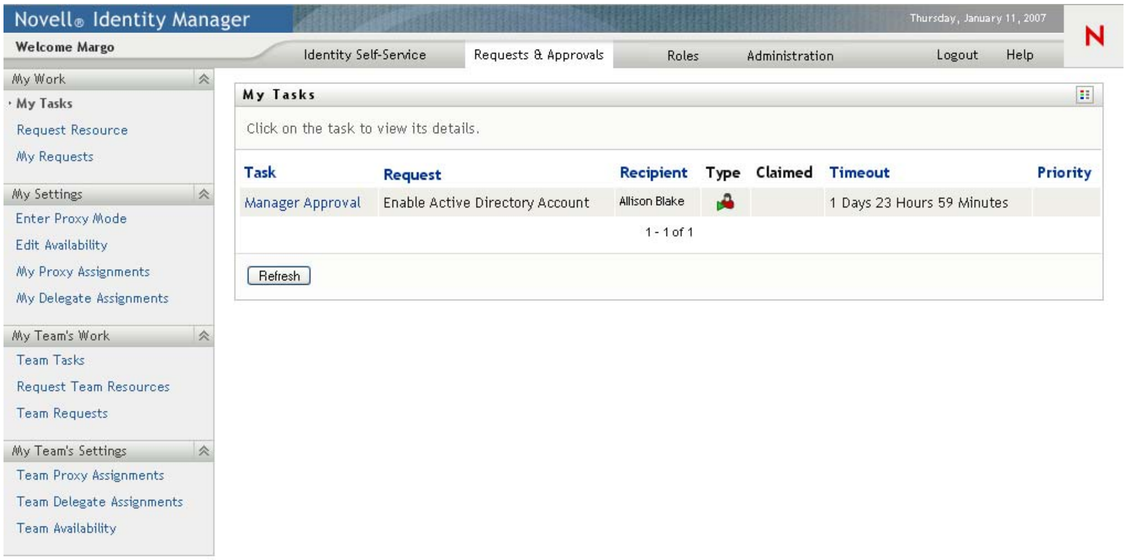
When a provisioning request is initiated, the Provisioning System tracks the initiator and the recipient. The initiator is the person who made the request. The recipient is the person for whom the request was made.

Your workflow designer and system administrator are responsible for setting up the contents of the *Requests & Approvals* tab for you and the others in your organization. The flow of control for a provisioning workflow, as well as the appearance of forms, can vary depending on how the provisioning request 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.

For details on customizing the design of a provisioning workflow, see the *Identity Manager User Application: Design Guide* (http://www.novell.com/documentation/idmrbpm361/index.html). For details on workflow administration, see the *Identity Manager User Application: Administration Guide* (http://www.novell.com/documentation/idmrbpm361/index.html).

9.2 Accessing the Requests & Approvals Tab

By default, after you have logged in to the Identity Manager user interface, the *Requests & Approvals* tab opens and displays the My Tasks page:



Click on the task to view its details.

Task	Request	Recipient	Type	Claimed	Timeout	Priority
Manager Approval	Enable Active Directory Account	Allison Blake			1 Days 23 Hours 59 Minutes	

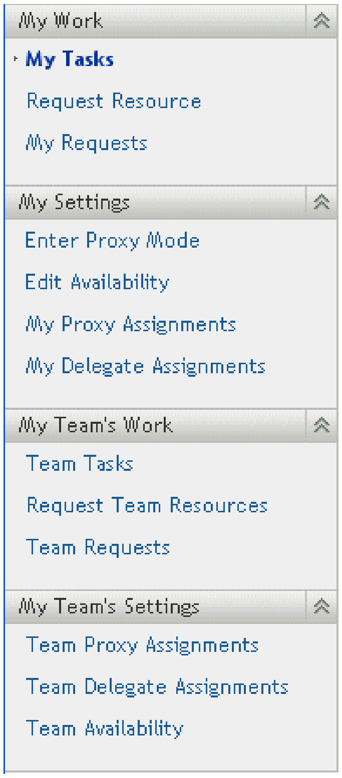
1 - 1 of 1

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

9.3 Exploring the Tab's Features

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

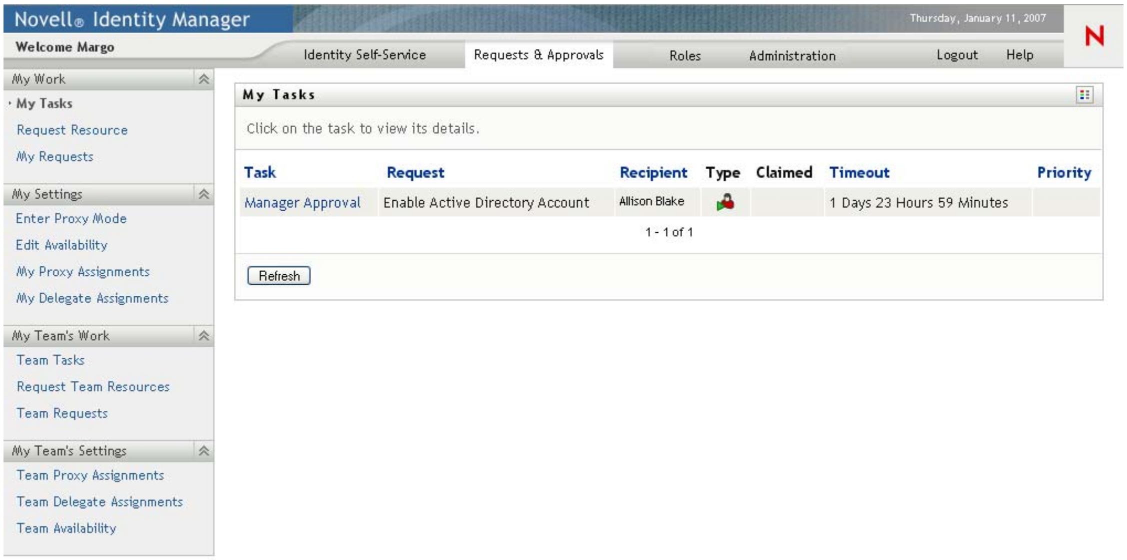
The left side of the *Requests & Approvals* tab displays a menu of actions you can perform. The actions are listed by category (*My Work, My Settings, My Team's Work,* and *My Team's Settings*):



The *My Team’s Work* and *My Team’s Settings* actions are only displayed if you are a team manager.

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 9-1 *Page Displayed for an Action*



Click on the task to view its details.

Task	Request	Recipient	Type	Claimed	Timeout	Priority
Manager Approval	Enable Active Directory Account	Allison Blake			1 Days 23 Hours 59 Minutes	

1 - 1 of 1

Most pages you work with on the *Requests & Approvals* tab include a button in the upper right corner that lets you display the *Requests & Approvals* legend:

▦

For details on the *Requests & Approvals* legend, see Section 9.5, “Understanding the Requests & Approvals Legend,” on page 115.

9.4 Requests & Approvals Actions You Can Perform

Here’s a summary of the actions that are available to you by default on the *Requests & Approvals* tab:

Table 9-1 Requests & Approvals Actions

Category	Action	Description
My Work	My Tasks	Displays the approval tasks currently assigned to you in your workflow queue. These tasks might be associated with resource requests, as well as role and attestation requests. If a task requires a digital signature, the My Tasks action provides a way to approve or disapprove the task with a digital signature. **WARNING:** You must use Novell Audit (or Sentinel) to preserve documents that you digitally sign. Digital signature documents are not stored with workflow data in the User Application database, but are stored in the logging database. You must enable logging to preserve these documents. If a task is assigned to multiple addressees, the My Tasks action provides a way to see the approval requirements for the task, as well as the list of addressees and the approval status. For details, see Chapter 10, "Managing Your Work," on page 119.
	Request Resource	Lets you make a request for a resource. If a resource requires a digital signature, the Request Resource action provides a way to associate a digital signature with the request. For details, see Chapter 10, "Managing Your Work," on page 119.
	My Requests	Displays the status of the requests made by or for you. The list of requests therefore includes those for which you are the initiator or the recipient for a request that authorizes view privileges for recipients. For details, see Chapter 10, "Managing Your Work," on page 119.

Category	Action	Description
My Settings	Enter Proxy Mode	Lets you act as a proxy for another user. For details, see Chapter 11, "Configuring Your Provisioning Settings," on page 141.
	Edit Availability	Lets you specify which requests you are available to act on, and which requests your assigned delegates can act on. For details, see Chapter 11, "Configuring Your Provisioning Settings," on page 141.
	My Proxy Assignments	Lets you view or edit your proxy assignments. To edit proxy assignments, you must have the necessary authority. For details, see Chapter 11, "Configuring Your Provisioning Settings," on page 141.
	My Delegate Assignments	Lets you view or edit your delegate assignments. To edit delegate assignments, you must have the necessary authority. For details, see Chapter 11, "Configuring Your Provisioning Settings," on page 141.
My Team's Work	Team Tasks	Displays the approval tasks assigned to members of your team. Depending on the rights defined for the team, this action can also allow you to claim and/or reassign tasks. If a task requires a digital signature, the Team Tasks action provides a way to approve or disapprove the task with a digital signature. If a task is assigned to multiple addressees, the Team Tasks action provides a way to see the approval requirements for the task, as well as the list of addressees. For details, see Chapter 12, "Managing Your Team's Work," on page 157.
	Request Team Resource	Lets you make a request for a resource for a member of your team. If a resource requires a digital signature, the Request Team Resource action provides a way to associate a digital signature with the request. For details, see Chapter 12, "Managing Your Team's Work," on page 157.
	Team Requests	Displays the status of requests made by or for members of your team. For details, see Chapter 12, "Managing Your Team's Work," on page 157.

Category	Action	Description
My Team’s Settings	Team Proxy Assignments	Lets you specify proxy assignments for members of your team. This capability must be enabled in the team definition. When this capability is disabled, this action is not allowed. For details, see Chapter 13, “Configuring Your Team’s Provisioning Settings,” on page 185.
	Team Delegate Assignments	Lets you specify delegate assignments for members of your team. This capability must be enabled in the team rights definition. 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 capability is disabled in the team rights definition, this action is not allowed. For details, see Chapter 13, “Configuring Your Team’s Provisioning Settings,” on page 185.
	Team Availability	Lets you specify which requests your team members are available to act on, and which requests the team member’s delegates can act on. This capability must be enabled in the team definition. When this capability is disabled, this action is not allowed. For details, see Chapter 13, “Configuring Your Team’s Provisioning Settings,” on page 185.

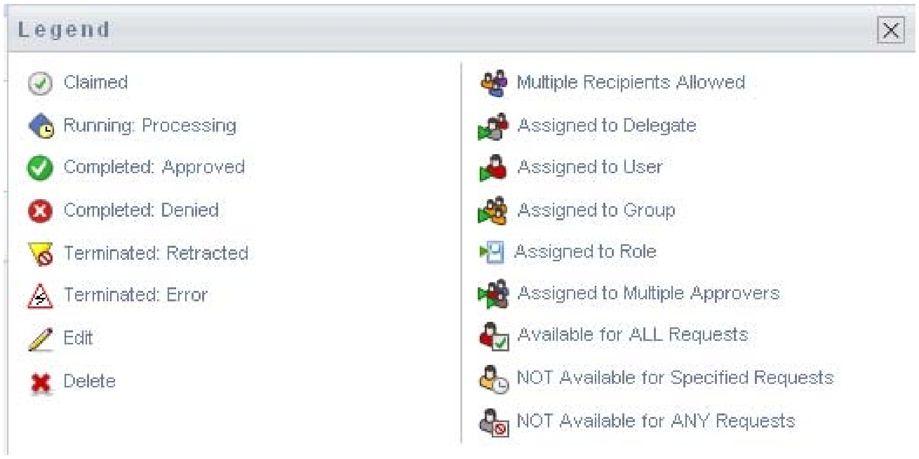
9.5 Understanding the Requests & Approvals Legend

Most pages you work with on the *Requests & Approvals* tab include a button in the upper right corner that lets you display the *Requests & Approvals* legend. To display the legend, click the Legend button, shown in Figure 9-2:

Figure 9-2 *The Legend Button*

The legend provides a brief description of the icons used throughout the *Requests & Approvals* tab. Figure 9-3 on page 116 shows the legend.

Figure 9-3 *The Requests & Approvals Legend*



Legend

Claimed

Running: Processing

Completed: Approved

Completed: Denied

Terminated: Retracted

Terminated: Error

Edit

Delete

Multiple Recipients Allowed

Assigned to Delegate

Assigned to User

Assigned to Group

Assigned to Role

Assigned to Multiple Approvers

Available for ALL Requests

NOT Available for Specified Requests

NOT Available for ANY Requests

The table below provides detailed descriptions of the icons in the legend:

Table 9-2 *Legend Icons*

Icon	Description
Claimed	Indicates whether a particular workflow task has been claimed by a user. Appears on the My Tasks page.
Running: Processing	Indicates that a particular request is still in process. Appears on the My Requests and Team Requests pages.
Completed: Approved	Indicates that a particular request has completed its processing and has been approved. Appears on the My Requests and Team Requests pages.
Completed: Denied	Indicates that a particular request has completed its processing and has been denied. Appears on the My Requests and Team Requests pages.
Terminated: Retracted	Indicates that a particular request was retracted by a user (either the user who submitted the request, a team manager, or the Provisioning Application Administrator). Appears on the My Requests and Team Requests pages.
Terminated: Error	Indicates that a particular request was terminated because of an error. Appears on the My Requests and Team Requests pages.
Edit	Lets you edit a proxy or delegate assignment. To edit the assignment, select it and click the *Edit* icon. Appears on the My Proxy Assignments, My Delegate Assignments, Team Proxy Assignments, Team Delegate Assignments, Edit Availability, and Team Availability pages.

Icon	Description
Delete	Lets you delete a proxy or delegate assignment. To delete the assignment, select it and click the *Delete* icon. Appears on the My Proxy Assignments, My Delegate Assignments, Team Proxy Assignments, Team Delegate Assignments, Edit Availability, and Team Availability pages.
Multiple Recipients Allowed	Indicates that this resource provides support for multiple recipients. When a resource supports multiple recipients, the *Request Team Resources* action lets you select multiple users as recipients. Appears on the Request Team Resources page.
Assigned to Delegate	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. Appears on the My Tasks and Team Tasks pages.
Assigned to User	Indicates that a particular workflow task was assigned to a user. Appears on the My Tasks and Team Tasks pages.
Assigned to Group	Indicates that a particular workflow task was assigned to a group. Appears on the My Tasks and Team Tasks pages.
Assigned to Role	Indicates that a particular workflow task was assigned to a role. Appears on the My Tasks and Team Tasks pages.
Assigned to Multiple Approvers	Indicates that a particular workflow task was assigned to more than one user. This icon 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. When this approval is given, task execution is considered finished. ◆ 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. Appears on the My Tasks and Team Tasks pages.
Available for ALL Requests	Indicates that a particular user is available for all kinds of requests. This setting applies to delegation. Appears on the Edit Availability and Team Availability pages.

Icon	Description
NOT Available for Specified Requests	Indicates that a particular user is not available for certain kinds of 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. Appears on the Edit Availability and Team Availability pages.
NOT Available for ANY Requests	Indicates that a particular user is not available for any 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. Appears on the Edit Availability and Team Availability pages.

Managing Your Work 10

This section provides instructions for managing your provisioning work. Topics include:

10.1 About the My Work Actions

The *Requests & Approvals* tab in the Identity Manager User Application includes a group of actions called *My Work*. The *My Work* actions give you the ability to make resource requests, check the status of requests you've made, and perform tasks that have been assigned to you or to a group to which you belong. These tasks might be associated with resource requests, as well as role and attestation requests.

The *My Work* actions also let you perform tasks as a delegate for another user. A delegated task appears in your queue when the original assignee for the task has declared himself or herself to be unavailable and has designated you as a delegate.

NOTE: The flow of control for a provisioning workflow, as well as the appearance of forms, can vary depending on how the provisioning request was defined in the Designer for Identity Manager. For details on customizing the design of a provisioning workflow, see the *Identity Manager User Application: Design Guide* (http://www.novell.com/documentation/idmrbpm361/index.html).

10.2 Managing Your Tasks

The *My Tasks* action lets you check your workflow queue for tasks that have been assigned to you. 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

NOTE: You must have the appropriate authority to reassign tasks. To reassign a task, you must be a Provisioning Application Administrator or a Team Manager who has been given this permission in the team rights definition.

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

When you claim a task associated with a resource request or role 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.

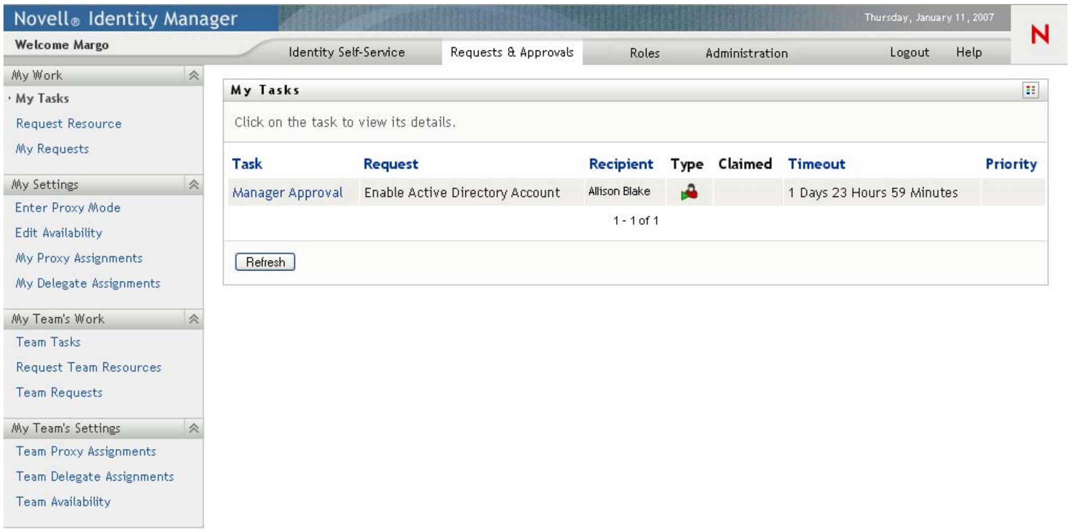
When you claim a task associated with an attestation request, you need to review the information displayed in the attestation form. In addition, you need to answer the required attestation question, which indicates whether you attest to the correctness of the data, and, in some cases, respond to one 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.

10.2.1 Viewing Your Tasks

To see the tasks that have been assigned to you:

1 Click *My Tasks* in the *My Work* group of actions.

The list of tasks in your queue is displayed.



Click on the task to view its details.

Task	Request	Recipient	Type	Claimed	Timeout	Priority
Manager Approval	Enable Active Directory Account	Allison Blake			1 Days 23 Hours 59 Minutes	

1 - 1 of 1

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, which is the same as the name of the individual currently logged on to the User Application.

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:

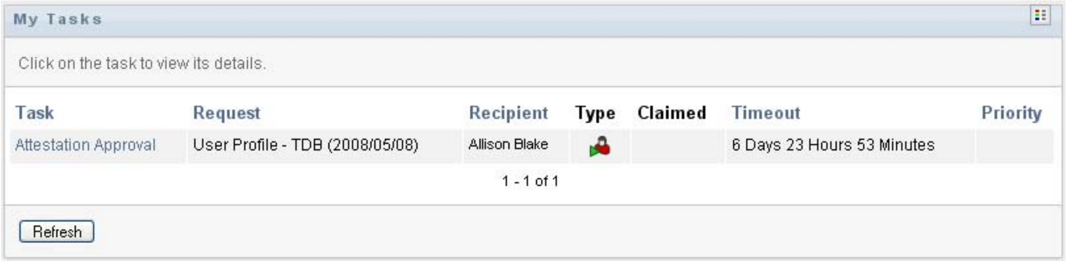
- The task has been assigned to a group of addressees, but only one addressee can claim and approve the task. After this approval is given, task execution is considered complete.
- The task has been assigned to multiple addressees, and all of them must claim and approve the task before the activity can 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*, as shown below:

Figure 10-1 *Workflow Task for an Attestation Request*



My Tasks

Click on the task to view its details.

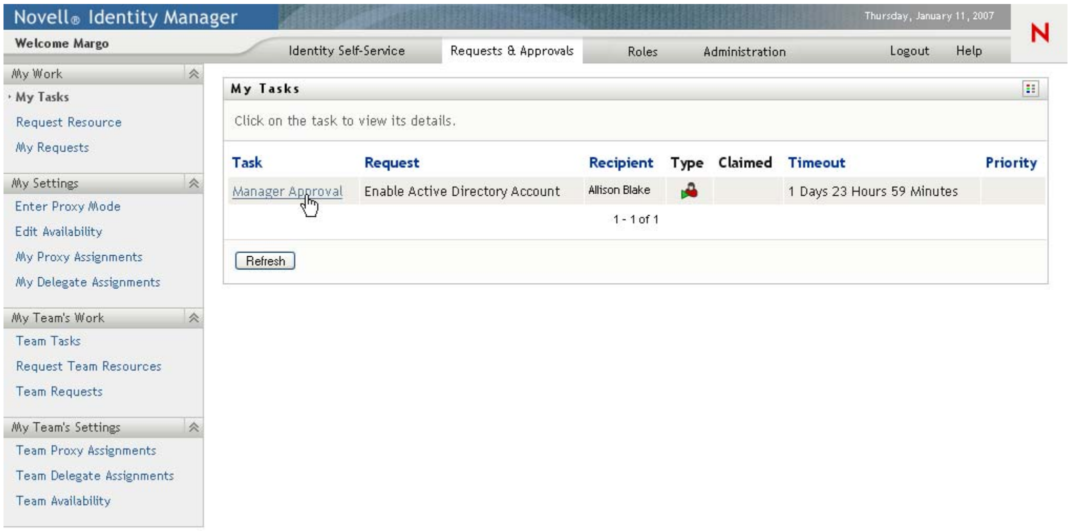
Task	Request	Recipient	Type	Claimed	Timeout	Priority
Attestation Approval	User Profile - TDB (2008/05/08)	Allison Blake			6 Days 23 Hours 53 Minutes	

1 - 1 of 1

10.2.2 Selecting a Task

To select a task in the queue list:

1 Click the name of the task in the queue.



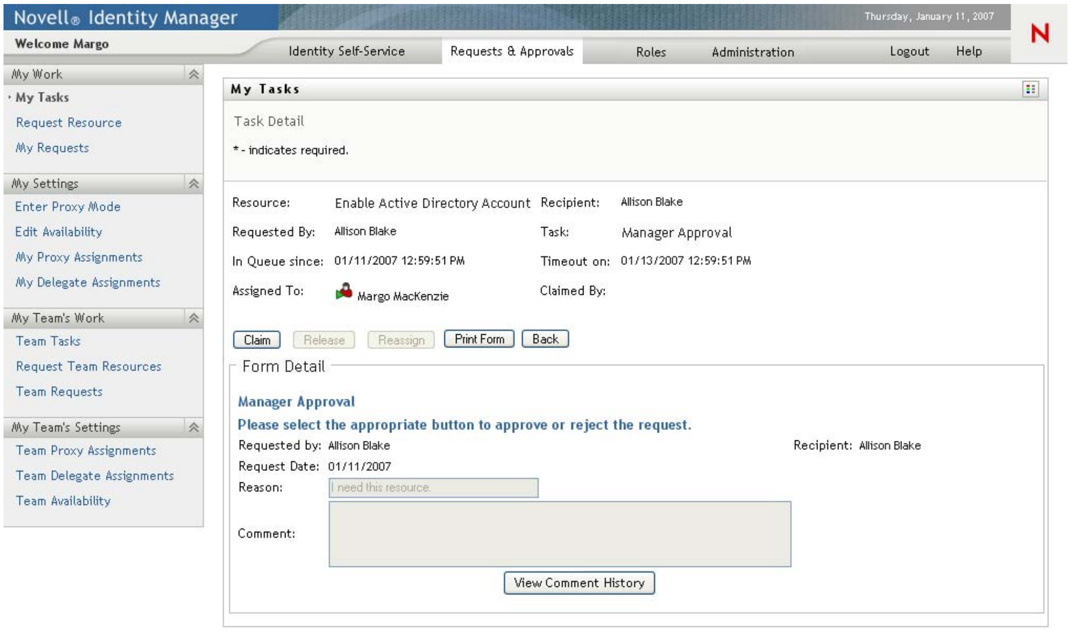
My Tasks

Click on the task to view its details.

Task	Request	Recipient	Type	Claimed	Timeout	Priority
Manager Approval	Enable Active Directory Account	Allison Blake			1 Days 23 Hours 59 Minutes	

1 - 1 of 1

The Task Detail form is displayed.



My Tasks

Task Detail

* - indicates required.

Resource: Enable Active Directory Account
Recipient: Allison Blake
Requested By: Allison Blake
Task: Manager Approval
In Queue since: 01/11/2007 12:59:51 PM
Timeout on: 01/13/2007 12:59:51 PM
Assigned To: Margo MacKenzie
Claimed By:

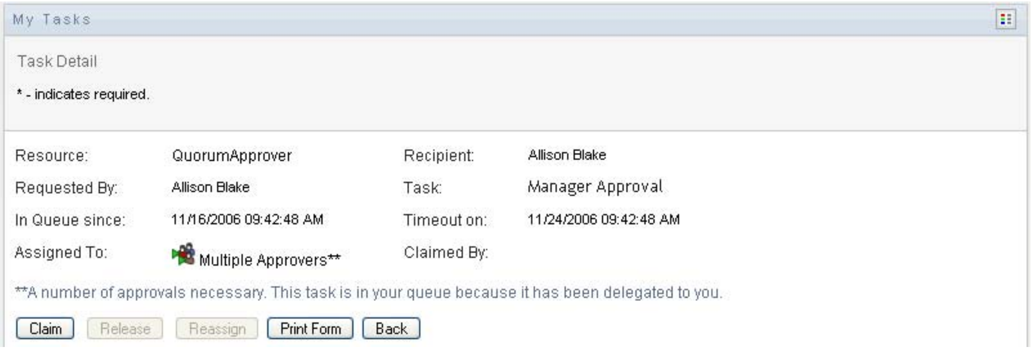
Form Detail

Manager Approval

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

Requested by: Allison Blake
Recipient: Allison Blake
Request Date: 01/11/2007
Reason: I need this resource.
Comment:

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.



My Tasks

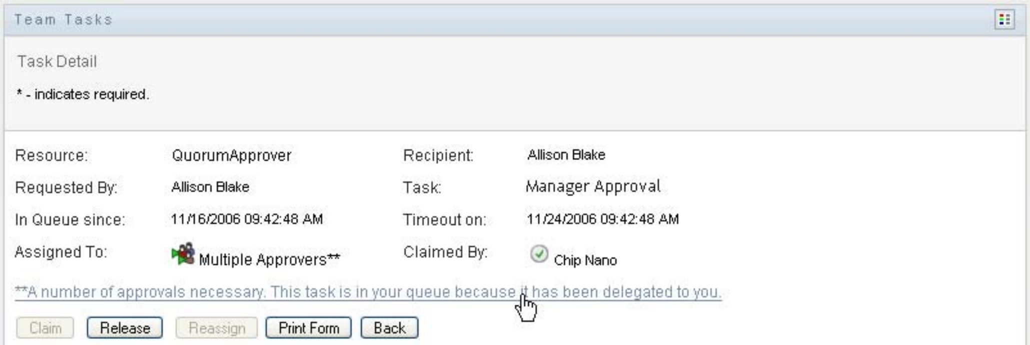
Task Detail

* - indicates required.

Resource:	QuorumApprover	Recipient:	Allison Blake
Requested By:	Allison Blake	Task:	Manager Approval
In Queue since:	11/16/2006 09:42:48 AM	Timeout on:	11/24/2006 09:42:48 AM
Assigned To:	Multiple Approvers**	Claimed By:	

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

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



Team Tasks

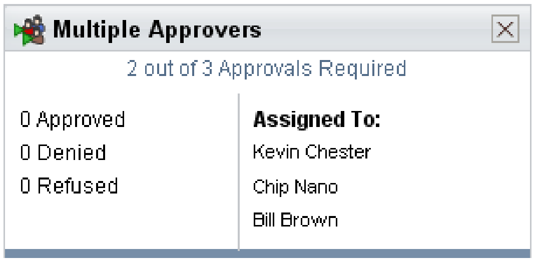
Task Detail

* - indicates required.

Resource:	QuorumApprover	Recipient:	Allison Blake
Requested By:	Allison Blake	Task:	Manager Approval
In Queue since:	11/16/2006 09:42:48 AM	Timeout on:	11/24/2006 09:42:48 AM
Assigned To:	Multiple Approvers**	Claimed By:	Chip Nano

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

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



Multiple Approvers

2 out of 3 Approvals Required

0 Approved	**Assigned To:**
0 Denied	Kevin Chester
0 Refused	Chip Nano
	Bill Brown

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.

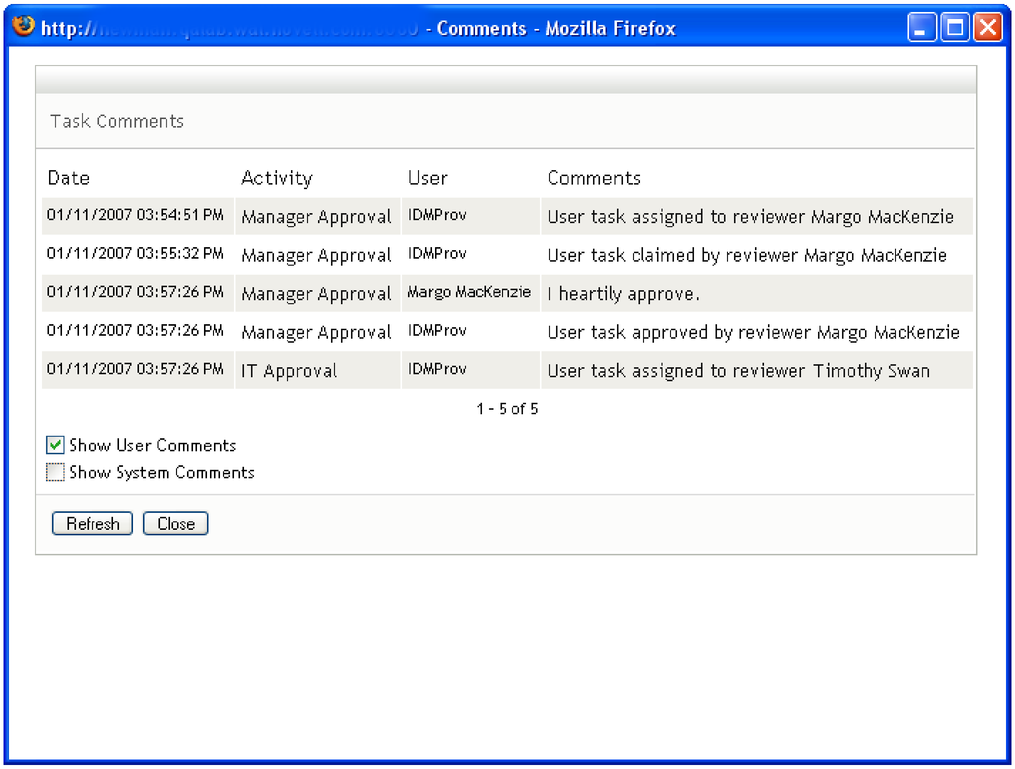
The workflow system performs *short circuit evaluation* to optimize quorums. Whenever a quorum approval condition reaches the point where a quorum is not possible, the activity is denied and the task is removed from the queues of all addressees.

3 To claim a task, follow the instructions under Section 10.2.3, "Claiming a Task," on page 126.

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 To display user comments, click *Show User Comments*.



Task Comments

Date	Activity	User	Comments
01/11/2007 03:54:51 PM	Manager Approval	IDMProv	User task assigned to reviewer Margo MacKenzie
01/11/2007 03:55:32 PM	Manager Approval	IDMProv	User task claimed by reviewer Margo MacKenzie
01/11/2007 03:57:26 PM	Manager Approval	Margo MacKenzie	I heartily approve.
01/11/2007 03:57:26 PM	Manager Approval	IDMProv	User task approved by reviewer Margo MacKenzie
01/11/2007 03:57:26 PM	IT Approval	IDMProv	User task assigned to reviewer Timothy Swan

1 - 5 of 5

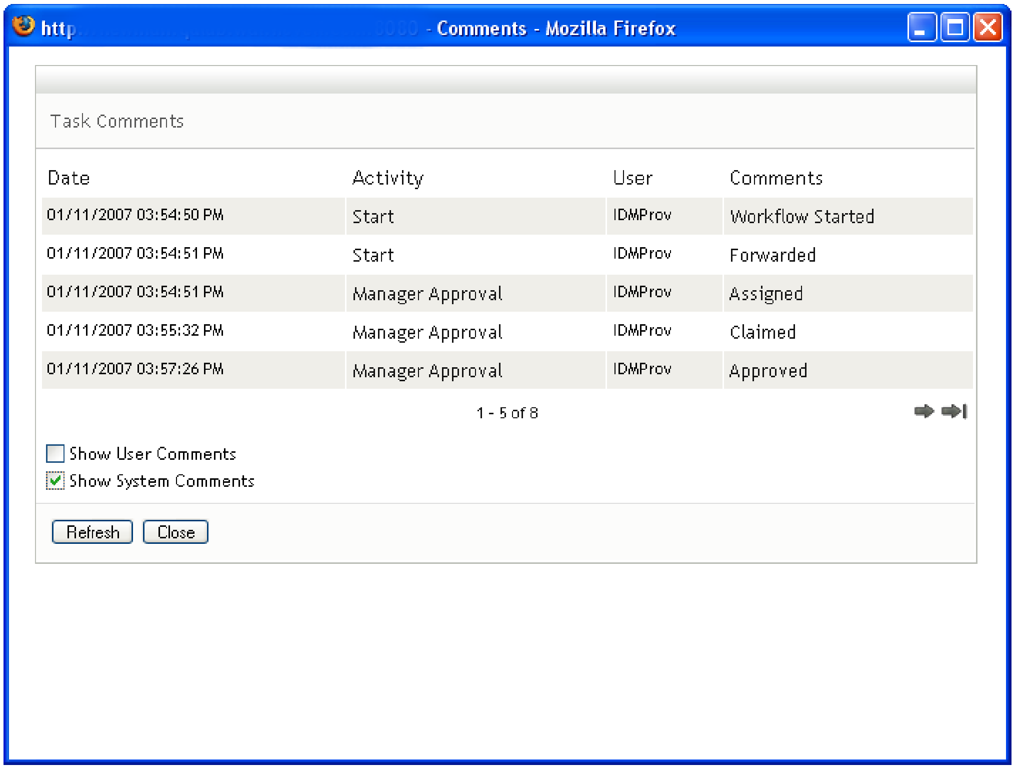
☑ Show User Comments
☐ Show System Comments

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.novell.com/documentation/idmrbpm361/index.html)

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



Task Comments

Date	Activity	User	Comments
01/11/2007 03:54:50 PM	Start	IDMProv	Workflow Started
01/11/2007 03:54:51 PM	Start	IDMProv	Forwarded
01/11/2007 03:54:51 PM	Manager Approval	IDMProv	Assigned
01/11/2007 03:55:32 PM	Manager Approval	IDMProv	Claimed
01/11/2007 03:57:26 PM	Manager Approval	IDMProv	Approved

1 - 5 of 8

□ Show User Comments
☑ Show System Comments

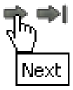
Refresh Close

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, `IDMProv`) 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.

4c 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.



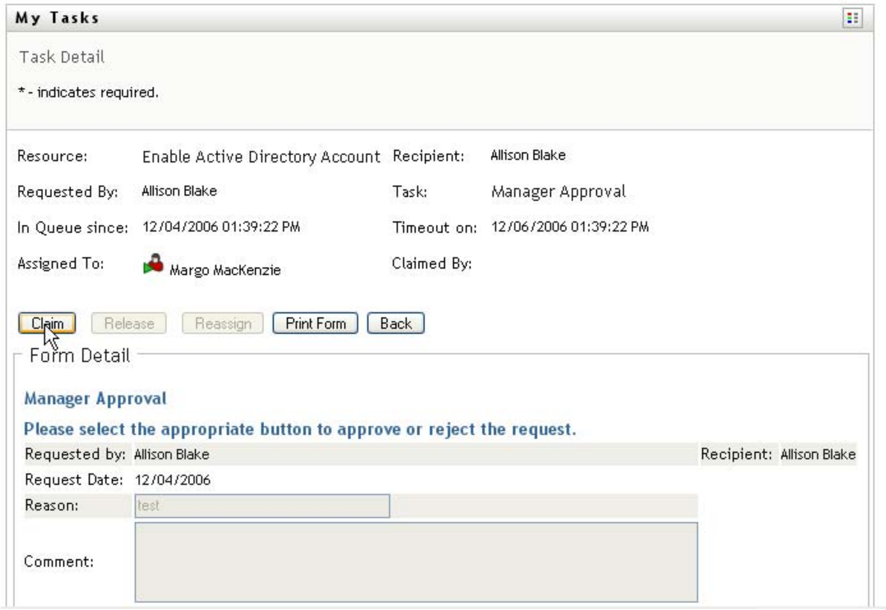
4d Click *Close* to close the window.

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

10.2.3 Claiming a Task

To claim a task to work on:

1 Click *Claim*.



My Tasks

Task Detail

* - indicates required.

Resource:	Enable Active Directory Account	Recipient:	Allison Blake
Requested By:	Allison Blake	Task:	Manager Approval
In Queue since:	12/04/2006 01:39:22 PM	Timeout on:	12/06/2006 01:39:22 PM
Assigned To:	Margo MacKenzie	Claimed By:	

Form Detail

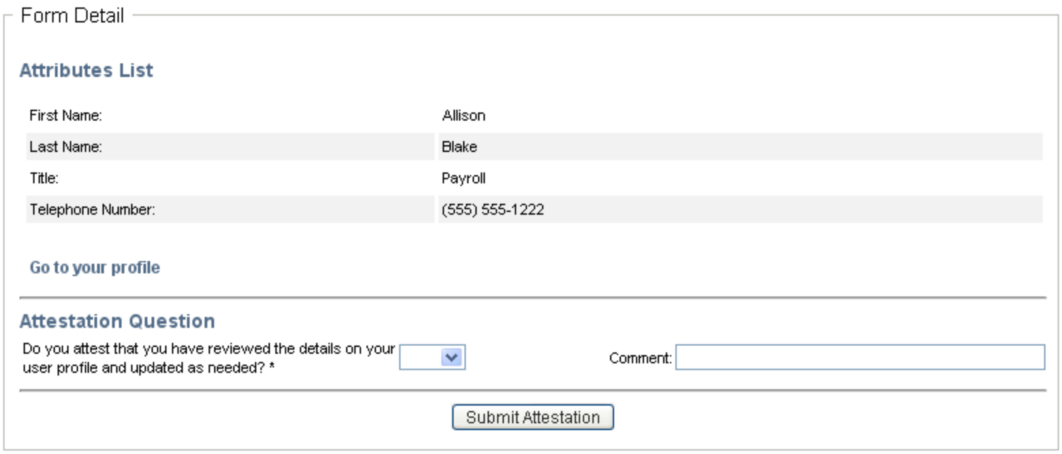
Manager Approval

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:			

For resource requests and role 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

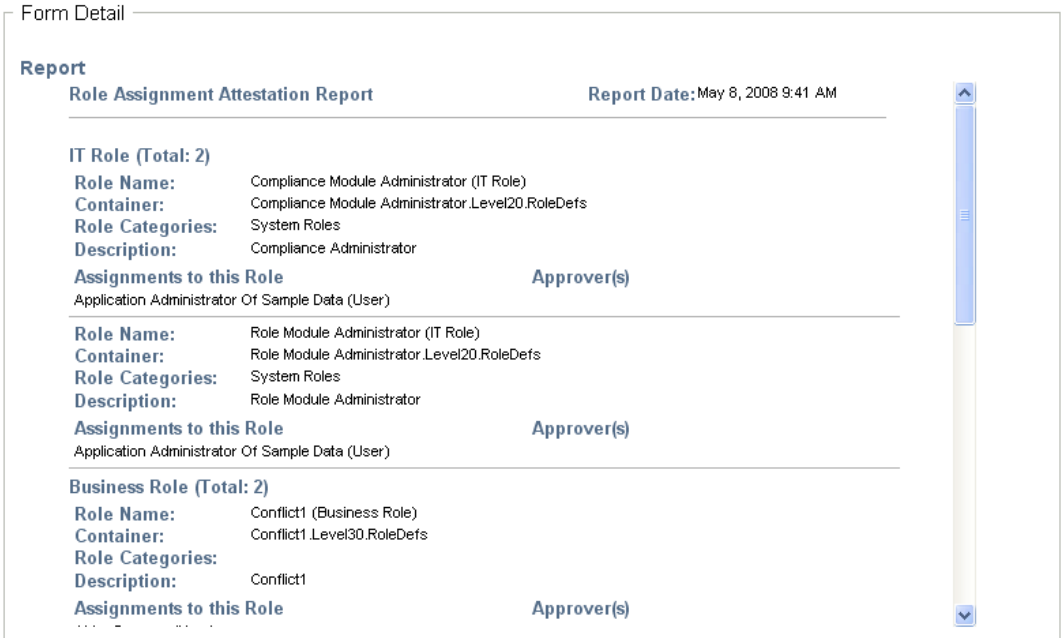
Go to your profile

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

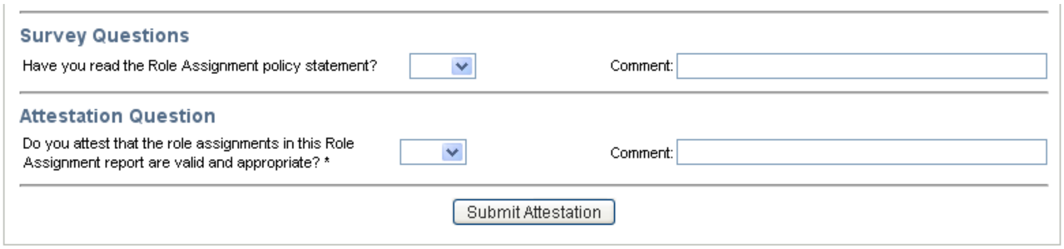
Assignments to this Role **Approver(s)**
Application Administrator Of Sample Data (User)

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

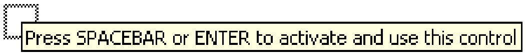
Have you read the Role Assignment policy statement? Comment:

Attestation Question

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

In the case of a resource request, if 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.



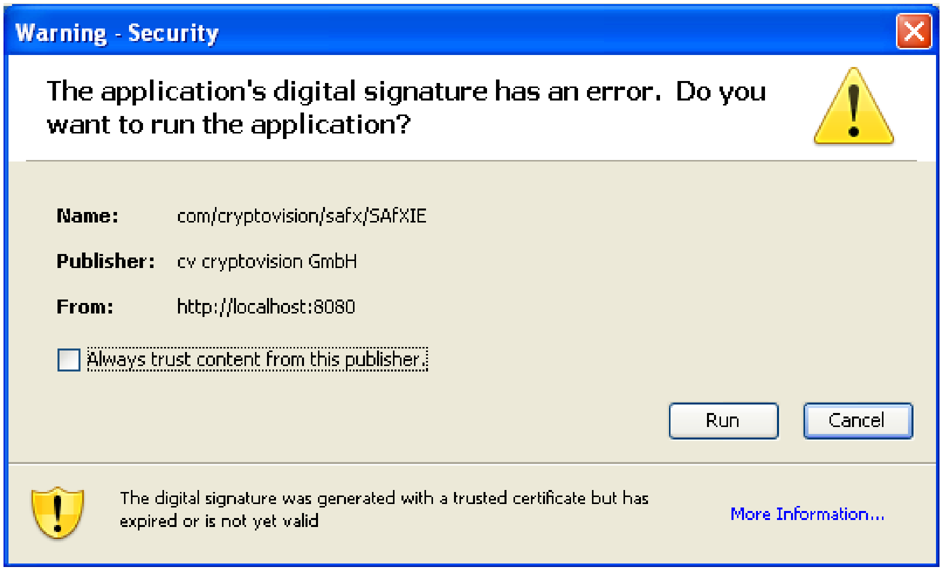
Press SPACEBAR or ENTER to activate and use this control

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.



Warning - Security

The application's digital signature has an error. Do you want to run the application?

Name: com/cryptovision/safx/SAfXIE

Publisher: cv cryptovision GmbH

From: http://localhost:8080

□ Always trust content from this publisher.

The digital signature was generated with a trusted certificate but has expired or is not yet valid

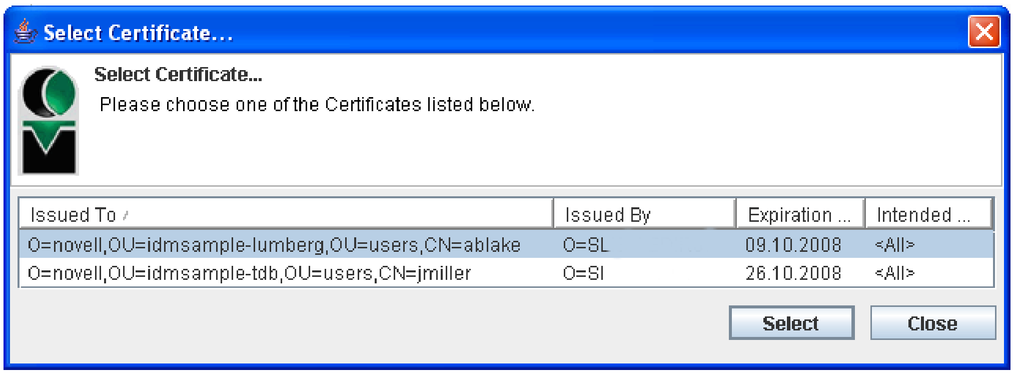
2c Click *Run* to proceed.

2d Fill in the fields in the approval form. The fields on the form vary depending on which resource you requested.

2e Click the 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).



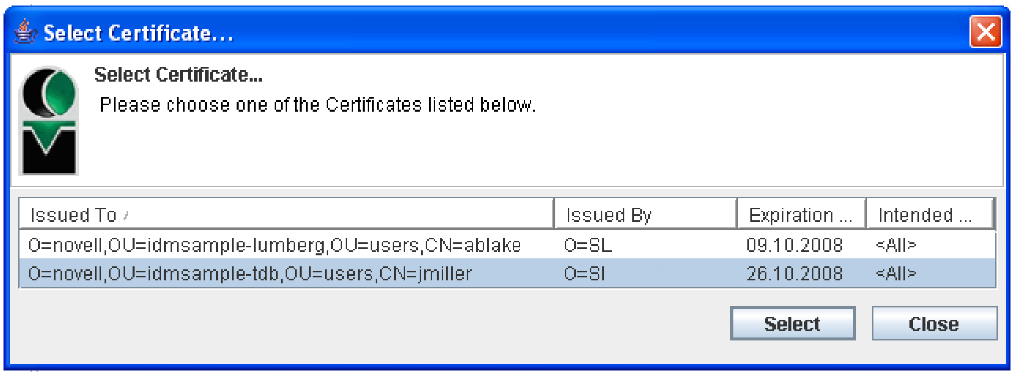
Select Certificate...

Select Certificate...

Please choose one of the Certificates listed below.

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*.



Select Certificate...

Select Certificate...

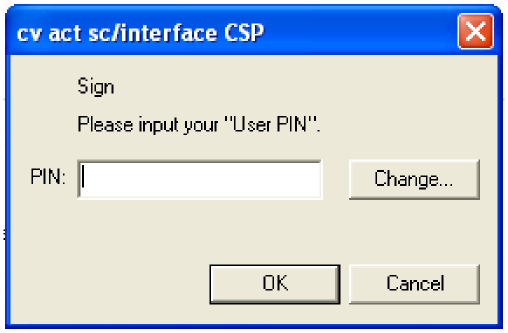
Please choose one of the Certificates listed below.

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>

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.



cv act sc/interface CSP

Sign

Please input your "User PIN".

PIN:

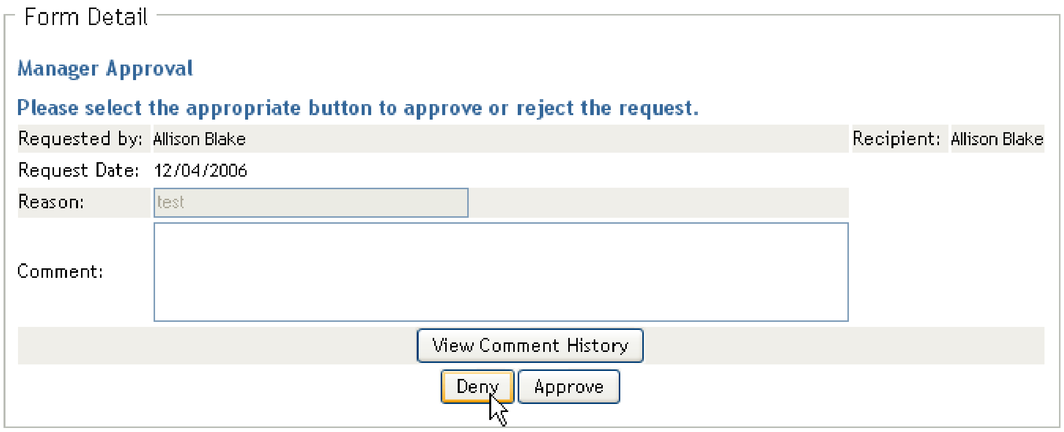
If your administrator has enabled the ability to preview the user agreement, the *Preview* button is enabled.

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

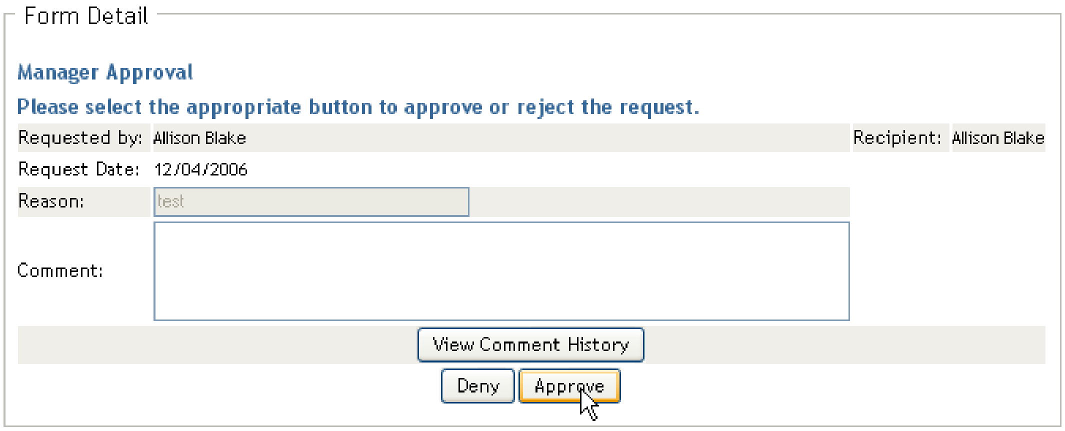
Recipient: Allison Blake

Request Date: 12/04/2006

Reason: test

Comment:

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:

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

10.3 Requesting a Resource

The *Request Resource* action allows you to make a resource request. 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.

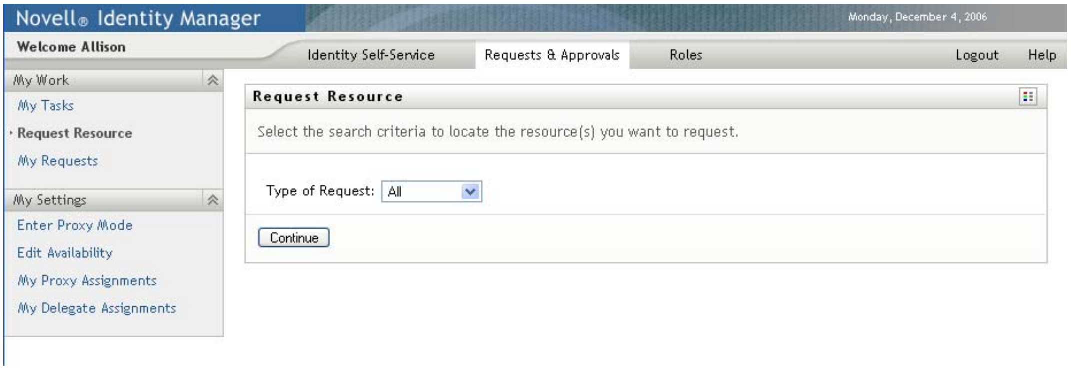
NOTE: The *Request Resource* action does not allow you to request role assignments or launch attestation requests. To request role assignments, you need to use the *Role Assignments* action on the *Roles* tab. To launch an attestation request, you need to use any of the actions listed under *Attestation Requests* on the *Compliance* tab.

When a resource request is submitted, the request starts a workflow. The workflow coordinates the approvals needed to fulfill the request. Some resource requests require approval from a single individual; others require approval from several individuals. In some instances, a request can be fulfilled without any approvals.

To request a resource:

1 Click *Request Resource* in the *My Work* group of actions.

The Request Resource page is displayed.



Request Resource

Select the search criteria to locate the resource(s) you want to request.

Type of Request: All

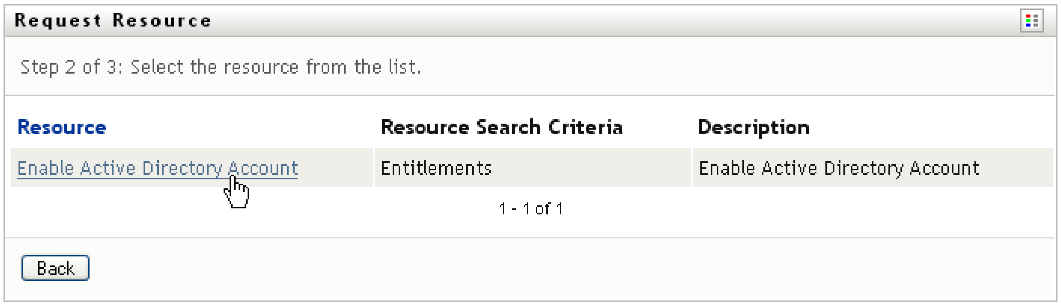
2 Select the category of the request in the *Type of Request* drop-down list. Select *All* to include requests from all available categories.

3 Click *Continue*.

The Request Resource page displays a list of resources 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 resource by clicking the resource name.



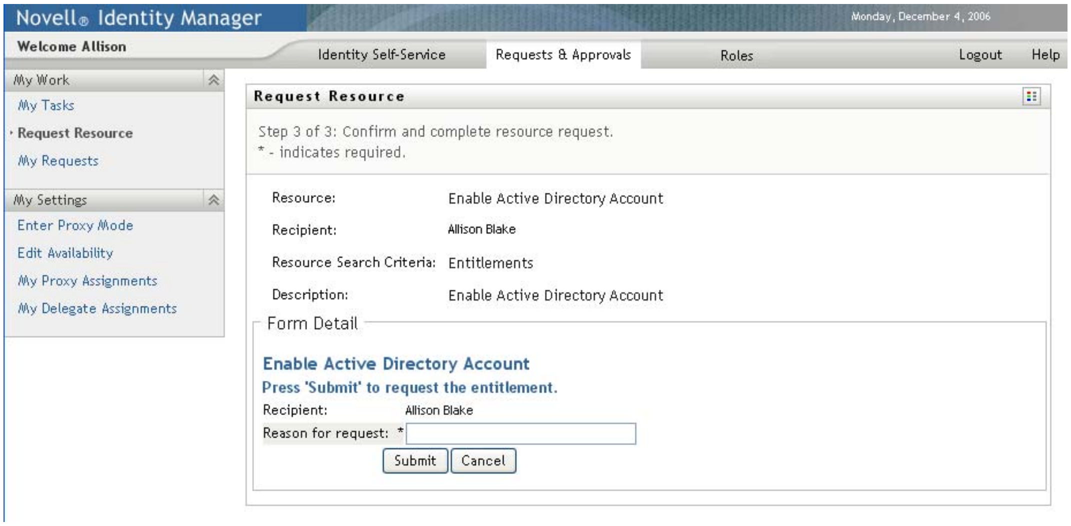
Request Resource

Step 2 of 3: Select the resource from the list.

Resource	Resource Search Criteria	Description
Enable Active Directory Account	Entitlements	Enable Active Directory Account

1 - 1 of 1

The Request Resource page displays the initial request form.



Request Resource

Step 3 of 3: Confirm and complete resource request.
* - indicates required.

Resource: Enable Active Directory Account

Recipient: Allison Blake

Resource Search Criteria: Entitlements

Description: Enable Active Directory Account

Form Detail

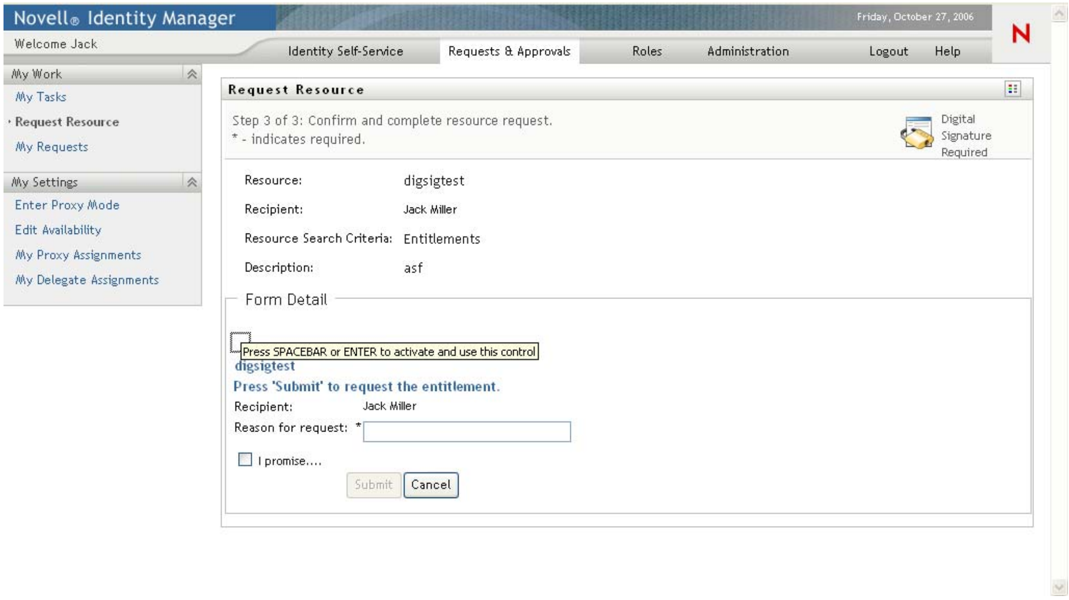
Enable Active Directory Account

Press 'Submit' to request the entitlement.

Recipient: Allison Blake

Reason for request: *

If the resource 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:



Step 3 of 3: Confirm and complete resource request.
* - indicates required.

Resource: digsigtest
Recipient: Jack Miller
Resource Search Criteria: Entitlements
Description: asf

Form Detail

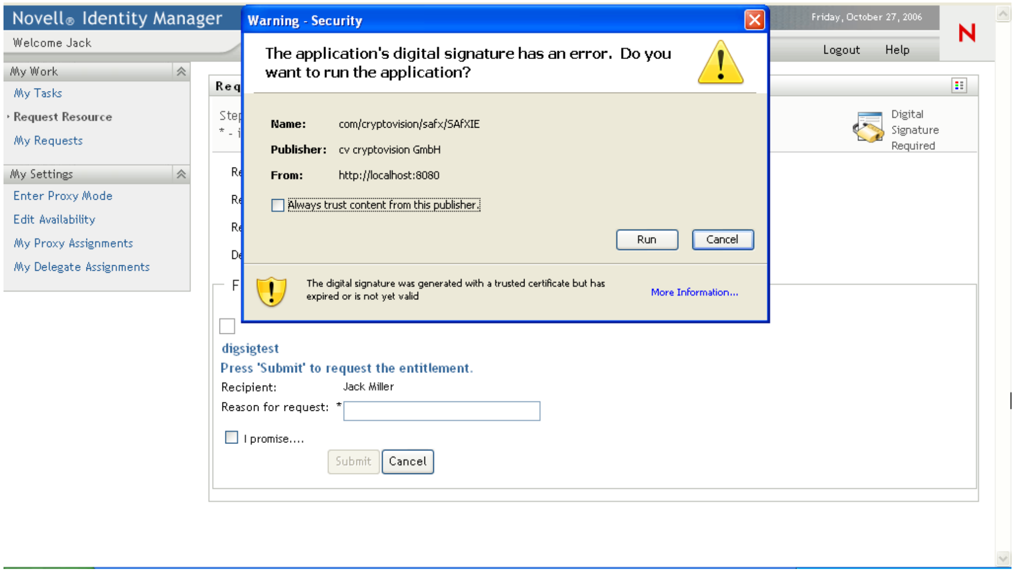
Press SPACEBAR or ENTER to activate and use this control
digsigtest
Press 'Submit' to request the entitlement.
Recipient: Jack Miller
Reason for request: *
□ I promise....

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.



The application's digital signature has an error. Do you want to run the application?

Name: com/cryptovision/safx/SAfXIE
Publisher: cv cryptovision GmbH
From: http://localhost:8080

□ Always trust content from this publisher.

The digital signature was generated with a trusted certificate but has expired or is not yet valid

digsigtest
Press 'Submit' to request the entitlement.
Recipient: Jack Miller
Reason for request: *
□ I promise....

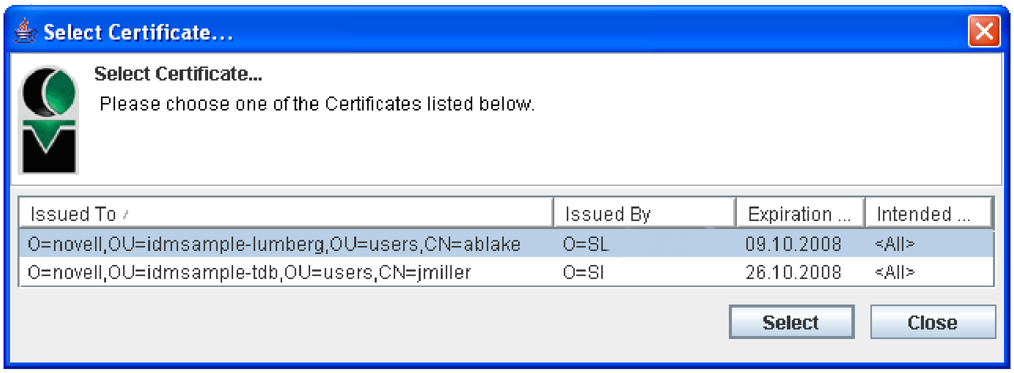
5c Click *Run* to proceed.

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).



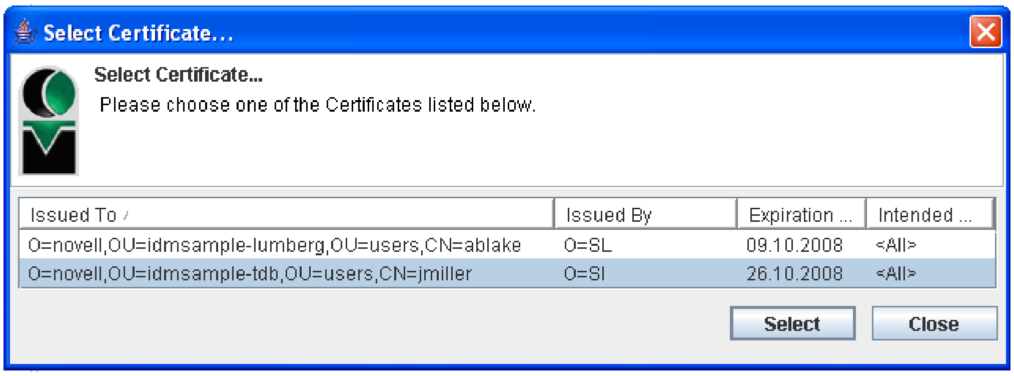
Select Certificate...

Select Certificate...

Please choose one of the Certificates listed below.

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*.



Select Certificate...

Select Certificate...

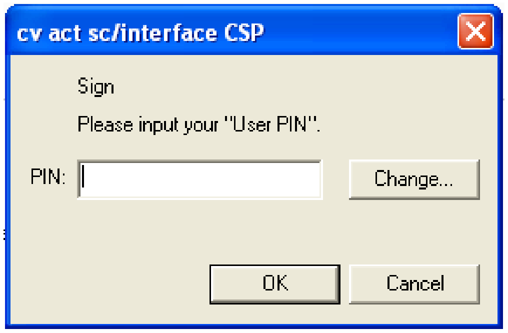
Please choose one of the Certificates listed below.

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>

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.

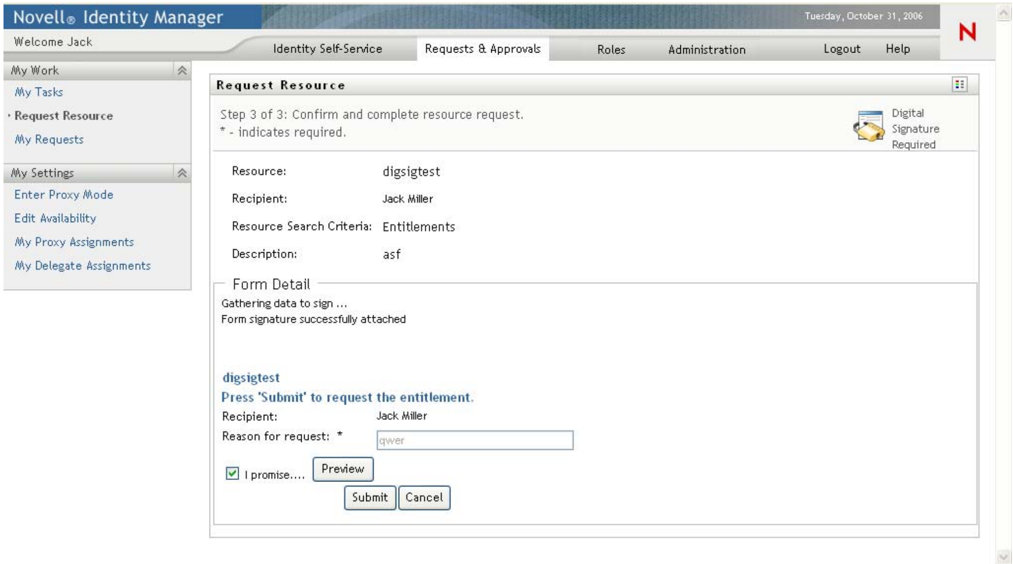


Sign

Please input your "User PIN".

PIN:

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



Request Resource

Step 3 of 3: Confirm and complete resource request.
* - indicates required.

Resource:	digsigtest
Recipient:	Jack Miller
Resource Search Criteria:	Entitlements
Description:	asf

Form Detail

Gathering data to sign ...
Form signature successfully attached

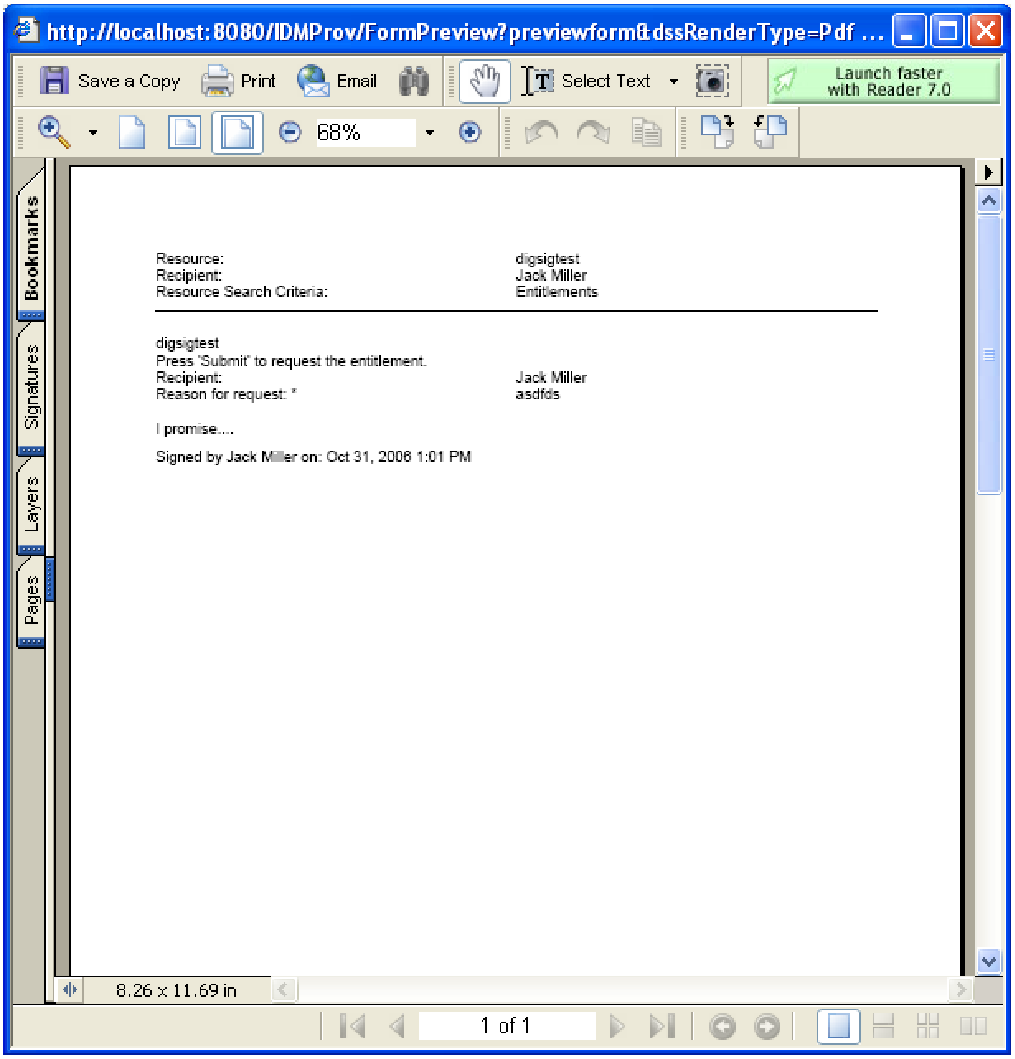
digsigtest
Press 'Submit' to request the entitlement.

Recipient: Jack Miller
Reason for request: * qwer

☑ I promise....

5i Click *Preview* to see the user agreement.

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


http://localhost:8080/IDMProv/FormPreview?previewform&dssRenderType=Pdf ...
Save a Copy
Print
Email
Select Text
Launch faster with Reader 7.0
68%
Bookmarks
Signatures
Layers
Pages
8.26 x 11.69 in
1 of 1

Resource:	digsigtest
Recipient:	Jack Miller
Resource Search Criteria:	Entitlements

digsigtest

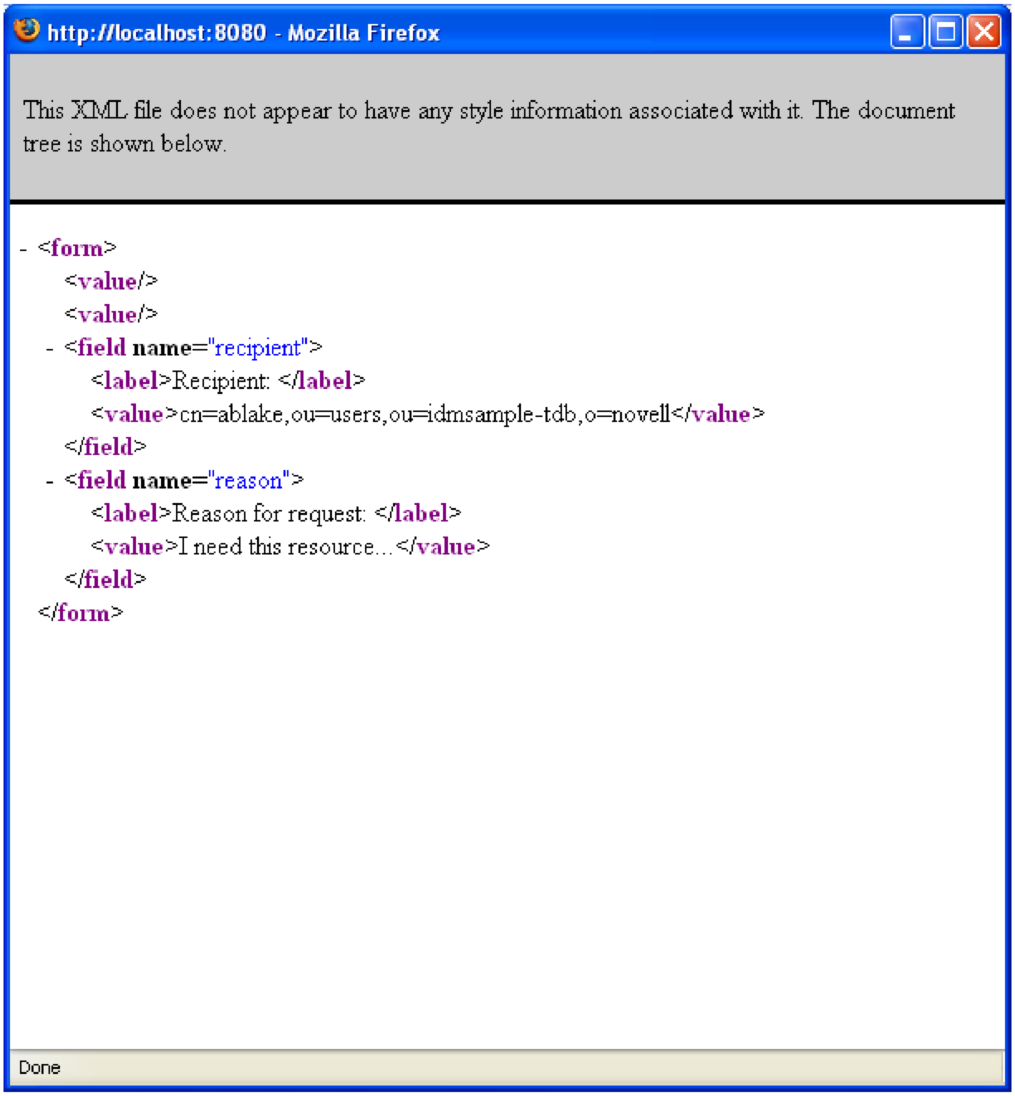
Press 'Submit' to request the entitlement.

Recipient:	Jack Miller
Reason for request: *	asdfds

I promise....

Signed by Jack Miller on: Oct 31, 2006 1:01 PM

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



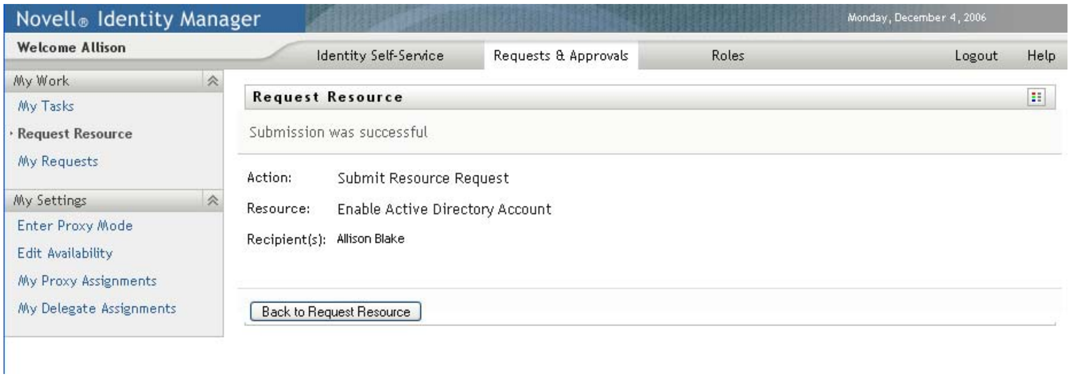
This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
- <form>
    <value/>
    <value/>
  - <field name="recipient">
      <label>Recipient: </label>
      <value>cn=ablake,ou=users,ou=idmsample-tdb,o=novell</value>
    </field>
  - <field name="reason">
      <label>Reason for request: </label>
      <value>I need this resource...</value>
    </field>
  </form>
```

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 Request Resource page displays a status message indicating whether the request was submitted successfully.



Submission was successful

Action: Submit Resource Request

Resource: Enable Active Directory Account

Recipient(s): Allison Blake

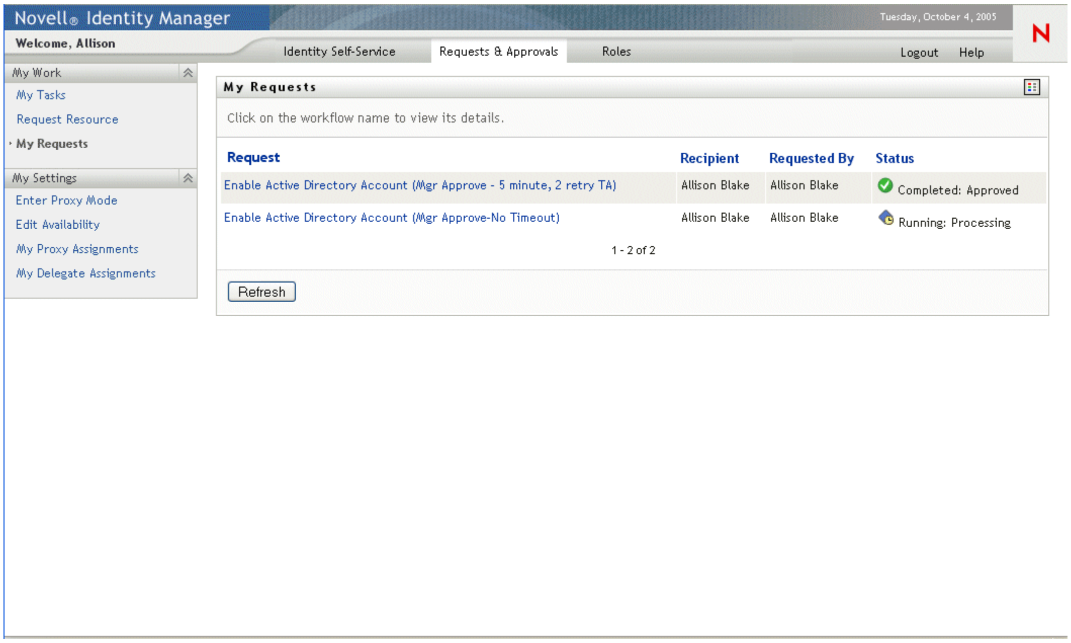
10.4 Checking the Status of Your Requests

The *My Requests* action allows you to see the status of the requests you've made. It lets you see the history and 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.

NOTE: The *My Requests* action does not display role or attestation requests. To see the status of a role request, you need to use the *View Request Status* action on the *Roles* tab. To see the status of an attestation request, you need to use the *View Attestation Request Status* action on the *Compliance* tab.

To view a list of your requests:

1 Click *My Requests* in the *My Work* group of actions.



Click on the workflow name to view its details.

Request	Recipient	Requested By	Status
Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	Allison Blake	Allison Blake	✓ Completed: Approved
Enable Active Directory Account (Mgr Approve-No Timeout)	Allison Blake	Allison Blake	Running: Processing

1 - 2 of 2

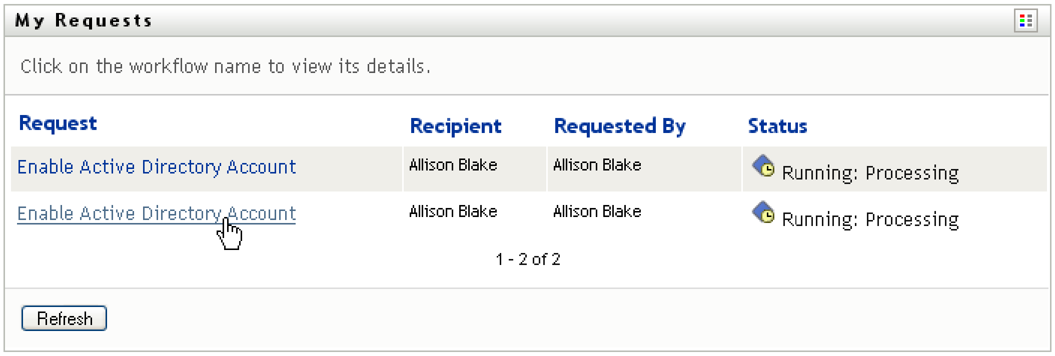
2 Select the category of the request in the *Type of Request* drop-down list. Select *All* to include requests from all available categories.

3 Optionally filter the list of requests by date by selecting *on*, *before*, or *after*, and filling in the *Request Date* field. To include all requests for the selected categories, leave the *Request Date* field blank.

4 Click *Continue*.

The Request Resource page displays your requests. 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.

5 To view details about a particular request, select the request by clicking the name:



My Requests

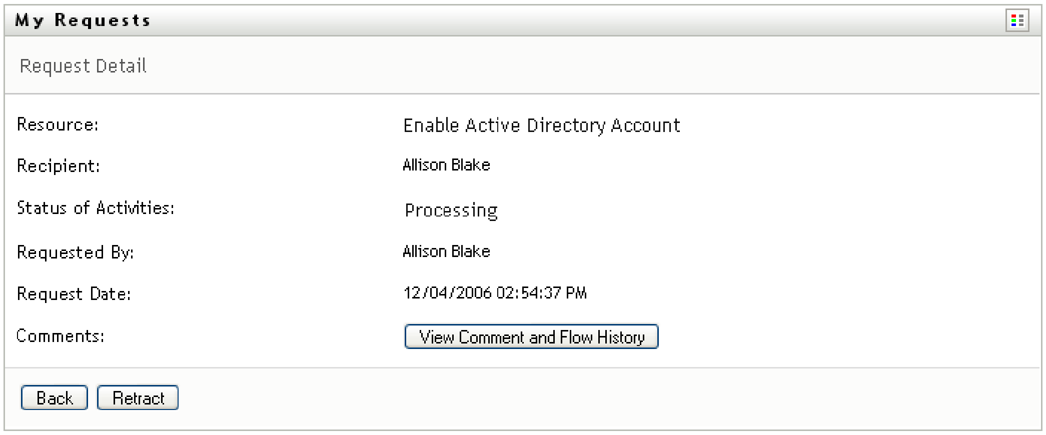
Click on the workflow name to view its details.

Request	Recipient	Requested By	Status
Enable Active Directory Account	Allison Blake	Allison Blake	Running: Processing
Enable Active Directory Account	Allison Blake	Allison Blake	Running: Processing

1 - 2 of 2

The My Requests page displays details such as when the request was initiated and what the current state of the workflow is.

You can review the status to determine whether a workflow is still running or has encountered an error. For example, if a request shows the *Running: Processing* status for an unusually long period of time, you might want to contact your administrator to be sure there is not a problem.



My Requests

Request Detail

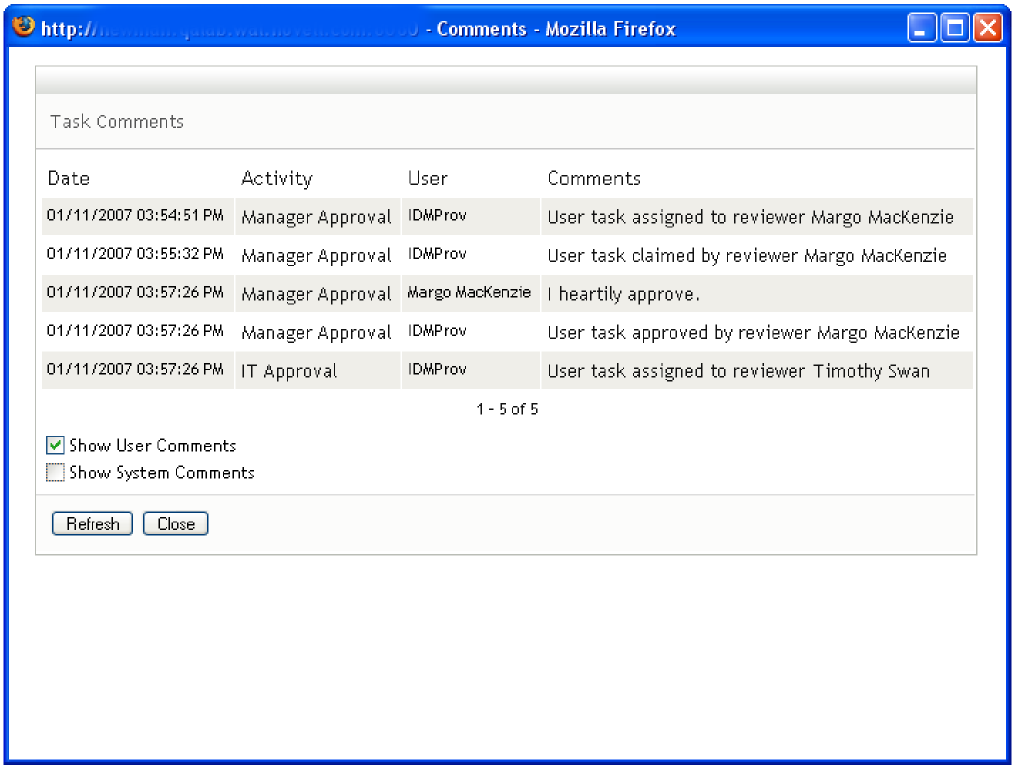
Resource:	Enable Active Directory Account
Recipient:	Allison Blake
Status of Activities:	Processing
Requested By:	Allison Blake
Request Date:	12/04/2006 02:54:37 PM
Comments:	View Comment and Flow History

6 To retract the request, click *Retract*.

7 To view comment history for the request, click *View Comment and Flow 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.

7a To display user comments, click *Show User Comments*.



Task Comments

Date	Activity	User	Comments
01/11/2007 03:54:51 PM	Manager Approval	IDMProv	User task assigned to reviewer Margo MacKenzie
01/11/2007 03:55:32 PM	Manager Approval	IDMProv	User task claimed by reviewer Margo MacKenzie
01/11/2007 03:57:26 PM	Manager Approval	Margo MacKenzie	I heartily approve.
01/11/2007 03:57:26 PM	Manager Approval	IDMProv	User task approved by reviewer Margo MacKenzie
01/11/2007 03:57:26 PM	IT Approval	IDMProv	User task assigned to reviewer Timothy Swan

1 - 5 of 5

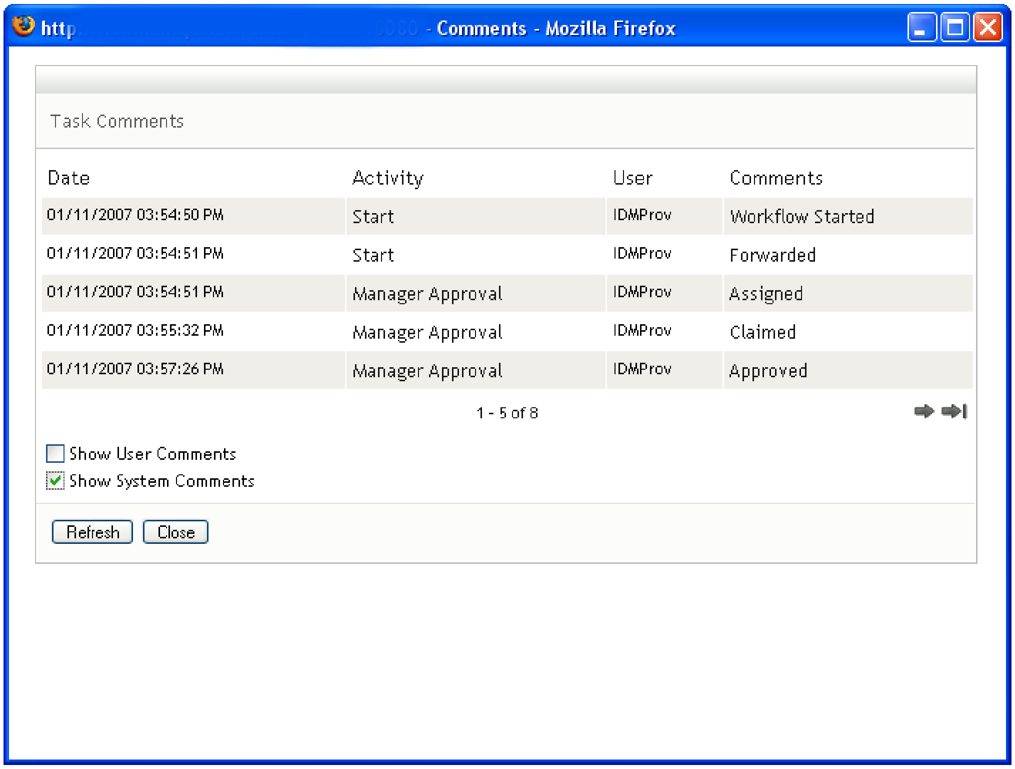
☑ Show User Comments
□ Show System Comments

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.novell.com/documentation/idmrbpm361/index.html)*.

7b To display system comments, click *Show System Comments*.



Task Comments

Date	Activity	User	Comments
01/11/2007 03:54:50 PM	Start	IDMProv	Workflow Started
01/11/2007 03:54:51 PM	Start	IDMProv	Forwarded
01/11/2007 03:54:51 PM	Manager Approval	IDMProv	Assigned
01/11/2007 03:55:32 PM	Manager Approval	IDMProv	Claimed
01/11/2007 03:57:26 PM	Manager Approval	IDMProv	Approved

1 - 5 of 8

□ Show User Comments

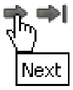
☑ Show System Comments

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, `IDMProv`) 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.

7c 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.



7d Click *Close* to close the window.

Configuring Your Provisioning Settings 11

This section provides instructions for configuring your provisioning settings. Topics include:

11.1 About the My Settings Actions

The *Requests & Approvals* tab in the Identity Manager User Application includes a group of actions called *My Settings*. The *My 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 team manager or Provisioning Application Administrator, you might also be permitted to define proxy and delegate assignments, as well as team availability settings.

11.1.1 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 resource 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 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 conflicts with the roles of the person for whom they will act as proxy.

11.1.2 Sample Usage Scenarios

This section describes two business scenarios where proxies and delegates might be used:

- "Proxy Usage Scenario" on page 142
- "Delegate Usage Scenario" on page 142

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

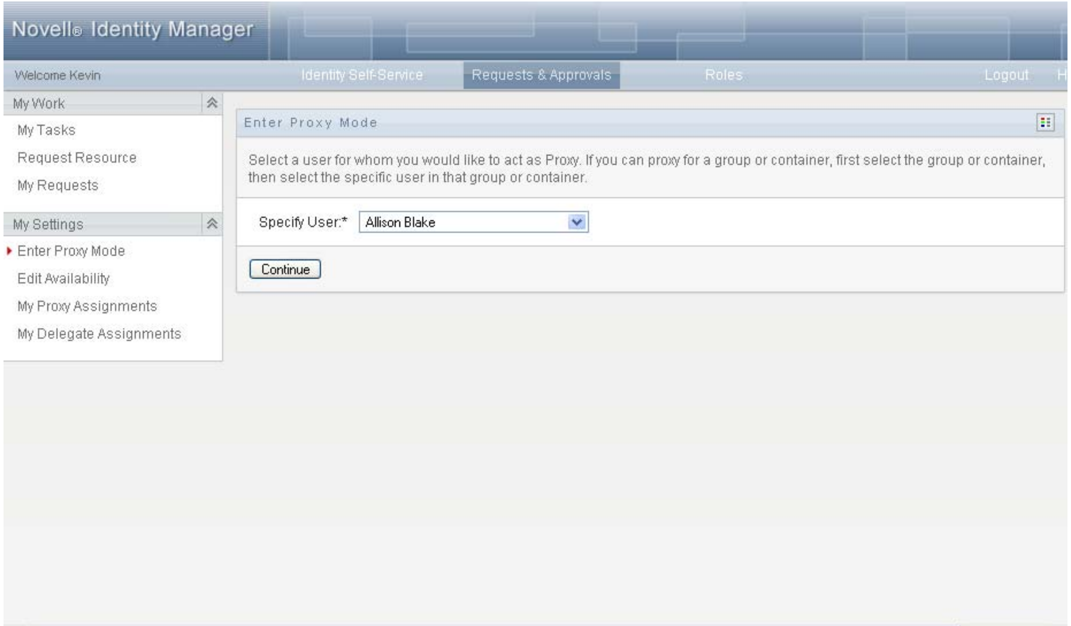
Suppose you are a manager who is responsible for approving or denying requests for ten different types of provisioned resources. All ten request types need regular attention, but you would rather have another individual in your organization attend to six of them. In this case, you could define a delegate for these six resource 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.

11.2 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 *My Settings* group of actions.

   If you are authorized to act as a proxy for at least one other user, the User Application displays a list of users.

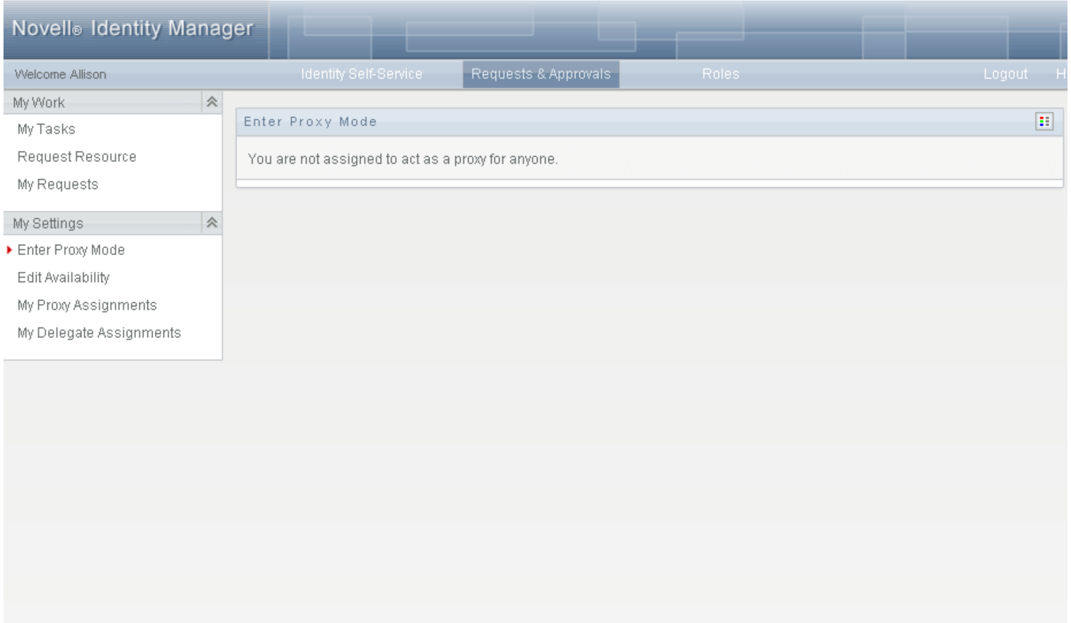


Enter Proxy Mode

Select a user for whom you would like to act as Proxy. If you can proxy for a group or container, first select the group or container, then select the specific user in that group or container.

Specify User:* Allison Blake

If you are not authorized to act as a proxy for any other user, the User Application displays this message:

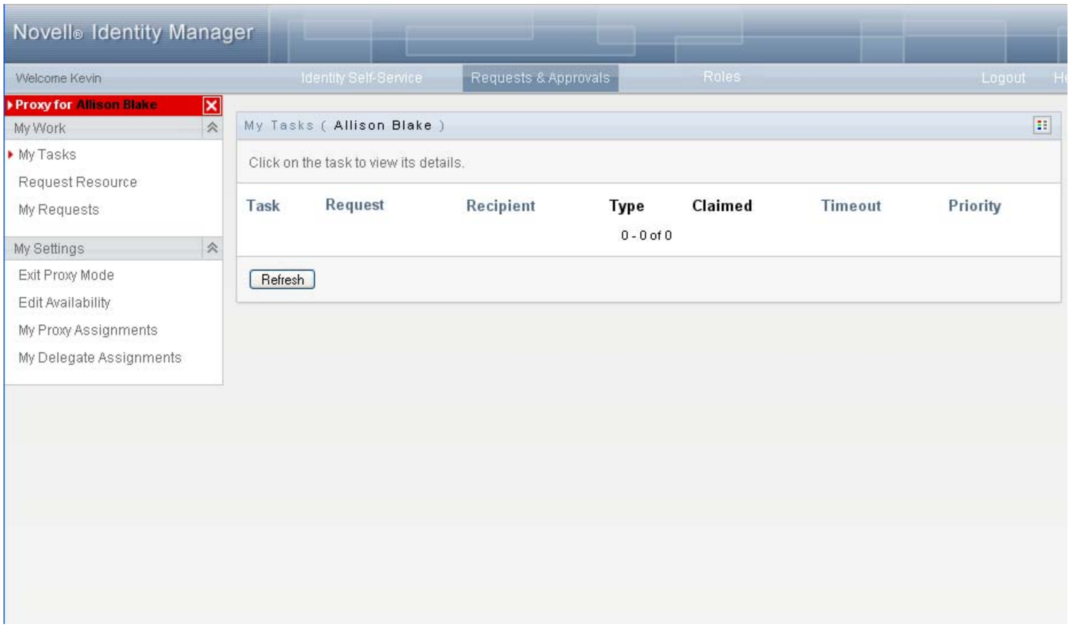


You are not assigned to act as a proxy for anyone.

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.



Click on the task to view its details.

Task	Request	Recipient	Type	Claimed	Timeout	Priority
			0 - 0 of 0			

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.

11.3 Specifying Your Availability

The *Edit Availability* action allows you to specify which 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 request definition individually, you can use the *Edit Availability* action to establish global settings pertaining to delegation.

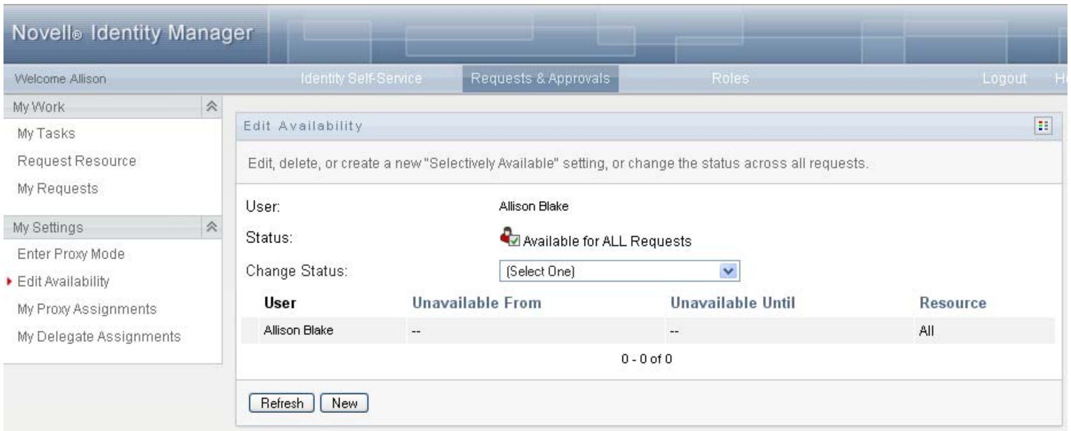
TIP: Before using the *Edit Availability* action, you need to have at least one delegate assignment to work on. You need to have your team manager (or the Provisioning Application Administrator) create delegate assignments for you.

- Section 11.3.1, "Setting Your Availability Status," on page 144
- Section 11.3.2, "Creating or Editing an Availability Setting," on page 146
- Section 11.3.3, "Deleting an Availability Setting," on page 149

11.3.1 Setting Your Availability Status

1 Click *Edit Availability* in the *My 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

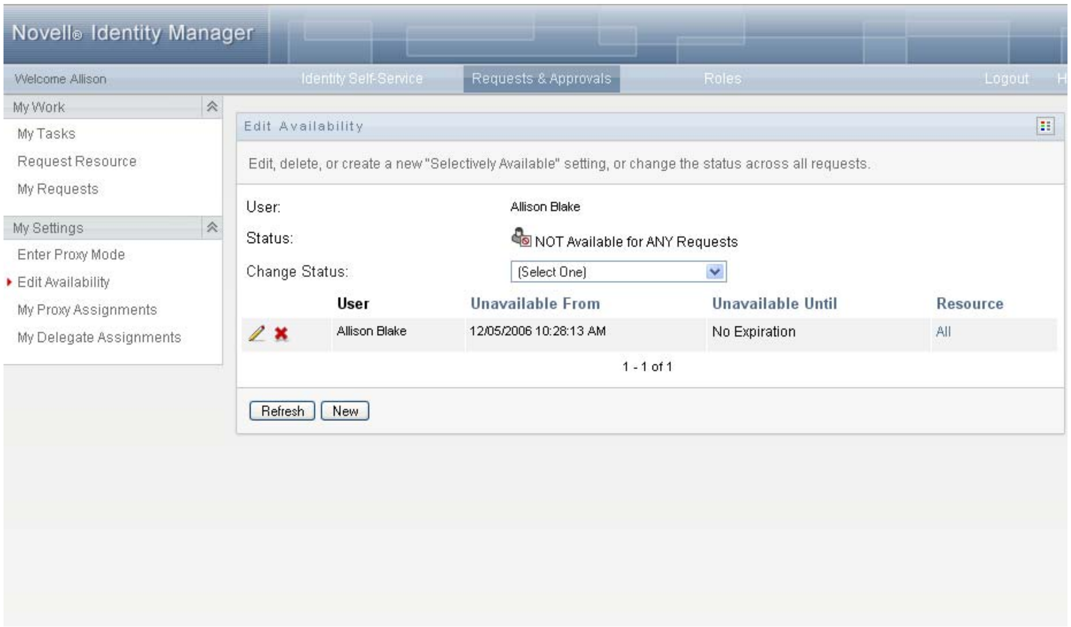
Change Status: [Select One]

User	Unavailable From	Unavailable Until	Resource
Allison Blake	--	--	All

0 - 0 of 0

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

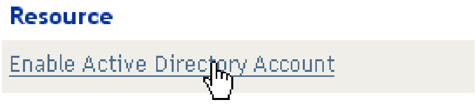
Status: NOT Available for ANY Requests

Change Status: [Select One]

	User	Unavailable From	Unavailable Until	Resource
✎ ✖	Allison Blake	12/05/2006 10:28:13 AM	No Expiration	All

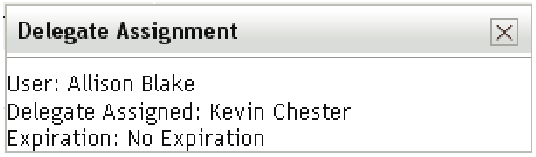
1 - 1 of 1

2 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:



Delegate Assignment

User: Allison Blake
Delegate Assigned: Kevin Chester
Expiration: No Expiration

This information is particularly helpful in situations where the same resource 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
Available for ALL Requests	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. The *Available for ALL Requests* status overrides other settings. If you change the status to one of the other settings, and then change it back to *Available for ALL Requests*, any *Selectively Available* settings previously defined are removed.
NOT Available for ANY Requests	Specifies that you are globally unavailable for any request definitions currently in the system. Choosing the *Not Available for ANY Requests* status indicates that you are unavailable for each existing delegate assignment and changes the current status to *Not Available for Specified Requests*. Assignments are effective immediately until the delegate assignment expires. This setting does not affect availability for new assignments created after this point.
NOT Available for Specified Requests	Specifies that you are not available for certain resource 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. The *NOT Available for Specified Requests* option takes you to the Edit Availability page. It is the same action as clicking the *New* button.

11.3.2 Creating or Editing an Availability Setting

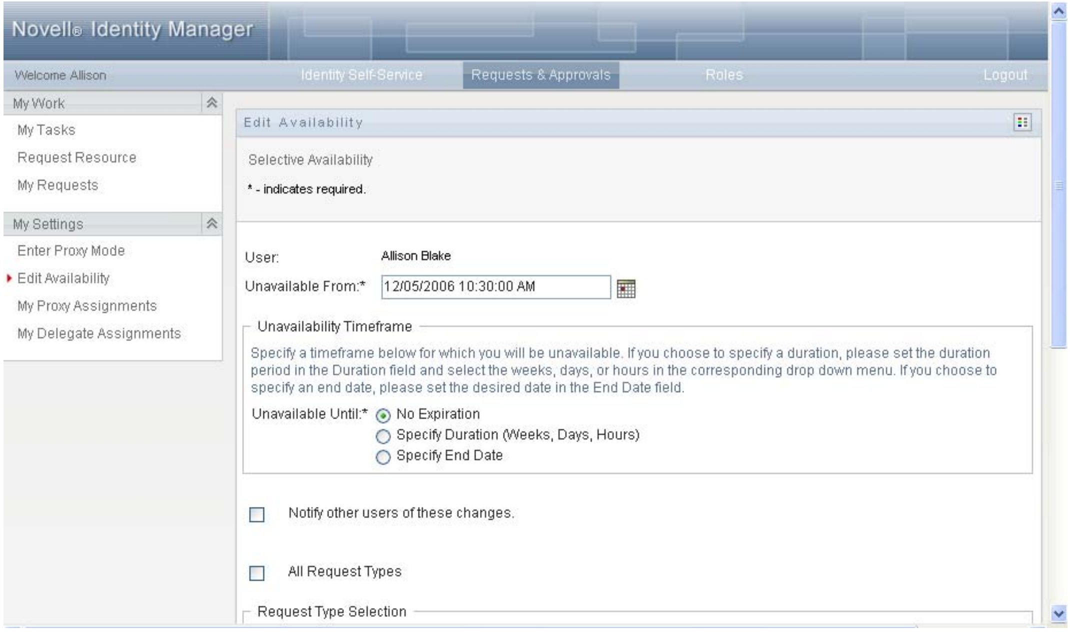
1 To create a new availability setting, click *New* (or select *NOT Available for Specified Requests* in the *Change Status* drop-down list).

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 requests displayed includes only those that have a delegate assignment.



Edit Availability

Selective Availability

* - indicates required.

User: Allison Blake

Unavailable From:* 12/05/2006 10:30:00 AM

Unavailability Timeframe

Specify a timeframe below for which you will be unavailable. If you choose to specify a duration, please set the duration period in the Duration field and select the weeks, days, or hours in the corresponding drop down menu. If you choose to specify an end date, please set the desired date in the End Date field.

Unavailable Until:* ● No Expiration
○ Specify Duration (Weeks, Days, Hours)
○ Specify End Date

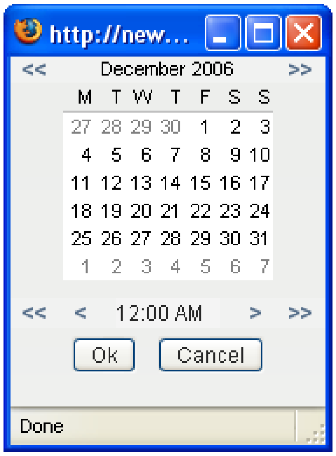
□ Notify other users of these changes.

□ 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
Duration	Lets you specify the time period in weeks, days, or hours.
End date	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.
No Expiration	Indicates that this unavailability setting does not expire.

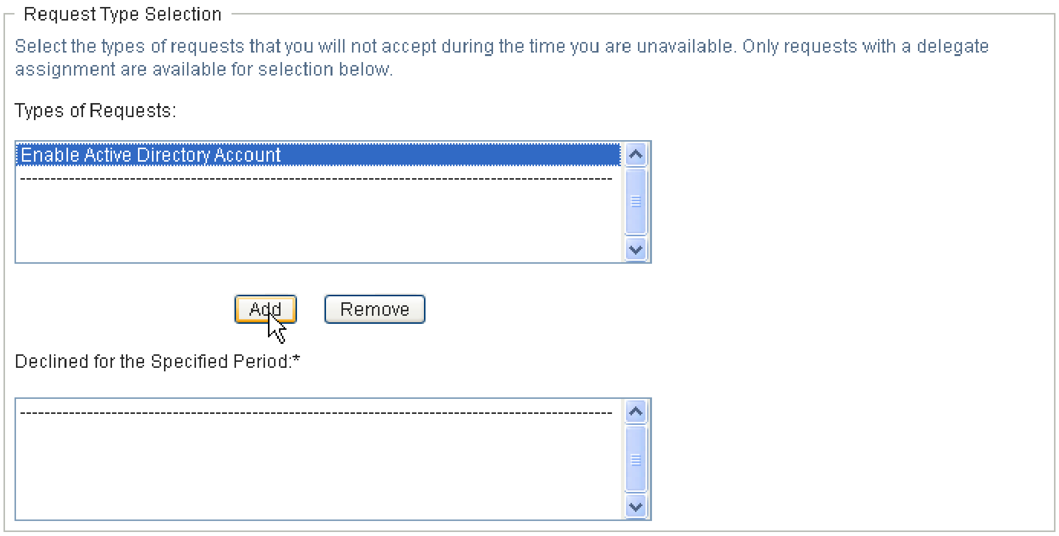
The end date you specify must be within the time period allowed by the delegate assignment. For example, if the delegate assignment expires on October 31, 2007, you cannot specify an expiration date of November 15, 2007 for the availability setting. If you specify an expiration date of November 15, 2007, it is automatically adjusted when it is submitted to expire on October 31, 2007.

4 Specify whether you want to send e-mail notifications to other users by filling in these fields:

Field	Description
Notify other users of these changes	Indicates whether you want to send an e-mail message to notify one or more users of this availability assignment.
Addressee	Specifies which users should receive e-mail notifications: **Selective:** Allows you to send e-mail notifications to any users you select.

5 Select one or more 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

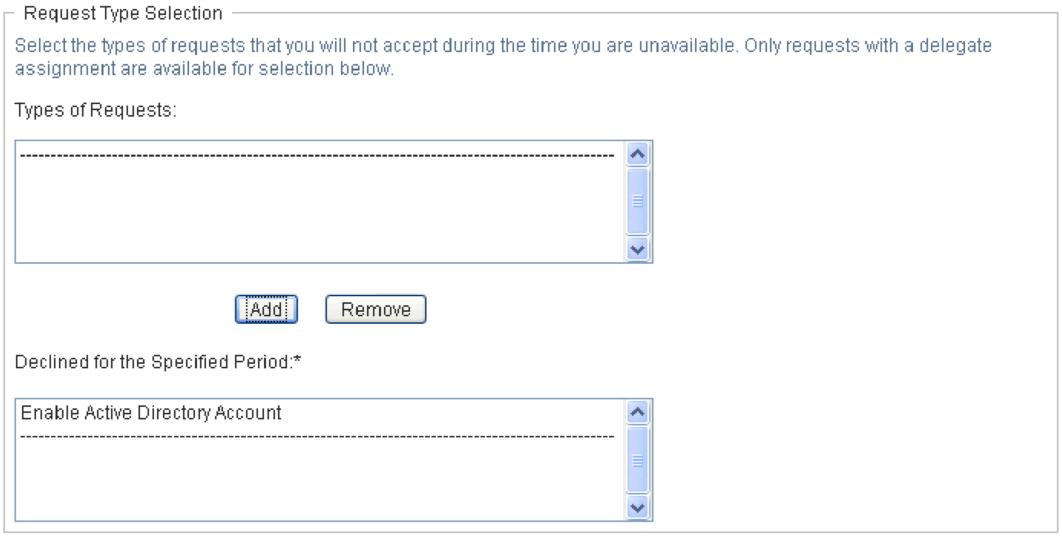
Select the types of requests that you will not accept during the time you are unavailable. Only requests with a delegate assignment are available for selection below.

Types of Requests:

Enable Active Directory Account

Declined for the Specified Period:*

Each request you add is included in the *Declined for the Specified Period* list.



Request Type Selection

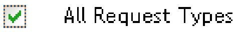
Select the types of requests that you will not accept during the time you are unavailable. Only requests with a delegate assignment are available for selection below.

Types of Requests:

Declined for the Specified Period:*

Enable Active Directory Account

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.

11.3.3 Deleting an Availability Setting

To delete an existing availability setting:

1 Click *Remove* next to the setting:

✖

11.4 Viewing and Editing Your Proxy Assignments

The *My Proxy Assignments* action allows you to view your proxy assignments. If you are a Provisioning Application Administrator, you can also use this action to edit proxy assignments.

Only Provisioning Application Administrators and team managers can assign proxies, as described below:

- The Provisioning Application Administrator has 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.

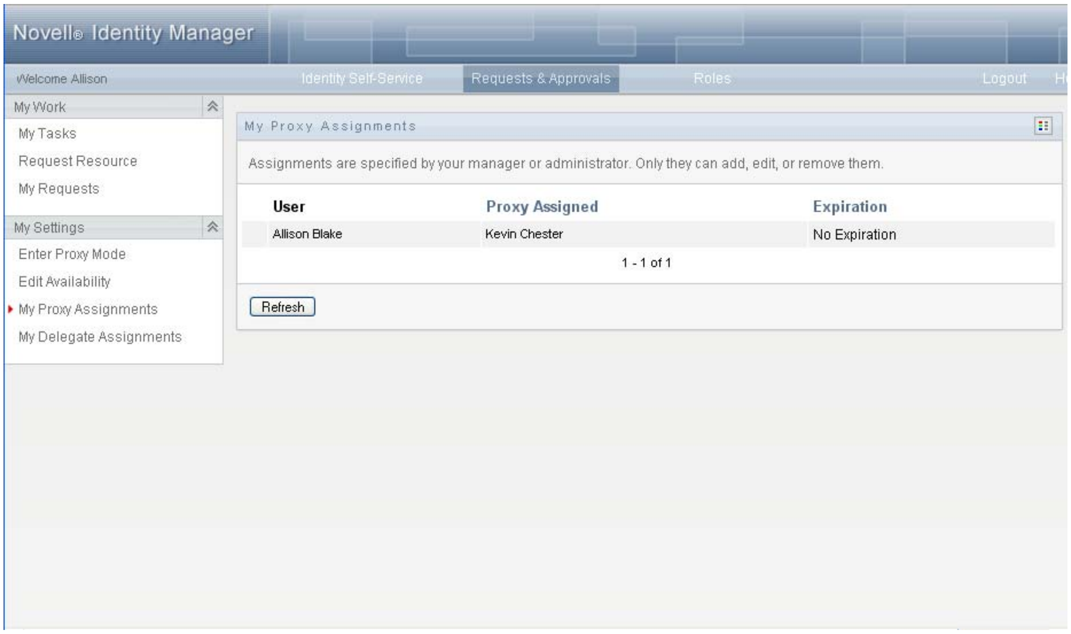
If a team manager needs to select a proxy who is not within the team, the manager must request that the Provisioning Application Administrator define the proxy relationship.

11.4.1 Displaying Your Proxy Settings

1 Click *My Proxy Assignments* in the *My 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 Application Administrator, you see a read-only view of your proxy assignments:



My Proxy Assignments

Assignments are specified by your manager or administrator. Only they can add, edit, or remove them.

User	Proxy Assigned	Expiration
Allison Blake	Kevin Chester	No Expiration

1 - 1 of 1

If you have administrative privileges, you are provided with buttons that let you create and edit proxy assignments.

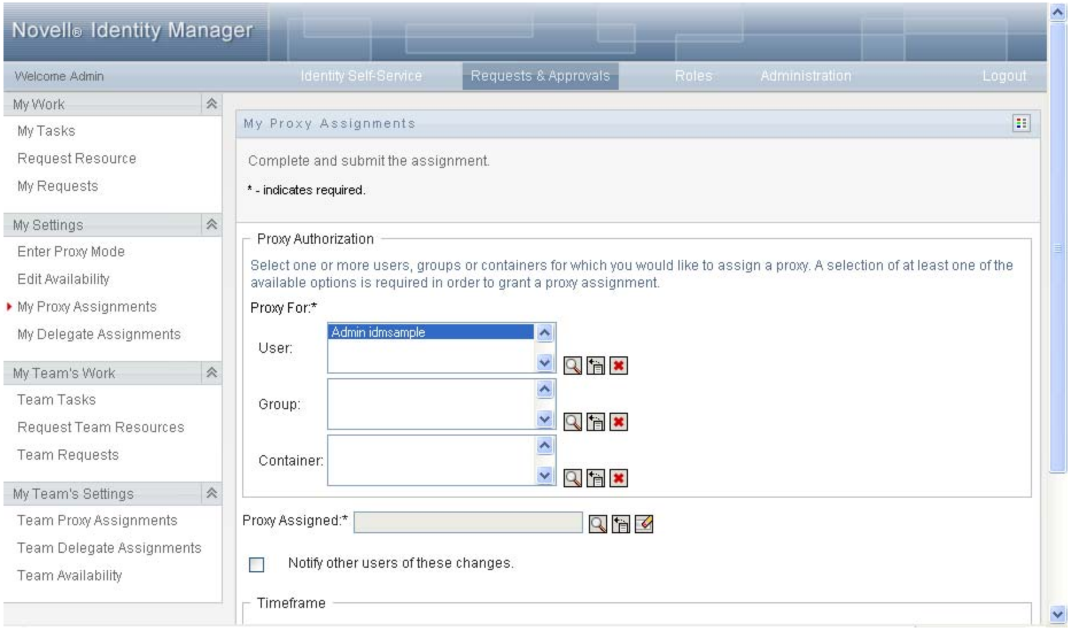
2 To refresh the list, click *Refresh*.

11.4.2 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: Admin idmsample

Group:

Container:

Proxy Assigned:*

□ Notify other users of these changes.

Timeframe

3 If you are the Provisioning Application 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
No Expiration	Indicates that this proxy assignment does not expire.
Specify Expiration	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.

11.4.3 Deleting Proxy Assignments

To delete an existing proxy assignment:

1 Click *Remove* next to the assignment:

✖

11.5 Viewing and Editing Your Delegate Assignments

The *My Delegate Assignments* action allows you to view your delegate assignments. If you are a Provisioning Application Administrator, you can also use this action to edit delegate assignments.

Only Provisioning Application Administrators and team managers can assign delegates, as described below:

- The Provisioning Application Administrator has 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 Application Administrator define the delegate relationship.

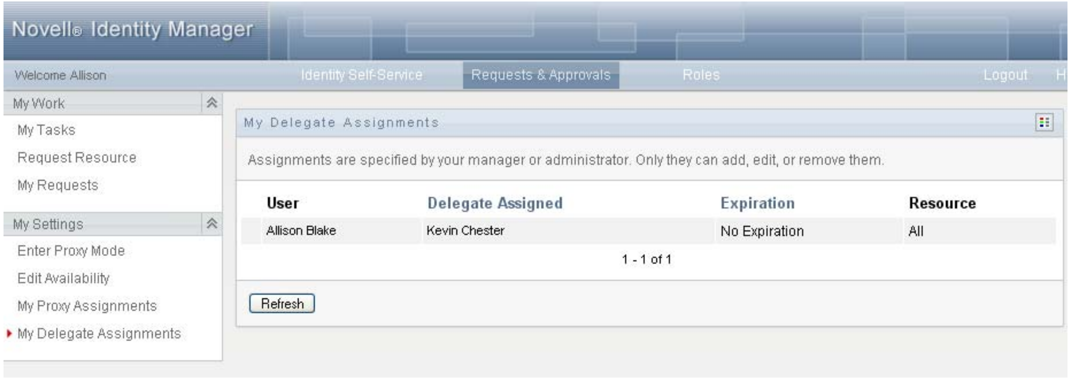
TIP: Before using the *Edit Availability* action, you need to have at least one delegate assignment to work on.

11.5.1 Displaying Your Delegate Settings

1 Click *My Delegate Assignments* in the *My Settings* group of actions.

The User Application displays your current settings.

If you are not a Provisioning Application Administrator, you see a read-only view of your delegate assignments:



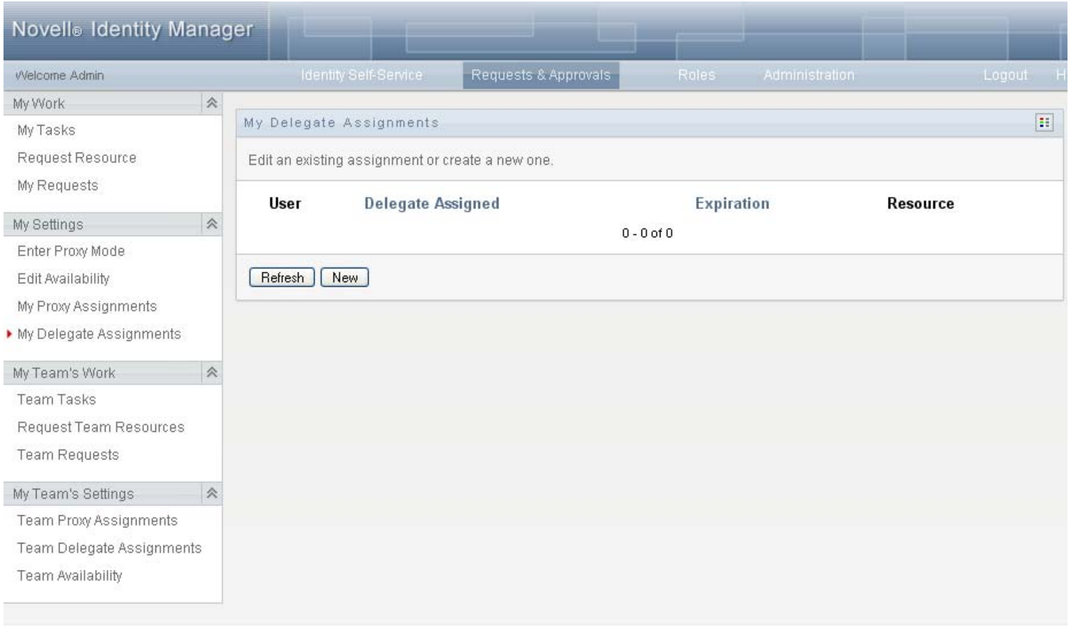
My Delegate Assignments

Assignments are specified by your manager or administrator. Only they can add, edit, or remove them.

User	Delegate Assigned	Expiration	Resource
Allison Blake	Kevin Chester	No Expiration	All

1 - 1 of 1

If you have administrative privileges, you are provided with buttons that let you create and edit delegate assignments.



My Delegate Assignments

Edit an existing assignment or create a new one.

User	Delegate Assigned	Expiration	Resource

0 - 0 of 0

2 To refresh the list, click *Refresh*.

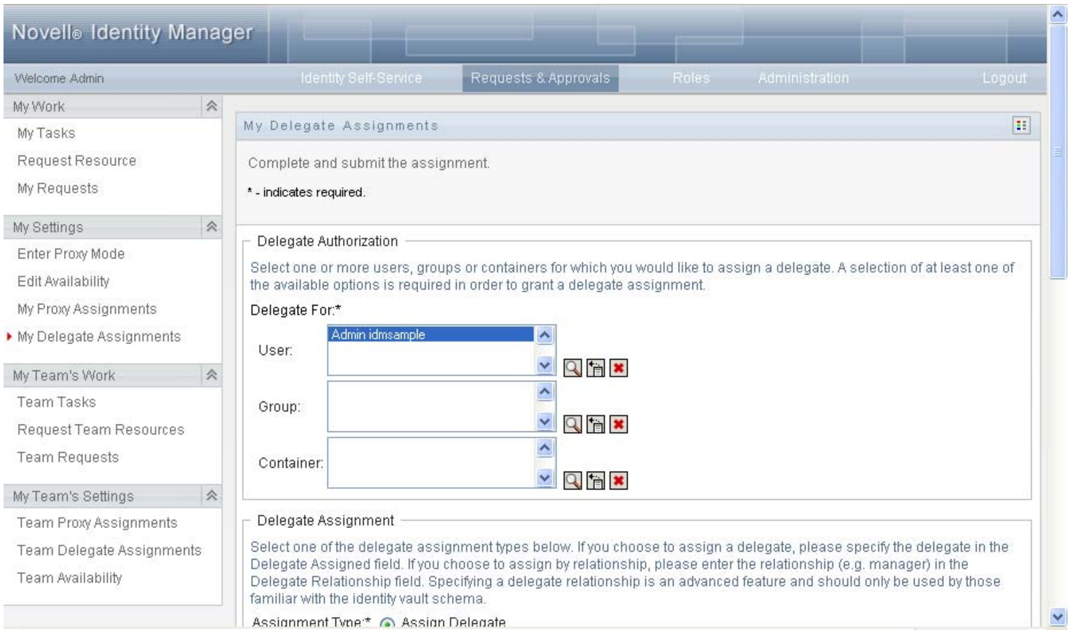
11.5.2 Creating or Editing Delegate Assignments

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:



My Delegate Assignments

Complete and submit the assignment.

* - indicates required.

Delegate Authorization

Select one or more users, groups or containers for which you would like to assign a delegate. A selection of at least one of the available options is required in order to grant a delegate assignment.

Delegate For:*

User: Admin idmsample

Group:

Container:

Delegate Assignment

Select one of the delegate assignment types below. If you choose to assign a delegate, please specify the delegate in the Delegate Assigned field. If you choose to assign by relationship, please enter the relationship (e.g. manager) in the Delegate Relationship field. Specifying a delegate relationship is an advanced feature and should only be used by those familiar with the identity vault schema.

Assignment Type:* ● Assign Delegate

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.

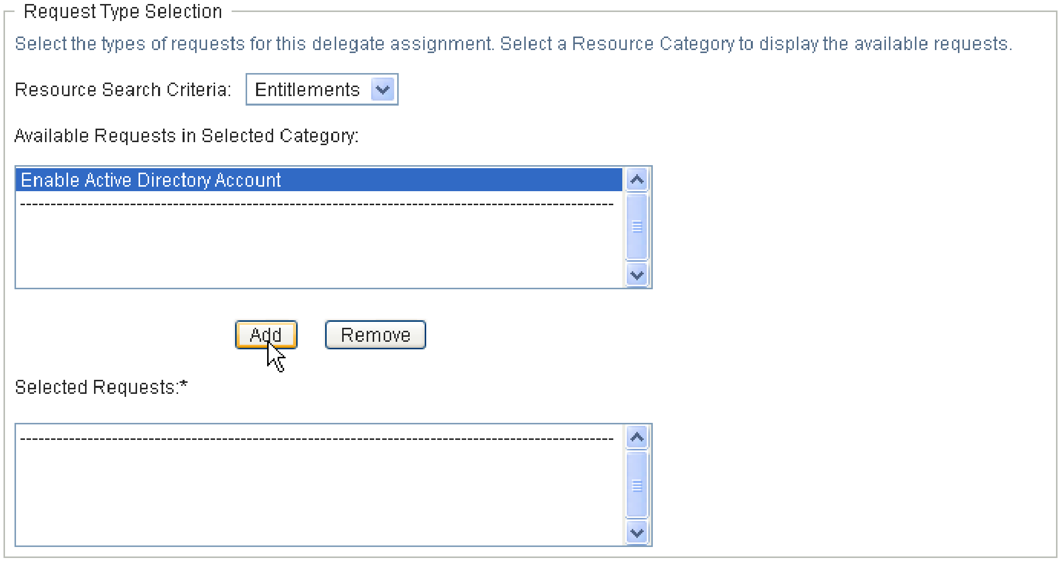
3 Click *Assign Delegate*. Specify the user who is the delegate in the *Delegate Assigned* field. Alternatively, click *Assign by Relationship*, then select a relationship in the *Delegate Relationship* field.

4 Specify when the time period ends by clicking one of the following:

Button	Description
No Expiration	Indicates that this delegate assignment does not expire.
Specify Expiration	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 resource 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.

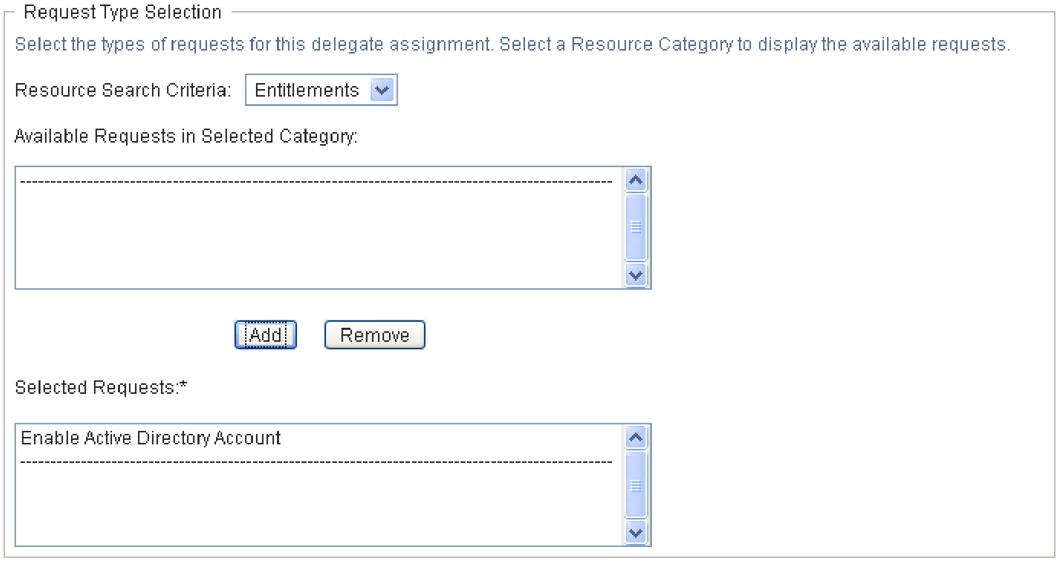
Resource Search Criteria: Entitlements

Available Requests in Selected Category:

Enable Active Directory Account

Selected Requests:*

Each 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:

Selected Requests:*

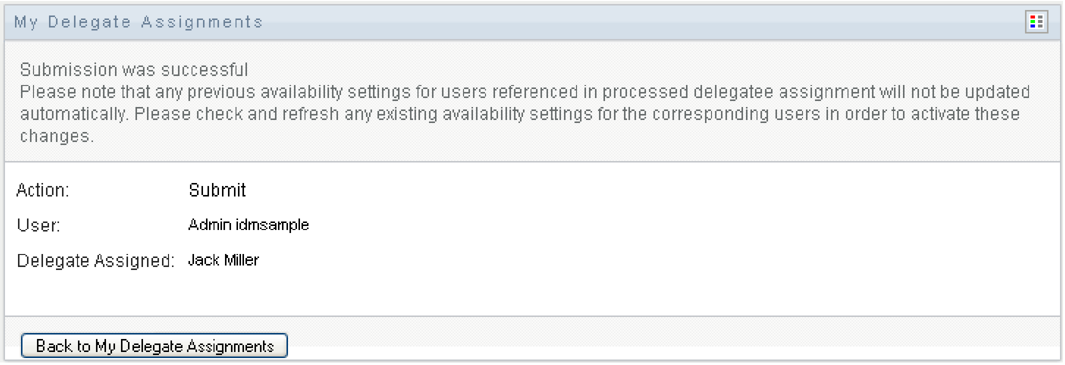
Enable Active Directory Account

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:



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.

Action:	Submit
User:	Admin idmsample
Delegate Assigned:	Jack Miller

11.5.3 Deleting a Delegate Assignment

To delete an existing delegate assignment:

1 Click *Remove* next to the assignment:

✖

Managing Your Team's Work

12

This section describes how to use the *Requests & Approvals* tab to manage your team's provisioning work. Topics include:

- Section 12.1, "About My Team's Work Actions," on page 157
- Section 12.2, "Managing Your Team's Tasks," on page 158
- Section 12.3, "Make Team Requests," on page 174
- Section 12.4, "Managing Your Team's Requests," on page 180

12.1 About My Team's Work Actions

The *Requests & Approvals* tab in the Identity Manager User Application includes a group of actions called *My Team's Work*. The *My Team's Work* actions give you the ability to work with team member tasks and requests in a workflow. Some actions are the same as those described in Chapter 10, "Managing Your Work," on page 119. The actions you can perform are determined by the definition of the team and the team request rights. The *Requests & Approvals* tab works with existing users and teams. To add new users and teams, refer to Chapter 8, "Creating Users or Groups," on page 97.

NOTE: The flow of control for a provisioning workflow, as well as the appearance of forms, can vary depending on how the provisioning request was defined in the Designer for Identity Manager. For details on customizing the design of a provisioning workflow, see the *Identity Manager User Application: Design Guide (http://www.novell.com/documentation/idmrbpm361/index.html)*.

12.1.1 About Teams

A *team* identifies a group of users. It determines who can manage provisioning requests and approval tasks associated with this team. The team definition consists of a list of team managers, team members, and team options, as described below:

- The *team managers* are those users who can administer requests and tasks for the team. Team managers can also be given permission to set proxies and delegates for team members. Team managers can be users or groups.
- The *team members* are those users who are allowed to participate on the team. Team members can be users, groups, or containers within the directory. Alternatively, they can be derived through directory relationships. For example, the list of members could be derived by the manager-employee relationship within the organization. In this case, the team members would be all users who report to the team manager.

NOTE: The Provisioning Application Administrator can configure the directory abstraction layer to support cascading relationships, in which case several levels within an organization might be included within a team. The number of levels to include is configurable by the administrator.

- The *team options* determine the provisioning request scope, which specifies whether the team can act on an individual provisioning request, one or more categories of requests, or all requests. The team options also determine whether team managers can set proxies for team members and/or set the availability of team members for the purpose of delegation.

The Provisioning Application Administrator can perform all team management functions.

The team definition itself is managed within iManager by one or more administrative managers.

12.1.2 About Team Request Rights

The *team request rights* specify a list of requests that fall within the domain of a team, as well as the actions that team managers can perform on the provisioning requests and tasks.

The team request rights are managed within iManager by one or more administrative managers. The team manager is not permitted to set these rights.

Your administrator has the ability to define a scope of control for team managers depending on the business needs of the specific team. Because of this you might have different rights over requests and tasks, depending on the team for which you are acting as a manager. If you have questions about the access rights for a specific team, please contact your administrator.

12.2 Managing Your Team's Tasks

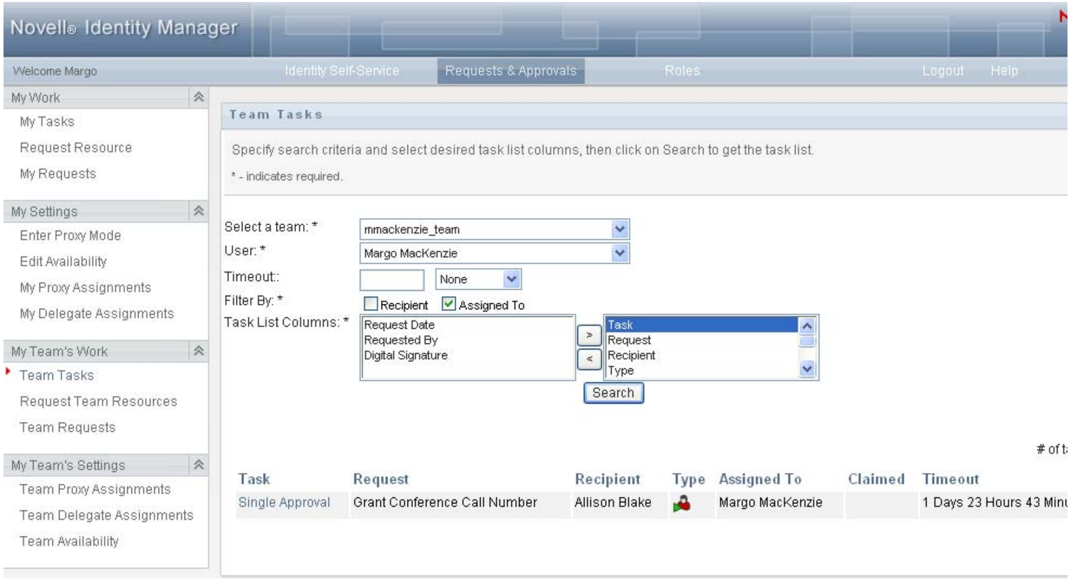
When a task is in a workflow queue, you can perform the following actions:

- Section 12.2.1, "Viewing Tasks by Team Member," on page 158
- Section 12.2.2, "Viewing Tasks by User or Group," on page 160
- Section 12.2.3, "Using the Task Displays," on page 162
- Section 12.2.4, "Selecting a Task," on page 166
- Section 12.2.5, "Claiming a Task," on page 170
- Section 12.2.6, "Reassigning a Task," on page 173
- Section 12.2.7, "Releasing a Task," on page 174

12.2.1 Viewing Tasks by Team Member

A team manager can view a team member's tasks. Only tasks available to the team can be listed in the task list.

1 Click *Team Tasks* in the *My Team's Work* group of actions to display the Team Tasks window.



Team Tasks

Specify search criteria and select desired task list columns, then click on Search to get the task list.

* - indicates required.

Select a team: *	mmackenzie_team
User: *	Margo MacKenzie
Timeout::	None
Filter By: *	□ Recipient ☑ Assigned To
Task List Columns: *	Request Date Requested By Digital Signature → Task Request Recipient Type

# of t

Task	Request	Recipient	Type	Assigned To	Claimed	Timeout
Single Approval	Grant Conference Call Number	Allison Blake		Margo MacKenzie		1 Days 23 Hours 43 Minu

2 Click the *Select a team* down-arrow to display teams. Select a team for which you have been designated a team manager.

3 Select a user.

If the *User* selection box contains a name, click the *User* down-arrow to display all the members of the selected team. Click the name of the person whose tasks you want to display.

If the *User* selection box is empty, click the *Object Selector* icon to open the Object Lookup window. Specify search criteria for the team member, click *Search,* and select the team member.

Your administrator defines your team and defines whether you see an automatically populated selection list or an empty list with an *Object Selector* icon 🔍 beside the selection box.

4 (Optional) Specify a *Timeout* interval to find tasks that expire within the time you select. Specify one or more digits, for example 10.

If you specify a *Timeout* interval, choose whether the interval is days, weeks, or months.

5 Use *Filter by* to select the subset of tasks you want to see for a team member. To see tasks that grant or revoke resources for the team member, select *Recipient*. To see tasks that the team member is responsible for doing, select *Assigned to*. You can select both kinds of tasks.

6 In the *Task List Columns* selection box, select one or more task columns to display and click the right-arrow to add them to the task list. The order in which you select the columns is the order in which they appear in the display. Columns can include:

Task. (Required.)
Request
Recipient
Request Date
Type
Assigned to
Requested by
Claimed
Timeout

Priority

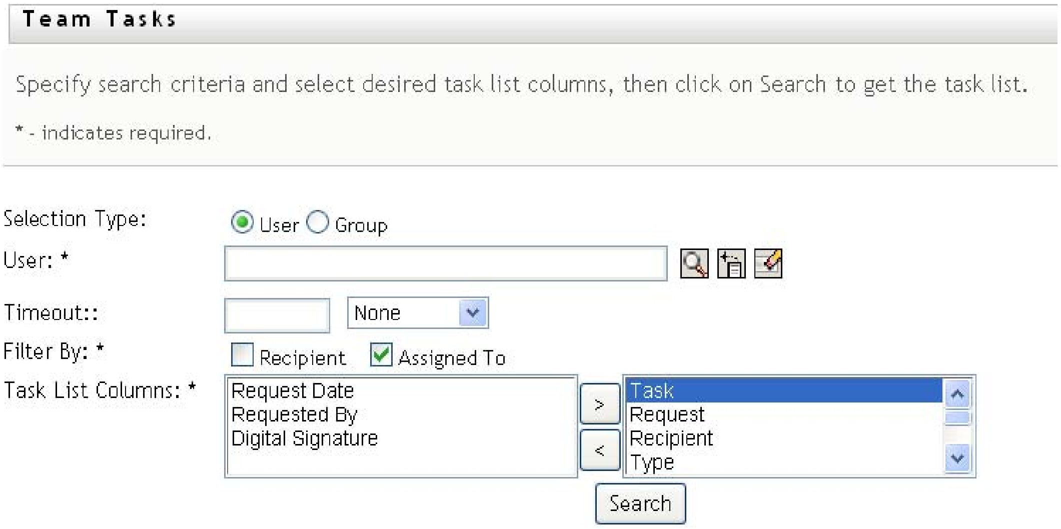
Digital Signature

7. Click *Search* to list the selected user’s tasks.
8. To see another team member’s tasks, or tasks for another team, return to Step 2 and define a new search.

12.2.2 Viewing Tasks by User or Group

A Provisioning Application Administrator can view tasks by user or group.

1. Click *Team Tasks* in the *My Team’s Work* group of actions to display the Team Tasks window.
2. For *Selection Type*, choose *User* or *Group*.



Team Tasks

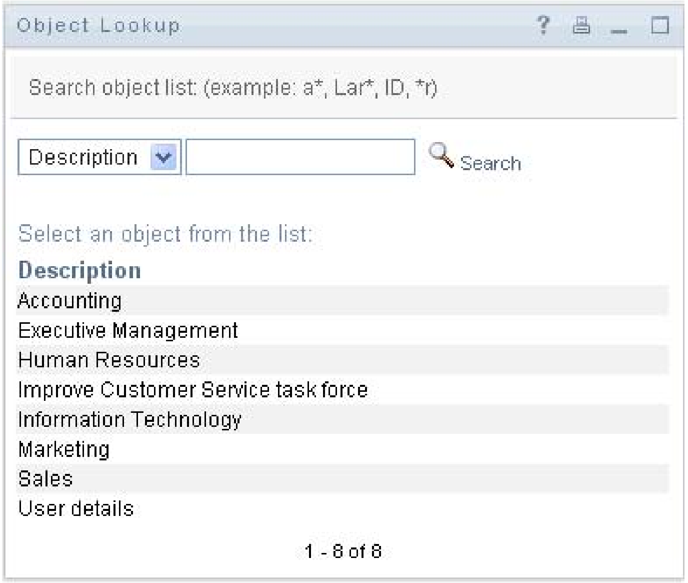
Specify search criteria and select desired task list columns, then click on Search to get the task list.

* - indicates required.

Selection Type:	● User ○ Group
User: *	
Timeout::	None
Filter By: *	□ Recipient ☑ Assigned To
Task List Columns: *	Request Date Requested By Digital Signature
	Task Request Recipient Type

3. To look up a name, click the *Object Selector* icon 🔍, specify lookup criteria, and click *Search*.

   Click a user name or group name to select it. The following sample of the object lookup page was a lookup of all groups:



Object Lookup

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

Description ▾ 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

4 Optionally, specify a *Timeout* interval to find tasks that expire within the interval. Specify one or more digits.

If you specify a *Timeout* interval, choose whether the interval is days, weeks, or months.

5 Use *Filter by* to select a subset of tasks. To see tasks that grant or revoke resources to the user or group, select *Recipient*. To see tasks that the user or group is responsible for doing, select *Assigned to*. You can select both kinds of tasks.

6 In the *Task List Columns* selection box, select one or more task descriptions to display, then click the right-arrow to add the descriptions to the task list. The order in which you add the descriptions is the order in which they appear as column headers in the task list. Your choices are:

Task. (Required.)
Request
Recipient
Request Date
Type
Assigned to
Requested by
Claimed
Timeout
Priority
Digital Signature

7 Click *Search* to display the tasks.

Group tasks displayed are those explicitly assigned to the group, not those assigned to each member of the group. To see tasks assigned to an individual, view the tasks for that person.

8 To see tasks for another user or group, return to Step 2 and define a new search.

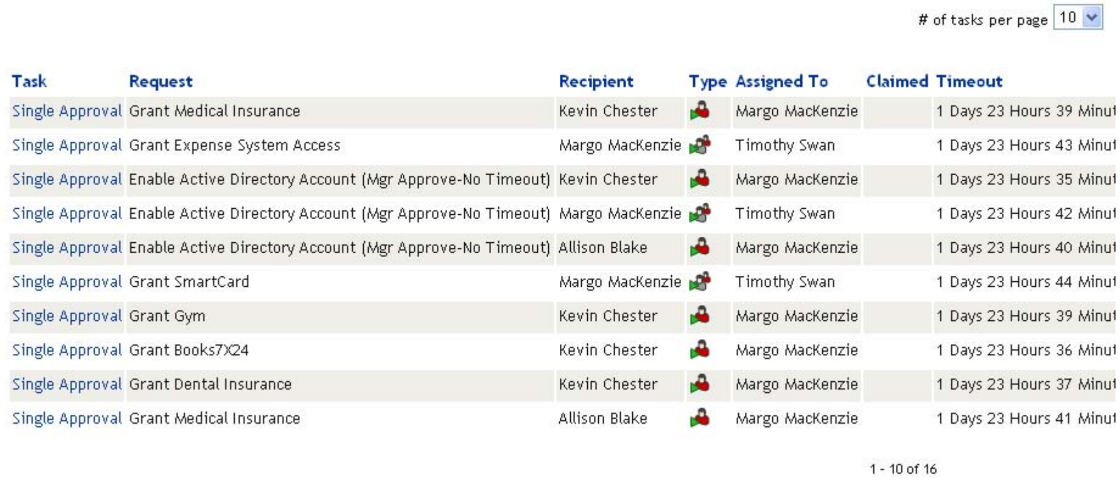
12.2.3 Using the Task Displays

The task list appears in the Template Display or the Exhibit Display format. Your administrator chooses your display format.

The Template Display Format

The Template Display is the default display format. Figure 12-1 shows an example:

Figure 12-1 *Example of Task List in Template Display Format*



# of tasks per page 10

Task	Request	Recipient	Type	Assigned To	Claimed	Timeout
Single Approval	Grant Medical Insurance	Kevin Chester		Margo MacKenzie		1 Days 23 Hours 39 Minut
Single Approval	Grant Expense System Access	Margo MacKenzie		Timothy Swan		1 Days 23 Hours 43 Minut
Single Approval	Enable Active Directory Account (Mgr Approve-No Timeout)	Kevin Chester		Margo MacKenzie		1 Days 23 Hours 35 Minut
Single Approval	Enable Active Directory Account (Mgr Approve-No Timeout)	Margo MacKenzie		Timothy Swan		1 Days 23 Hours 42 Minut
Single Approval	Enable Active Directory Account (Mgr Approve-No Timeout)	Allison Blake		Margo MacKenzie		1 Days 23 Hours 40 Minut
Single Approval	Grant SmartCard	Margo MacKenzie		Timothy Swan		1 Days 23 Hours 44 Minut
Single Approval	Grant Gym	Kevin Chester		Margo MacKenzie		1 Days 23 Hours 39 Minut
Single Approval	Grant Books7X24	Kevin Chester		Margo MacKenzie		1 Days 23 Hours 36 Minut
Single Approval	Grant Dental Insurance	Kevin Chester		Margo MacKenzie		1 Days 23 Hours 37 Minut
Single Approval	Grant Medical Insurance	Allison Blake		Margo MacKenzie		1 Days 23 Hours 41 Minut

1 - 10 of 16

The template display lets you sort columns by value, set the number of tasks per page, and page through the task list.

Sorting a Column by Value

1 Click the heading of a column to sort the values in the column.

2 Click the heading again to reverse the order of the sort.

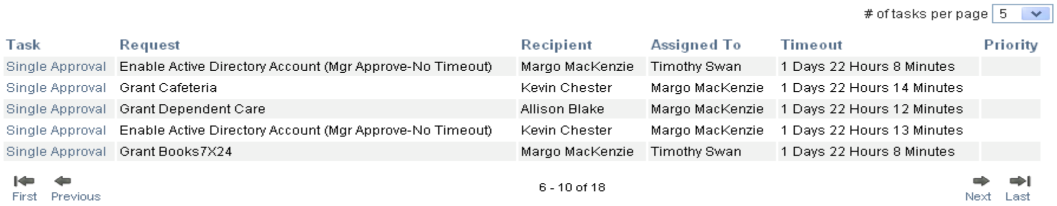
Setting the Number of Tasks per Page

1 Click the down-arrow of the *# of tasks per page* selection box on the right side above the task list.

2 Choose a page length of 5, 10, or 25 tasks per page.

Paging Through the Task List

1 Click *First, Previous, Next,* and *Last* to page through the task list.



# of tasks per page 5

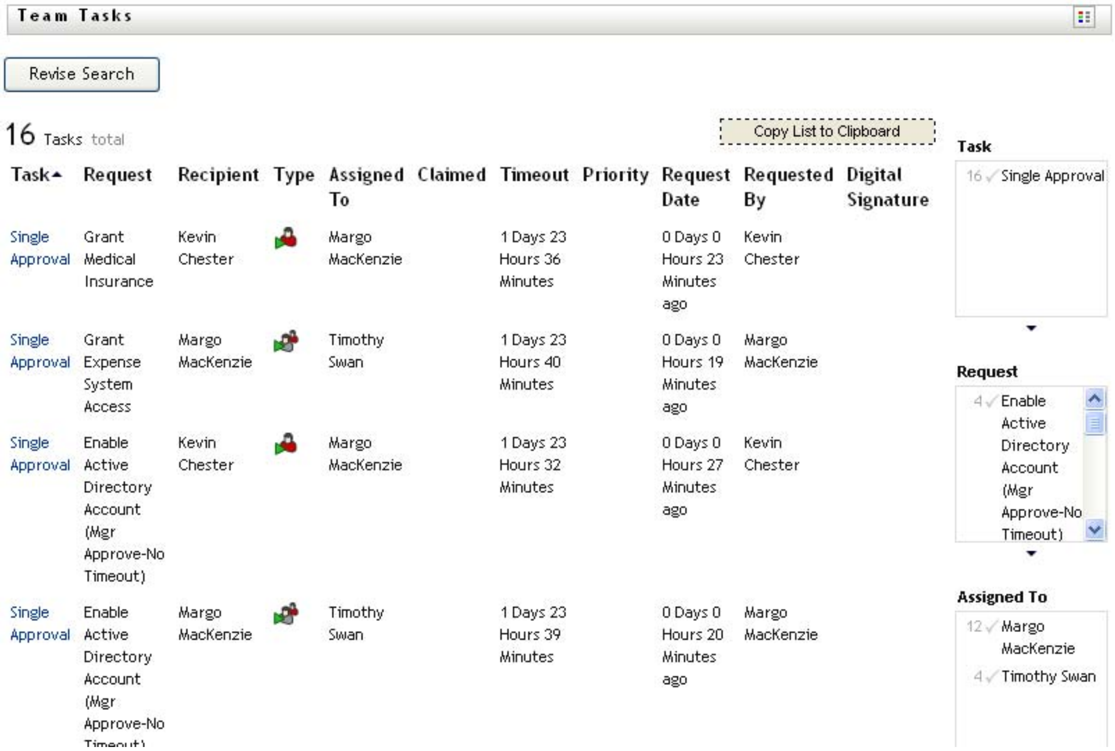
Task	Request	Recipient	Assigned To	Timeout	Priority
Single Approval	Enable Active Directory Account (Mgr Approve-No Timeout)	Margo MacKenzie	Timothy Swan	1 Days 22 Hours 8 Minutes	
Single Approval	Grant Cafeteria	Kevin Chester	Margo MacKenzie	1 Days 22 Hours 14 Minutes	
Single Approval	Grant Dependent Care	Allison Blake	Margo MacKenzie	1 Days 22 Hours 12 Minutes	
Single Approval	Enable Active Directory Account (Mgr Approve-No Timeout)	Kevin Chester	Margo MacKenzie	1 Days 22 Hours 13 Minutes	
Single Approval	Grant Books7X24	Margo MacKenzie	Timothy Swan	1 Days 22 Hours 8 Minutes	

6 - 10 of 18

The Exhibit Display Format

The Exhibit Display format enables you to filter your retrieved data. Figure 12-2 shows an example of the Exhibit Display format:

Figure 12-2 *Example of Task List in Exhibit Display Format*



16 Tasks total

Task▲	Request	Recipient	Type	Assigned To	Claimed	Timeout	Priority	Request Date	Requested By	Digital Signature
Single Approval	Grant Medical Insurance	Kevin Chester		Margo MacKenzie		1 Days 23 Hours 36 Minutes		0 Days 0 Hours 23 Minutes ago	Kevin Chester	
Single Approval	Grant Expense System Access	Margo MacKenzie		Timothy Swan		1 Days 23 Hours 40 Minutes		0 Days 0 Hours 19 Minutes ago	Margo MacKenzie	
Single Approval	Enable Active Directory Account (Mgr Approve-No Timeout)	Kevin Chester		Margo MacKenzie		1 Days 23 Hours 32 Minutes		0 Days 0 Hours 27 Minutes ago	Kevin Chester	
Single Approval	Enable Active Directory Account (Mgr Approve-No Timeout)	Margo MacKenzie		Timothy Swan		1 Days 23 Hours 39 Minutes		0 Days 0 Hours 20 Minutes ago	Margo MacKenzie	

Task

16 ✓ Single Approval

Request

4 ✓ Enable Active Directory Account (Mgr Approve-No Timeout)

Assigned To

12 ✓ Margo MacKenzie

4 ✓ Timothy Swan

Sorting a Column by Value

1. Click the heading of a column to sort the values in the column.
2. Click the heading again to reverse the order of the sort.

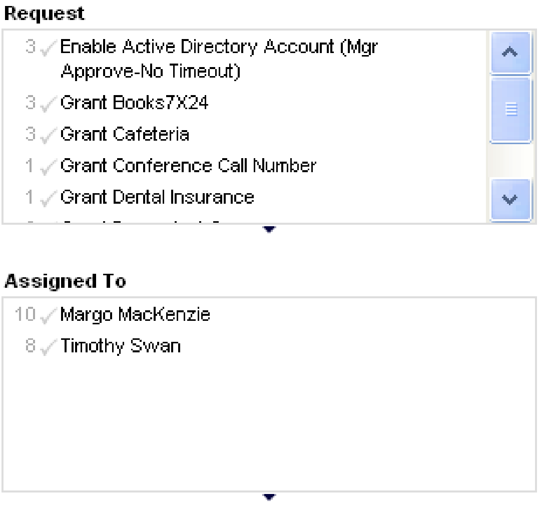
Filtering Your View of the Data

The Exhibit Display format shows the whole data set returned by your search. You can use filters to filter the data set. The filters are on the right side of the display and have the names of column headings from your search. You can filter the data by *Task, Request, Assigned To,* and *Requested By* column values. Filters only appear if the corresponding columns are included in the display.

NOTE: The Exhibit Display refers to filters as *facets*.

Figure 12-3 shows an example with a Request filter and an Assigned To filter:

Figure 12-3 *Two Filters in the Exhibit Display*



Request

- 3 ✓ Enable Active Directory Account (Mgr Approve-No Timeout)
- 3 ✓ Grant Books7X24
- 3 ✓ Grant Cafeteria
- 1 ✓ Grant Conference Call Number
- 1 ✓ Grant Dental Insurance

Assigned To

- 10 ✓ Margo MacKenzie
- 8 ✓ Timothy Swan

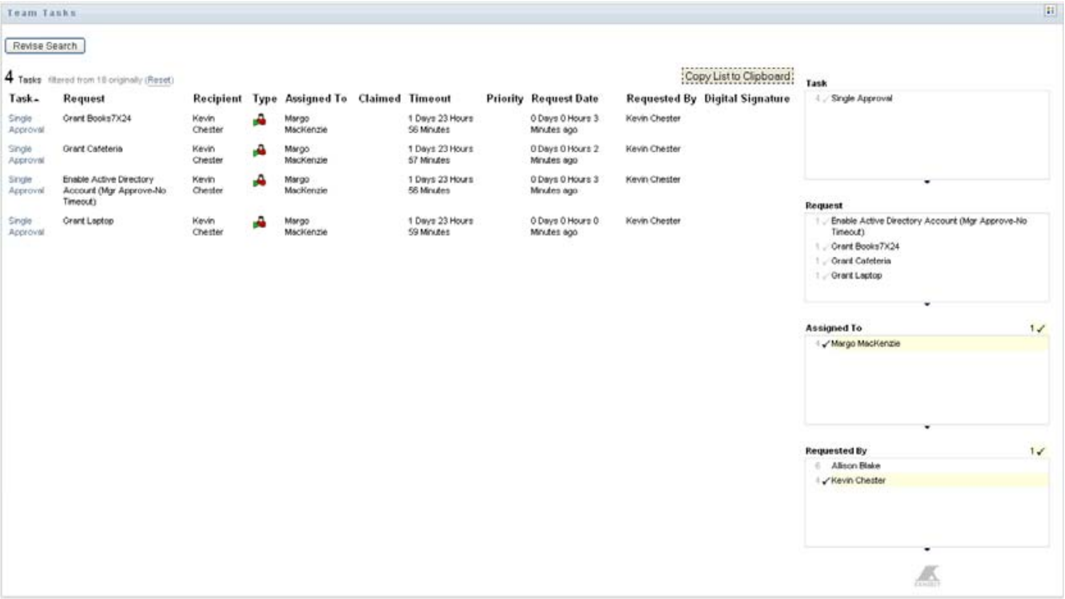
Beside each filter parameter is a number and optionally a check mark. The number indicates the number of tasks that match that parameter within the current filter set. The check mark indicates whether the filter parameter is selected. Initially, all filter parameters are selected, enabling you to see all the data from your search. If a filter has only one parameter, that parameter is automatically selected.

1 To view a subset of data, click one or more parameters in one or more filter boxes.

NOTE: Selecting a parameter in one filter can change the parameters available in other filters.

For example, if you click Margo's name in the Assigned To filter and Kevin's name in the Requested By filter, you see only tasks that are both assigned to Margo Mackenzie and requested by Kevin Chester, as shown in Figure 12-4:

Figure 12-4 *Example of Task List After Applying Two Filters*



Team Tasks

Revise Search

4 Tasks filtered from 18 originally (Reset)

Copy List to Clipboard

Task	Request	Recipient	Type	Assigned To	Claimed	Timeout	Priority	Request Date	Requested By	Digital Signature
Single Approval	Grant Books7X24	Kevin Chester		Margo MacKenzie		1 Days 23 Hours 56 Minutes		0 Days 0 Hours 3 Minutes ago	Kevin Chester	
Single Approval	Grant Cafeteria	Kevin Chester		Margo MacKenzie		1 Days 23 Hours 57 Minutes		0 Days 0 Hours 2 Minutes ago	Kevin Chester	
Single Approval	Enable Active Directory Account (Mgr Approve-No Timeout)	Kevin Chester		Margo MacKenzie		1 Days 23 Hours 56 Minutes		0 Days 0 Hours 3 Minutes ago	Kevin Chester	
Single Approval	Grant Laptop	Kevin Chester		Margo MacKenzie		1 Days 23 Hours 59 Minutes		0 Days 0 Hours 0 Minutes ago	Kevin Chester	

Task

- 4 ✓ Single Approval

Request

- 1 ✓ Enable Active Directory Account (Mgr Approve-No Timeout)
- 1 ✓ Grant Books7X24
- 1 ✓ Grant Cafeteria
- 1 ✓ Grant Laptop

Assigned To 1 ✓

- 4 ✓ Margo MacKenzie

Requested By 1 ✓

- 6 Allison Blake
- 4 ✓ Kevin Chester

Exporting Data from Your Display

1. To export the data that you see in your display, click *Copy List to Clipboard* (at the top of the display).
2. Choose *Tab Separated Values* or *Generated HTML of this view*. The Exhibit Display generates a coded text file.
3. Copy the contents to your clipboard.
4. Paste from your clipboard to a destination file.
5. Click *Close* or *ESC* to close the window of coded text.

Understanding the Display Icons

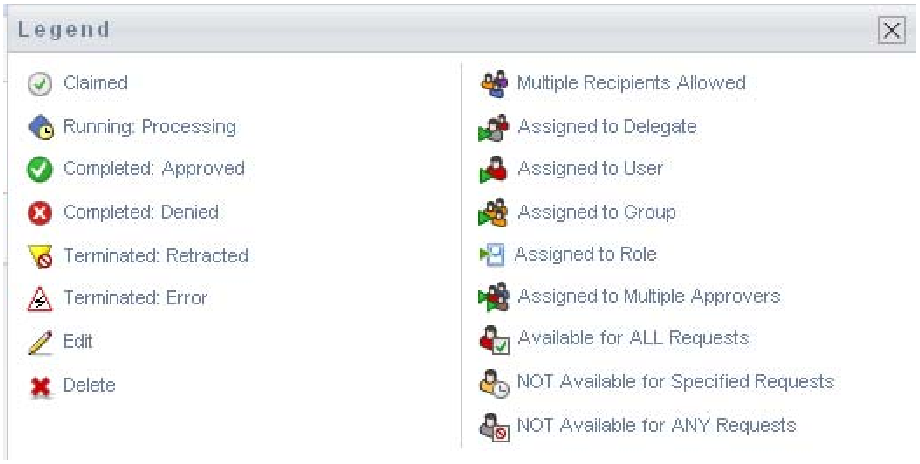
The Template and Exhibit views both show icons that indicate the status of each task in the result set. This section describes the display icons that appear in the task list:

- "Type Column" on page 165
- "Priority Column" on page 165
- "Claimed Column" on page 165
- "Digital Signature Column" on page 166

Type Column

Status flags appear under the *Type* column. Flags are defined in the Legend. To access the Legend, click the multicolored icon in the right side of the Team Tasks title bar. Figure 12-5 on page 165 shows the Legend.

Figure 12-5 *Icons that appear in the Team Tasks displays*



Legend

Claimed	Multiple Recipients Allowed
Running: Processing	Assigned to Delegate
Completed: Approved	Assigned to User
Completed: Denied	Assigned to Group
Terminated: Retracted	Assigned to Role
Terminated: Error	Assigned to Multiple Approvers
Edit	Available for ALL Requests
Delete	NOT Available for Specified Requests
	NOT Available for ANY Requests

Priority Column

A red flag identifies a high-priority task. This priority is set in the Provisioning Request Definition created by your administrator.

Claimed Column

The *Claimed* icon ✓ in the *Claimed* column indicates that the task has been claimed.

Digital Signature Column

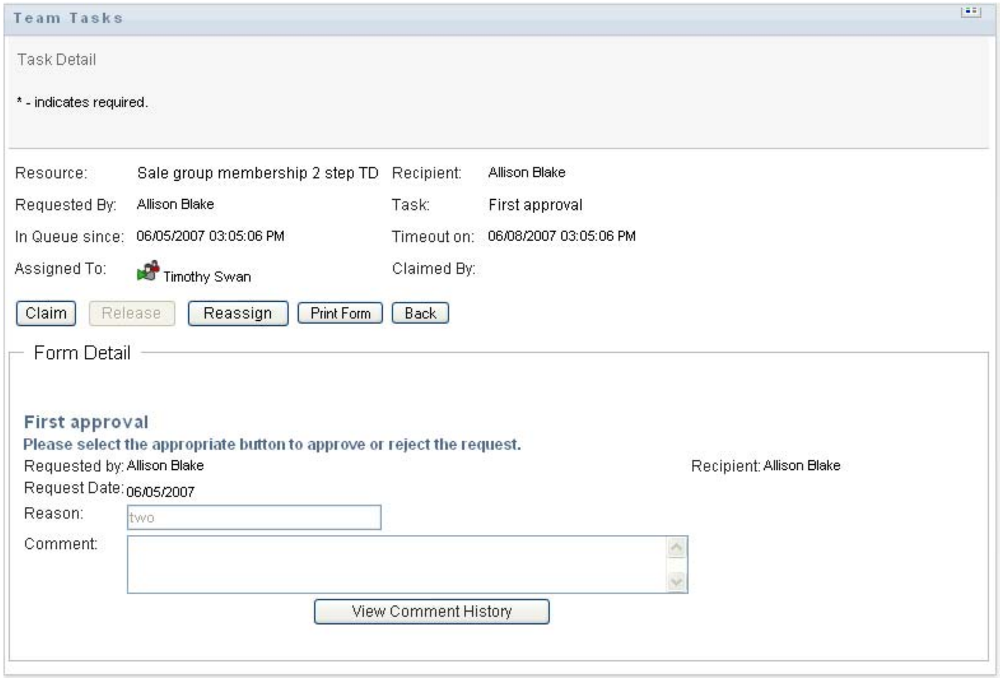
The *Digital Signature* icon in the *Digital Signature* column indicates that a digital signature is required to approve or deny the task.

12.2.4 Selecting a Task

To select and open a task in the task list:

1 Click the name of the task.

The Team Tasks Task Detail form is displayed.



Team Tasks

Task Detail

* - indicates required.

Resource:	Sale group membership 2 step TD	Recipient:	Allison Blake
Requested By:	Allison Blake	Task:	First approval
In Queue since:	06/05/2007 03:05:06 PM	Timeout on:	06/08/2007 03:05:06 PM
Assigned To:	Timothy Swan	Claimed By:	

Form Detail

First approval

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

Requested by: Allison Blake

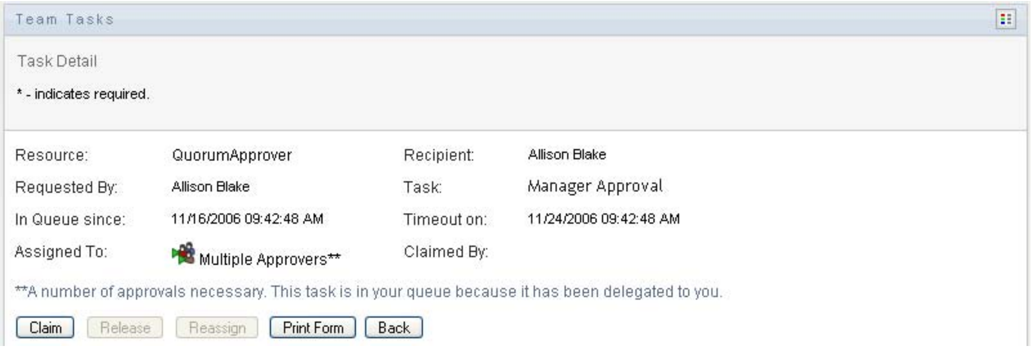
Recipient: Allison Blake

Request Date: 06/05/2007

Reason: two

Comment:

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.



Team Tasks

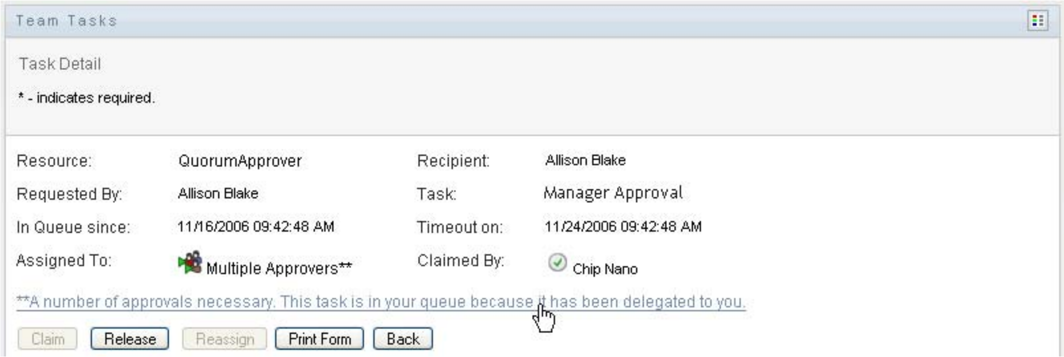
Task Detail

* - indicates required.

Resource:	QuorumApprover	Recipient:	Allison Blake
Requested By:	Allison Blake	Task:	Manager Approval
In Queue since:	11/16/2006 09:42:48 AM	Timeout on:	11/24/2006 09:42:48 AM
Assigned To:	Multiple Approvers**	Claimed By:	

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

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



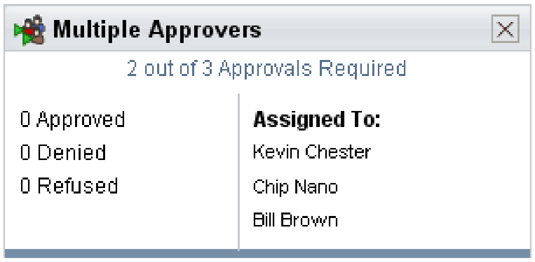
Task Detail

* - indicates required.

Resource: QuorumApprover
Recipient: Allison Blake
Requested By: Allison Blake
Task: Manager Approval
In Queue since: 11/16/2006 09:42:48 AM
Timeout on: 11/24/2006 09:42:48 AM
Assigned To: Multiple Approvers**
Claimed By: Chip Nano

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

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



2 out of 3 Approvals Required

0 Approved
0 Denied
0 Refused

Assigned To:
Kevin Chester
Chip Nano
Bill Brown

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 *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.

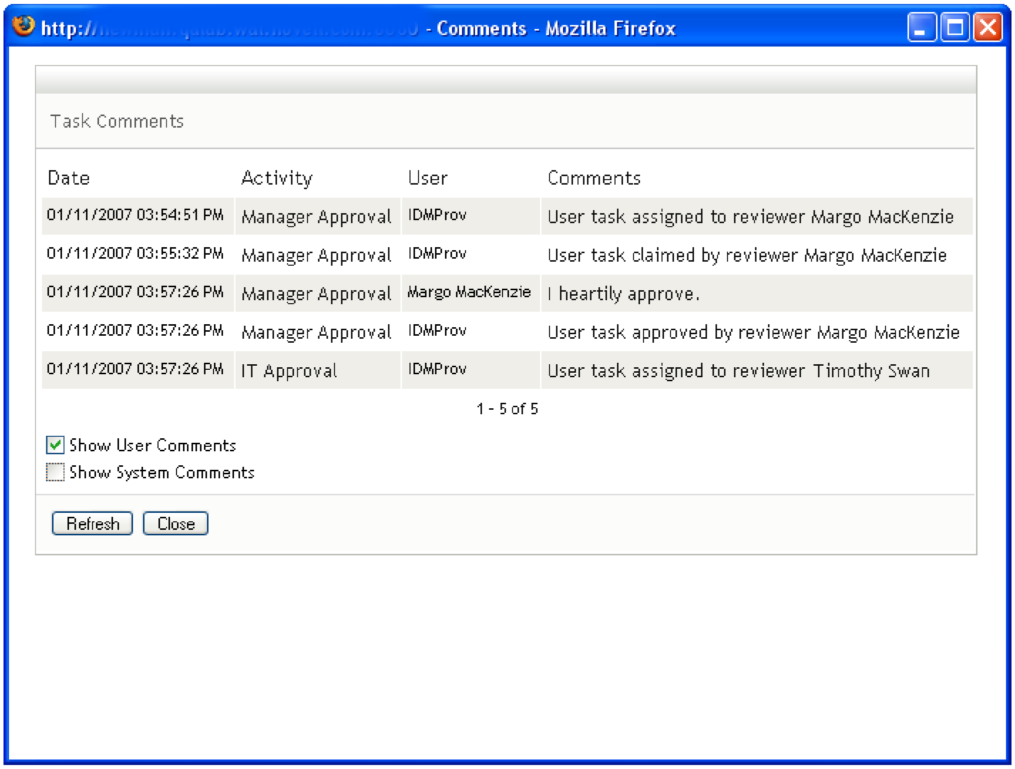
3 To claim a task, follow the instructions at Section 12.2.5, “Claiming a Task,” on page 170.

4 To reassign a task, follow the instructions at Section 12.2.6, “Reassigning a Task,” on page 173

5 To view 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.

5a To display user comments, click *Show User Comments*.



Task Comments

Date	Activity	User	Comments
01/11/2007 03:54:51 PM	Manager Approval	IDMProv	User task assigned to reviewer Margo MacKenzie
01/11/2007 03:55:32 PM	Manager Approval	IDMProv	User task claimed by reviewer Margo MacKenzie
01/11/2007 03:57:26 PM	Manager Approval	Margo MacKenzie	I heartily approve.
01/11/2007 03:57:26 PM	Manager Approval	IDMProv	User task approved by reviewer Margo MacKenzie
01/11/2007 03:57:26 PM	IT Approval	IDMProv	User task assigned to reviewer Timothy Swan

1 - 5 of 5

☑ Show User Comments

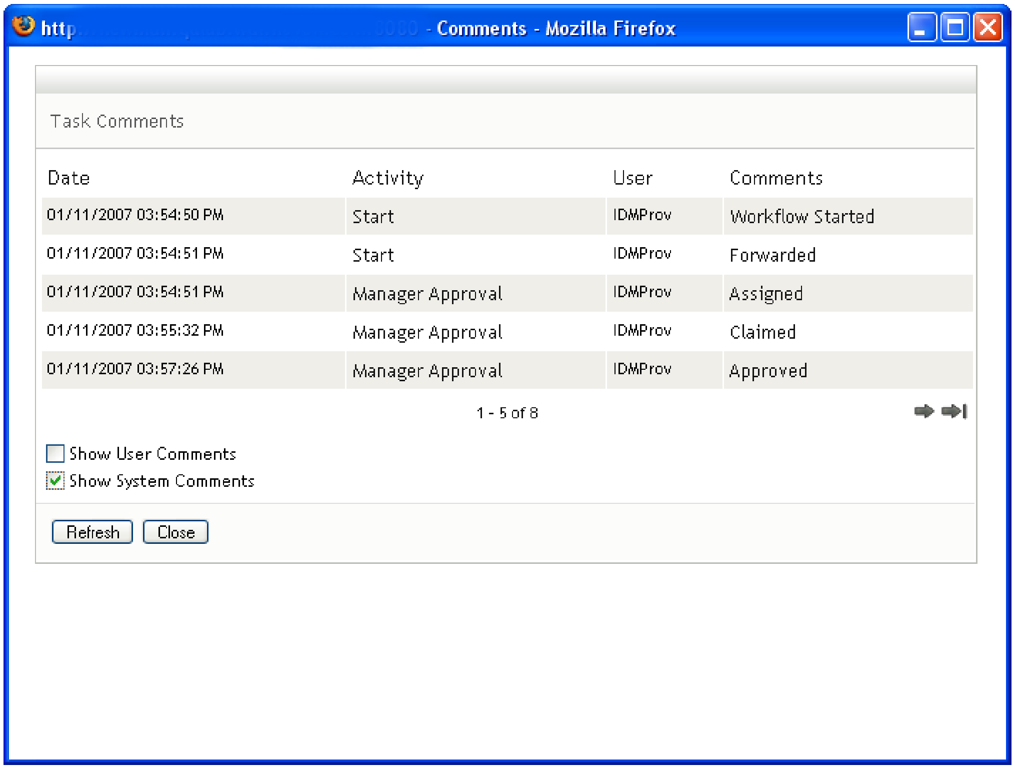
□ Show System Comments

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.

NOTE: 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.novell.com/documentation/idmrbpm361/index.html)*.

5b To display system comments, click *Show System Comments*.



Task Comments

Date	Activity	User	Comments
01/11/2007 03:54:50 PM	Start	IDMProv	Workflow Started
01/11/2007 03:54:51 PM	Start	IDMProv	Forwarded
01/11/2007 03:54:51 PM	Manager Approval	IDMProv	Assigned
01/11/2007 03:55:32 PM	Manager Approval	IDMProv	Claimed
01/11/2007 03:57:26 PM	Manager Approval	IDMProv	Approved

1 - 5 of 8

□ Show User Comments

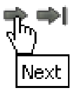
☑ Show System Comments

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, `IDMProv`) 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.

5c 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.



5d Click *Close* to close the window.

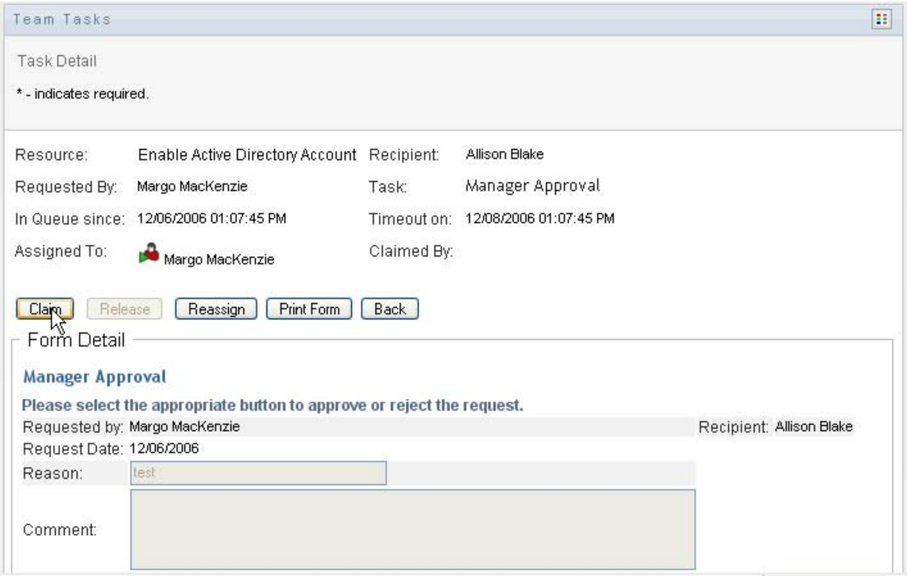
6 To return to the task list, click *Back*.

NOTE: The *Claim* and *Reassign* buttons are visible only if these actions are permitted by the team request rights.

12.2.5 Claiming a Task

To claim a team member's task to work on:

1 Click *Claim*.



Task Detail

* - indicates required.

Resource:	Enable Active Directory Account	Recipient:	Allison Blake
Requested By:	Margo MacKenzie	Task:	Manager Approval
In Queue since:	12/06/2006 01:07:45 PM	Timeout on:	12/08/2006 01:07:45 PM
Assigned To:	Margo MacKenzie	Claimed By:	

Form Detail

Manager Approval

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

Requested by: Margo MacKenzie Recipient: Allison Blake

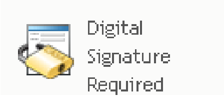
Request Date: 12/06/2006

Reason: test

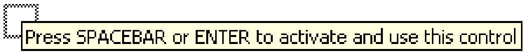
Comment:

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.

If the resource 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.



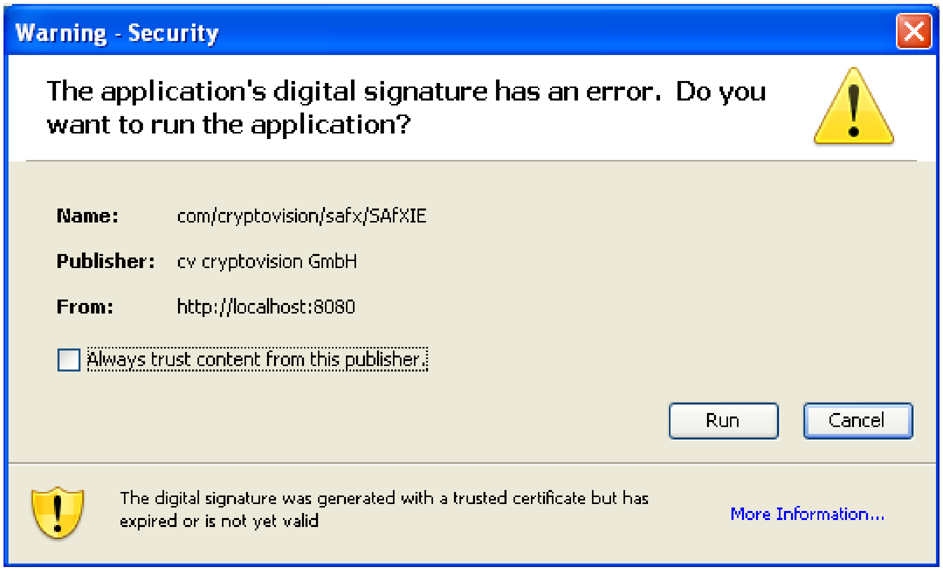
Press SPACEBAR or ENTER to activate and use this control

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.


Warning - Security

The application's digital signature has an error. Do you want to run the application?

Name: com/cryptovision/safx/SAfXIE

Publisher: cv cryptovision GmbH

From: http://localhost:8080

□ Always trust content from this publisher.

The digital signature was generated with a trusted certificate but has expired or is not yet valid

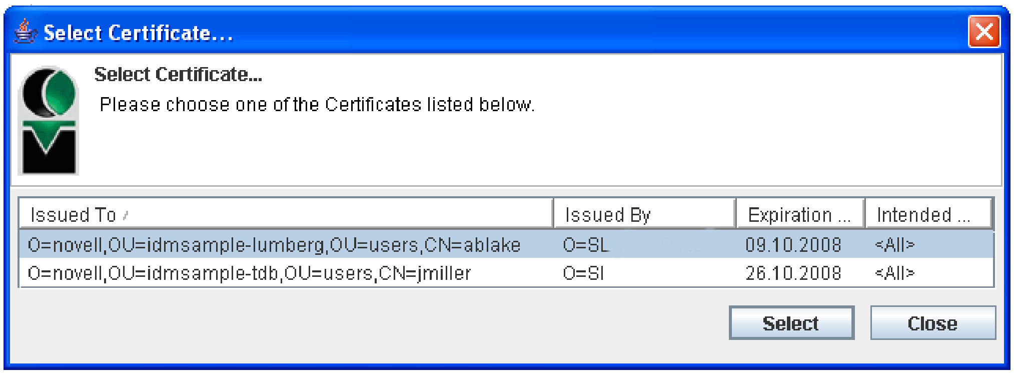
2c Click *Run* to proceed.

2d Fill in the fields in the approval form. The fields on the form vary depending on which resource you requested.

2e Click the 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).

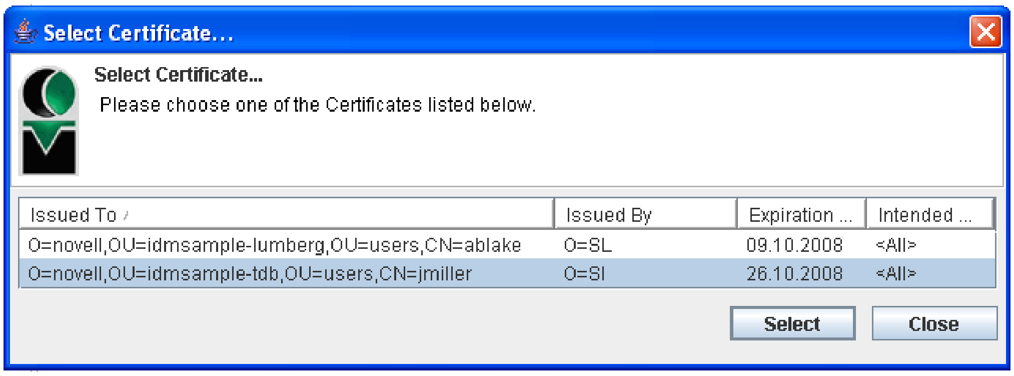

Select Certificate...

Select Certificate...

Please choose one of the Certificates listed below.

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*.



Select Certificate...

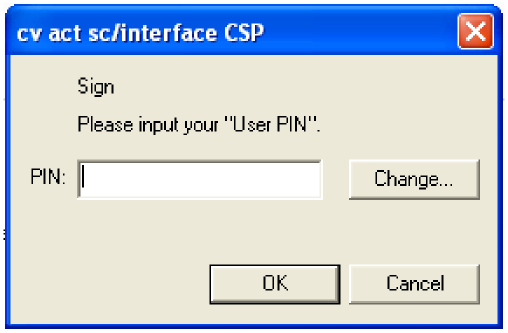
Please choose one of the Certificates listed below.

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>

2g 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.

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.



Sign

Please input your "User PIN".

PIN:

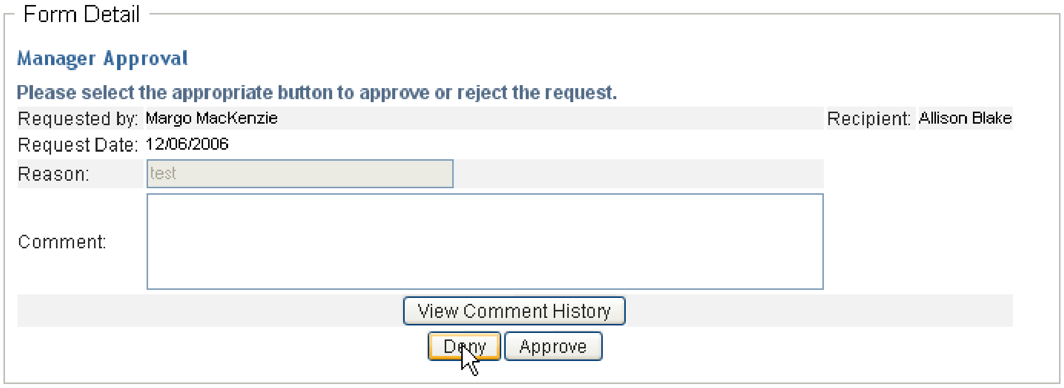
If your administrator has enabled the ability to preview the user agreement, the *Preview* button is enabled.

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 the request, click *Deny*.



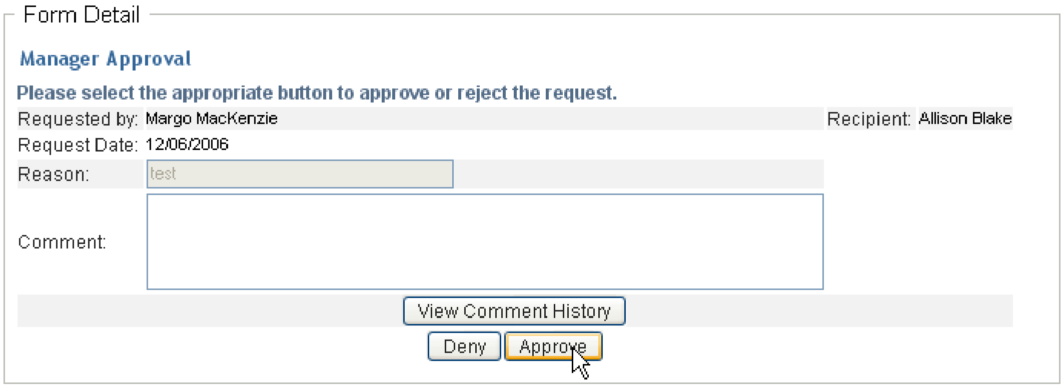
Form Detail

Manager Approval

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

Requested by:	Margo MacKenzie	Recipient:	Allison Blake
Request Date:	12/06/2006		
Reason:	test		
Comment:			

4 To approve the request, click *Approve*.



Form Detail

Manager Approval

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

Requested by: Margo MacKenzie Recipient: Allison Blake

Request Date: 12/06/2006

Reason: test

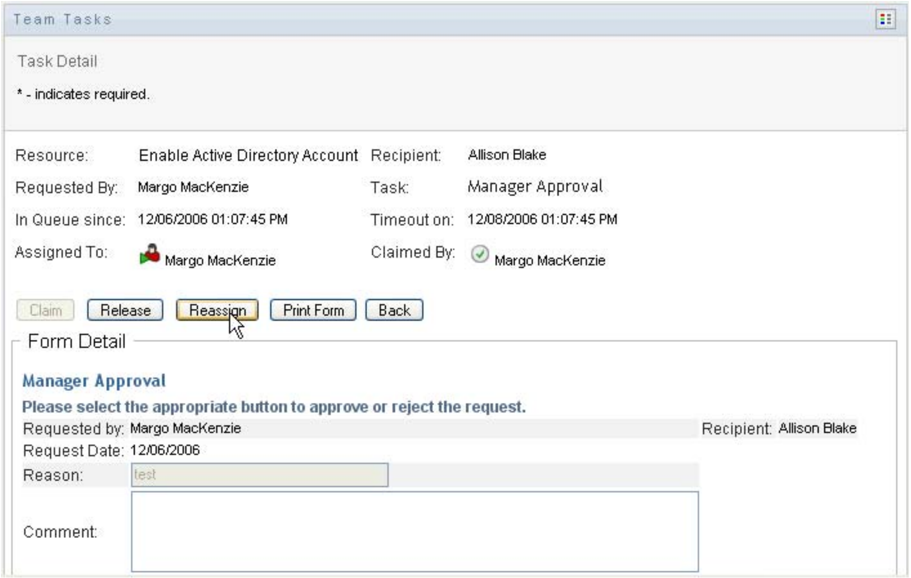
Comment:

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

12.2.6 Reassigning a Task

To reassign a team member's task:

1 Click *Reassign* in the Team Tasks task detail window.



Team Tasks

Task Detail

* - indicates required.

Resource: Enable Active Directory Account Recipient: Allison Blake

Requested By: Margo MacKenzie Task: Manager Approval

In Queue since: 12/06/2006 01:07:45 PM Timeout on: 12/08/2006 01:07:45 PM

Assigned To: Margo MacKenzie Claimed By: Margo MacKenzie

Form Detail

Manager Approval

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

Requested by: Margo MacKenzie Recipient: Allison Blake

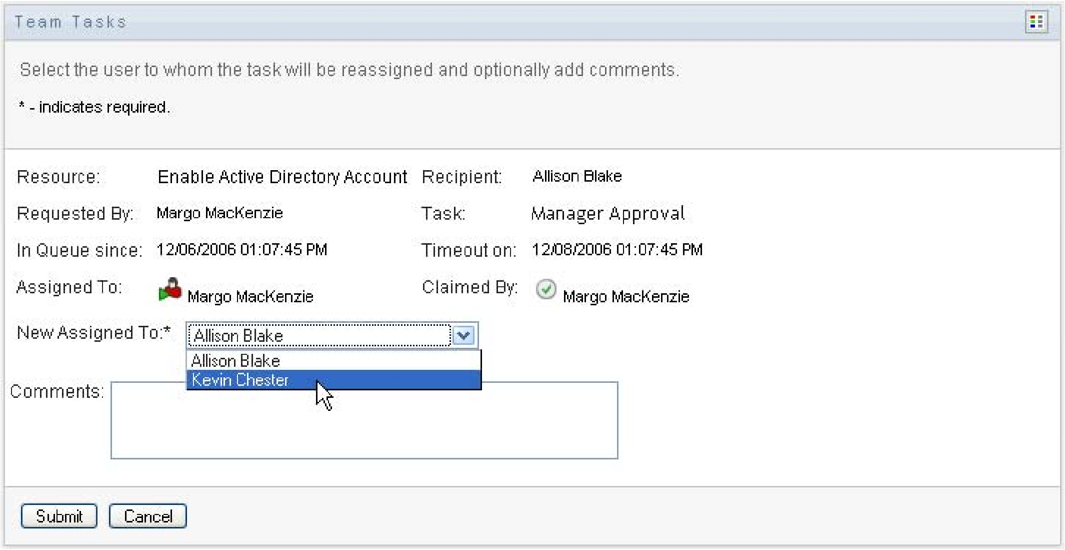
Request Date: 12/06/2006

Reason: test

Comment:

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.



Select the user to whom the task will be reassigned and optionally add comments.

* - indicates required.

Resource:	Enable Active Directory Account	Recipient:	Allison Blake
Requested By:	Margo MacKenzie	Task:	Manager Approval
In Queue since:	12/06/2006 01:07:45 PM	Timeout on:	12/08/2006 01:07:45 PM
Assigned To:	Margo MacKenzie	Claimed By:	✓ Margo MacKenzie

New Assigned To:* Allison Blake

Allison Blake
Kevin Chester

Comments:

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

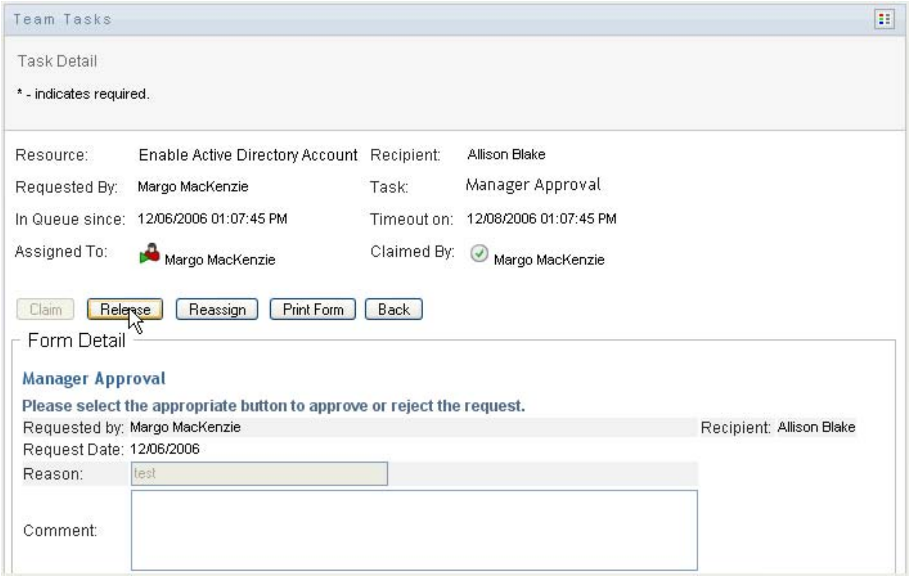
5 Click *Submit*.

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

12.2.7 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 Team Tasks Task Detail window.



Task Detail

* - indicates required.

Resource:	Enable Active Directory Account	Recipient:	Allison Blake
Requested By:	Margo MacKenzie	Task:	Manager Approval
In Queue since:	12/06/2006 01:07:45 PM	Timeout on:	12/08/2006 01:07:45 PM
Assigned To:	Margo MacKenzie	Claimed By:	✓ Margo MacKenzie

Form Detail

Manager Approval

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

Requested by: Margo MacKenzie Recipient: Allison Blake

Request Date: 12/06/2006

Reason: test

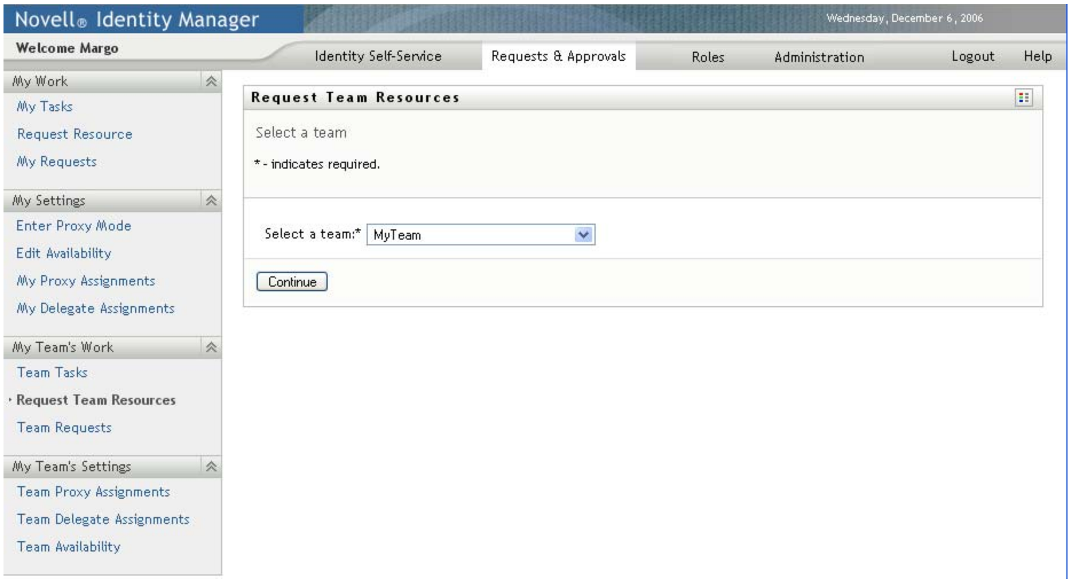
Comment:

12.3 Make Team Requests

The *Request Team Resources* action enables you to request resources for team members.

1 Click *Request Team Resources* in the *My Team's Work* group of actions.

The Request Team Resources page is displayed.



Request Team Resources

Select a team

* - indicates required.

Select a team:* MyTeam

2 Click *Select a team* to select a team for which you have been designated as a team manager. Then click *Continue*.

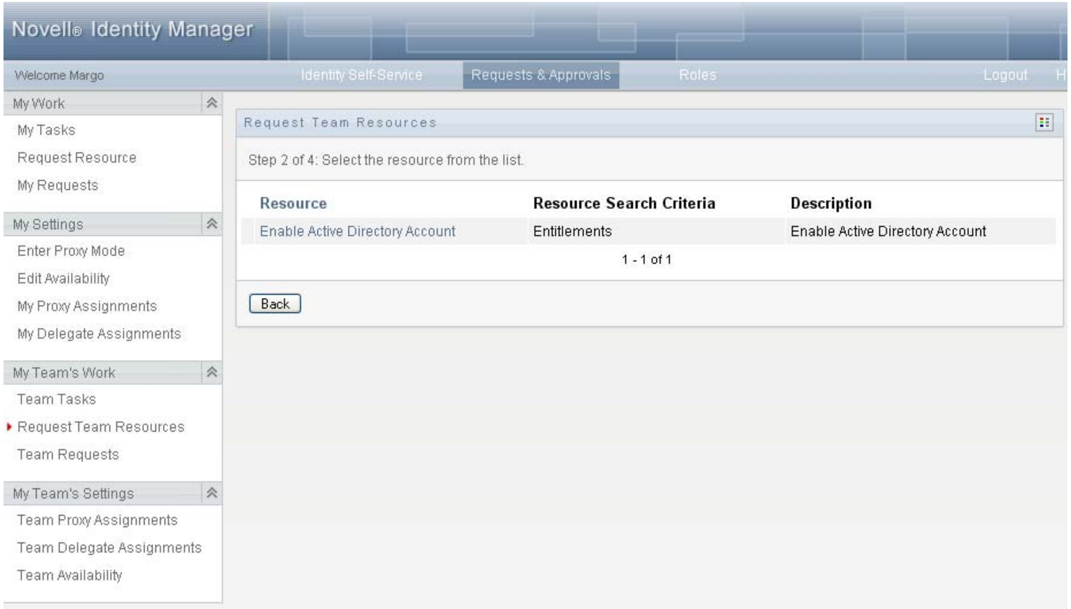
The application displays a page that lets you pick a category.

3 Select the category of the request in the *Type of Request* drop-down list. Select *All* to include requests from all available categories.

The list of categories available depends on the team request rights. If the provisioning request scope for the team does not include resource categories, the category list is not displayed. In this case, skip to the next step to select a resource.

4 Click *Continue*.

The Request Team Resources page displays a list of resources that you can request. The list includes only those resources for which team managers are permitted to initiate requests.



Request Team Resources

Step 2 of 4: Select the resource from the list.

Resource	Resource Search Criteria	Description
Enable Active Directory Account	Entitlements	Enable Active Directory Account

1 - 1 of 1

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.

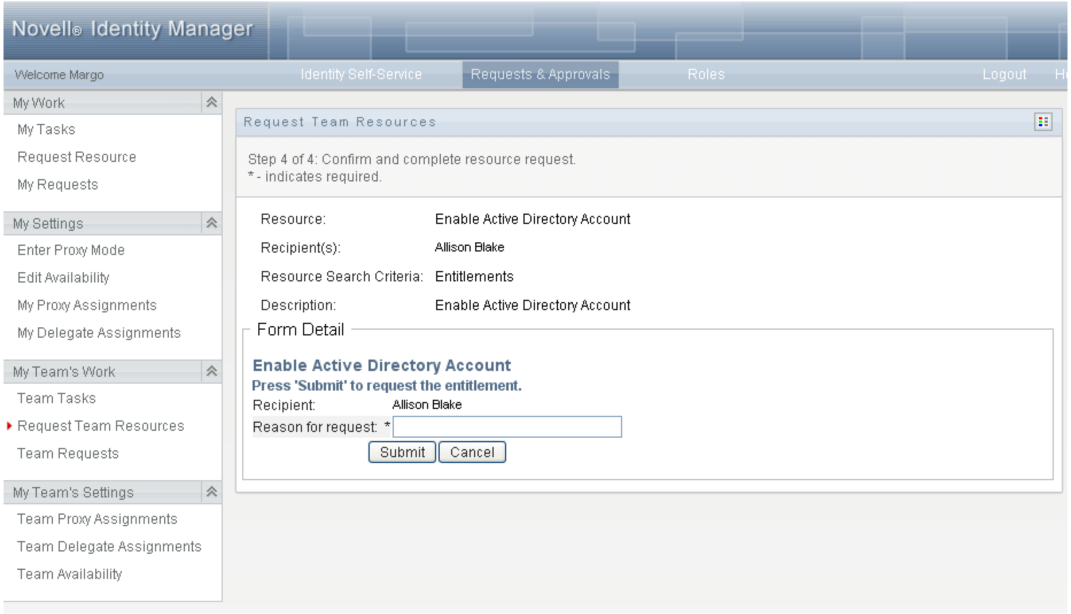
Depending on how the team was defined, you might see an *Object Selector* icon 🔍 beside the *Recipient* selection box, instead of a list of team members. In this case, click the icon to open the Object Lookup window. Specify search criteria for the team member, click *Search,* and select the team member.

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 Request Team Resources 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 resource you requested.



Request Team Resources

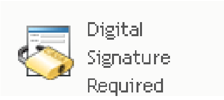
Step 4 of 4: Confirm and complete resource request.
* - indicates required.

Resource: Enable Active Directory Account
Recipient(s): Allison Blake
Resource Search Criteria: Entitlements
Description: Enable Active Directory Account

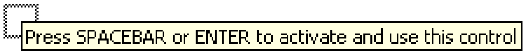
Form Detail

Enable Active Directory Account
Press 'Submit' to request the entitlement.
Recipient: Allison Blake
Reason for request: *

If the resource you've requested requires a digital signature, the *Digital Signature Required* icon appears in the upper right corner of the page.


Digital Signature Required

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:

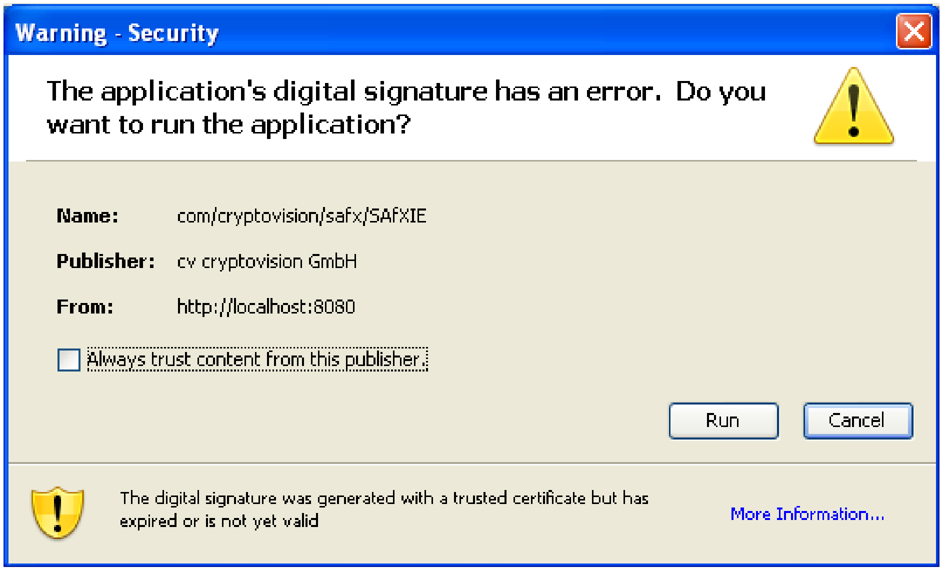

Press SPACEBAR or ENTER to activate and use this control

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.


Warning - Security

The application's digital signature has an error. Do you want to run the application?

Name: com/cryptovision/safx/SAfXIE

Publisher: cv cryptovision GmbH

From: http://localhost:8080

□ Always trust content from this publisher.

The digital signature was generated with a trusted certificate but has expired or is not yet valid

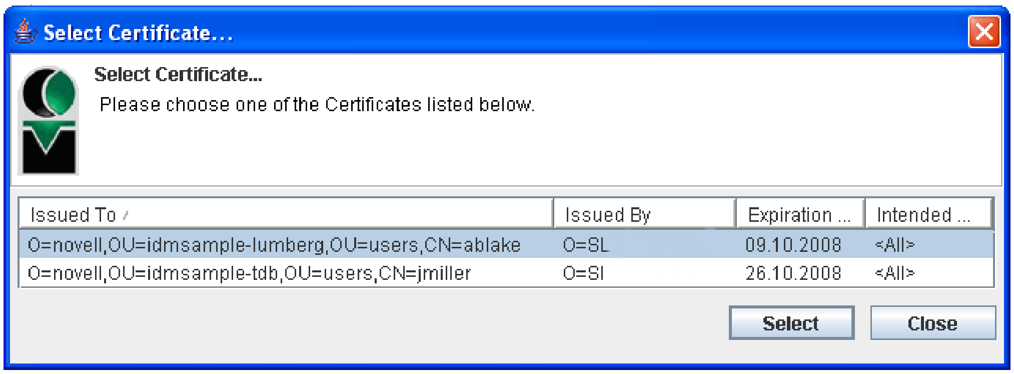
9c Click *Run* to proceed.

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).

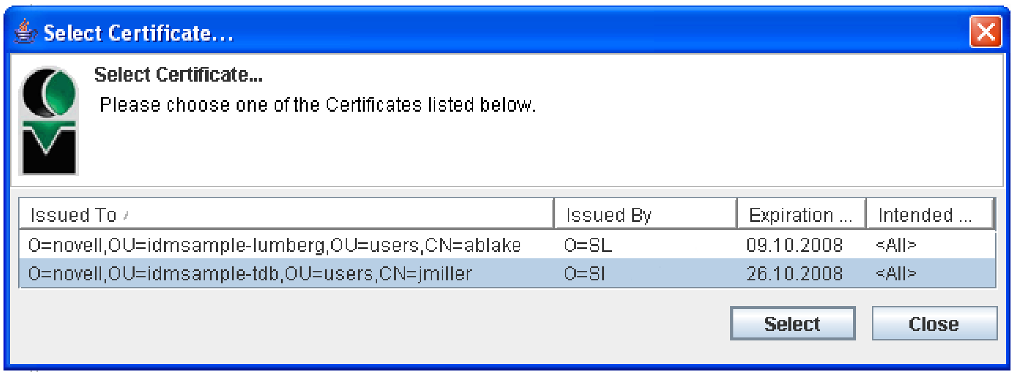

Select Certificate...

Select Certificate...

Please choose one of the Certificates listed below.

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*.



Select Certificate...

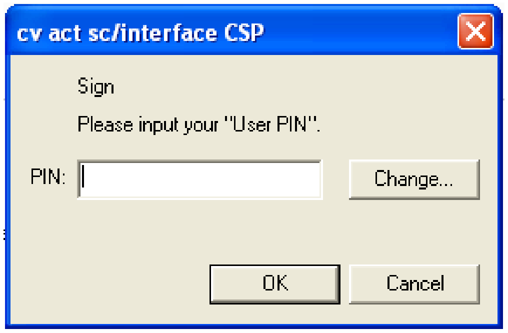
Please choose one of the Certificates listed below.

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>

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.



Sign

Please input your "User PIN".

PIN:

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 Request Team Resources 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.

12.4 Managing Your Team's Requests

The Team Requests action allows team managers and the Provisioning Application Administrator to view the status and history of resource requests and can retract resource requests.

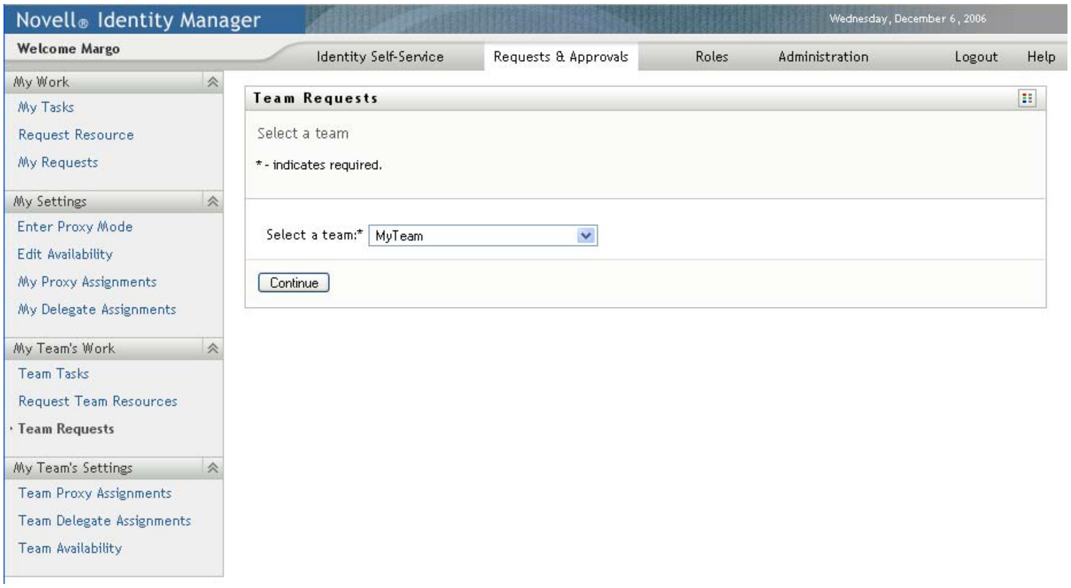
NOTE: The *Team Requests* action does not display role or attestation requests. To see the status of a role request, you need to use the *View Request Status* action on the *Roles* tab. To see the status of an attestation request, you need to use the *View Attestation Request Status* action on the *Compliance* tab.

1 Click *Team Requests* in the *My Team's Work* 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 Application Administrator, you do not see the *Select a team* box.

The Provisioning Application Administrator cannot filter the list of team requests by container or group. The administrator must select team members individually.



Team Requests

Select a team

* - indicates required.

Select a team:* MyTeam

3 Click *Continue*.

The Request Team Resources page prompts you to select a *Team Member*, a *Type of Request* (a category), and a *Request Date* filter.

4 Click a *Team Member* name to select it.

Depending on how the team was defined, you might see an *Object Selector* icon 🔍 beside the *Team Member* 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.

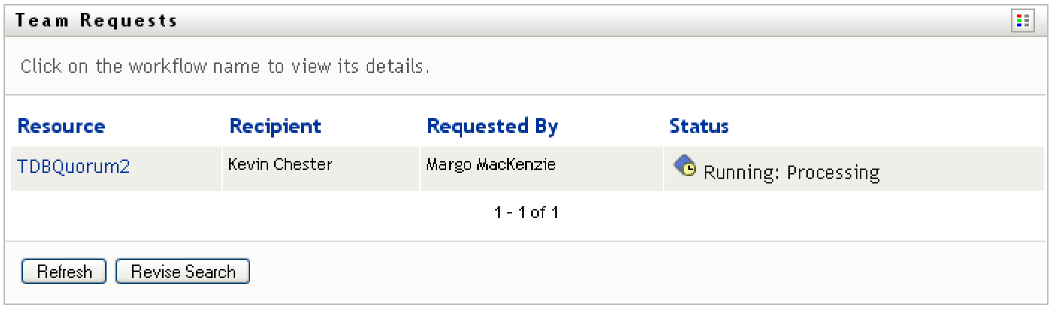
5 After you select a team member, you can select the *Type of Request* (category) and a *Request Date* filter. Click *Continue*.

The Team Requests page lists:

- Each requested resource
- Who is to receive it

- Who requested it
- Status of the request

The team requests are displayed. The list of requests includes only those requests available to the team.



Team Requests

Click on the workflow name to view its details.

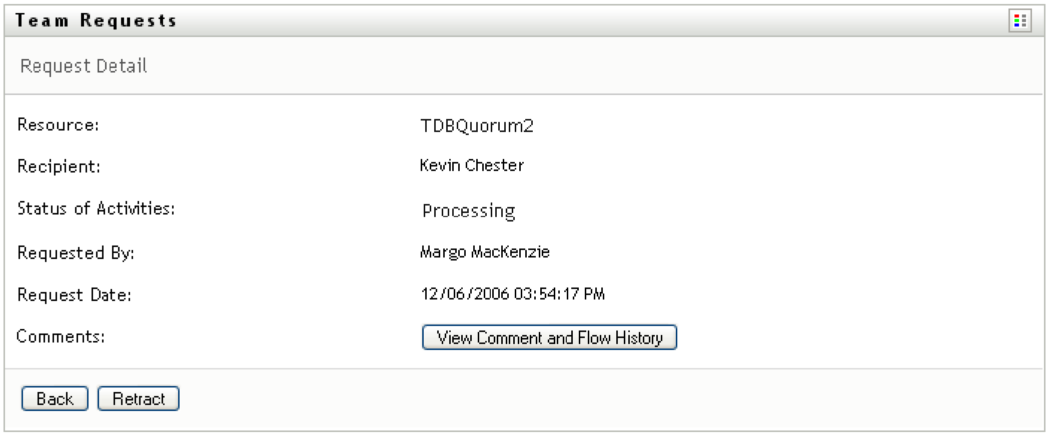
Resource	Recipient	Requested By	Status
TDBQuorum2	Kevin Chester	Margo MacKenzie	Running: Processing

1 - 1 of 1

6 To view the details of a request, click the request name in the list.

The Request Detail page displays details such as

- Name of resource
- Recipient of resource
- Status of activities supporting the request
- Who requested the resource
- When the request was made
- Comments



Team Requests

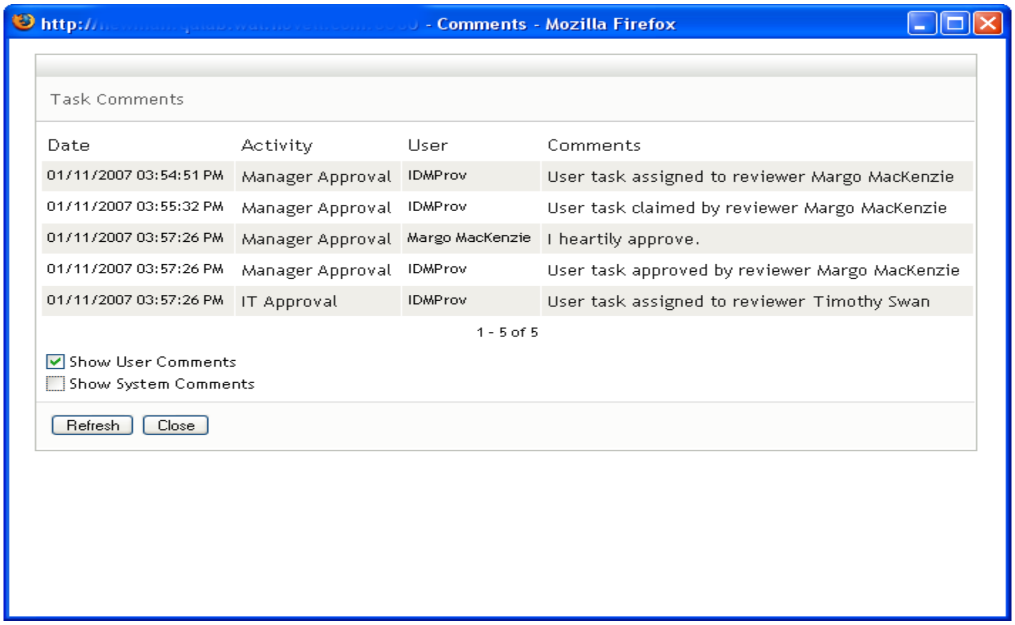
Request Detail

Resource:	TDBQuorum2
Recipient:	Kevin Chester
Status of Activities:	Processing
Requested By:	Margo MacKenzie
Request Date:	12/06/2006 03:54:17 PM
Comments:	View Comment and Flow History

7 To view comment history for the request, click *View Comment and Flow 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.

7a To display user comments, click *Show User Comments*.



Task Comments

Date	Activity	User	Comments
01/11/2007 03:54:51 PM	Manager Approval	IDMProv	User task assigned to reviewer Margo MacKenzie
01/11/2007 03:55:32 PM	Manager Approval	IDMProv	User task claimed by reviewer Margo MacKenzie
01/11/2007 03:57:26 PM	Manager Approval	Margo MacKenzie	I heartily approve.
01/11/2007 03:57:26 PM	Manager Approval	IDMProv	User task approved by reviewer Margo MacKenzie
01/11/2007 03:57:26 PM	IT Approval	IDMProv	User task assigned to reviewer Timothy Swan

1 - 5 of 5

☑ Show User Comments

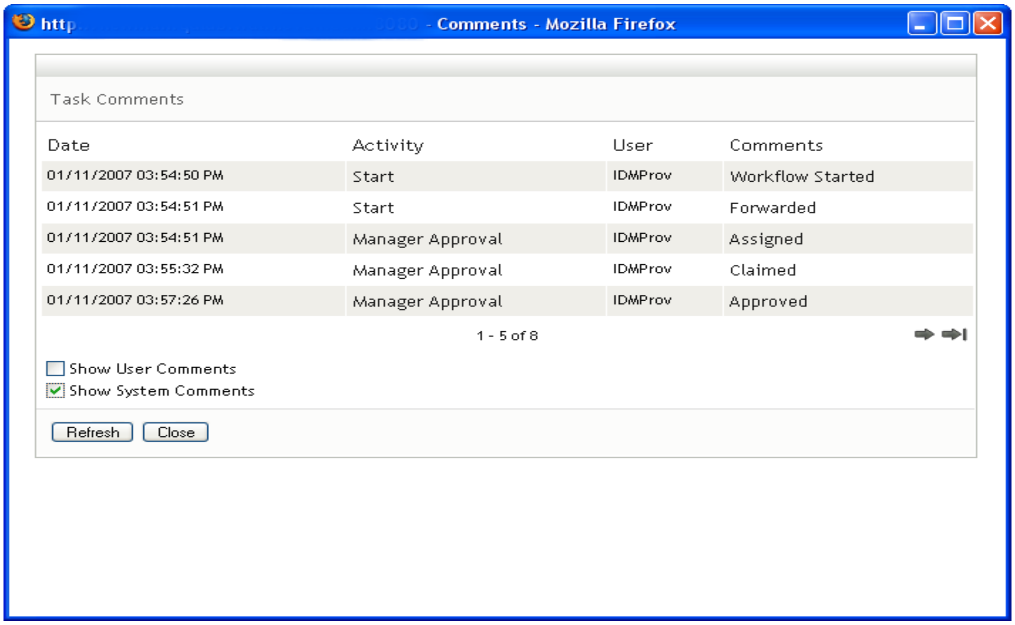
□ Show System Comments

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.novell.com/documentation/idmrbpm361/index.html)

7b To display system comments, click *Show System Comments*.



Task Comments

Date	Activity	User	Comments
01/11/2007 03:54:50 PM	Start	IDMProv	Workflow Started
01/11/2007 03:54:51 PM	Start	IDMProv	Forwarded
01/11/2007 03:54:51 PM	Manager Approval	IDMProv	Assigned
01/11/2007 03:55:32 PM	Manager Approval	IDMProv	Claimed
01/11/2007 03:57:26 PM	Manager Approval	IDMProv	Approved

1 - 5 of 8

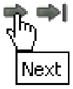
□ Show User Comments
☑ Show System Comments

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, `IDMProv`) 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.

7c 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.



7d Click *Close* to close the window.

8 To retract the request, click *Retract* on the Request Detail page. *Retract* is enabled for running processes. In processes that are no longer running, *Retract* is disabled.

The *Retract* button is not displayed unless team managers have been given permission to retract requests in the team request rights.

Configuring Your Team's Provisioning Settings

13

This section tells you how to use the *My Team's Settings* actions on the *Requests & Approvals* tab of the Identity Manager user interface. Topics include:

13.1 About the My Team's Settings Actions

The *Requests & Approvals* tab in the Identity Manager User Application includes a group of actions called *My Team's Settings*. The *My Team's Settings* actions let you:

- Create, view, and modify the current proxy assignments for your team.
- Create, view, and modify the current delegate assignments for your team.
- Define and view team members' availability for delegate assignments.

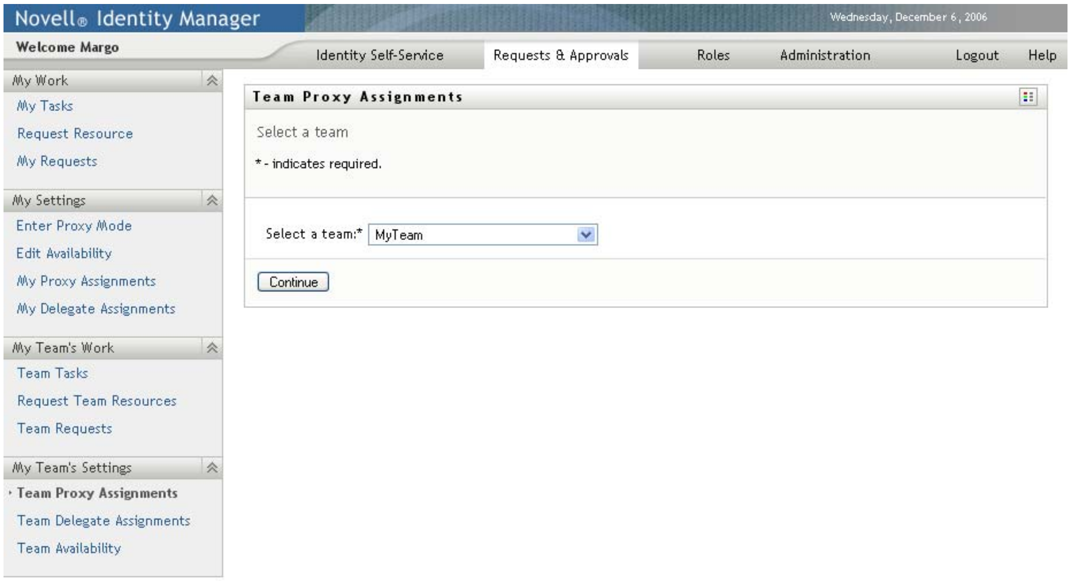
13.2 Viewing and Editing Your Team's Proxy Assignments

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. The authority to define proxies is determined by the team definition.
- The people whom you specify as proxies must also be within your team.
- The Provisioning Application Administrator has the ability to set proxies for any user, group, or container in the organization.

To assign a proxy for a team member:

1 Click *Team Proxy Assignments* in the *My Team's Settings* group of actions.



Team Proxy Assignments

Select a team

* - indicates required.

Select a team:* MyTeam

2 Click *Select a team* to select a team for which you have been designated as a team manager.

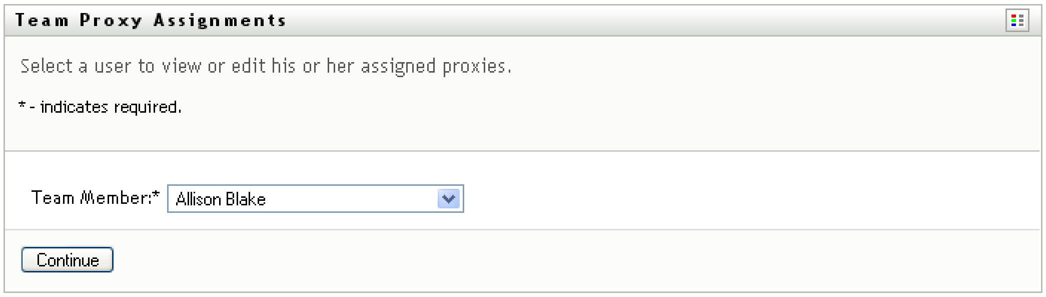
If you are a Provisioning Application Administrator, you do not see the *Select a team* box.

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 Click a *Team Member* name to select it.

Depending on how the team was defined, you might see an *Object Selector* icon 🔍 beside the *Team Member* 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.



Team Proxy Assignments

Select a user to view or edit his or her assigned proxies.

* - indicates required.

Team Member:* Allison Blake

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**
User	Select the team member for whom you want to assign a proxy. You can select multiple users.
Proxy Assigned	Select the team member who is to act as proxy.
Notify other users of these changes	Indicates whether you want to send an e-mail message to notify one or more users of this proxy assignment.
Addressee	Specifies which users should receive e-mail notifications: **All:** 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. **Assign From:** Specifies that only the team member(s) for whom the proxy has been assigned receives an e-mail notification. **Assign To:** Specifies that only the team member who is to act as proxy receives an e-mail notification. **Selective:** Allows you to send e-mail notifications to any users you select, including users who are not on the team.
Expiration	**No Expiration:** Select *No Expiration* if you want the proxy assignment to remain in effect until it is removed or modified. **Specify Expiration:** Select *Specify Expiration* to define an *End Date*. 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 *My Team's 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 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.

If you are a Provisioning Application Administrator, you do not see the *Select a team* box.

3 Click *Continue*.

4. Click a *Team Member* name to select it.

   Depending on how the team was defined, you might see an *Object Selector* icon 🔍 beside the *Team Member* 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.

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**
User	Select the team member for whom you want to assign a proxy. You can select multiple users.
Proxy Assigned	Select the team member who is to act as proxy.
Notify other users of these changes	Indicates whether you want to send an e-mail message to notify one or more users of this proxy assignment.
Addressee	Specifies which users should receive e-mail notifications: **All:** Specifies that the user assigned as proxy, as well as the team member for whom the proxy has been assigned, receives e-mail notifications. **Assign From:** Specifies that only the team member(s) for whom the proxy has been assigned receives an e-mail notification. **Assign To:** Specifies that only the team member who is to act as proxy receives an e-mail notification. **Selective:** Allows you to send e-mail notifications to any users you select, including users who are not on the team.
Expiration	**No Expiration:** Select *No Expiration* if you want the proxy assignment to remain in effect until it is removed or modified. **Specify Expiration:** Select *Specify Expiration* to define an *End Date*. 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 *My Team's 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.

13.3 Viewing and Editing Your Team's Delegate Assignments

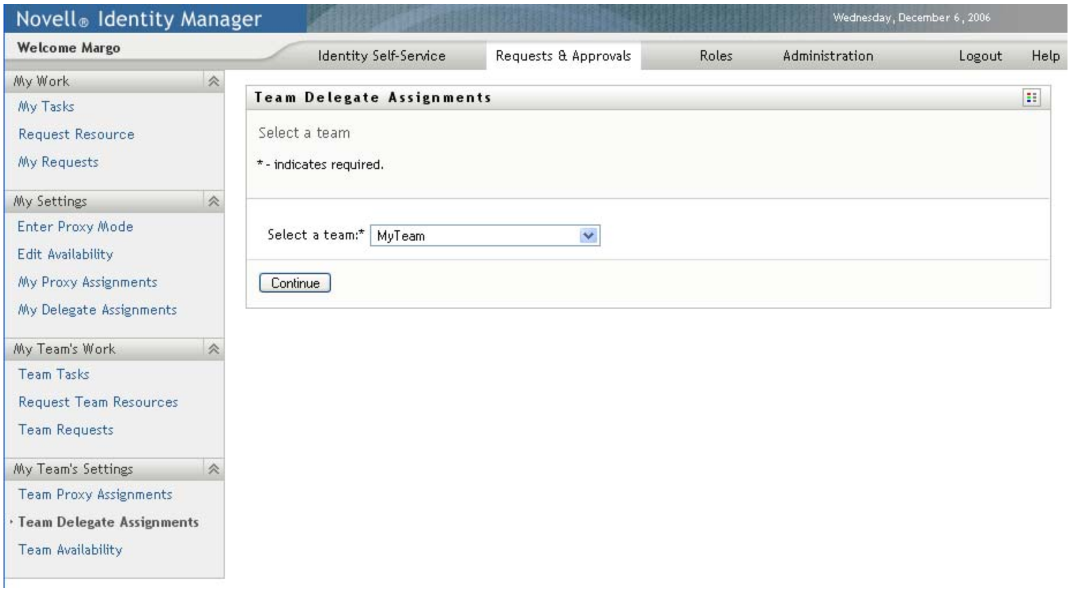
The *Team Delegate Assignments* action allows you to manage the delegate assignments for team members. The rules for defining delegates are as follows:

- 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.
- The people whom you specify as delegates must also be within your team.
- The Provisioning Application Administrator has the ability to define delegate assignments for any user, group, or container in the organization.

To define a delegate assignment:

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.



Team Delegate Assignments

Select a team

* - indicates required.

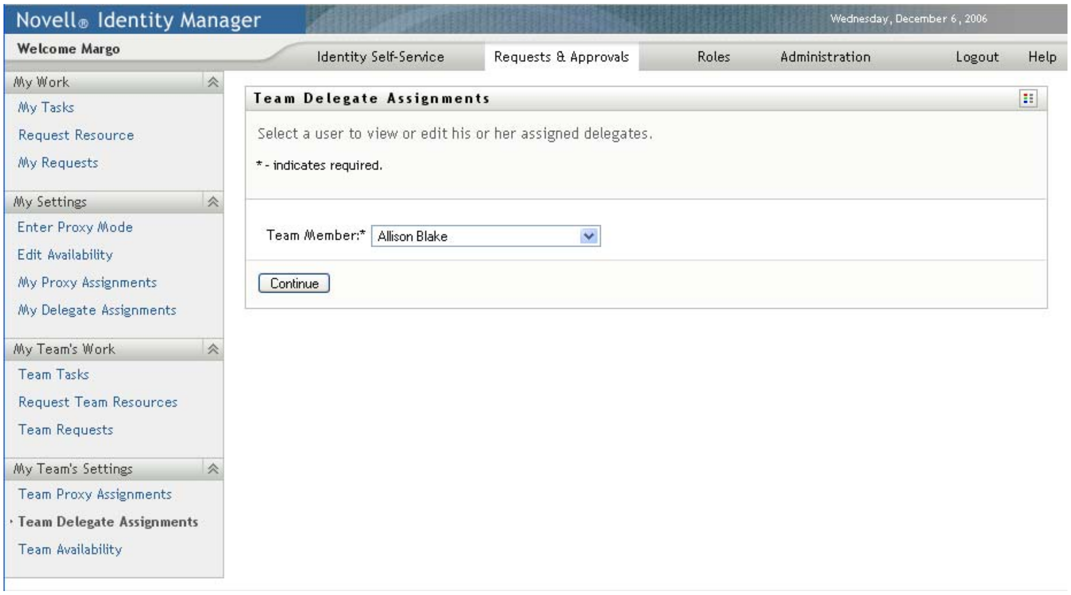
Select a team:* MyTeam

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 Click a *Team Member* name to select it.



Team Delegate Assignments

Select a user to view or edit his or her assigned delegates.

* - indicates required.

Team Member:* Allison Blake

Depending on how the team was defined, you might see an *Object Selector* icon beside the *Team Member* 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.

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
User	Select one or more users whose work you want to delegate.
Assignment Type	Assign the user who can perform the delegated work by selecting one of the following: ◆ **Assign Delegate:** Select a user from the list. ◆ **Assign by Relationship:** Select the delegate relationship from the drop-down list.

Field	Description
Notify other users of these changes	Indicates whether you want to send an e-mail message to notify one or more users of this delegate assignment.
Addressee	Specifies which users should receive e-mail notifications: **All:** Specifies that the user assigned as delegate, as well as the team member for whom the delegate has been assigned, receives e-mail notifications. **Assign From:** Specifies that only the team member(s) for whom the delegate has been assigned receives an e-mail notification. **Assign To:** Specifies that only the team member who is to act as delegate receives an e-mail notification. **Selective:** Allows you to send e-mail notifications to any users you select, including users who are not on the team.
Expiration	**No Expiration:** Select *No Expiration* if you want the delegation to remain in effect until it is removed or modified. This, in effect, makes the delegation permanent. **Specify Expiration:** Select *Specify Expiration* to define an *End Date*. Click the Calendar and select a date and time when the delegate assignment expires.
Type of Request	Select a category from the list. This populates the list of *Available Requests* in *Selected Category*.
Available Requests in Selected Category	Select one or more resource requests from this list and click *Add*.
Selected Requests	This list shows the resource request types that have been delegated. To remove a request type, select it from the list and click *Remove*.

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. Click a *Team Member* name to select it.

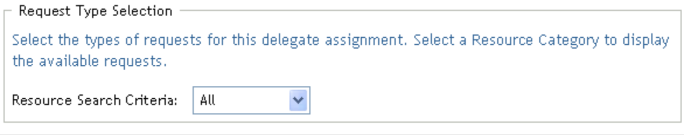
   Depending on how the team was defined, you might see an *Object Selector* icon 🔍 beside the *Team Member* selection box, instead of a list of team members. In this case, click the icon to open the Object Lookup window. Specify search criteria for the team member, click *Search,* and select the team member.

   The 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
User	Select one or more users whose work you want to delegate.
Assignment Type	Assign the user who can perform the delegated work by selecting one of the following: ◆ **Assign Delegate:** Select a user from the list. ◆ **Assign by Relationship:** Select the delegate relationship from the drop-down list.
Notify other users of these changes	Indicates whether you want to send an e-mail message to notify one or more users of this delegate assignment.
Addressee	Specifies which users should receive e-mail notifications: **All:** Specifies that the user assigned as delegate, as well as the team member for whom the delegate has been assigned, receives e-mail notifications. **Assign From:** Specifies that only the team member for whom the delegate has been assigned receives an e-mail notification. **Assign To:** Specifies that only the team member who is to act as delegate receives an e-mail notification. **Selective:** Allows you to send e-mail notifications to any users you select, including users who are not on the team.
Expiration	**No Expiration:** Select *No Expiration* if you want the delegation to remain in effect until it is removed or modified. This, in effect, makes the delegation permanent. **Specify Expiration:** Select *Specify Expiration* to define an *End Date*. Click the Calendar and select a date and time when the delegate assignment expires.
Type of Request	Select a category from the list. This populates the list of *Available Requests* in *Selected Category*. To specify that this delegate assignment applies to all categories, set the type of request for the delegate assignment to *All*.  Request Type Selection Select the types of requests for this delegate assignment. Select a Resource Category to display the available requests. Resource Search Criteria: All **NOTE:** The All option is available only if the Provisioning Administrator has enabled the Allow All Requests option for your application.

Field	Description
Available Requests in Selected Category	Select one or more resource requests from this list and click *Add*. 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.
Selected Requests	This list shows the resource request types that have been delegated. To remove a request type, select it from the list and click *Remove.*

8 Click *Submit* to save your selections.

To delete a delegate assignment:

1 Click *Team Delegate Assignments* in the *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.

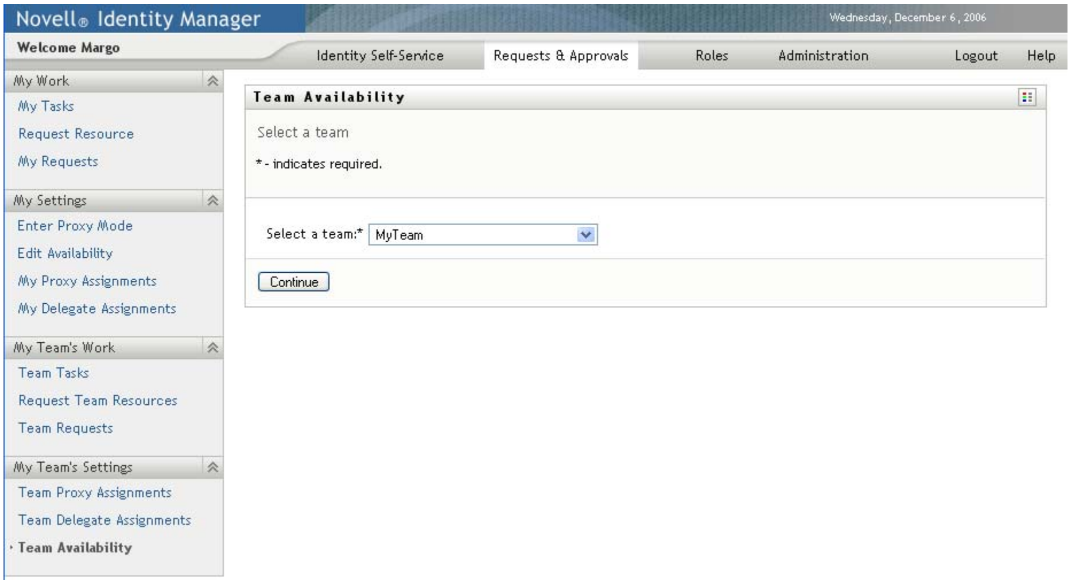
13.4 Specifying Your Team's Availability

The *Team Availability* action allows you to specify the resource requests your team members are not available to work on. During the time period when you or your team members are not available, any resource requests of that type are forwarded to the delegate's queue.

You can specify availability for each resource request individually or globally. You can only specify the availability for users who have delegates already assigned.

1 Click *Team Availability* in the *My Team's 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:* MyTeam

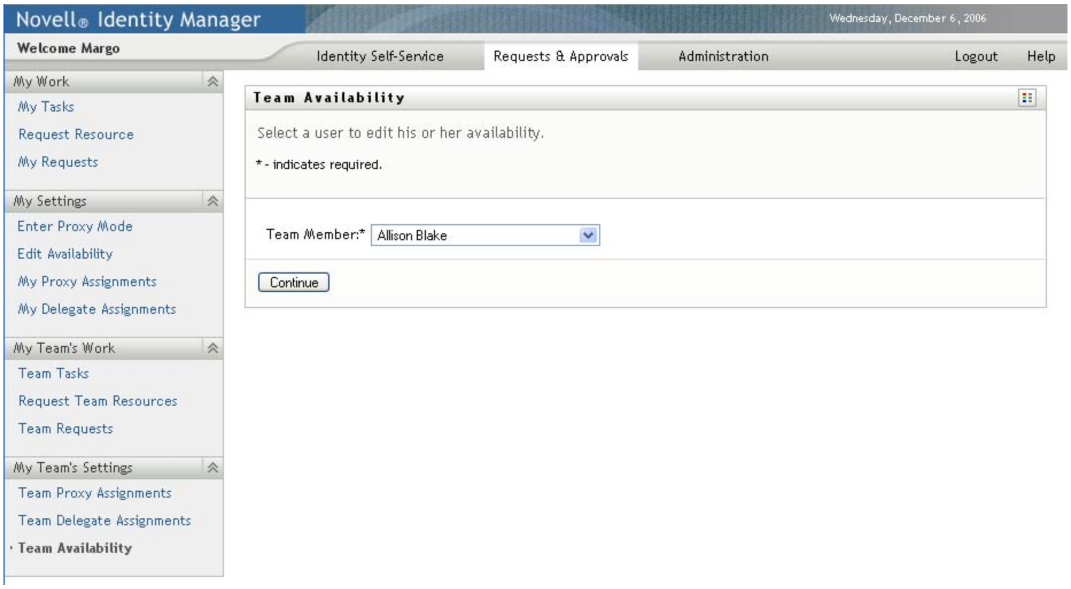
The list of teams includes teams for which team managers are permitted to define availability (specified in the team definition), as well as teams for which the ability to define availability has been disabled. If the team definition does not permit team managers to define availability, the manager can 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.

If you are a Provisioning Application Administrator, you do not see the *Select a team* box.

3 Click *Continue*.

4 Click a *Team Member* name to select it, and click *Continue*.

Depending on how the team was defined, you might see an *Object Selector* icon 🔍 beside the *Team Member* 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.



Team Availability

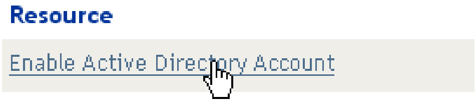
Select a user to edit his or her availability.

* - indicates required.

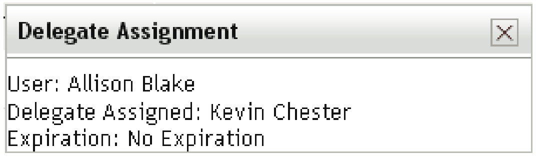
Team Member:* Allison Blake

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:



The page then displays a pop-up window that provides information about the delegate assignment:



Delegate Assignment

User: Allison Blake
Delegate Assigned: Kevin Chester
Expiration: No Expiration

This information is particularly helpful in situations where the same resource name appears more than once in the availability settings list.

6 Click *New*.

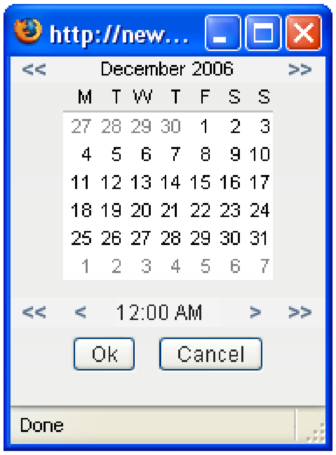
The *New* button is enabled only for those teams for which team managers are permitted to define availability settings for team members.

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. **NOTE:** If you change the status and then change it back to *Available for ALL Requests*, any *Selectively Available* settings previously defined are removed.
NOT Available for ANY Requests	Specifies that the team member is not available for any resource requests currently in the system. (This is also known as globally unavailable.) Choosing this status indicates that the team member is unavailable for each existing delegate assignment and changes the current status to *Not Available for Specified Requests*. Assignments are effective immediately and last until the delegate assignment expires. **NOTE:** This setting does not affect availability for new assignments created after this point.
NOT Available for Specified Requests	When you select this option, you are prompted to specify the team member's availability. (This is the same as clicking the *New* button.) You'll be prompted to specify: ◆ The types of requests the team member is not available for. ◆ The time period when the team member is unavailable. 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.

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.



M	T	W	T	F	S	S
27	28	29	30	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	31
1	2	3	4	5	6	7

8b Specify when the time period ends by clicking one of the following:

Button	Description
No Expiration	Indicates that this unavailability setting does not expire.
Specify Duration	Lets you specify the time period in weeks, days, or hours.
Specify End Date	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.

9 Specify whether you want to send e-mail notifications to other users by filling in these fields:

Field	Description
Notify other users of these changes	Indicates whether you want to send an e-mail message to notify one or more users of this availability assignment.
Addressee	Specifies which users should receive e-mail notifications: **Selective:** Allows you to send e-mail notifications to any users you select, including users who are not on the team.

10 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.

11 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*.

12 To remove a request from the list, click *Remove*.

13 Click *Submit* to save your changes.

Using the Roles Tab

IV

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

Introducing the Roles Tab

14

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

For more general information about accessing and working with the Identity Manager user interface, see Chapter 1, "Getting Started," on page 15.

14.1 About the Roles Tab

The purpose of the *Roles* 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. Role assignments can be mapped to resources within a company, such as user accounts, computers, and databases. For example, you might use the *Roles* tab to:

- Make role 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 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 role 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.

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* tab for you and the others in your organization. The flow of control for a roles-based workflow or separation of duties 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.

Roles and Proxy mode

Proxy mode works only on the *Requests & Approvals* tab and is not supported on the *Roles* tab. If you enter proxy mode on the *Requests & Approvals* tab, and then switch to the *Roles* tab, proxy mode is turned off for both tabs.

14.1.1 About Roles

This section provides an overview of terms and concepts used in the *Roles* tab:

- "Roles and Role Assignments" on page 204
- "Roles Catalog and Role Hierarchy" on page 204
- "Separation of Duties" on page 206
- "Roles Reporting and Auditing" on page 206
- "Roles Security" on page 207
- "Role Service Driver" on page 208

Roles and Role Assignments

A *role* defines a set of permissions related to one or more target systems or applications. The *Roles* tab allows users to request *role assignments*, which are associations between a role and a user, group, or container. The *Roles* 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.

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 Roles Subsystem manages the life cycle of the role request. To see which actions have been taken on the request by users or by the Roles Subsystem, you can check the status of the request on the View Request Status page.

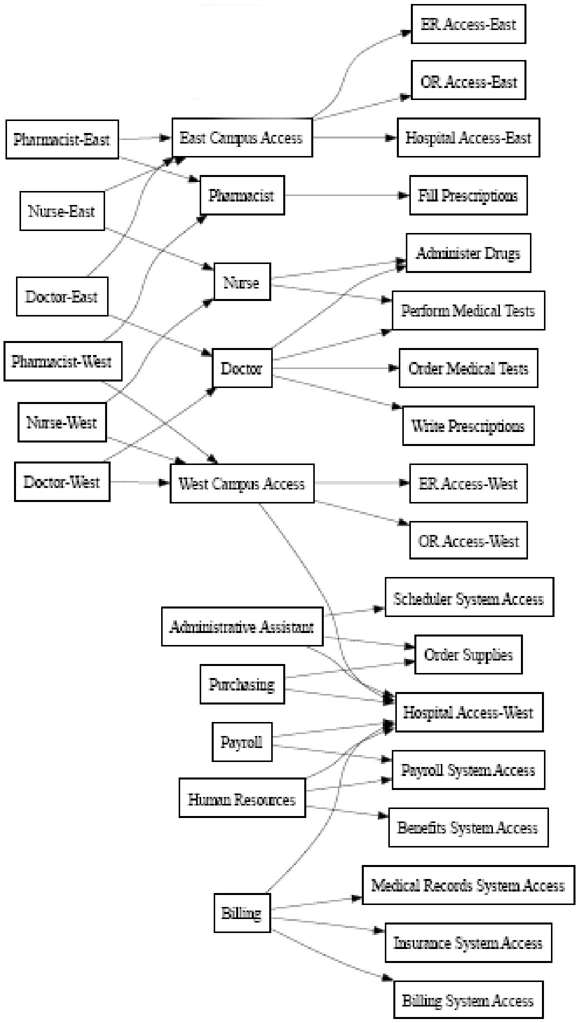
Roles Catalog and Role Hierarchy

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 Roles 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 14-1 *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 Roles 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 Roles 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 Subsystem configuration. However, this list can be overridden in the definition of an SoD constraint.

Roles Reporting and Auditing

The Roles 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 Roles Subsystem can be configured to log events to Novell® Audit.

Roles Security

The Roles Subsystem uses a set of system roles to secure access to functions within the *Roles* tab. Each menu action in the *Roles* 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* 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 Module Administrator
- Roles Manager
- Roles Auditor
- Security Officer

The system roles are described in detail below:

Table 14-1 *System Roles*

Role	Description
Roles Module Administrator	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: ◆ Create, remove, and modify roles. ◆ Modify role relationships for roles. ◆ Request assignment of users, groups or containers to roles. ◆ Create, remove, and modify SoD constraints. ◆ Browse the Role Catalog. ◆ Configure the Roles Subsystem. ◆ View the status of all requests. ◆ Retract role assignment requests. ◆ Run any and all reports.

Role	Description
Roles Manager	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: ◆ Create new roles and modify existing roles to which the user has browse rights. ◆ Modify role relationships for roles to which the user has browse rights. ◆ Request assignment of users, groups, or containers to roles to which the user has browse rights. ◆ Browse the Role Catalog (limited in scope by browse rights). ◆ Browse role assignment requests for users, groups, and containers (limited in scope by directory browse rights to role, user, group, and container objects). ◆ Retract role assignment requests for users, groups, and containers (limited in scope by directory browse rights to role, user, group, and container objects).
Roles Auditor	A system role that allows members to run any reports to which they have directory browse rights.
Security Officer	A system role that allows members to create, remove, or modify SoD constraints. The Security Officer must have browse rights to the SoD constraints.

Authenticated user

In addition to supporting the system roles, the Roles 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 Service Driver

The Roles Subsystem uses the Role 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.

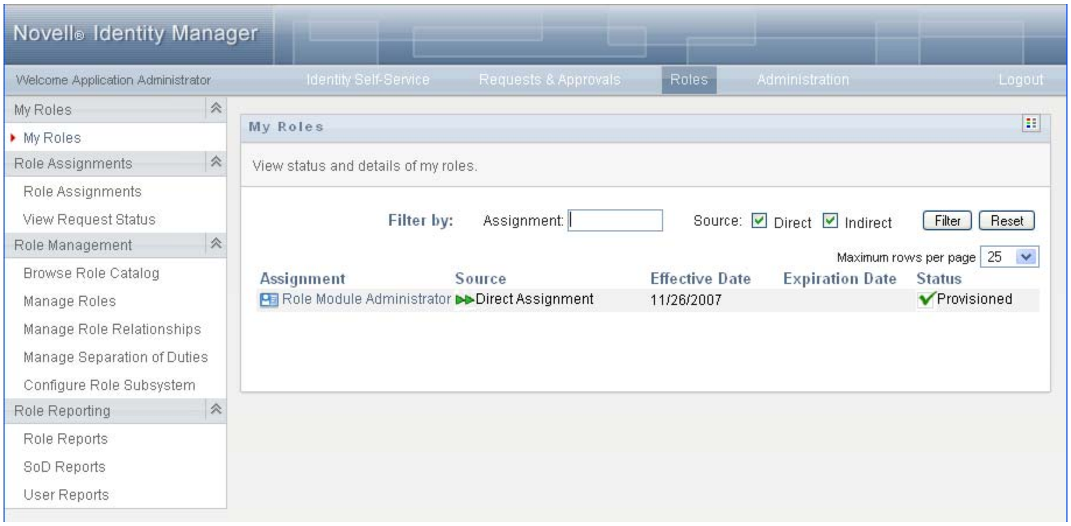
For details on the Role Service driver, see the *Identity Manager User Application: Administration Guide* (http://www.novell.com/documentation/idmrbpm361/index.html).

14.2 Accessing the Roles Tab

To access the *Roles* tab:

1 Click *Roles* in the User Application.

By default, the *Roles* tab opens and displays the My Roles page.



View status and details of my roles.

Filter by: Assignment: Source: ☑ Direct ☑ Indirect

Maximum rows per page 25

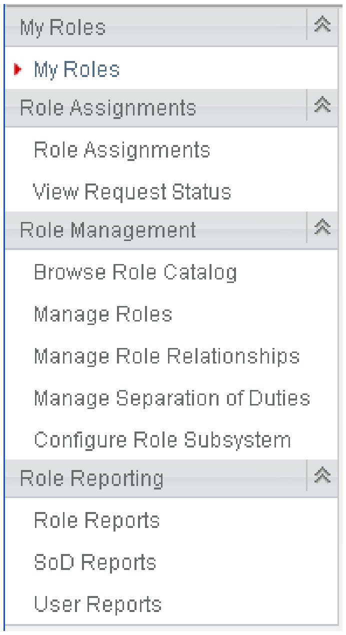
Assignment	Source	Effective Date	Expiration Date	Status
Role Module Administrator	Direct Assignment	11/26/2007		✓Provisioned

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

14.3 Exploring the Tab's Features

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

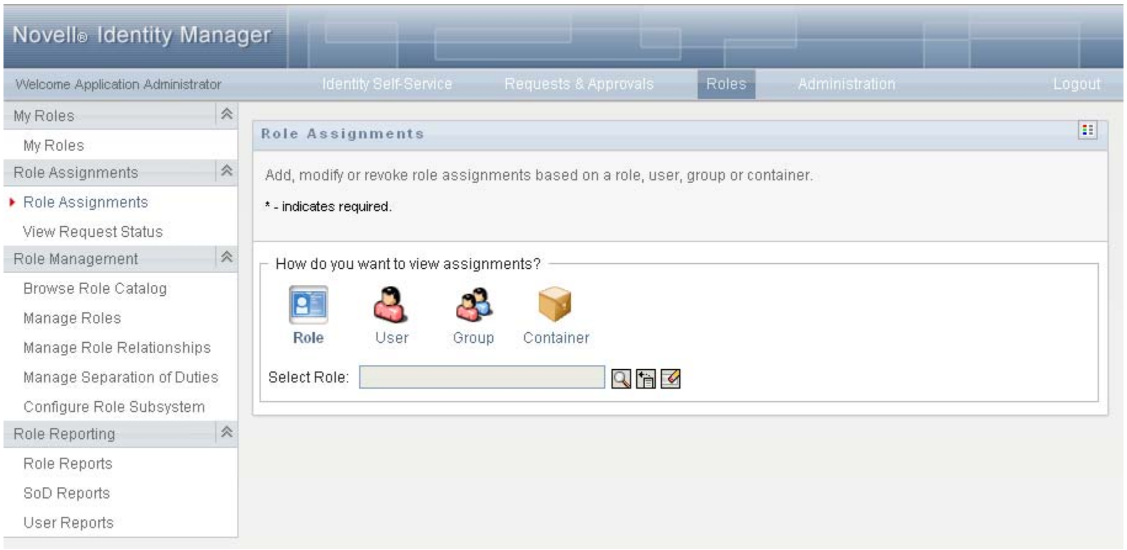
The left side of the *Roles* tab displays a menu of actions you can perform. The actions are listed by category (*My Roles, Role Assignments, Role Management,* and *Role Reporting*):



The *Role Management* actions are only displayed if you are a Role Module Administrator or Role Manager. The *Manage Separation of Duties* action within *Role Management* is only displayed if you are a Role Module Administrator or Security Officer. The *Role Reporting* actions are only displayed if you are a Role Module Administrator or Role Auditor.

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 14-2 *Page Displayed for an Action*



Add, modify or revoke role assignments based on a role, user, group or container.

* - indicates required.

How do you want to view assignments?

Select Role:

Most pages you work with on the *Roles* tab include a button in the upper right corner that lets you display the *Roles* legend:

For details on the *Roles* legend, see Section 14.5, “Understanding the Roles Legend,” on page 212.

14.4 Roles Actions You Can Perform

Here’s a summary of the actions that are available to you by default on the *Roles* tab:

Table 14-2 *Roles Actions*

Category	Action	Description
My Roles	My Roles	Lets you look at the status and details for your approved roles. It shows roles that have a status of Provisioned or Pending Activation, but not roles that have not yet been approved. For details, see Chapter 15, “Viewing Your Roles,” on page 215.
Role Assignments	Role Assignments	The *Role Assignments* action lets users request role assignments. This action is available to Role Module Administrators, Role Managers, and other authenticated users not specifically assigned to any of the installed system roles. ◆ Role Module Administrators can request assignment of users, groups, and containers to roles. The Role Module Administrator has unlimited scope within the directory. ◆ Role Managers can request assignment of users, groups, and containers to roles to which they have browse rights. ◆ Other authenticated users can request assignment for themselves to roles to which they have browse rights. For details, see Section 16.2, “Assigning Roles,” on page 217.
	View Request Status	Allows you to see the status of your role requests (including requests you’ve made explicitly 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. For details, see Section 16.3, “Checking the Status of Your Requests,” on page 227.

Category	Action	Description
Role Management	Browse Role Catalog	Lets you look at existing roles in the Roles Catalog. You can also delete roles, access the Manage Role Relationships and the Role Assignments actions. For details, see Section 17.1, "Browsing the Role Catalog," on page 237.
	Manage Roles	Allows you to create, modify, or delete a role. For details, see "Managing Roles" on page 238.
	Manage Role Relationships	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. For details, see "Managing Role Relationships" on page 243.
	Manage Separation of Duties	Allows you to define a Separation of Duties (SoD) constraint. 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. For details, see "Managing Separation of Duties Constraints" on page 246.
	Configure Roles Subsystem	Allows you to specify administrative settings for the Roles Subsystem. For details, see "Configuring the Role Subsystem" on page 250.
Role Reporting	Role Reports	Enables you to create and view reports that describe the current state of roles and role assignments. For details, see Section 18.2, "Role Reports," on page 253.
	SoD Reports	Enables you to create and view reports that describe the current state of Separation of Duties constraints, violations, and approved exceptions. For details, see Section 18.3, "SoD Reports," on page 257.
	User Reports	Enables you to create and view reports that describe the current state of role memberships and entitlements for users. For details, see Section 18.4, "User Reports," on page 259.

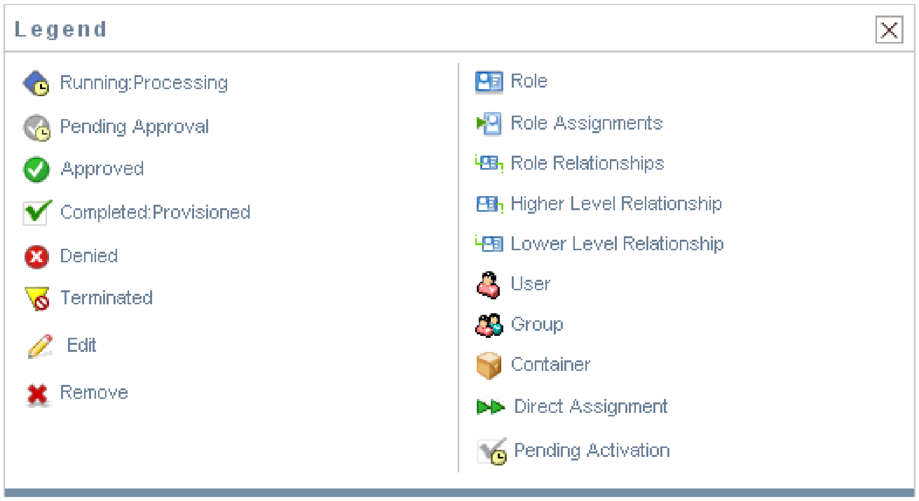
14.5 Understanding the Roles Legend

Most pages you work with on the *Roles* tab include a button in the upper right corner that lets you display the *Roles* legend. To display the legend, click the *Legend* button, shown in Figure 9-2:

Figure 14-3 The Legend Button

The legend provides a brief description of the icons used throughout the *Roles* tab. The figure below shows the legend.

Figure 14-4 Roles Legend



Legend

Running:Processing

Pending Approval

Approved

Completed:Provisioned

Denied

Terminated

Edit

Remove

Role

Role Assignments

Role Relationships

Higher Level Relationship

Lower Level Relationship

User

Group

Container

Direct Assignment

Pending Activation

The table below provides detailed descriptions of the icons in the legend:

Table 14-3 Legend Icons

Icon	Description
Running: Processing	Indicates that a role request is still in process. Appears on the View Request Status page.
Pending Approval	Indicates that a role request is awaiting approval, either for a separation of duties exception or for the role assignment itself. Appears on the View Request Status page.
Approved	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. Appears on the View Request Status page.
Completed: Provisioned	Indicates that a role request has been approved and the role has been assigned to the recipient (user, group, or container). Appears on the My Roles, Role Assignments, and View Request Status pages.

Icon	Description
Denied	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. Appears on the View Request Status pages.
Terminated	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. Appears on the View Request Status pages.
Role	Indicates that an object is a role. Appears on the My Roles, Role Assignments, and View Request Status pages.
Higher Level Relationship	Indicates that a role has a higher-level relationship to the currently selected role, which means that it contains the currently selected role. Appears on the Manage Role Relationships pages.
Lower Level Relationship	Indicates that a role has a lower-level relationship to the currently selected role, which means that is contained by the currently selected role. Appears on the Manage Role Relationships pages.
User	Indicates that an object is a user. Appears on the My Roles and Role Assignments pages.
Group	Indicates that an object is a group. Appears on the My Roles and Role Assignments pages.
Container	Indicates that an object is a container. Appears on the My Roles and Role Assignments pages.
Direct Assignment	Indicates that a role was assigned directly to the currently selected user, group, or container. Appears on the My Roles and Roles Assignments pages.
Pending Activation	Indicates that a role request has completed its processing and has been approved, but has an activation date that is in the future. Appears on the My Roles and View Request Status pages.

Viewing Your Roles

15

This section provides instructions for looking at your roles. Topics include:

- Section 15.1, "About the My Roles Actions," on page 215
- Section 15.2, "Looking at Your Approved Role Requests," on page 215

15.1 About the My Roles Actions

The *Roles* tab in the Identity Manager User Application includes a group of actions called *My Roles*. The *My Roles* actions give you the ability to look at your roles.

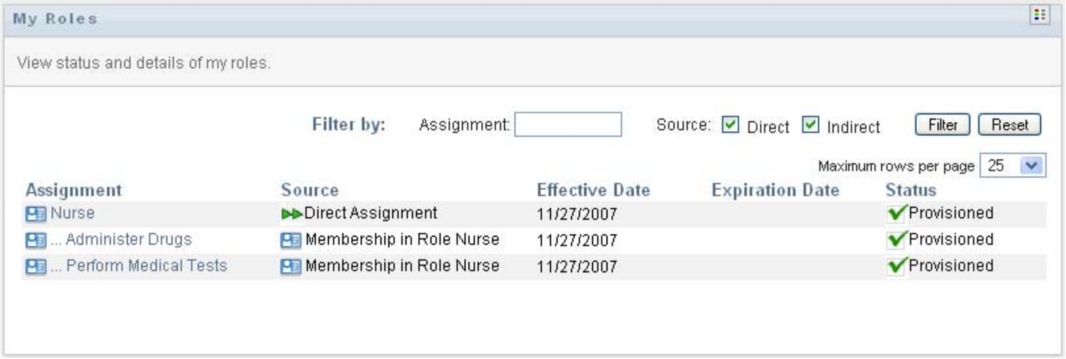
15.2 Looking at Your Approved Role Requests

The *My Roles* action lets you look at the status and details for your approved roles. It shows roles that have a status of Provisioned or Pending Activation, but not role requests that have not yet been approved.

To look at your approved roles:

1 Click *My Roles* in the list of *My Roles* actions.

The User Application displays the current status of role assignments for the currently authenticated user.



My Roles

View status and details of my roles.

Filter by: Assignment: Source: ☑ Direct ☑ Indirect

Maximum rows per page 25

Assignment	Source	Effective Date	Expiration Date	Status
Nurse	▶▶Direct Assignment	11/27/2007		✓Provisioned
... Administer Drugs	Membership in Role Nurse	11/27/2007		✓Provisioned
... Perform Medical Tests	Membership in Role Nurse	11/27/2007		✓Provisioned

The columns in the assignment list table are described below:

- The *Assignment* column provides the name of the role assigned to the current user.
- The *Source* column indicates the manner in which the role assignment was made for the user, as described below:

Source	Description
Direct Assignment	Indicates that this role was assigned directly to the current user.
Membership in Role *role name*	Indicates that the user received this role by being a member in a related role.

Source	Description
Membership in Group *group name*	Indicates that the user received this role by being a member in a group.
Membership in Container *container name*	Indicates that the user received this role by being a member in a container.

- The *Effective Date* column shows the date when the assignment goes into effect. If no date is displayed, the assignment went into effect immediately after it was requested.
- The *Expiration Date* column shows the date when the assignment expires. If no date is displayed, the assignment remains in effect indefinitely.
- The *Status* column shows whether the assignment has been granted:

Status	Description
Provisioned	Approved (if necessary) and activated.
Pending Activation	Approved (if necessary) but not yet activated because the effective date for the role assignment is in the future.

2 You can filter the list of assignments as follows:

2a To view only those assignments that start with a particular string of characters, see "Filtering Data" on page 27 for information about what to enter in the *Assignment* box.

2b To view those roles that were assigned directly to the user, select the *Direct* box.

2c To view those assigned roles that the user receives through a role relationship, or by being a member in a group or container only, select the *Indirect* box.

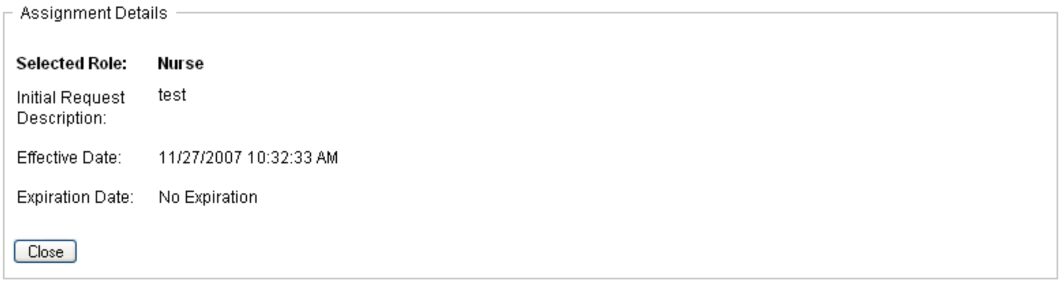
2d To apply the filter criteria you've specified to the display, click *Filter*.

NOTE: Filtering does not occur automatically. You must click the *Filter* button to apply your criteria.

2e To clear the currently specified filter criteria, click *Reset*.

3 To set the maximum number of assignments displayed on each page, select a number in the *Maximum rows per page* drop-down list.

4 To see the details for a particular role assignment, click the assignment name in the *Assignment* column and scroll down until you see the Assignment Details group box.



Assignment Details

Selected Role: **Nurse**

Initial Request Description: test

Effective Date: 11/27/2007 10:32:33 AM

Expiration Date: No Expiration

Making Role Assignments

16

This section provides instructions for making role assignments. Topics include:

- Section 16.1, "About the Role Assignments Actions," on page 217
- Section 16.2, "Assigning Roles," on page 217
- Section 16.3, "Checking the Status of Your Requests," on page 227

16.1 About the Role Assignments Actions

The *Roles* tab in the Identity Manager User Application includes a group of actions called *Role Assignments*. The *Role Assignments* actions give you the ability to make role assignment requests and check the status of requests you've made.

16.2 Assigning Roles

The *Role Assignments* action lets users request role assignments. This action is available to Role Module Administrators, Role Managers, and other authenticated users not specifically assigned to any of the installed system roles.

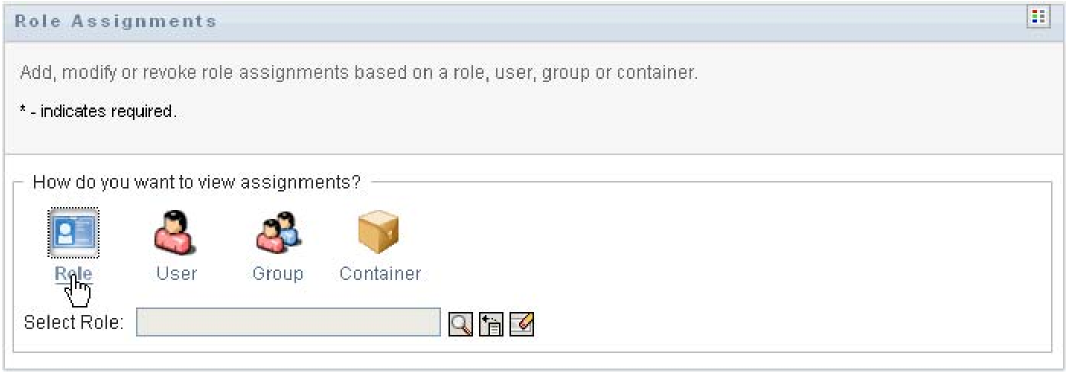
- Role Module Administrators can request assignment of users, groups, and containers to roles. The Role Module Administrator has unlimited scope within the directory.
- Role Managers can request assignment of users, groups, and containers to roles to which they have browse rights.
- Other authenticated users can request assignment to roles to which they have browse rights.

16.2.1 Assigning Users, Groups, and Containers to a Role

To request assignment of one or more users, groups, or containers to a single role:

1 Click *Role Assignments* in the list of *Role Assignments* actions.

2 Click the *Role* icon under *How do you want to view assignments?*.



Role Assignments

Add, modify or revoke role assignments based on a role, user, group or container.

* - indicates required.

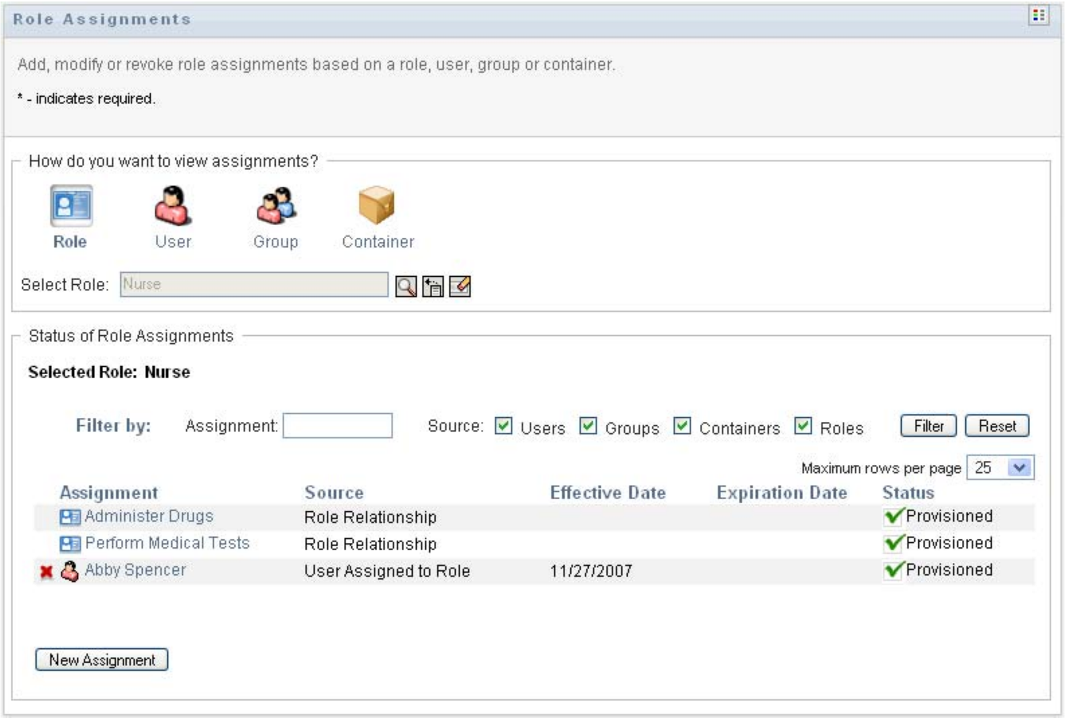
How do you want to view assignments?

Select Role:

3 Select the role to which you want to assign the users, groups, or containers.

Use the *Object Selector* or the *Show History* tool to select the role. For details on using the *Object Selector* and *Show History* tools, see Section 1.4.4, "Common User Actions," on page 25.

The User Application displays the current status of assignments for the selected role.



Add, modify or revoke role assignments based on a role, user, group or container.

* - indicates required.

Select Role: Nurse

Status of Role Assignments

Selected Role: Nurse

Filter by: Assignment: Source: ☑ Users ☑ Groups ☑ Containers ☑ Roles

Maximum rows per page 25

Assignment	Source	Effective Date	Expiration Date	Status
Administer Drugs	Role Relationship			✓ Provisioned
Perform Medical Tests	Role Relationship			✓ Provisioned
✖ Abby Spencer	User Assigned to Role	11/27/2007		✓ Provisioned

The columns in the assignment list table are described below:

- The *Assignment* column provides the name of the object assigned to the currently selected role.
- The *Source* column indicates the manner in which the object has been assigned to the role, as described below:

Source	Description
Role Relationship	Indicates that this assignment represents a role relationship. The name in the Assignment column is the name of the related role.
User Assigned to Role	Indicates that the user named in the Assignment column has been previously assigned to the currently selected role.
Group Assigned to Role	Indicates that the group named in the Assignment column has been previously assigned to the currently selected role.
Container Assigned to Role	Indicates that the container named in the Assignment column has been previously assigned to the currently selected role.

- The *Effective Date* column shows the date when the assignment goes into effect. If no date is displayed, the assignment went into effect immediately after it was requested.
- The *Expiration Date* column shows the date when the assignment expires. If no date is displayed, the assignment remains in effect indefinitely.
- The *Status* column shows whether the assignment has been granted:

Status	Description
Provisioned	Approved (if necessary) and activated.

4 You can filter the list of assignments, as follows:

4a To view only those assignments, see "Filtering Data" on page 27 for information about what to enter in the *Assignment* box.

4b To view users assignments only, select the *Users* box.

4c To view group assignments only, select the *Groups* box.

4d To view container assignments only, select the *Containers* box.

4e To view role relationships only, select the *Roles* box.

4f To apply the filter criteria you've specified to the display, click *Filter*.

4g To clear the currently specified filter criteria, click *Reset*.

5 To set the maximum number of assignments displayed on each page, select a number in the *Maximum rows per page* drop-down list.

6 To create a new assignment, click *New Assignment*.

Specify the details for the assignment in the *Assignment Details* group box.

- In the *Type of Assignment* drop-down, select *User*, *Group*, or *Container* to indicate what type of object you want to assign to the currently selected role.
- In the *Select User(s)* field, specify the users to assign.

NOTE: If you select *Group* as the type of assignment, the user interface displays the *Select Group(s)* field. If you select *Container*, it displays the *Select Container(s)* field.

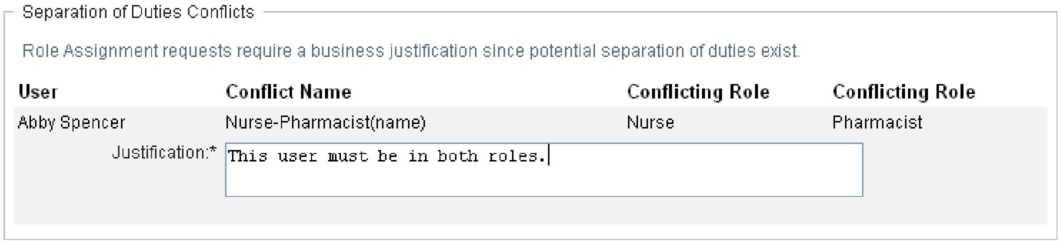
- In the *Initial Request Description* field, type text to describe the reason for the assignment request.
- In the *Effective Date* field, specify the date when you want the assignment to take effect. You can use the Calendar control to select the date.
- In the *Expiration Date* field, indicate whether you want the assignment to have an expiration date. If the assignment will remain in effect indefinitely, select *No Expiration*. If you want to define an expiration date, select *Specify Expiration* and use the Calendar control to select the date.
- Click *Submit* to submit the role assignment request.

NOTE: The *Role Assignments* action allows you to see roles that are related to the currently selected role, but does not permit you to create role relationships. To do this, you need to use the *Manage Role Relationships* action.

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.

To provide a justification:

1 Type a description in the *Justification* field that explains why an exception to the separation of duties constraint is needed in this situation.



Separation of Duties Conflicts

Role Assignment requests require a business justification since potential separation of duties exist.

User	Conflict Name	Conflicting Role	Conflicting Role
Abby Spencer	Nurse-Pharmacist(name)	Nurse	Pharmacist

Justification:* This user must be in both roles.

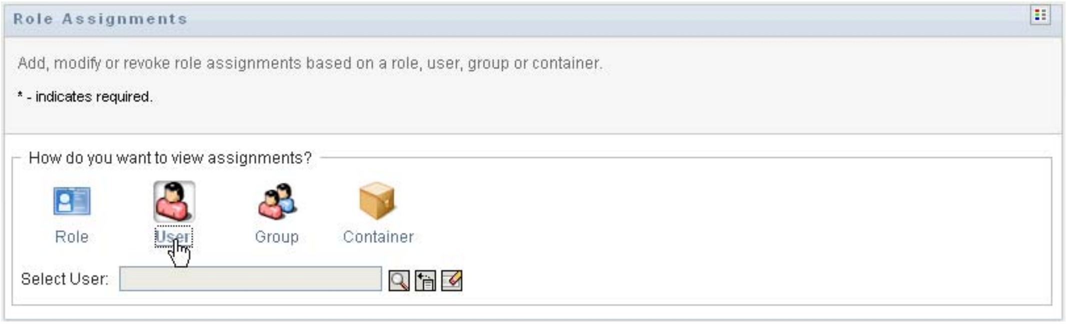
NOTE: You do not need to provide a justification in cases where the new role assignment conflicts with an existing assignment that the user acquired indirectly, either through a role relationship, or by membership in a group or container. If a user is added to a role indirectly, and a potential separation 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.

16.2.2 Assigning Roles to a Single User

To request assignment of one or more roles to a single user:

1 Click *Role Assignments* in the list of *Role Assignments* actions.

2 Click the *User* icon under *How do you want to view assignments?*.



Role Assignments

Add, modify or revoke role assignments based on a role, user, group or container.

* - indicates required.

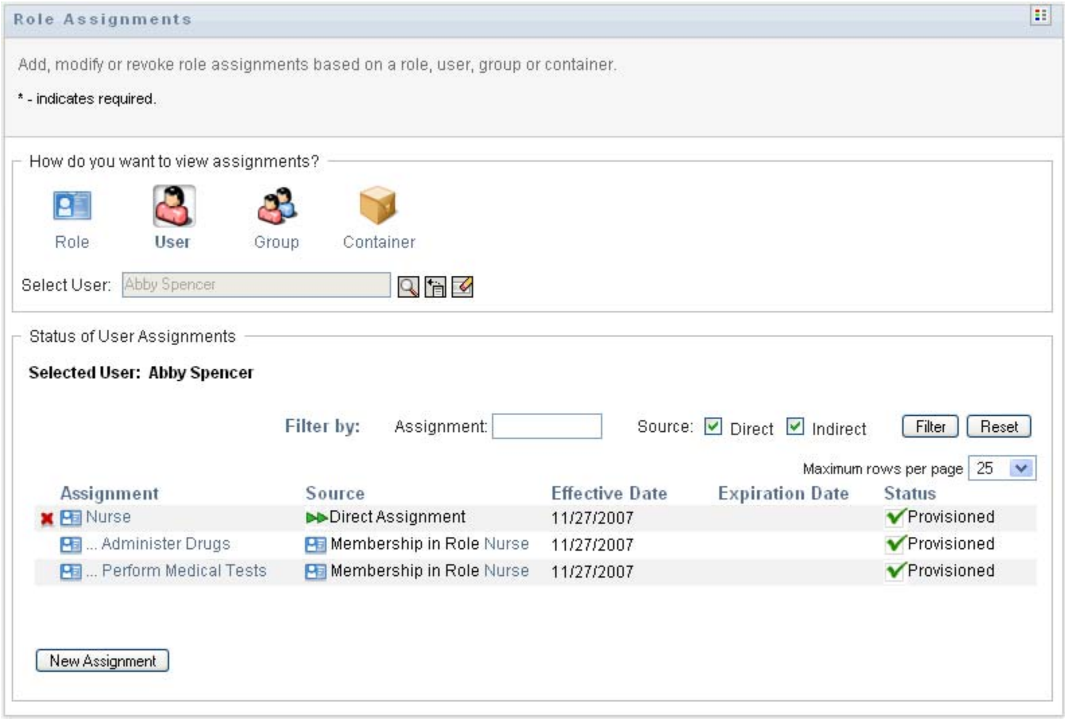
How do you want to view assignments?

Select User:

3 Select the user to whom you want to assign one or more roles.

Use the *Object Selector* or the *Show History* tool to select the user. For details on using the *Object Selector* and *Show History* tools, see "Using the Object Selector Button for Searching" on page 26.

The User Application displays the current status of assignments for the selected user.



Role Assignments

Add, modify or revoke role assignments based on a role, user, group or container.

* - indicates required.

How do you want to view assignments?

Select User: Abby Spencer

Status of User Assignments

Selected User: Abby Spencer

Filter by: Assignment: Source: ☑ Direct ☑ Indirect Filter Reset

Maximum rows per page 25

Assignment	Source	Effective Date	Expiration Date	Status
✖ Nurse	▶▶Direct Assignment	11/27/2007		✓Provisioned
... Administer Drugs	Membership in Role Nurse	11/27/2007		✓Provisioned
... Perform Medical Tests	Membership in Role Nurse	11/27/2007		✓Provisioned

New Assignment

The columns in the assignment list table are described below:

- The *Assignment* column provides the name of the role assigned to the currently selected user.
- The *Source* column indicates how the role was assigned to the user, as described below:

Source	Description
Direct Assignment	Indicates that this role was assigned directly to the currently selected user.
Membership in Role *role name*	Indicates that the user received this role by being a member in a related role.
Membership in Group *group name*	Indicates that the user received this role by being a member in a group.
Membership in Container *container name*	Indicates that the user received this role by being a member in a container.

- The *Effective Date* column shows the date when the assignment goes into effect. If no date is displayed, the assignment went into effect immediately after it was requested.
- The *Expiration Date* column shows the date when the assignment expires. If no date is displayed, the assignment remains in effect indefinitely.
- The *Status* column shows whether the assignment has been granted and provisioned:

Status	Description
Provisioned	Approved (if necessary) and activated.

4 You can filter the list of assignments, as follows:

- **4a** To view only those assignments that start with a particular string of characters, see "Filtering Data" on page 27 for information about what to type in the *Assignment* box.
- **4b** To view only those assignments that were assigned directly to the user, select the *Direct* box.
- **4c** To view only those assignments that were assigned indirectly, select the *Indirect* box. Indirect assignments are those assignments that a user receives through a role relationship, or by being a member in a group or container.
- **4d** To apply the filter criteria you've specified to the display, click *Filter*.
- **4e** To clear the currently specified filter criteria, click *Reset*.

5 To set the maximum number of assignments displayed on each page, select a number in the *Maximum rows per page* drop-down list.

6 To create a new assignment, click *New Assignment*.

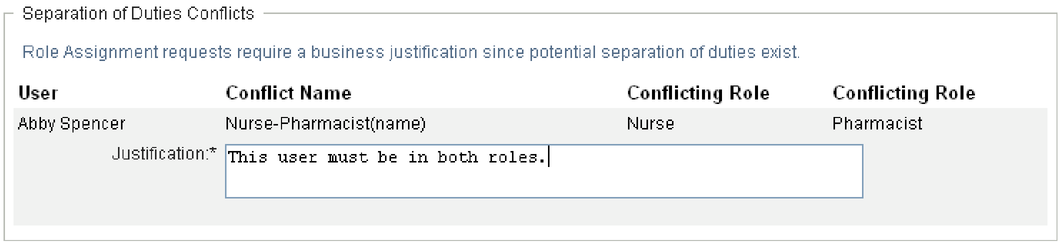
Specify the details for the assignment in the *Assignment Details* group box.

- In the *Select Role(s)* field, specify the roles to assign.
- In the *Initial Request Description* field, type text to describe the reason for the assignment request.
- In the *Effective Date* field, specify the date when you want the assignment to take effect. You can use the Calendar control to select the date.
- In the *Expiration Date* field, indicate whether you want the assignment to have an expiration date. If the assignment will remain in effect indefinitely, select *No Expiration*. If you want to define an expiration date, select *Specify Expiration* and use the Calendar control to select the date.
- Click *Submit* to submit the role assignment request.

If a separation of duties conflict will occur if a role is assigned to the currently selected user, 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.

To provide a justification:

1 Type a description in the *Justification* field that explains why an exception to the separation of duties constraint is needed in this situation.



Separation of Duties Conflicts

Role Assignment requests require a business justification since potential separation of duties exist.

User	Conflict Name	Conflicting Role	Conflicting Role
Abby Spencer	Nurse-Pharmacist(name)	Nurse	Pharmacist

Justification:* This user must be in both roles.

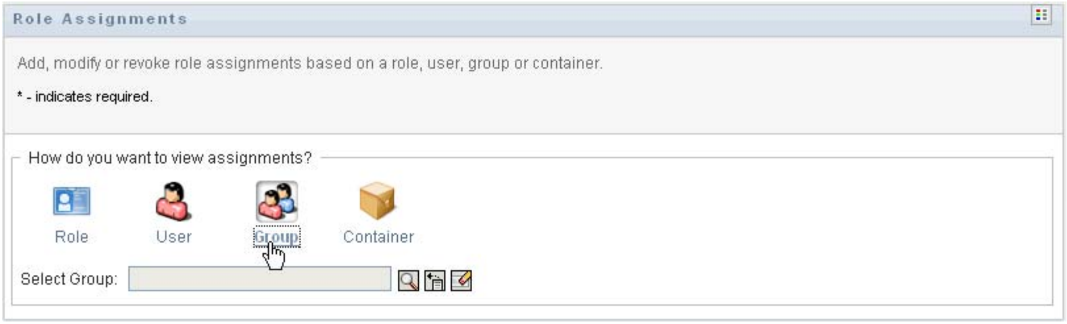
Indirect role assignments and SoD conflicts You do not need to provide a justification in cases where the new role assignment conflicts with an existing assignment that the user acquired indirectly, either through a role relationship, or by membership in a group or container. If a user is added to a 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.

16.2.3 Assigning Roles to a Single Group

To request assignment of one or more roles to a single group:

1 Click *Role Assignments* in the list of *Role Assignments* actions.

2 Click the *Group* icon under *How do you want to view assignments?*.



Role Assignments

Add, modify or revoke role assignments based on a role, user, group or container.

* - indicates required.

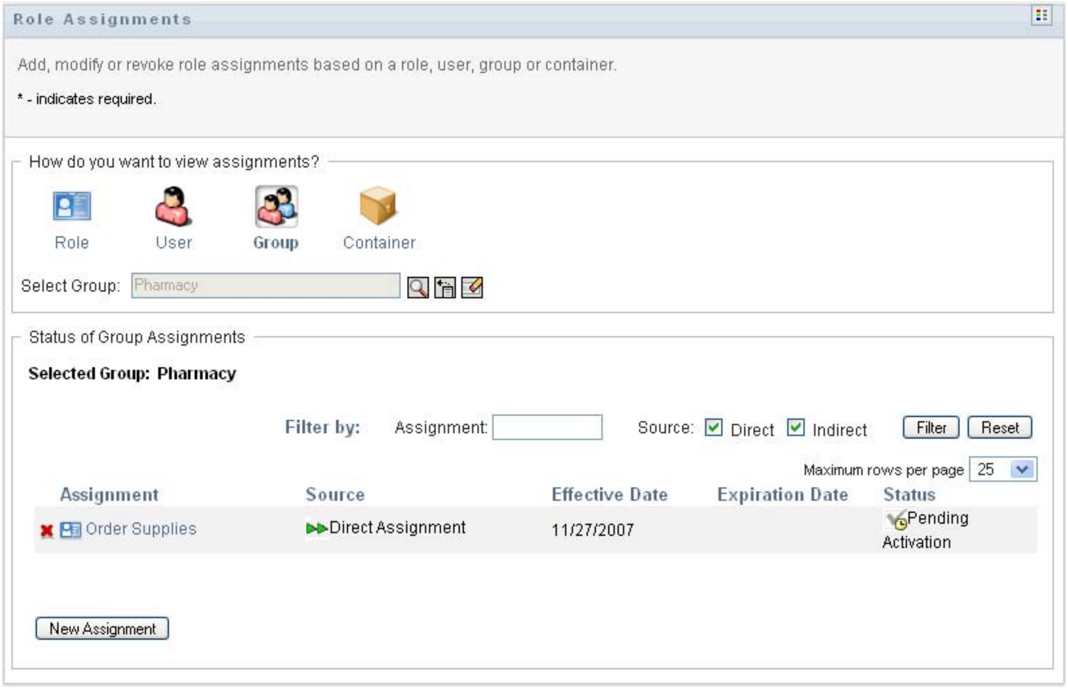
How do you want to view assignments?

Select Group:

3 Select the group to which you want to assign one or more roles.

Use the *Object Selector* or the *Show History* tool to select the group. For details on using the *Object Selector* and *Show History* tools, see "Using the Object Selector Button for Searching" on page 26.

The User Application displays the current status of assignments for the selected group.



Role Assignments

Add, modify or revoke role assignments based on a role, user, group or container.

* - indicates required.

How do you want to view assignments?

Select Group: Pharmacy

Status of Group Assignments

Selected Group: Pharmacy

Filter by: Assignment: Source: ☑ Direct ☑ Indirect

Maximum rows per page 25

Assignment	Source	Effective Date	Expiration Date	Status
✖ Order Supplies	▶▶Direct Assignment	11/27/2007		Pending Activation

The columns in the assignment list table are described below:

- The *Assignment* column provides the name of the role assigned to the currently selected group.
- The *Source* column indicates how the role was assigned to the group, as described below:

Source	Description
Direct Assignment	Indicates that this role was assigned directly to the currently selected group.
Membership in Role *role name*	Indicates that the group was given this role because it is assigned to a related role.

- The *Effective Date* column shows the date when the assignment goes into effect. If no date is displayed, the assignment went into effect immediately after it was requested.
- The *Expiration Date* column shows the date when the assignment expires. If no date is displayed, the assignment remains in effect indefinitely.
- The *Status* column shows whether the assignment has been granted and provisioned:

Status	Description
Provisioned	Approved (if necessary) and activated.

4 You can filter the list of assignments, as follows:

4a To view only those assignments that start with a particular string of characters, see "Filtering Data" on page 27, for information about what to enter in the *Assignment* box.

4b To view only those assignments that were assigned directly to the group, select the *Direct* box.

4c To view only those assignments that were assigned indirectly, select the *Indirect* box. Indirect assignments are those assignments that a group receives through a role relationship.

4d To apply the filter criteria you've specified to the display, click *Filter*.

4e To clear the currently specified filter criteria, click *Reset*.

5 To set the maximum number of assignments displayed on each page, select a number in the *Maximum rows per page* drop-down list.

6 To create a new assignment, click *New Assignment*.

Specify the details for the assignment in the *Assignment Details* group box.

- In the *Select Role(s)* field, specify the roles to assign.
- In the *Initial Request Description* field, type text to describe the reason for the assignment request.
- In the *Effective Date* field, specify the date when you want the assignment to take effect. You can use the Calendar control to select the date.

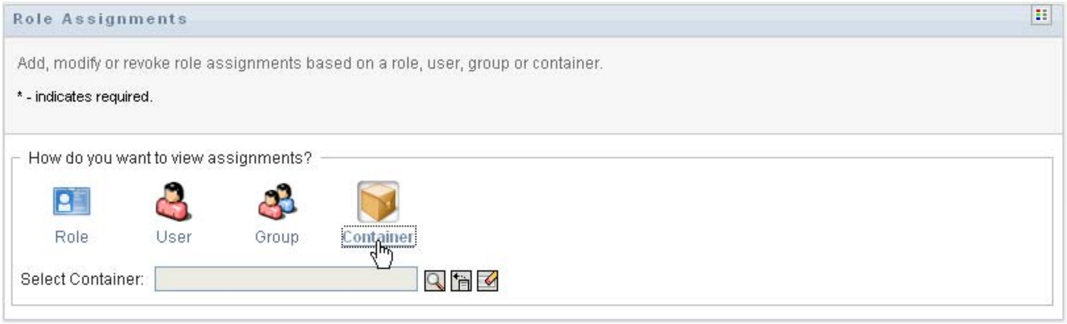
- In the *Expiration Date* field, indicate whether you want the assignment to have an expiration date. If the assignment will remain in effect indefinitely, select *No Expiration*. If you want to define an expiration date, select *Specify Expiration* and use the Calendar control to select the date.
- Click *Submit* to submit the role assignment request.

16.2.4 Assigning Roles to a Single Container

To request assignment of one or more roles to a single container:

1 Click *Role Assignments* in the list of *Role Assignments* actions.

2 Click the *Container* icon under *How do you want to view assignments?*.



Role Assignments

Add, modify or revoke role assignments based on a role, user, group or container.

* - indicates required.

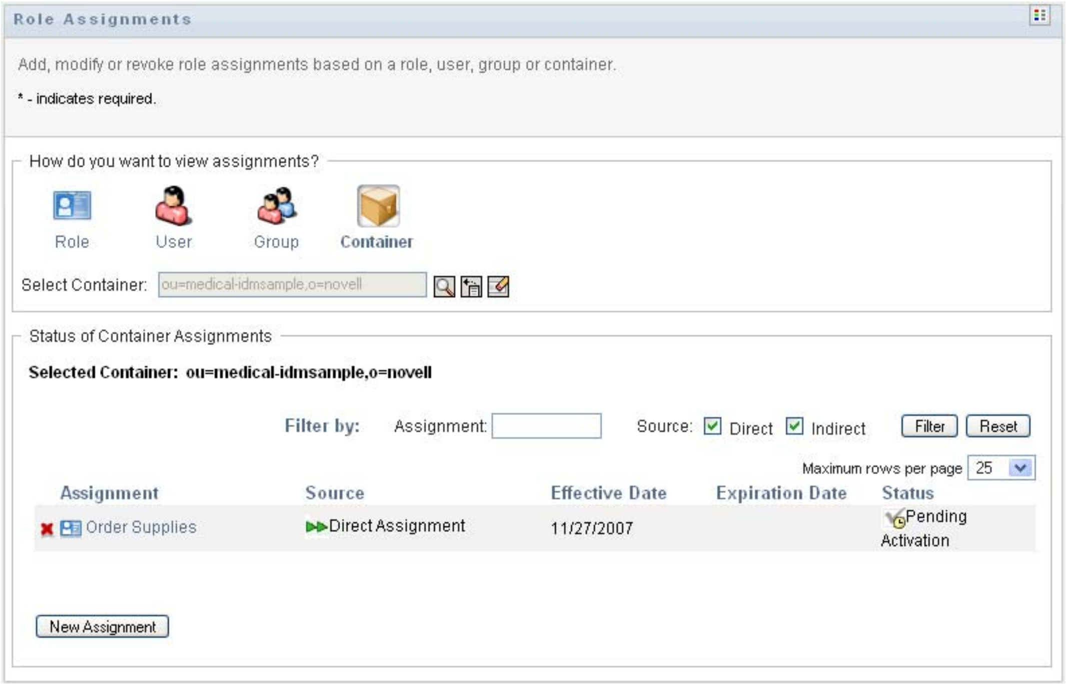
How do you want to view assignments?

Select Container:

3 Select the container to which you want to assign one or more roles.

Use the *Object Selector* or the *Show History* tool to select the container. For details on using the *Object Selector* and *Show History* tools, see "Using the Object Selector Button for Searching" on page 26.

The User Application displays the current status of assignments for the selected container.



Role Assignments

Add, modify or revoke role assignments based on a role, user, group or container.

* - indicates required.

How do you want to view assignments?

Select Container: ou=medical-idmsample,o=novell

Status of Container Assignments

Selected Container: ou=medical-idmsample,o=novell

Filter by: Assignment: Source: ☑ Direct ☑ Indirect

Maximum rows per page 25

Assignment	Source	Effective Date	Expiration Date	Status
✗ Order Supplies	Direct Assignment	11/27/2007		Pending Activation

The columns in the assignment list table are described below:

- The *Assignment* column provides the name of the role assigned to the currently selected container.
- The *Source* column indicates how the role was assigned to the container, as described below:

Source	Description
Direct Assignment	Indicates that this role assignment was assigned directly to the currently selected container.
Membership in Role *role name*	Indicates that the container was given this role because it is assigned to a related role.
Membership in Container *container name*	Indicates that the container was assigned this role because it is nested within a higher-level container.

- The *Effective Date* column shows the date when the assignment goes into effect. If no date is displayed, the assignment went into effect immediately after it was requested.
- The *Expiration Date* column shows the date when the assignment expires. If no date is displayed, the assignment remains in effect indefinitely.
- The *Status* column shows whether the assignment has been granted and provisioned:

Status	Description
Provisioned	Approved (if necessary) and activated.

4 You can filter the list of assignments, as follows:

4a To view only those assignments that start with a particular string of characters, see "Filtering Data" on page 27 for information about what to enter in the *Assignment* box.

4b To view only those assignments that were assigned directly to the container, select the *Direct* box.

4c To view only those assignments that were assigned indirectly, select the *Indirect* box. Indirect assignments are those assignments that a container receives through a role relationship.

4d To apply the filter criteria you've specified to the display, click *Filter*.

4e To clear the currently specified filter criteria, click *Reset*.

5 To set the maximum number of assignments displayed on each page, select a number in the *Maximum rows per page* drop-down list.

6 To create a new assignment, click *New Assignment*.

Specify the details for the assignment in the *Assignment Details* group box.

- In the *Select Role(s)* field, specify the roles to assign.
- In the *Initial Request Description* field, type text to describe the reason for the assignment request.

- In the *Effective Date* field, specify the date when you want the assignment to take effect. You can use the Calendar control to select the date.
- In the *Expiration Date* field, indicate whether you want the assignment to have an expiration date. If the assignment will remain in effect indefinitely, select *No Expiration*. If you want to define an expiration date, select *Specify Expiration* and use the Calendar control to select the date.
- To propagate this role assignment to users in all subcontainers, select *Apply role assignment(s) to sub-containers*.
- Click *Submit* to submit the role assignment request.

16.3 Checking the Status of Your Requests

The *View Request Status* action allows you to see the status of your role requests, including requests you've made directly as well as role assignment requests for groups for 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 *View Request Status* action shows all role assignment requests, including those that are running, pending approval, approved, completed, denied, or terminated. The *View Request Status* action also shows requests made to create role relationships through the *Manage Role Relationships* action.

What you can see and do on the View Request Status page depends on your security role, as described below:

Table 16-1 *Capabilities of Each Security Role*

Security Role	Capabilities
Roles Module Administrator	A Roles Module Administrator can perform these functions on the View Request Status page: ◆ View all role assignment requests. ◆ Filter requests based on status, as well as User. When the Roles Module Administrator filters requests on User, the results show requests where the specified user is requester or recipient. The controls for filtering requests based on requester or recipient are not available to the Roles Module Administrator. ◆ Retract any role assignment requests, provided these requests are still in a retractable state (not yet approved, denied, completed, or terminated).

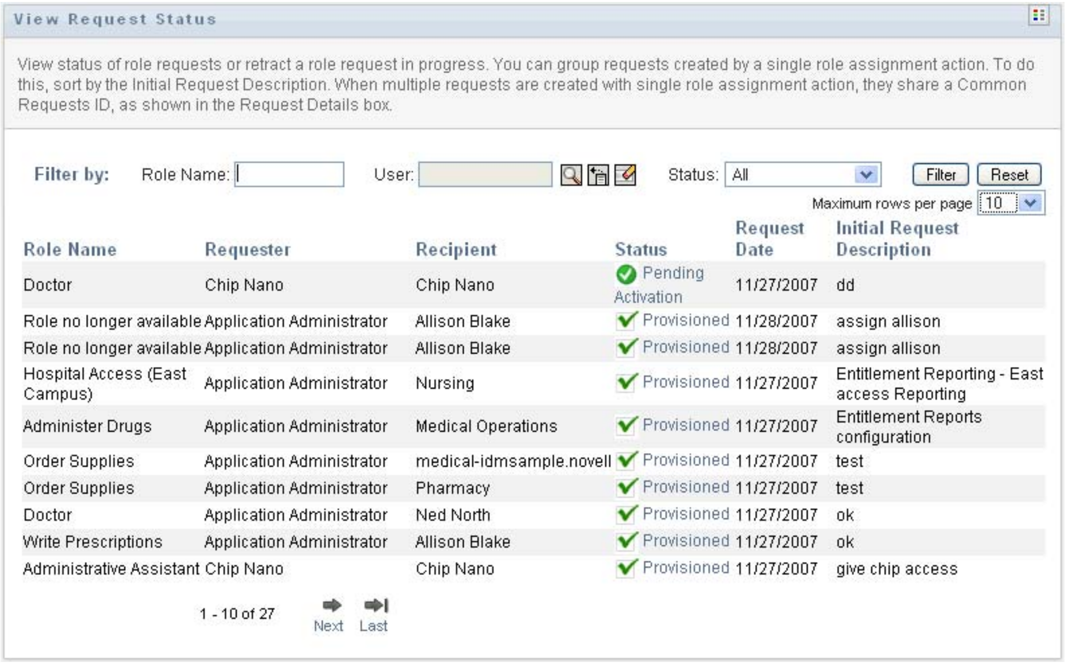
Security Role	Capabilities
Roles Manager	A Roles Manager can perform these functions on the View Request Status page: ◆ View the status of requests for which the user has browse rights to the role, and for which the user is either the requester or recipient. ◆ Filter requests based on status, as well as User. When the Roles Manager filters requests on User, the results show requests where the specified user is requester or recipient. The controls for filtering requests based on requester or recipient are not available to the Roles Manager. ◆ Retract requests for users, groups, and containers for which the user has directory browse rights for the role and target (user, group, or container) objects. The requests must still be in a retractable state (not yet approved, denied, completed, or terminated).
Authenticated user	A typical user logged in to the User Application who is not a member of a system role can perform any of the following functions on the View Request Status page: ◆ View the status of requests for which the user is either a requester or recipient. ◆ Filter the requests based on status, as well as requester or recipient. The control for filtering requests based on User is not available to the authenticated user, since the authenticated user can see only requests for himself. ◆ Retract requests for which the user is both requester and recipient. The requests must still be in a retractable state (not yet approved, denied, completed, or terminated), and the user must have browse rights to the role as well.

Large result sets By default, the View Request Status page retrieves up to 10,000 request objects. If you attempt to retrieve a larger result set, you will see a message indicating that you have reached the limit. In this case, you should narrow your search (by specifying a particular user or status, for example) to limit the number of objects returned in the result set. Note that when you apply a filter to a role name, the filter limits what you see and its order, not the number of objects returned.

To look at your role requests:

1. Click *View Request Status* in the list of *Role Assignments* actions.

   The User Application displays the current status of role requests for the currently authenticated user.



View Request Status

View status of role requests or retract a role request in progress. You can group requests created by a single role assignment action. To do this, sort by the Initial Request Description. When multiple requests are created with single role assignment action, they share a Common Requests ID, as shown in the Request Details box.

Filter by: Role Name: User: Status: All Filter Reset

Maximum rows per page 10

Role Name	Requester	Recipient	Status	Request Date	Initial Request Description
Doctor	Chip Nano	Chip Nano	✓ Pending Activation	11/27/2007	dd
Role no longer available	Application Administrator	Allison Blake	✓ Provisioned	11/28/2007	assign allison
Role no longer available	Application Administrator	Allison Blake	✓ Provisioned	11/28/2007	assign allison
Hospital Access (East Campus)	Application Administrator	Nursing	✓ Provisioned	11/27/2007	Entitlement Reporting - East access Reporting
Administer Drugs	Application Administrator	Medical Operations	✓ Provisioned	11/27/2007	Entitlement Reports configuration
Order Supplies	Application Administrator	medical-idmsample.novell	✓ Provisioned	11/27/2007	test
Order Supplies	Application Administrator	Pharmacy	✓ Provisioned	11/27/2007	test
Doctor	Application Administrator	Ned North	✓ Provisioned	11/27/2007	ok
Write Prescriptions	Application Administrator	Allison Blake	✓ Provisioned	11/27/2007	ok
Administrative Assistant	Chip Nano	Chip Nano	✓ Provisioned	11/27/2007	give chip access

1 - 10 of 27 Next Last

The columns in the role request list are described below:

- The *Role Name* column provides the name of the role 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 role, 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 *Role Name* 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	Indicates that this is a new request that is currently being processed. A request with this status can be retracted.
Running:Processing	SoD Approval Start - Pending	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. A request with this status can be retracted.

Status summary icon	Detailed Status	Description
Running:Processing	SoD Approval Start - Suspended	Indicates that the Role Service driver is unable to start a separation of duties approval process and the process has been suspended temporarily. 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. 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. A request with this status can be retracted.
Running:Processing	Approval Start - Pending	Indicates that the Role Service driver is attempting to restart an approval process for the request following an Approval Start - Suspended condition. A request with this status can be retracted.

Status summary icon	Detailed Status	Description
Running:Processing	Approval Start - Suspended	Indicates that an approval process has been initiated for the request, but the process has been suspended temporarily. 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. 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. A request with this status can be retracted.
Pending Approval	SoD Exception - Approval Pending	Indicates that a separation of duties approval process has been started and is waiting for one or more approvals. A request with this status can be retracted.
Pending Approval	Approval Pending	Indicates that an approval process has been started for the request and is waiting for one or more approvals. A request with this status can be retracted.
✓ Approved	SoD Exception - Approved	Indicates that a separation of duties exception has been approved for this request. A request with this status can be retracted.
✓ Approved	Approved	Indicates that the request has been approved. A request with this status can be retracted.

Status summary icon	Detailed Status	Description
✓ Approved	Provisioning	Indicates that the request has been approved (if approvals were required), and the activation time for the role assignment has been reached. The Role Service driver is in the process of granting the role assignment. You are not permitted to retract a request with this status.
✓ Pending Activation	Pending Activation	Indicates that the request has been approved, but the activation time for the role 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. A request with this status can be retracted.
✖ Denied	SoD Exception - Denied	Indicates that a separation of duties exception has been denied for this request. You are not permitted to retract a request with this status.
✖ Denied	Denied	Indicates that the request has been denied. You are not permitted to retract a request with this status.
✓ Completed:Provisioned	Provisioned	Indicates the request has been approved (if approvals were required), and the role assignment has been granted. You are not permitted to retract a request with this status.
✓ Completed:Provisioned	Cleanup	Indicates that the request has been processed and the Role Service driver is in the process removing the internal objects created for the request. You are not permitted to retract a request with this status.

Status summary icon	Detailed Status	Description
Terminated	Canceling	Indicates that the Role Service driver is canceling the request because of a user action. You are not permitted to retract a request with this status.
Terminated	Canceled	Indicates that the request has been canceled by a user action. You are not permitted to retract a request with this status.
Terminated	Provisioning Error	Indicates that an error occurred during the course of provisioning (granting) or deprovisioning (revoking) the role assignment. 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. You are not permitted to retract a request with this status.

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 View Request Status and Role Assignments pages. For example, if you request a role assignment that does not require approval, you might see the status as Provisioned on the View Request Status page, but the status on the Role Assignments page shows Pending Activation. If you wait for a minute or so, you might then see the status on the Role Assignments page changes 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.
- The *Initial Request Description* column shows the description provided by the requester at the time the request was made.

2 You can filter the list of requests, as follows:

2a To view only those assignments that start with a particular string of characters, see "Filtering Data" on page 27 for information about what to type in the *Role Name* box.

2b To view only those requests that apply to a particular user, use the *Object Selector* or the *Show History* tool to select the user. To see your own requests, you need to select yourself from the User list. For details on using the *Object Selector* and *Show History* tools, see "Using the Object Selector Button for Searching" on page 26.

NOTE: The User control is not available if the logged in user is not a Role Module Administrator or Role Manager.

2c To view those role requests that have a particular status summary, select the status in the *Status* drop-down list.

Status	Description
All	Includes all requests.
Running	Includes requests that have been started and are currently being processed.
Pending Approval	Includes requests that are awaiting approval, either for a separation of duties exception or for the role assignment itself.
Approved	Includes requests that have been approved, as well as requests for which a separation of duties exception was detected and approved.
Completed	Includes requests that have been approved and where the role has been assigned to the recipient (user, group, or container).
Denied	Includes requests that have been denied, as well as requests for which a separation of duties exception was detected and denied.
Terminated	Includes requests that have terminated before reaching completion, either because the user cancelled the action or because an error occurred during the course of processing.

2d To view only those requests for which you are a requester, select the *Requester* box.

NOTE: The *Requester* control is not available if the current user is a Role Module Administrator or Role Manager.

2e To view only those requests for which you are a recipient, select the *Recipient* box.

NOTE: The *Recipient* control is not available if the logged in user is a Role Module Administrator or Role Manager.

2f To apply the filter criteria you've specified to the display, click *Filter*.

2g To clear the currently specified filter criteria, click *Reset*.

3 To set the maximum number of requests displayed on each page, select a number in the *Maximum rows per page* drop-down list.

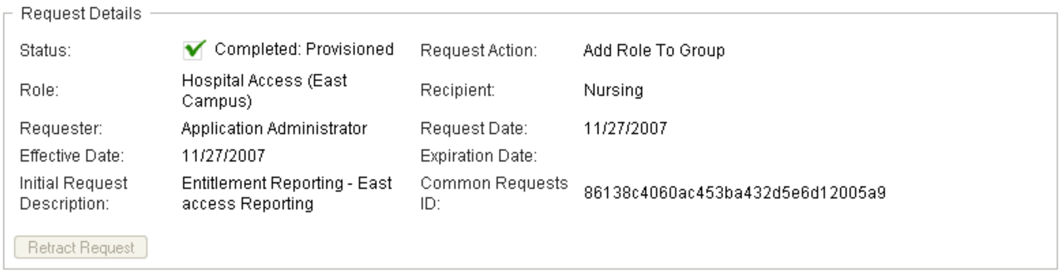
4 To sort the list of requests, click on the column heading that contains the data you want to sort.

If several role assignment requests share a *Common Requests ID*, you might want to sort the data by the Initial Request Description to see the set of related requests together. The Common Requests ID is an internal identifier (shown only in the Request Details group box) 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 Common Requests ID:

- 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 Common Requests ID, a user can retract each assignment individually. In addition, each role assignment can be approved or denied separately.

5 To see the details for a particular request, click on the status in the *Status* column and scroll down until you see the Request Details group box.



Request Details

Status:	✓ Completed: Provisioned	Request Action:	Add Role To Group
Role:	Hospital Access (East Campus)	Recipient:	Nursing
Requester:	Application Administrator	Request Date:	11/27/2007
Effective Date:	11/27/2007	Expiration Date:	
Initial Request Description:	Entitlement Reporting - East access Reporting	Common Requests ID:	86138c4060ac453ba432d5e6d12005a9

The Status field shows the status for the request, along with the status summary icon and text describing the icon. The icon (and the associated text) provides a convenient way to see the status at a glance. The table below shows how the various status codes are mapped to the status icons:

Status Icon	Associated Status Codes
Running:Processing	◆ New Request ◆ SoD Approval Start - Pending ◆ SoD Approval Start - Suspended ◆ Approval Start - Pending ◆ Approval Start - Suspended
Pending Approval	◆ SoD Exception - Approval Pending ◆ Approval Pending
Approved	◆ SoD Exception - Approved ◆ Approved ◆ Pending Activation ◆ Provisioning
Pending Activation	◆ Pending Activation
Denied	◆ SoD Exception - Denied ◆ Denied
Completed: Provisioned	◆ Provisioned ◆ Cleanup
Terminated	◆ Canceling ◆ Canceled ◆ Provisioning Error

6 To retract a request, click *Retract Request*.

The *Retract Request* button is disabled if the request has been completed or terminated.

If a request shares a Common Requests ID with a set of related requests, you can retract each of the role assignments individually.

Managing Roles

17

This section tells you how to work with the *Role Management* category of actions. It includes these sections:

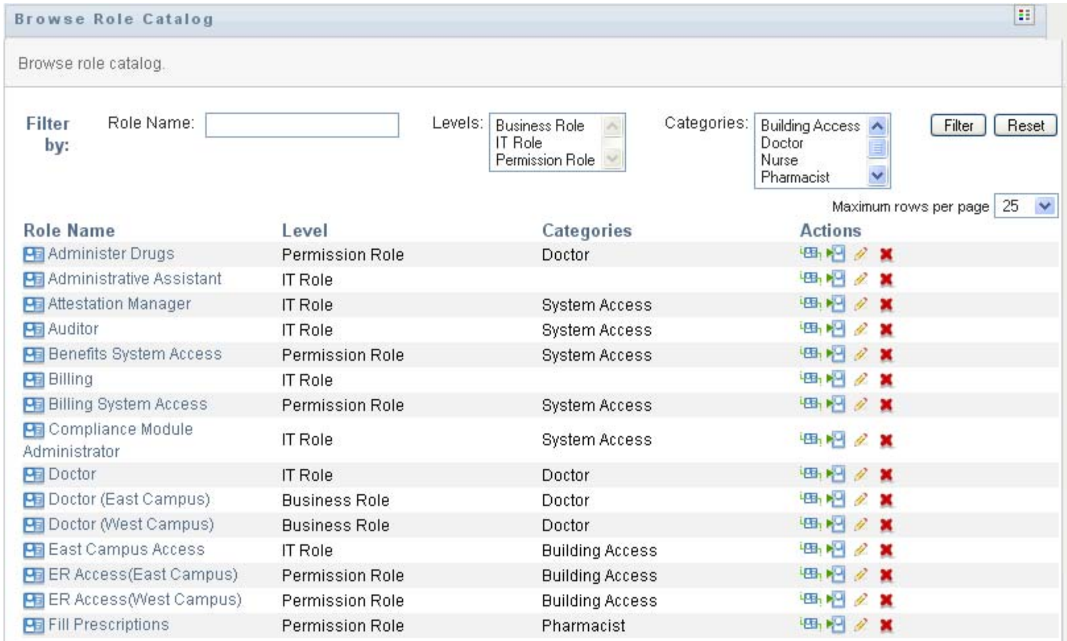
- Section 17.1, "Browsing the Role Catalog," on page 237
- Section 17.2, "Managing Roles," on page 238
- Section 17.3, "Managing Role Relationships," on page 243
- Section 17.4, "Managing Separation of Duties Constraints," on page 246
- Section 17.5, "Configuring the Role Subsystem," on page 250

17.1 Browsing the Role Catalog

To browse the Role Catalog:

1 Click *Browse Role Catalog* in the list of *Role Management* actions.

The User Application displays the current list of roles in the Role Catalog.



Browse Role Catalog

Browse role catalog.

Filter by: Role Name: Levels: Business Role, IT Role, Permission Role Categories: Building Access, Doctor, Nurse, Pharmacist

Maximum rows per page 25

Role Name	Level	Categories	Actions
Administer Drugs	Permission Role	Doctor	
Administrative Assistant	IT Role		
Attestation Manager	IT Role	System Access	
Auditor	IT Role	System Access	
Benefits System Access	Permission Role	System Access	
Billing	IT Role		
Billing System Access	Permission Role	System Access	
Compliance Module Administrator	IT Role	System Access	
Doctor	IT Role	Doctor	
Doctor (East Campus)	Business Role	Doctor	
Doctor (West Campus)	Business Role	Doctor	
East Campus Access	IT Role	Building Access	
ER Access(East Campus)	Permission Role	Building Access	
ER Access(West Campus)	Permission Role	Building Access	
Fill Prescriptions	Permission Role	Pharmacist	

The columns in the assignment list table are described below:

- The *Role Name* column provides the name of each role in the catalog.
- The *Level* column indicates the level of the role within the catalog. By default, the catalog supports three levels with the following names:

Level	Description
Business Role	The highest level in the roles hierarchy.

Level	Description
IT Role	The middle level in the roles hierarchy.
Permission Role	The lowest level in the roles hierarchy.

- The *Categories* column lists the categories associated with the role. Categories allow a business to organize the roles in the Role Catalog. Once a role has been associated with a category, it can be used as a filter when browsing the catalog.
- The *Actions* column provides quick access to other pages.

  Click to go to the *Manage Role Relationships* page.

  Click to go to the *Role Assignments* page.

  Click ✎ to go to the *Manage Roles* page.

  Click ☒ to delete the role in the corresponding row.

2 You can filter the list of roles, as follows:

2a To view only those assignments that start with a particular string of characters, see "Filtering Data" on page 27 for information about what to enter in the *Role Name* box.

2b To view those roles that have a specific level in the hierarchy, select the desired level in the *Levels* box.

2c To view those roles that have been associated with a particular category, select the desired category in the *Categories* box.

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 set the maximum number of assignments displayed on each page, select a number in the *Maximum rows per page* drop-down list.

4 To see the details for a particular role, click the role name in the *Role Name* column.

The User Application takes you to the *Manage Roles* page, where you can view details of the role or make changes.

17.2 Managing Roles

The *Manage Roles* action on the *Roles* tab of the Identity Manager user interface allows you to create a new role or modify or delete an existing role.

- Section 17.2.1, "Creating New Roles," on page 239
- Section 17.2.2, "Modifying or Deleting Existing Roles," on page 240
- Section 17.2.3, "Role Properties," on page 241

NOTE: You cannot use this action to create new or delete existing system roles. You can use it to modify system roles.

What you can see and do on this page depends on your security role, as described in Table 17-1.

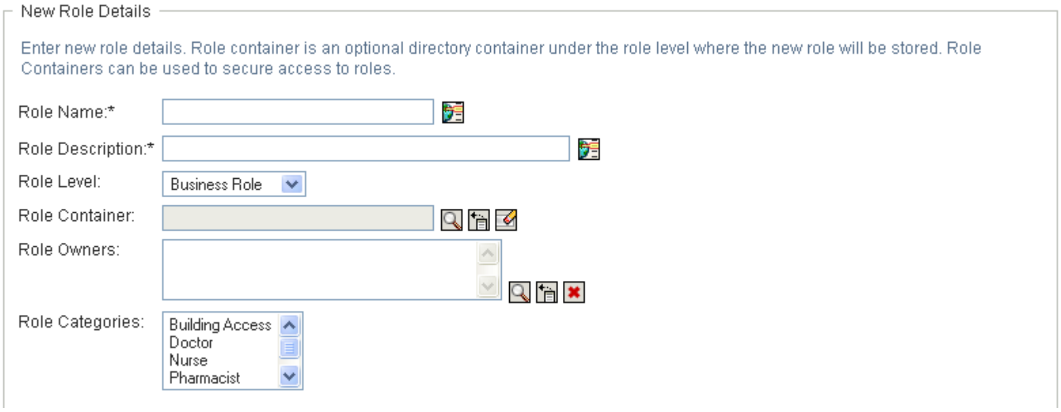
Table 17-1 *Security Role Capabilities*

Security Role	Capabilities
Roles Module Administrator	A Roles Module Administrator can: ◆ Create new roles in all containers. ◆ Modify all existing roles. ◆ Delete all existing roles (except system roles).
Roles Manager	A Roles Manager can: ◆ Create new roles in all containers. All required rights are granted for the user upon role creation. ◆ Modify only the roles for which they have browse rights. ◆ Delete only the roles for which they have browse rights. The user interface shows only those levels and containers for which a Roles Manager has browse rights. If the manager does not have browse rights for a particular level, but does have rights to the child container, the interface shows the level. If the manager has browse rights to a child container, but not to the parent container, the parent container is visible, but cannot be selected. When a Roles Manager attempts to create a new role, the user interface verifies whether the manager has rights to the chosen level and container. If the user does not have the necessary rights, the interface disables the New button and displays an error message.

17.2.1 Creating New Roles

1. Click *Manage Roles* in the list of *Role Management* actions.
2. Click *New*.

   The User Application prompts you to provide a *Role Name* in the *New Role Details* section of the Manage Roles page. For more information on each of the fields in this section, see Table 17-2, "Role Details," on page 242.



New Role Details

Enter new role details. Role container is an optional directory container under the role level where the new role will be stored. Role Containers can be used to secure access to roles.

Role Name:*

Role Description:*

Role Level: Business Role

Role Container:

Role Owners:

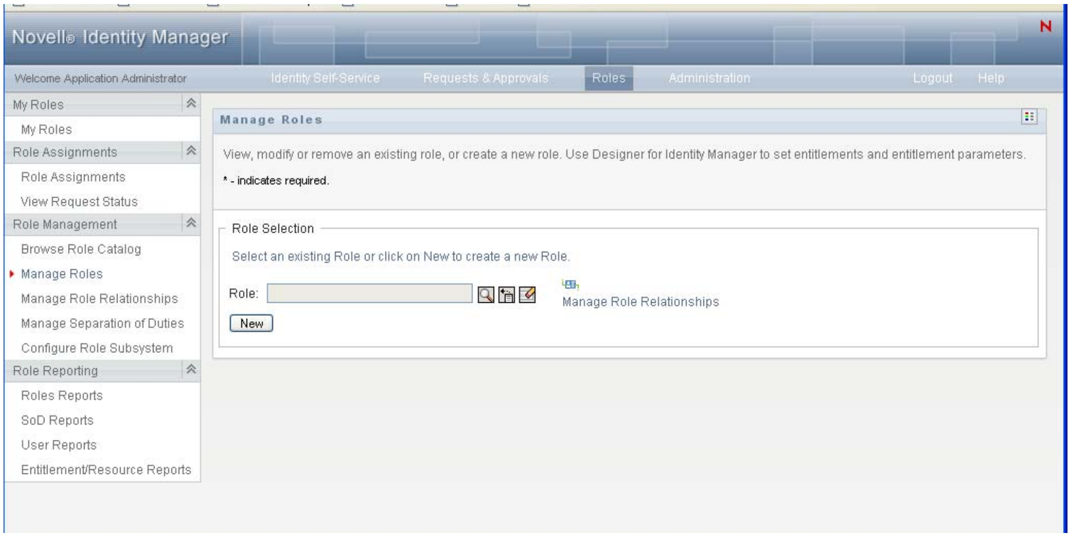
Role Categories: Building Access, Doctor, Nurse, Pharmacist

3 Navigate to *Approval Details*, and complete the fields as described in Table 17-3, "Approval Details," on page 242.

4 Click *Save* to make your changes permanent.

17.2.2 Modifying or Deleting Existing Roles

1 Click *Manage Roles* in the list of *Role Management* actions.



View, modify or remove an existing role, or create a new role. Use Designer for Identity Manager to set entitlements and entitlement parameters.

* - indicates required.

Role Selection

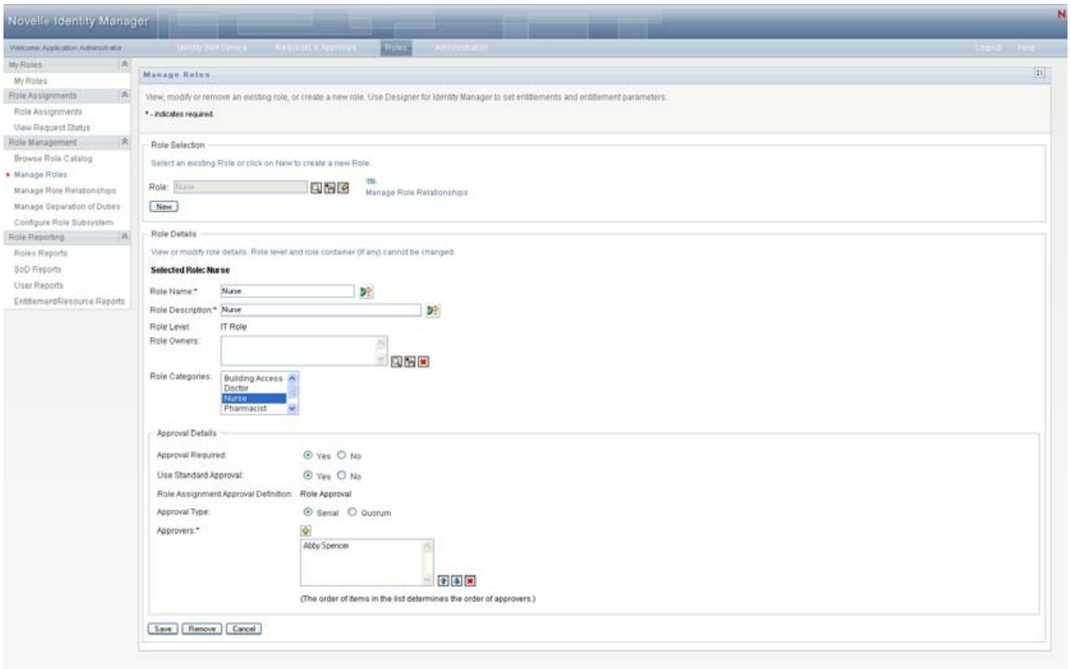
Select an existing Role or click on New to create a new Role.

Role:

2 To find the role whose details you want to modify, use the *Object Selector* or the *Show History* tool to select the constraint. For details on using the *Object Selector* and *Show History* tools, see "Common User Actions" on page 25.

3 When you select the role you want from the list, the lookup page closes and displays the *Role Details* and *Approval Details* for the selected role.

The Manage Roles page displays the name of the role that is currently selected in the *Role Details* section.



View, modify or remove an existing role, or create a new role. Use Designer for Identity Manager to set entitlements and entitlement parameters.

* - indicates required.

Role Selection

Select an existing Role or click on New to create a new Role.

Role: Nurse

Role Details

View or modify role details. Role level and role container (if any) cannot be changed.

Selected Role: Nurse

Role Name:* Nurse

Role Description:* Nurse

Role Level: IT Role

Role Owners:

Role Categories: Building Access, Doctor, Nurse, Pharmacist

Approval Details

Approval Required: ● Yes ○ No

Use Standard Approval: ● Yes ○ No

Role Assignment Approval Definition: Role Approval

Approval Type: ● Serial ○ Quorum

Approvers:* Abby Spencer

(The order of items in the list determines the order of approvers.)

TIP: The *Manage Role Relationships* link provides quick way access to the *Manage Role Relationships* page. If you have selected a role, it displays the contents of the selected role for editing.

4 To delete the currently selected role, click *Remove*.

For more information on the role details you can modify, see Table 17-2, “Role Details,” on page 242.

For more information on the Approval Details you can modify, see Table 17-3, “Approval Details,” on page 242.

5 After you complete the changes, click *Save*.

17.2.3 Role Properties

- “Role Details Properties” on page 242
- “Approval Details Properties” on page 242

Role Details Properties

***Table 17-2** Role Details*

Field	Description
Role Name	The text used when the role name displays in the User Application. You cannot include the following characters in the *Role Name* when you create a role: `< > , ; \ " +  # = / | & *` You can translate this name in any of the User Application's supported languages. For more information, see Table 1-1, "Common Buttons," on page 25.
Role Description	The text used when the role description displays in the User Application. Like the Role Name, you can translate it to any of the User Application's supported languages. For more information, see Table 1-1, "Common Buttons," on page 25.
Role Level	(Read-only when modifying a role.) Choose a role level from the drop-down list. Role levels are defined using the Designer for Identity Manager Role Configuration editor. For more information about Role levels, see Section 14.1, "About the Roles Tab," on page 203.
Role Container	(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.
Role Owners	A user who is designated as the owner 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.
Role Categories	Allow you to categorize roles for role organization. Categories are used for filtering lists of roles. Categories are multi-select.

Approval Details Properties

***Table 17-3** Approval Details*

Field	Description
Approval Required	Select *Yes* if the role requires approval when requested, and you want the approval process to execute the standard role assignment approval definition. Select *No* if the role does not require approval when requested.

Field	Description
Use Standard Approval	Select *Yes* if this role uses the standard role assignment approval definition specified in the Role Subsystem. The name of the approval definition displays as read-only in the *Role Assignment Approval Definition* below. You must select the type of approval (*Serial* or *Quorum*) and the valid approvers. When you select *No*, you are prompted for the name of a custom Role Assignment Approval Definition.
Role Assignment Approval Definition	The name of the provisioning request definition executed when the role is requested. If the value of *Use Standard Approval* is *Yes*, the value is derived from the Role Subsystem configuration settings. If the value is *No*, then you must select the name of the custom provisioning request definition to use.
Approval Type	Select *Serial* if you want the role to be approved by all of the users in the *Approvers* list. The approvers are processed sequentially in the order they appear in the list. Select *Quorum* if you want the role to be approved by a percentage of the users in the *Approvers* list. The approval is complete when the percentage of users specified is reached. 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. **TIP:** The Serial and Quorum fields have hover text that explains their behavior.
Approvers	Select *User* if the role approval task should be assigned to one or more users. Select *Group* if the role approval task should be assigned to a group. Select *Role* if the role approval task should be assigned to a role. 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 Section 1.4.4, “Common User Actions,” on page 25.

17.3 Managing Role Relationships

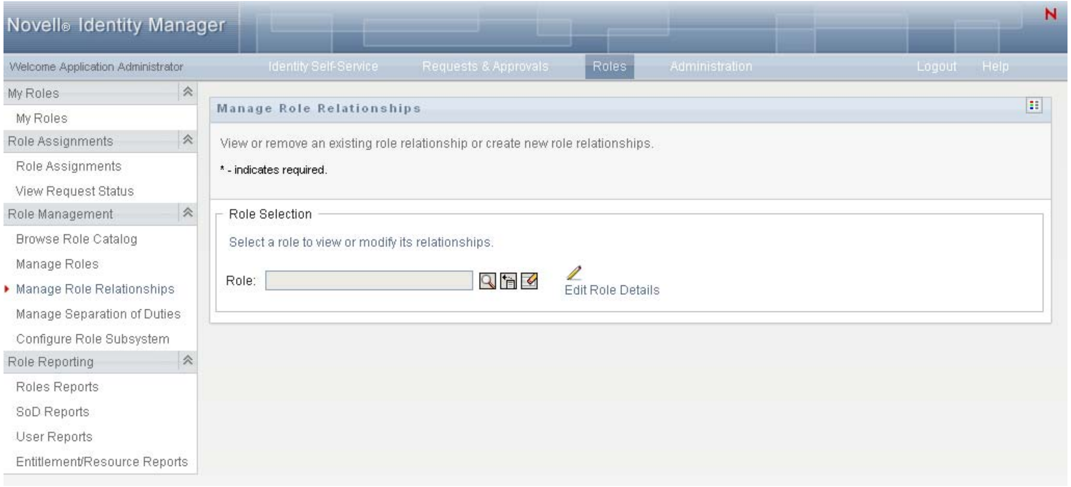
The *Manage Role Relationships* action on the *Roles* tab of the Identity Manager user interface allows you to define how roles are related in a higher and lower role containment hierarchy. This hierarchy enables you to group permissions or resources contained by lower-level roles into a higher-level 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 New Lower Level Roles 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 New Lower Level Roles or New Higher Level Roles.
- 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 New Higher Level Role.

17.3.1 Creating and Removing Role Relationships

1 Click *Manage Role Relationships* in the *Role Management* group of actions.



View or remove an existing role relationship or create new role relationships.

* - indicates required.

Select a role to view or modify its relationships.

Role:

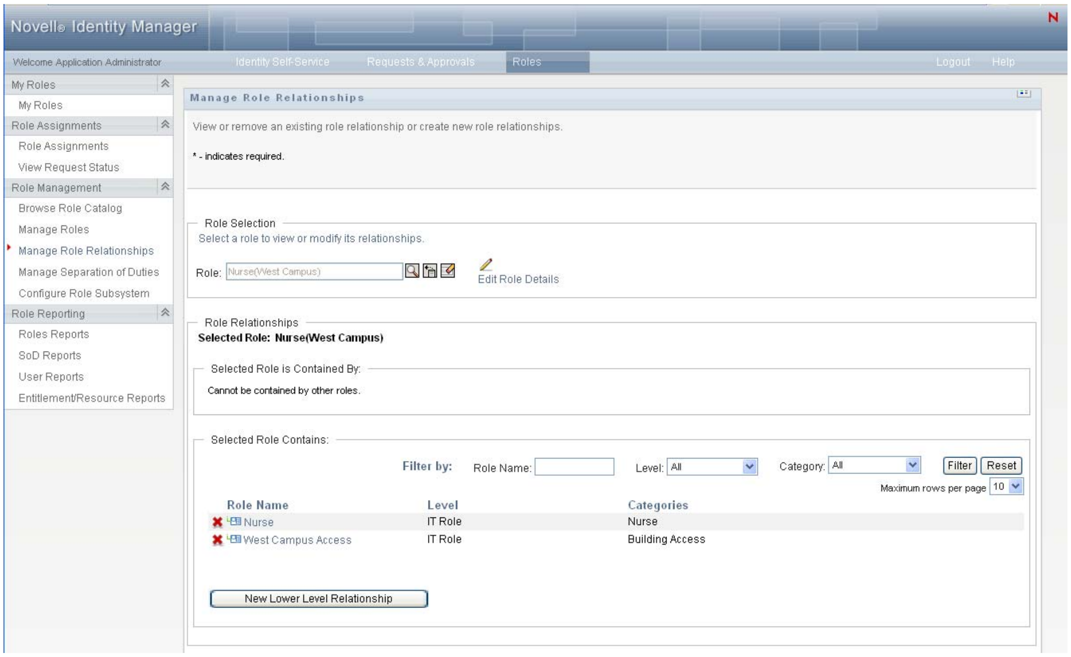
TIP: The *Edit Role Details* link provides quick way access to the *Manage Roles* page. If you have selected a role, it displays the contents of the selected role for editing.

---

2 To find the role for which you want to add or remove a relationship, use the *Object Selector* or *Show History* tool as described in Section 1.4.4, "Common User Actions," on page 25.

3 Select the role.

In this example, the Role is Nurse (West Campus). Because this role is at the highest level in the hierarchy of roles, the user interface displays a message in the *Selected Role Is Contained By* section.



Manage Role Relationships

View or remove an existing role relationship or create new role relationships.

* - indicates required.

Role Selection

Select a role to view or modify its relationships.

Role: Nurse(West Campus)

Role Relationships

Selected Role: Nurse(West Campus)

Selected Role is Contained By:

Cannot be contained by other roles.

Selected Role Contains:

Filter by: Role Name: Level: All Category: All

Maximum rows per page 10

Role Name	Level	Categories
✖ Nurse	IT Role	Nurse
✖ West Campus Access	IT Role	Building Access

Depending on the level of the role you chose, you see one or both of these buttons:

- *New Higher Level Relationship*
- *New Lower Level Relationship*

4 To add a relationship, click one of the buttons and fill out the Lower Level Relationship or Higher Level Relationship Details as described in Table 17-4 on page 246

5 You can filter the list of higher and lower level relationships, as follows:

5a To view only those relationships that start with a particular string of characters, see "Filtering Data" on page 27 for information about what to enter in the *Role Name* field.

5b To view those roles of a certain level, select it from the *Level* list box.

5c To view those roles of a specific category, select it from the *Category* list box.

5d To apply the filter criteria you've specified to the display, click *Filter*.

5e To clear the currently specified filter criteria, click *Reset*.

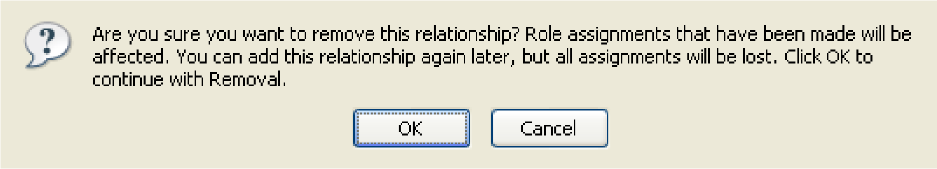
6 Click *Submit* to create a request to add the role relationships.

You can check the status of the request by going to *View Request Status*. When the status is *Provisioned*, the role relationship has been added.

7 To remove a relationship:

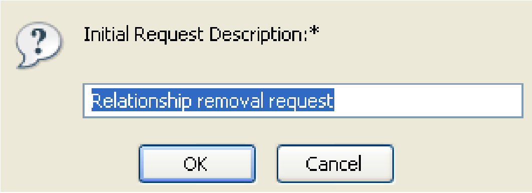
7a Navigate to the relationship you want to remove and click ✖.

You are asked to confirm that you want to remove it.



Are you sure you want to remove this relationship? Role assignments that have been made will be affected. You can add this relationship again later, but all assignments will be lost. Click OK to continue with Removal.

7b Click *OK* to continue with the removal or *Cancel* to return to the *Manage Role Relationships* page. You are prompted for an *Initial Request Description*.


Initial Request Description:*

Relationship removal request

The default text is *Relationship removal request*, but you can modify it as needed. This text displays in the *View Request Status* page.

7c Click *OK* to submit the removal request. You can view the status of this request in the *View Request Status* page. A status of *Provisioned* means that the relationship has been removed.

17.3.2 Managing Role Relationships Properties

Table 17-4 *Role Relationships Properties*

Field	Description
Initial Request Description	This value appears in *View Request Status*. You can use this option to group multiple requests created by one user interaction because they share the same Common Requests ID.
Add Roles to Selected Role	Available when you click *New Lower Level Relationship*. Use the Object Selector or History buttons to locate the lower-level role to add to the selected role. See "Using the Object Selector Button for Searching" on page 26.
Add Selected Role to Roles	Available when you click *New Higher Level Relationship*. Use the Object Selector or History buttons to locate the higher level role to add to the current role. See "Using the Object Selector Button for Searching" on page 26.

17.4 Managing Separation of Duties Constraints

The *Manage Separation of Duties* action on the *Roles* 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.

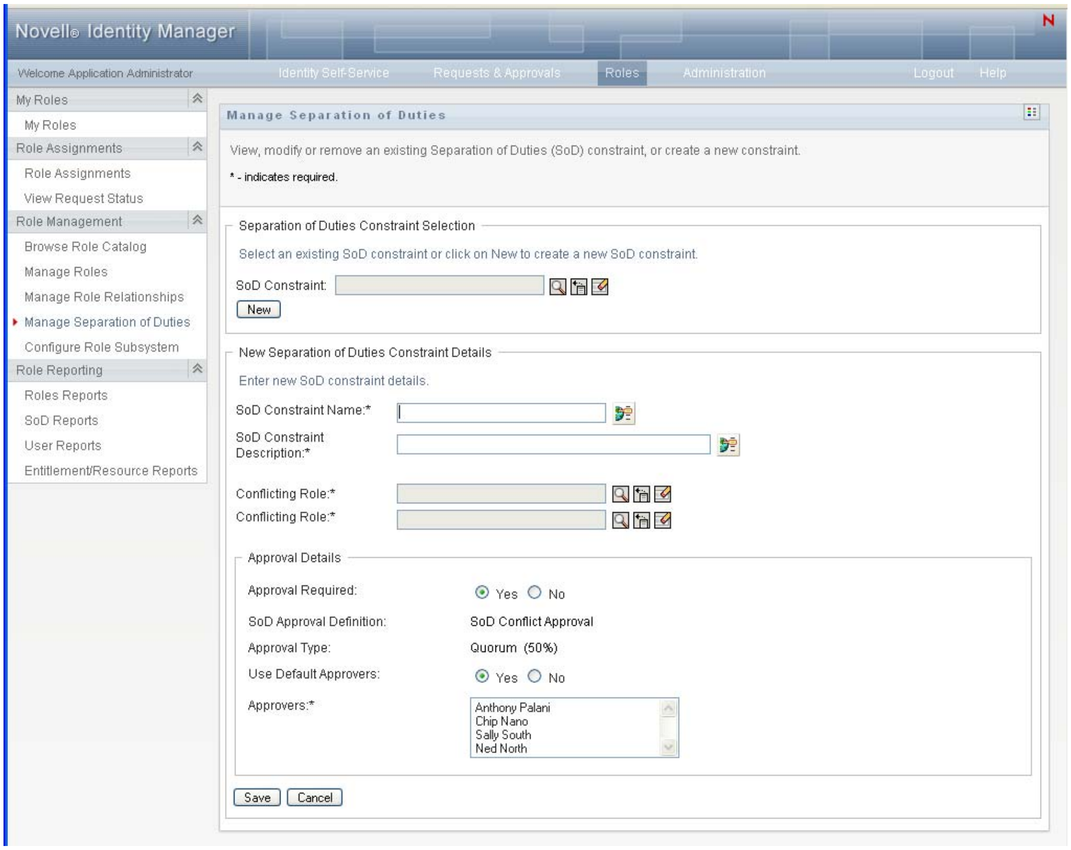
- Section 17.4.1, "Creating New Separation of Duties Constraints," on page 247
- Section 17.4.2, "Modifying Existing SoD Constraints," on page 248
- Section 17.4.3, "SoD Constraint Property Reference," on page 249

Page Access The Manage Separation of Duties page can be accessed by the Role Administrator or Security Officer. The Security Officer requires Browse rights to the SoDDef container in the Identity Vault, but does not require browse rights to roles.

17.4.1 Creating New Separation of Duties Constraints

1 Click *Manage Separation of Duties* in the list of *Role Management* actions.

2 Click *New*.



Manage Separation of Duties

View, modify or remove an existing Separation of Duties (SoD) constraint, or create a new constraint.

* - indicates required.

Separation of Duties Constraint Selection

Select an existing SoD constraint or click on New to create a new SoD constraint.

SoD Constraint:

New Separation of Duties Constraint Details

Enter new SoD constraint details.

SoD Constraint Name:*

SoD Constraint Description:*

Conflicting Role:*

Conflicting Role:*

Approval Details

Approval Required:	● Yes ○ No
SoD Approval Definition:	SoD Conflict Approval
Approval Type:	Quorum (50%)
Use Default Approvers:	● Yes ○ No
Approvers:*	Anthony Palani Chip Nano Sally South Ned North

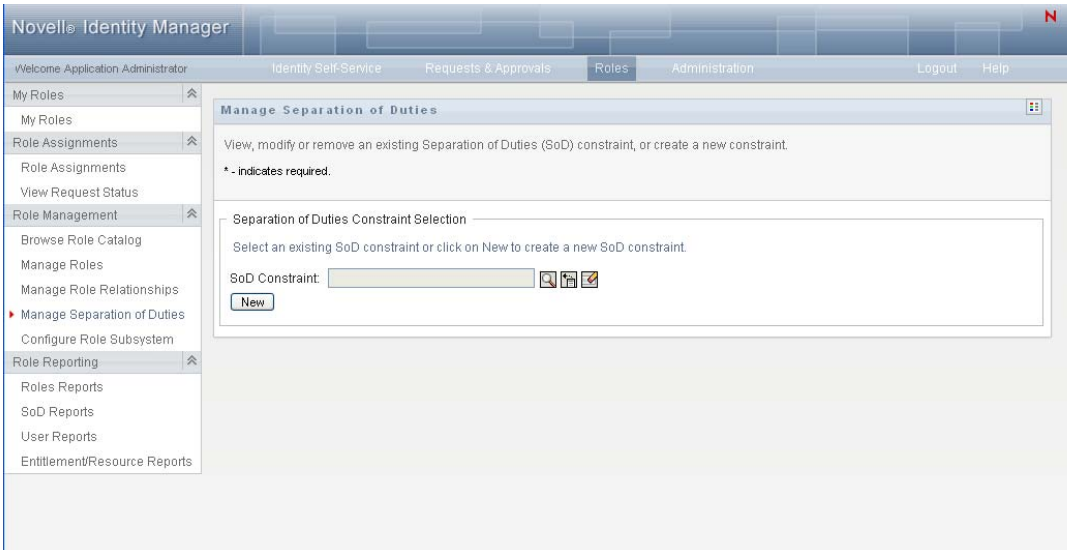
3 Navigate to the *New Separation of Duty Constraint Details*. For information on completing the fields, see Table 17-5 on page 249.

4 Navigate to the *Approval Details* section. For information on completing the fields, see Table 17-6 on page 250.

5 Click *Save* to make your changes permanent.

17.4.2 Modifying Existing SoD Constraints

1 Click *Manage Separation of Duties* in the *Role Management* group of actions.



Manage Separation of Duties

View, modify or remove an existing Separation of Duties (SoD) constraint, or create a new constraint.

* - indicates required.

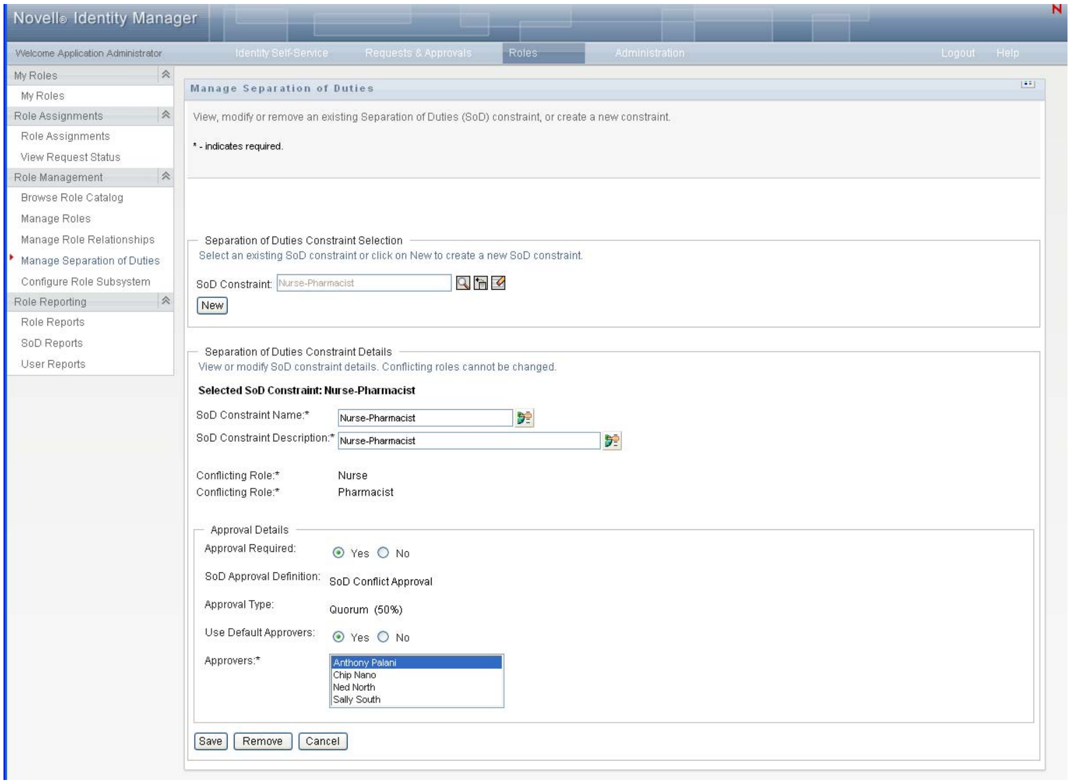
Separation of Duties Constraint Selection

Select an existing SoD constraint or click on New to create a new SoD constraint.

SoD Constraint:

2 To view or modify an existing SoD constraint, use the Use the *Object Selector* or the *Show History* tool to select the constraint. For details on using the *Object Selector* and *Show History* tools, see "Using the Object Selector Button for Searching" on page 26.

3 Select the SoD you want from the list. The lookup page closes and displays the *Separation of Duties Constraints Details* and *Approval Details* for the selected SoD.



Manage Separation of Duties

View, modify or remove an existing Separation of Duties (SoD) constraint, or create a new constraint.

* - indicates required.

Separation of Duties Constraint Selection

Select an existing SoD constraint or click on New to create a new SoD constraint.

SoD Constraint: Nurse-Pharmacist

Separation of Duties Constraint Details

View or modify SoD constraint details. Conflicting roles cannot be changed.

Selected SoD Constraint: Nurse-Pharmacist

SoD Constraint Name:* Nurse-Pharmacist

SoD Constraint Description:* Nurse-Pharmacist

Conflicting Role:* Nurse

Conflicting Role:* Pharmacist

Approval Details

Approval Required: ● Yes ○ No

SoD Approval Definition: SoD Conflict Approval

Approval Type: Quorum (50%)

Use Default Approvers: ● Yes ○ No

Approvers:* Anthony Palani, Chip Nano, Ned North, Sally South

4 For information on filling in the fields, see Table 17-5, “Separation of Duty Constraint Details,” on page 249 and Table 17-6, “Approval Details,” on page 250.

5 Click *Save* to make your changes permanent.

17.4.3 SoD Constraint Property Reference

- Table 17-5, “Separation of Duty Constraint Details,” on page 249
- Table 17-6, “Approval Details,” on page 250

Table 17-5 *Separation of Duty Constraint Details*

Field	Description
SoD Constraint Name	The name of the constraint. It is displayed in reports and when the user requests a constraint exception.You cannot include the following characters in the *SoD Constraint Name* when you create a constraint: `< > , ; \ " +  # = / | & *` You can localize it in any of the supported languages by clicking . This name can also be supplied in the SoD Editor in Designer for Identity Manager.
SoD Constraint Description	The description of the constraint. You can localize it in any of the supported languages by clicking . This name can be supplied in the SoD Editor in Designer for Identity Manager.
Conflicting Role	The name of the role for which you want to define a constraint. A role defines a set of privileges related to one or more target systems or applications. This field is read-only during a modify operation.
Conflicting Role	The name of the role in conflict. Click *Browse* to locate an existing role from the available roles. This field is read-only during a modify operation.

NOTE: It is important to specify the two roles in conflict. The order that you specify the roles in conflict does not matter.

Table 17-6 Approval Details

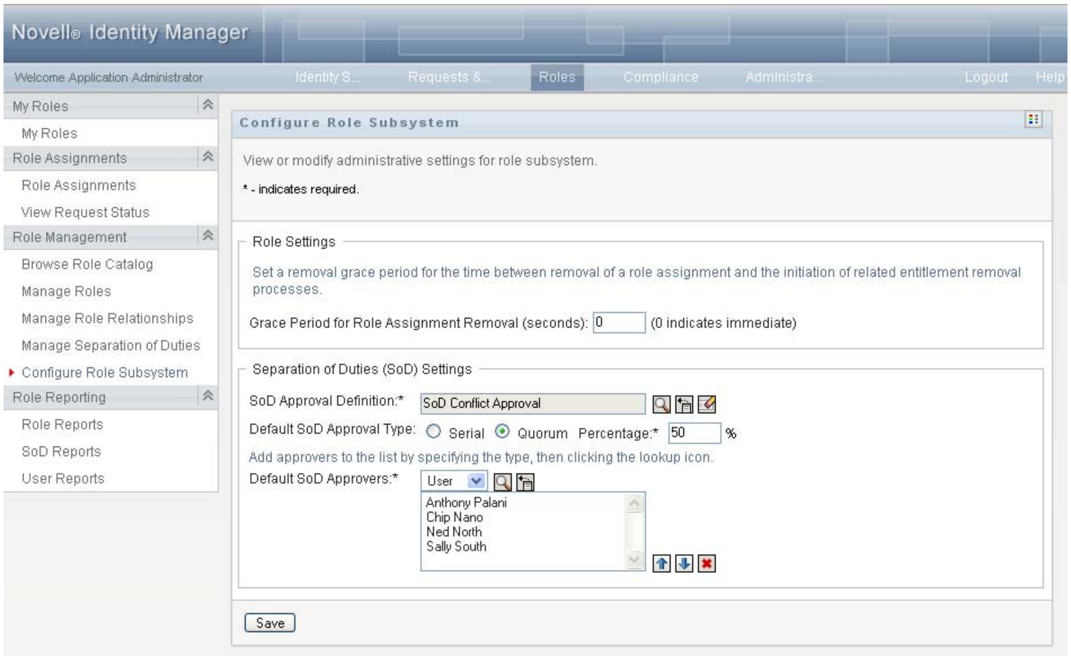
Field	Description
Approval Required	Select Yes if you want to launch a workflow when a user requests an exception to the SoD constraint. **NOTE:** If the is SoD Exception results from an implicit assignment, such as through group or container membership, choosing Yes does not result in approval workflow starting. The SoD exception is always granted, and it is logged as such. Select *No* if the user can request an exception to the SoD constraint and no approval is required. In this case, the exception is always approved.
SoD Approval Definition	Displays the read-only name of the provisioning request definition that executes when a user requests an SoD constraint exception. The value is derived from the Roles Configuration object. It is only executed when the *Approval Required* is *Yes*.
Approval Type	A read-only field that displays the processing type for the provisioning request definition displayed above. This value is derived from the Roles Configuration object.
Use Default Approvers	Select *Yes* if the approvers are specified in the Role Subsystem. Select *User* if the SoD approval task should be assigned to one or more users.Select *Group* if the SoD approval task should be assigned to a group. Select *Role* if the SoD approval task should be assigned to a role. To locate a specific user, group, or role, use the Object Selector or History buttons as described in Section 1.4.4, "Common User Actions," on page 25. To change the order of the approvers in the list or to delete an approver, use the buttons as described in Section 1.4.4, "Common User Actions," on page 25.

17.5 Configuring the Role Subsystem

The *Configuring Role Subsystem* action on the *Roles* tab of the Identity Manager user interface allows you to specify administrative settings for the Role Subsystem.

To define Role subsystem administrative settings:

1 Click *Configure Role Subsystem* in the *Role Management* group of actions.



Configure Role Subsystem

View or modify administrative settings for role subsystem.

* - indicates required.

Role Settings

Set a removal grace period for the time between removal of a role assignment and the initiation of related entitlement removal processes.

Grace Period for Role Assignment Removal (seconds): 0 (0 indicates immediate)

Separation of Duties (SoD) Settings

SoD Approval Definition:* SoD Conflict Approval

Default SoD Approval Type: ○ Serial ● Quorum Percentage:* 50 %

Add approvers to the list by specifying the type, then clicking the lookup icon.

Default SoD Approvers:* User

Anthony Palani
Chip Nano
Ned North
Sally South

2 Specify (in seconds) a *Grace Period for Role Assignment Removal*.

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.

3 Choose the provisioning request definition to run when an SoD exception request is made. You can specify one definition per User Application driver.

3a To find a provisioning request definition use the Object Selector or History buttons as described in Section 1.4.4, "Common User Actions," on page 25.

4 Choose a *Default SoD Approval Type* of *Serial* or *Quorum*.

Field	Description
Serial	Select Serial if you want the role to be approved by all of the users in the *Approvers* list. The approvers are processed sequentially in the order they appear in the list.
Quorum	Select *Quorum* if you want the role to be approved by a percentage of the users in the *Approvers* list. The approval is complete when the percentage of users specified is reached. 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.

5 Modify the *Default SoD Approvers*.

Field	Description
Default SoD Approvers	Select *User* if the role approval task should be assigned to one or more users.Select *Group* if the role approval task should be assigned to a group. Only one member of the group needs to approve. Select *Role* if the role approval task should be assigned to a role. Like groups, only one member of the role needs to approve. 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 Section 1.4.4, “Common User Actions,” on page 25

6 Click *Save* to make your choices permanent.

Creating and Viewing Role Reports

18

This section describes Role reports and how to create and view them. 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.

Topics in this section include:

- Section 18.1, "About the Role Reporting Actions," on page 253
- Section 18.2, "Role Reports," on page 253
- Section 18.3, "SoD Reports," on page 257
- Section 18.4, "User Reports," on page 259

18.1 About the Role Reporting Actions

The Roles 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.

18.2 Role Reports

Two role reports are available:

- Role List Report
- Role Assignment Report

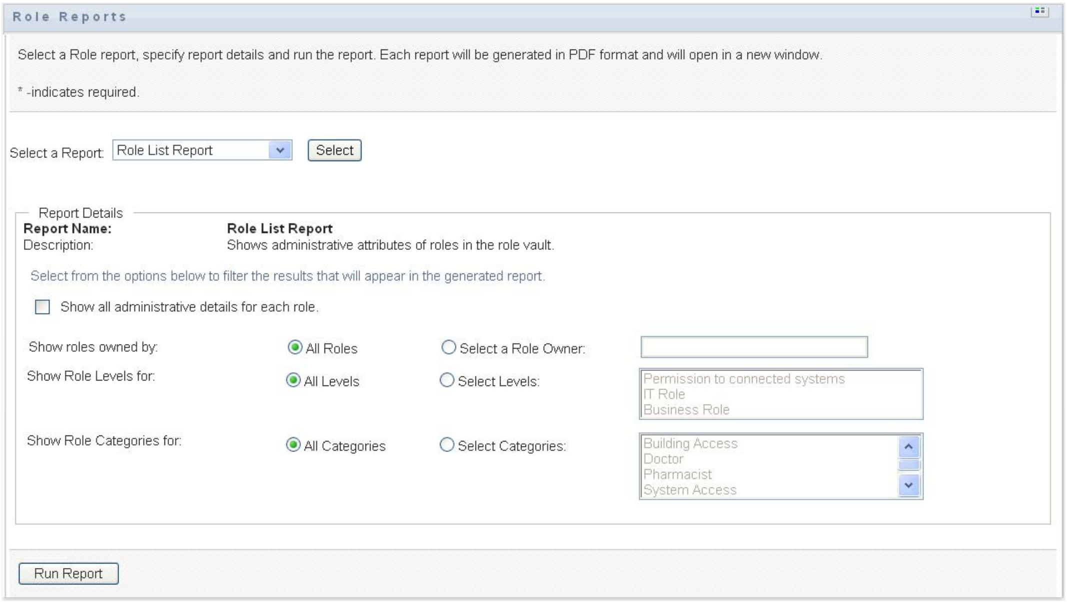
18.2.1 The Role List Report

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 *Roles* > *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 ▾ 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 Check *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 a Role Owner*, the owner selection box activates. Use these icons 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.

📋 Open the history selection dialog. Choose from the Description list of objects, or type characters in the Description box to filter your search and retrieve a shorter list of objects.

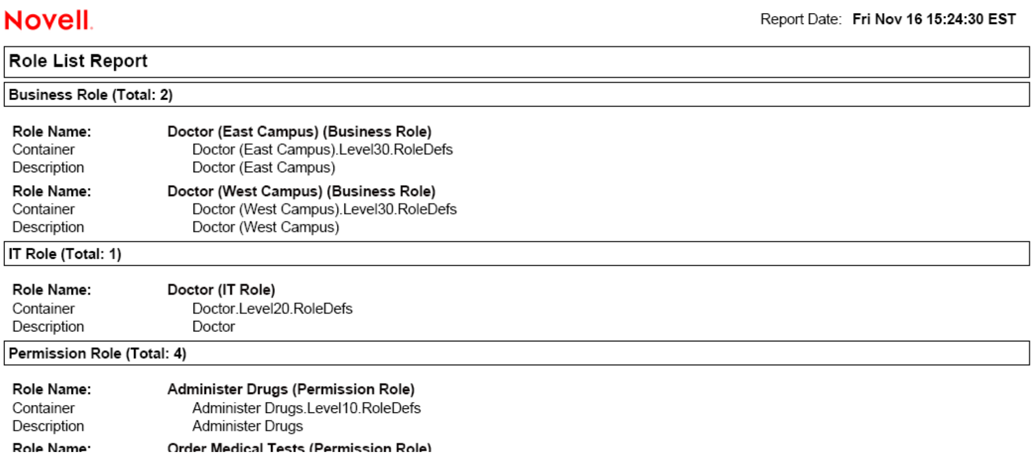
✎ Reset the current selection to no selection.

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 18-1.

***Figure 18-1** Sample Role List Report*



Novell. Report Date: **Fri Nov 16 15:24:30 EST**

Role List Report

Business Role (Total: 2)

Role Name: **Doctor (East Campus) (Business Role)**
Container Doctor (East Campus).Level30.RoleDefs
Description Doctor (East Campus)

Role Name: **Doctor (West Campus) (Business Role)**
Container Doctor (West Campus).Level30.RoleDefs
Description Doctor (West Campus)

IT Role (Total: 1)

Role Name: **Doctor (IT Role)**
Container Doctor.Level20.RoleDefs
Description Doctor

Permission Role (Total: 4)

Role Name: **Administer Drugs (Permission Role)**
Container Administer Drugs.Level10.RoleDefs
Description Administer Drugs

Role Name: **Order Medical Tests (Permission Role)**

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.

18.2.2 The Role Assignment Report

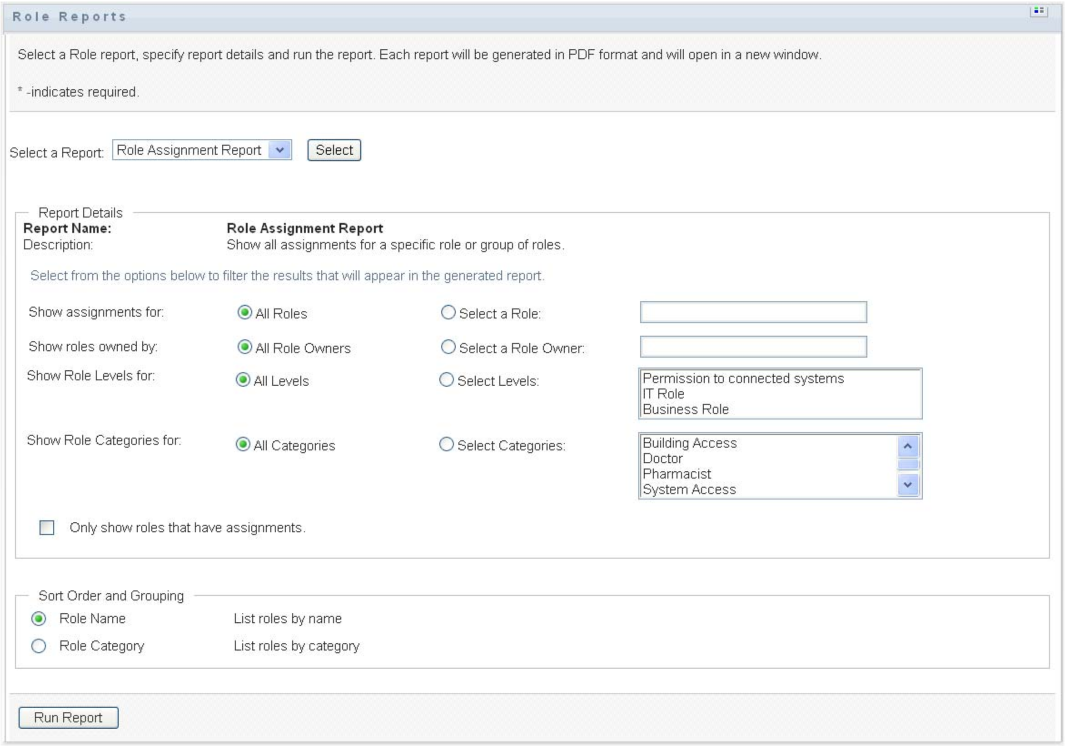
The Role Assignment Report shows:

- 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 *Roles > 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:	Permission to connected systems IT Role Business Role
Show Role Categories for:	● All Categories	○ Select Categories:	Building Access Doctor Pharmacist System Access

□ 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 a selected role. If you choose *Select a Role*, the selection box activates and presents the selection icons described in Step 4 on page 254.

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 254.

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.

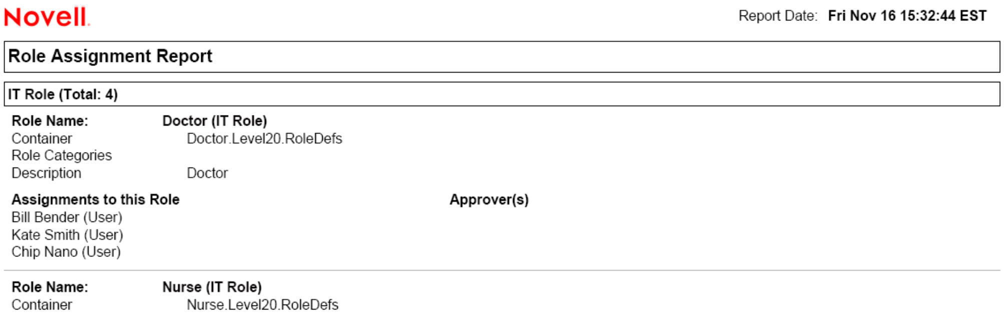
6 Choose to show roles for all role categories or to select one or more role categories. To select a category, click it in the selection pull-down box. To select more than one category, hold down the Shift key or Ctrl key as you click each category.

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 18-2.

Figure 18-2 *Sample Role Assignment Report*



Novell

Report Date: **Fri Nov 16 15:32:44 EST**

Role Assignment Report

IT Role (Total: 4)

Role Name:	**Doctor (IT Role)**
Container	Doctor.Level20.RoleDefs
Role Categories	
Description	Doctor

Assignments to this Role	**Approver(s)**
Bill Bender (User)	
Kate Smith (User)	
Chip Nano (User)	

Role Name:	**Nurse (IT Role)**
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.

18.3 SoD Reports

Two reports describe the current state of separation of duties:

- SoD Constraint Report
- SoD Violations and Exceptions Report

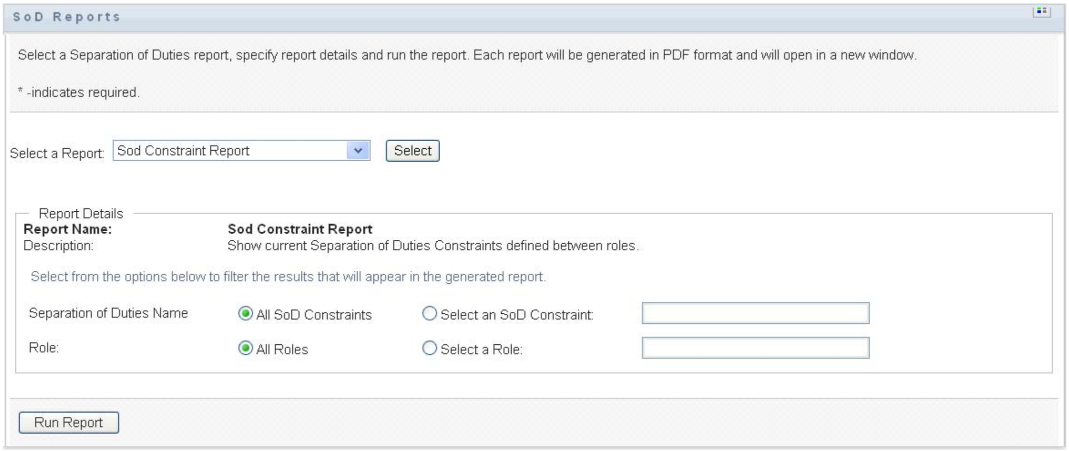
18.3.1 SoD Constraint Report

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 *Roles > 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.



SoD Reports

Select a Separation of Duties 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: Sod Constraint Report [Select]

Report Details

Report Name: **Sod Constraint Report**

Description: Show current Separation of Duties Constraints defined between roles.

Select from the options below to filter the results that will appear in the generated report.

Separation of Duties Name ● All SoD Constraints ○ Select an SoD Constraint:

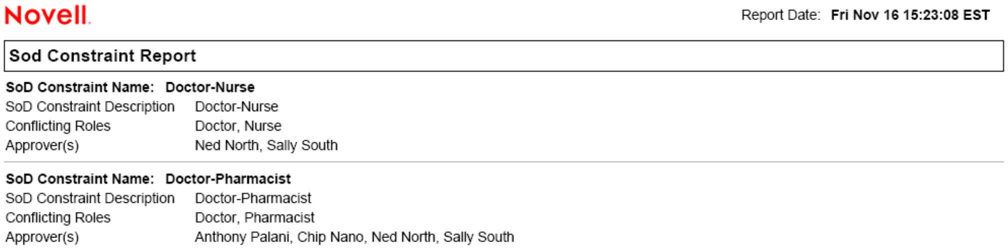
Role: ● All Roles ○ Select a Role:

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 254.

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 254.

5 Click *Run Report* to create and view a PDF report similar to the one in Figure 18-3.

Figure 18-3 *Sample SoD Constraint Report*



Report Date: **Fri Nov 16 15:23:08 EST**

Sod Constraint Report

SoD Constraint Name: Doctor-Nurse

SoD Constraint Description	Doctor-Nurse
Conflicting Roles	Doctor, Nurse
Approver(s)	Ned North, Sally South

SoD Constraint Name: Doctor-Pharmacist

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.

18.3.2 SoD Violations and Exceptions Report

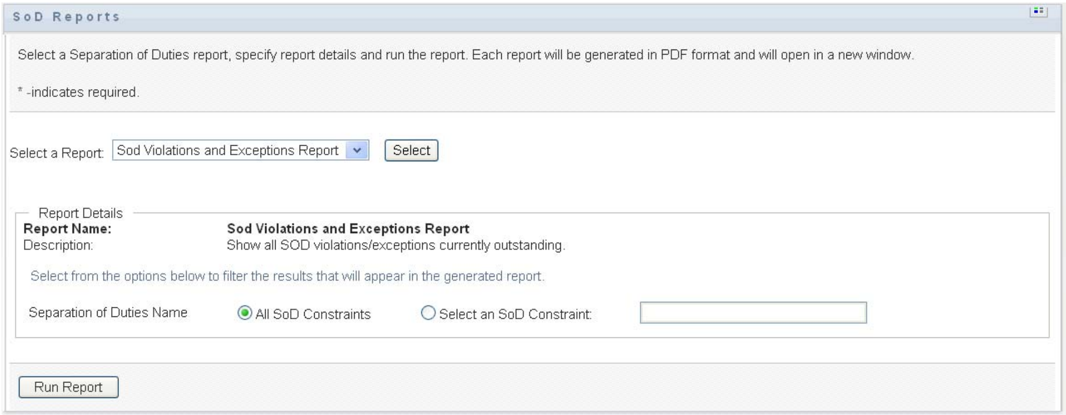
The SoD Violations and Exceptions Report shows:

- 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 *Roles > 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.



SoD Reports

Select a Separation of Duties 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: Sod Violations and Exceptions Report [Select]

Report Details

Report Name: **Sod Violations and Exceptions Report**

Description: Show all SOD violations/exceptions currently outstanding.

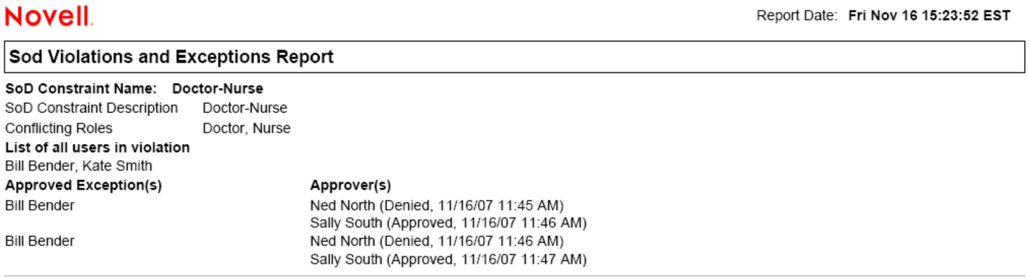
Select from the options below to filter the results that will appear in the generated report.

Separation of Duties Name ● All SoD Constraints ○ Select an SoD Constraint:

[Run 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)	**Approver(s)**
Bill Bender	Ned North (Denied, 11/16/07 11:45 AM) Sally South (Approved, 11/16/07 11:46 AM)
Bill Bender	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.

18.4 User Reports

Two user reports are available:

- User Roles Report
- User Entitlement Report

18.4.1 User Roles Report

The User Roles Report shows:

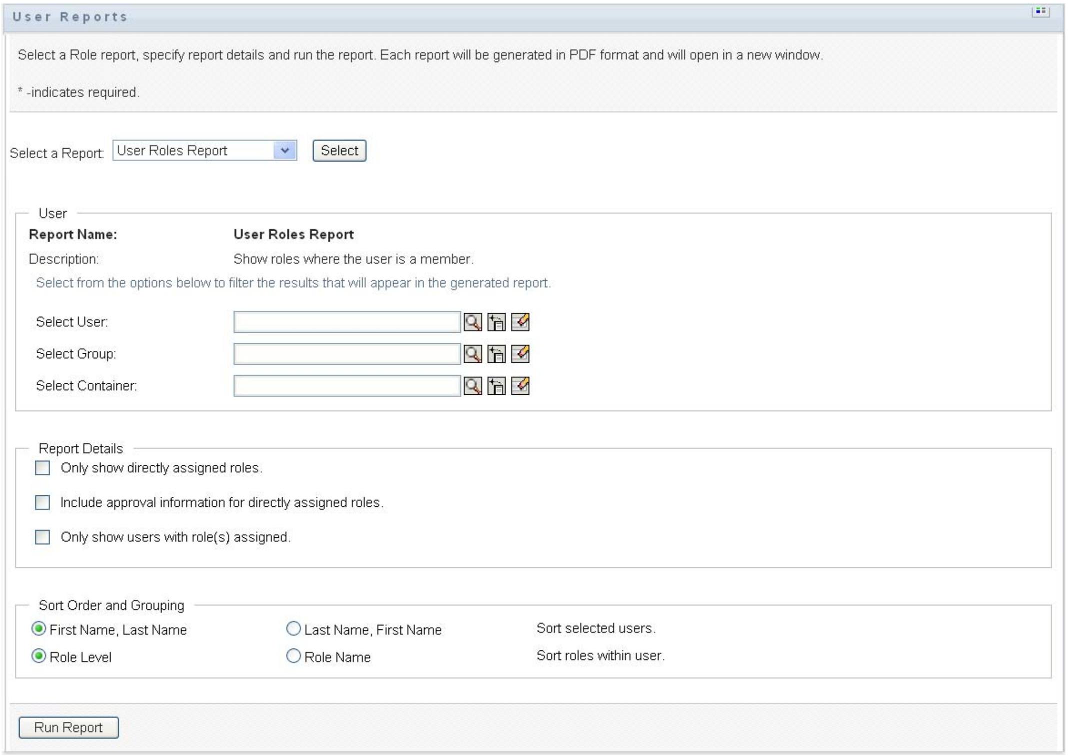
- Selected users, groups of users, or containers of users

- 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 *Roles > User Reports*.

2 Choose *User Roles 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 Roles Report [Select]

User

Report Name: **User Roles Report**

Description: Show roles where the user is a member.

Select from the options below to filter the results that will appear in the generated report.

Select User:

Select Group:

Select Container:

Report Details

□ Only show directly assigned roles.

□ Include approval information for directly assigned roles.

□ Only show users with role(s) assigned.

Sort Order and Grouping

● First Name, Last Name ○ Last Name, First Name Sort selected users.

● Role Level ○ Role Name Sort roles within user.

[Run Report]

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 254.

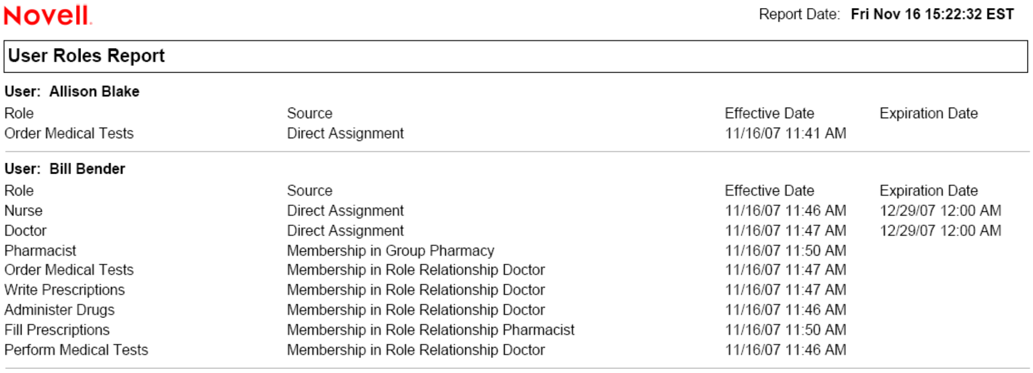
4 In the *Report Details* pane, choose one or more types of detail to report:

Detail	Meaning
Only show directly assigned roles.	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.
Include approval information for directly assigned roles.	The User Roles Report shows who approved each directly assigned role for each user.
Only show users with role(s) assigned.	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

User: Allison Blake

Role	Source	Effective Date	Expiration Date
Order Medical Tests	Direct Assignment	11/16/07 11:41 AM	

User: Bill Bender

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.

18.4.2 User Entitlements Report

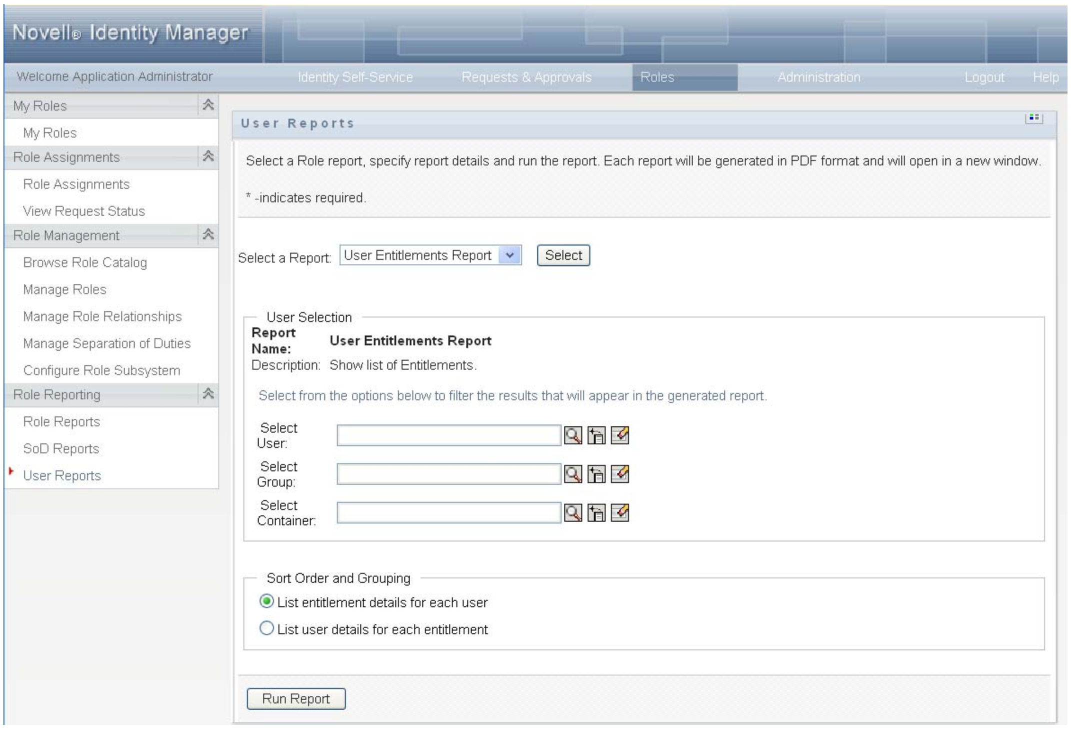
The User Entitlements Report shows:

- 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 *Roles > 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 Entitlements Report [Select]

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

[Run Report]

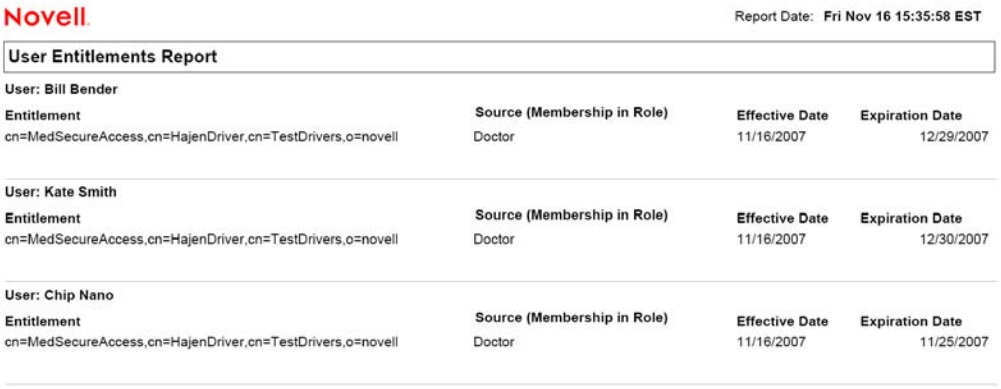
3 In the *User Selection* pane, select the kind of user: an individual user, group, or container. Descriptions of the selection icons are at Step 4 on page 254.

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 18-4 and Figure 18-5.

Figure 18-4 *Sample User Entitlements Report: Entitlement Details for Each User*



Report Date: **Fri Nov 16 15:35:58 EST**

User Entitlements Report

User: Bill Bender

Entitlement	Source (Membership in Role)	Effective Date	Expiration Date
cn=MedSecureAccess,cn=HajenDriver,cn=TestDrivers,o=novell	Doctor	11/16/2007	12/29/2007

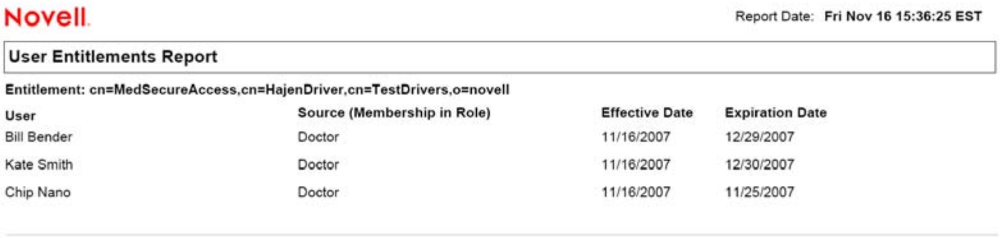
User: Kate Smith

Entitlement	Source (Membership in Role)	Effective Date	Expiration Date
cn=MedSecureAccess,cn=HajenDriver,cn=TestDrivers,o=novell	Doctor	11/16/2007	12/30/2007

User: Chip Nano

Entitlement	Source (Membership in Role)	Effective Date	Expiration Date
cn=MedSecureAccess,cn=HajenDriver,cn=TestDrivers,o=novell	Doctor	11/16/2007	11/25/2007

Figure 18-5 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.

Using the Compliance Tab

V

These sections tell you how to use the *Compliance* tab of the Identity Manager User Application:

Introducing the Compliance Tab 19

This section provides an overview of the Compliance tab. Topics include:

For more general information about accessing and working with the Identity Manager user interface, see Chapter 1, “Getting Started,” on page 15.

19.1 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

Compliance and Proxy mode

Proxy mode works only on the *Requests & Approvals* tab and is not supported on the *Compliance* tab. If you enter proxy mode on the *Requests & Approvals* tab, and then switch to the *Compliance* tab, proxy mode is turned off for both tabs.

19.1.1 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 *My Tasks* list on the *Requests & Approvals* 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 defined by the Compliance Module Administrator or Attestation Manager.

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 uses a set of system roles to secure access to compliance functions. Each menu action in the *Compliance* tab is mapped to one or more system roles. If a user is not a member of one of the security roles defined for compliance, the *Compliance* tab is not available.

The *system roles* for compliance are automatically defined by the system at install time. These include the following:

- Compliance Module Administrator
- Attestation Manager

A Compliance Module Administrator is designated at installation time. After installation, the Role Module Administrator can assign additional users to the Compliance Module Administrator and Attestation Manager roles. To make additional role assignments, the Role Module Administrator uses the *Roles > Role Assignments* page in the User Application.

The system roles are described in detail below:

Table 19-1 *System Roles*

Role	Description
Compliance Module Administrator	A system role that allows members to perform all functions on the Compliance tab, including those that the Attestation Manager can perform. **NOTE:** In release 3.6.1 of the Roles Based Provisioning Module, the capabilities of the Compliance Module Administrator are exactly the same as those given to the Attestation Manager. In a future release, the Compliance Module Administrator may be given additional capabilities, as new features are added to the *Compliance* tab.

Role	Description
Attestation Manager	A system role that allows members to perform all attestation functions. These functions are listed below: ◆ Request user profile attestation processes. ◆ Request SoD violation attestation processes. ◆ Request role assignment attestation processes. ◆ Request user assignment attestation processes. ◆ View the status for all attestation requests that have been submitted. **NOTE:** Any user can be defined as an attester for an attestation process. An attester does not need to belong to either the Attestation Manager or Compliance Module Administrator role.

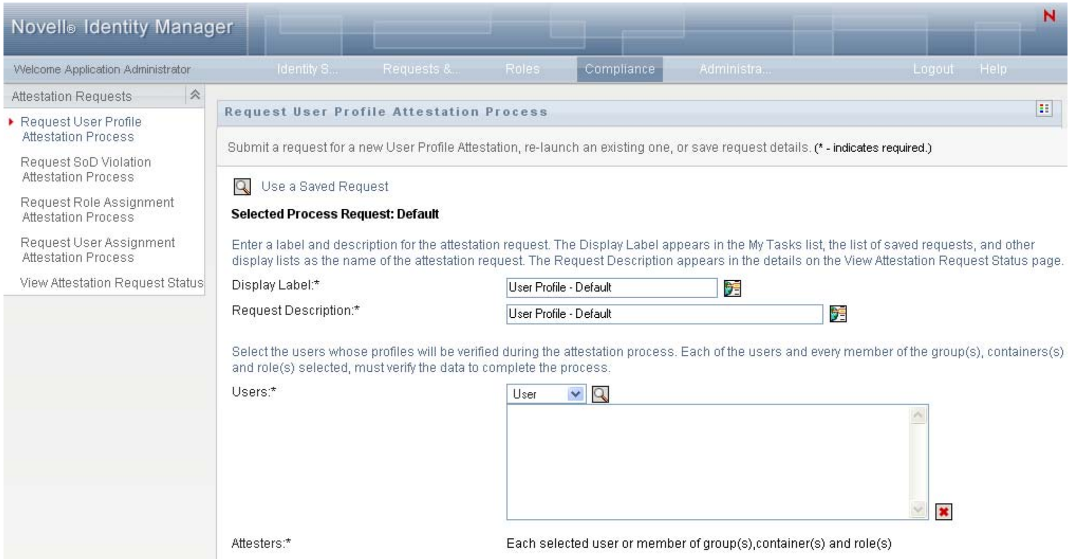
The *Compliance* tab does not allow access by authenticated users that do not have membership in either of the system roles listed above.

19.2 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.


Novell® Identity Manager
Welcome Application Administrator
Identity S...
Requests &...
Roles
Compliance
Administra...
Logout
Help
Attestation Requests
Request User Profile Attestation Process
Request SoD Violation Attestation Process
Request Role Assignment Attestation Process
Request User Assignment Attestation Process
View Attestation Request Status
Use a Saved Request

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.)

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:* User Profile - Default

Request Description:* User Profile - Default

Select the users whose profiles will be verified during the attestation process. Each of the users and every member of the group(s), containers(s) and role(s) selected, must verify the data to complete the process.

Users:* User

Attesters:* Each selected user or member of group(s),container(s) and role(s)

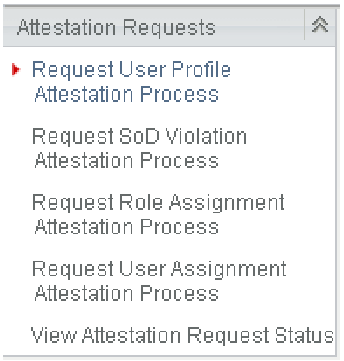
If you go to another tab in the user interface but then want to return, you just need to click the *Compliance* tab to open it again.

19.3 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 19-1 *Compliance Tab Menu*



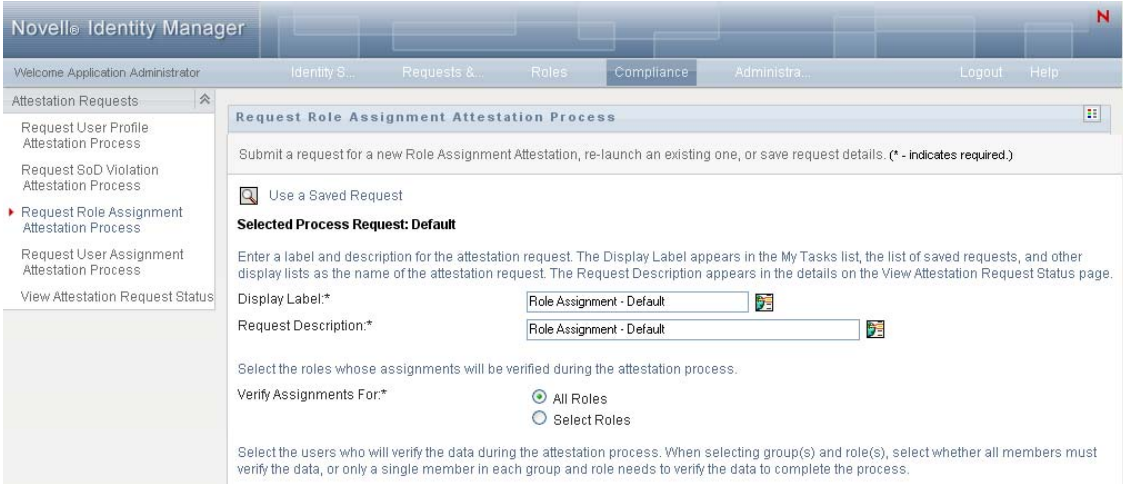
Attestation Requests

- Request User Profile Attestation Process
- Request SoD Violation Attestation Process
- Request Role Assignment Attestation Process
- Request User Assignment Attestation Process
- View Attestation Request Status

The *Attestation Requests* actions are only displayed if you are a Compliance Module Administrator or Attestation Manager.

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 19-2 *Page Displayed for an Action*



Novell® Identity Manager
Welcome Application Administrator
Identity S...
Requests &...
Roles
Compliance
Administra...
Logout
Help
Attestation Requests
Request User Profile Attestation Process
Request SoD Violation Attestation Process
Request Role Assignment Attestation Process
Request User Assignment Attestation Process
View Attestation Request Status

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:*	Role Assignment - Default
Request Description:*	Role Assignment - Default

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.

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 19.5, “Understanding the Attestation Requests Legend,” on page 272.

19.4 Compliance Actions You Can Perform

Here’s a summary of the actions that are available to you by default on the *Compliance* tab:

Table 19-2 *Compliance Actions*

Category	Action	Description
Attestation Requests	Request User Profile Attestation Process	Submits a request for an attestation process to verify user profile information. For details, see Section 20.2, “Requesting User Profile Attestation Processes,” on page 281.
	Request SoD Violation Attestation Process	Submits a request for an attestation process to verify the violations and exceptions for a set of SoD constraints. For details, see Section 20.3, “Requesting SoD Violation Attestation Processes,” on page 283.
	Request Role Assignment Attestation Process	Submits a request for an attestation process to verify assignments for selected roles. For details, see Section 20.4, “Requesting Role Assignment Attestation Processes,” on page 285.
	Request User Assignment Attestation Process	Submits a request for an attestation process to verify assignments for selected users. For details, see Section 20.5, “Requesting User Assignment Attestation Process,” on page 287.
	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. For details, see Section 20.6, “Checking the Status of Your Attestation Requests,” on page 289.

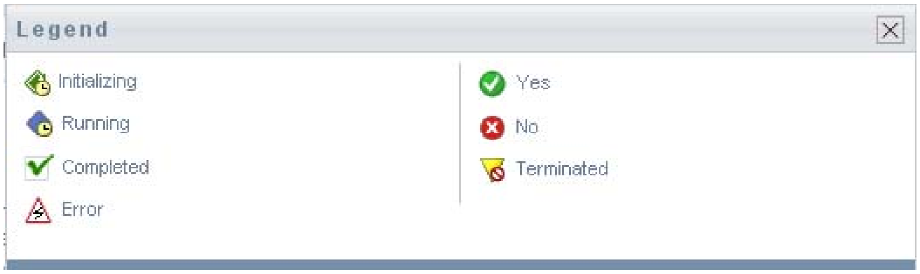
19.5 Understanding the Attestation Requests Legend

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 9-2:

Figure 19-3 *The Legend Button*

The legend provides a brief description of the icons used throughout the *Compliance* tab. The figure below shows the legend.

Figure 19-4 Compliance Legend



The table below provides detailed descriptions of the icons in the legend:

Table 19-3 Legend Icons

Icon	Description
Initializing	Indicates that an attestation request has started. 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.
Running	Indicates that an attestation request is still in process. Appears on the View Attestation Request Status page.
Completed	Indicates that an attestation request has completed processing. Appears on the View Attestation Request Status page.
Error	Indicates that an error occurred during the course of processing. Appears on the View Attestation Request Status page.
Yes	Indicates that an attester verified that the information for an attestation process is correct. Appears on the View Attestation Request Status page.
No	Indicates that an attester has invalidated the information for an attestation process. Appears on the View Attestation Request Status page.
Terminated	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. Appears on the View Attestation Request Status page.

19.6 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 19.6.1, "Specifying the Label and Description for a Request," on page 274

- Section 19.6.2, “Defining the Attesters,” on page 274
- Section 19.6.3, “Specifying the Deadline,” on page 275
- Section 19.6.4, “Defining the Attestation Form,” on page 276
- Section 19.6.5, “Submitting an Attestation Request,” on page 277
- Section 19.6.6, “Saving Request Details,” on page 278
- Section 19.6.7, “Using a Saved Request,” on page 279

19.6.1 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*.

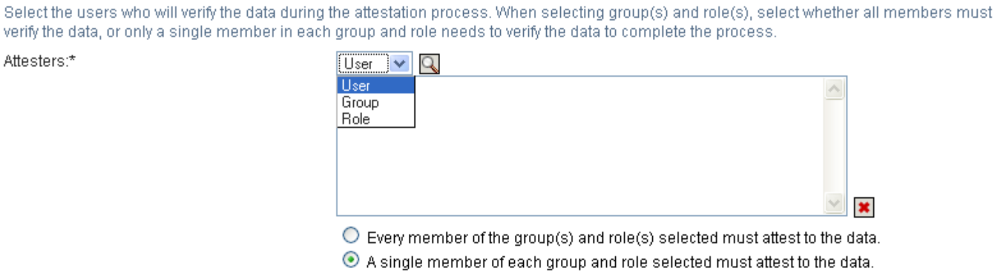
19.6.2 Defining the Attesters

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:* User

○ 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.

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 25.

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.

19.6.3 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.

19.6.4 Defining the Attestation Form

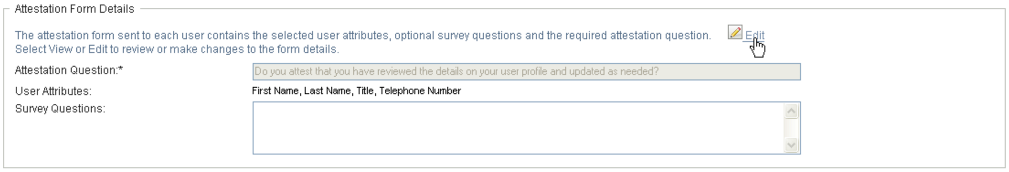
You need to define an attestation form for all attestation types. The *Compliance* tab provides a consistent interface for doing this.

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.



Attestation Form Details

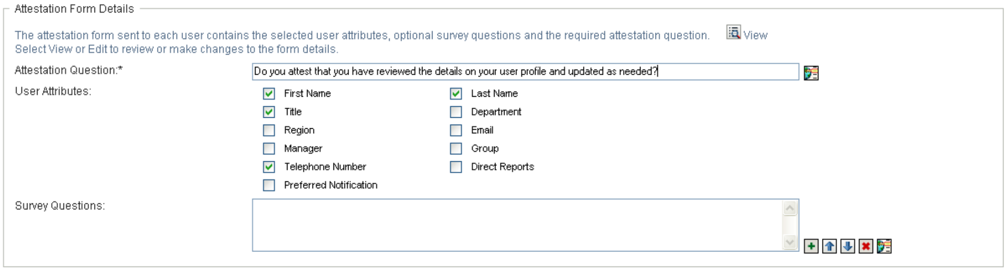
The attestation form sent to each user contains the selected user attributes, optional survey questions and the required attestation question.
Select View or Edit to review or make changes to the form details.

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

User Attributes: First Name, Last Name, Title, Telephone Number

Survey Questions:

2b Type the attestation question in the *Attestation Question* field.



Attestation Form Details

The attestation form sent to each user contains the selected user attributes, optional survey questions and the required attestation question.
Select View or Edit to review or make changes to the form details.

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

User Attributes:

☑ First Name
☑ Title
□ Region
□ Manager
☑ Telephone Number
□ Preferred Notification
☑ Last Name
□ Department
□ Email
□ Group
□ Direct Reports

Survey Questions:

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*.

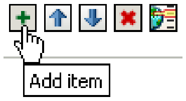
2c For a user profile attestation process, you need to indicate which user attributes you want to verify. In the *User Attributes* field, select each attribute you want to include.

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.

19.6.5 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.

The following fields are required to launch a request:

Table 19-4 *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.

19.6.6 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 19-5 *Fields Required for a Saved Request*

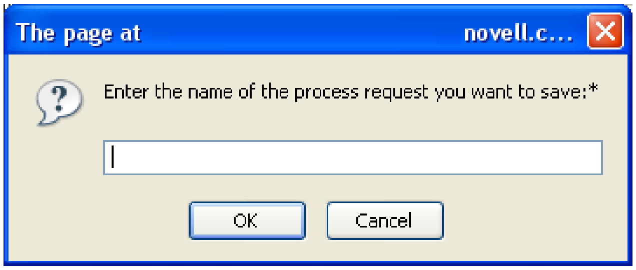
Attestation Type	Required Fields
User Profile	Display Label, Request Description, Attestation Question
SoD Violation	Display Label, Request Description, SoD Constraints, Report Locale, Attestation Question
Role Assignment	Display Label, Request Description, Roles, Report Locale, Attestation Question
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 page at novell.c...

Enter the name of the process request you want to save:*

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.

19.6.7 Using a Saved Request

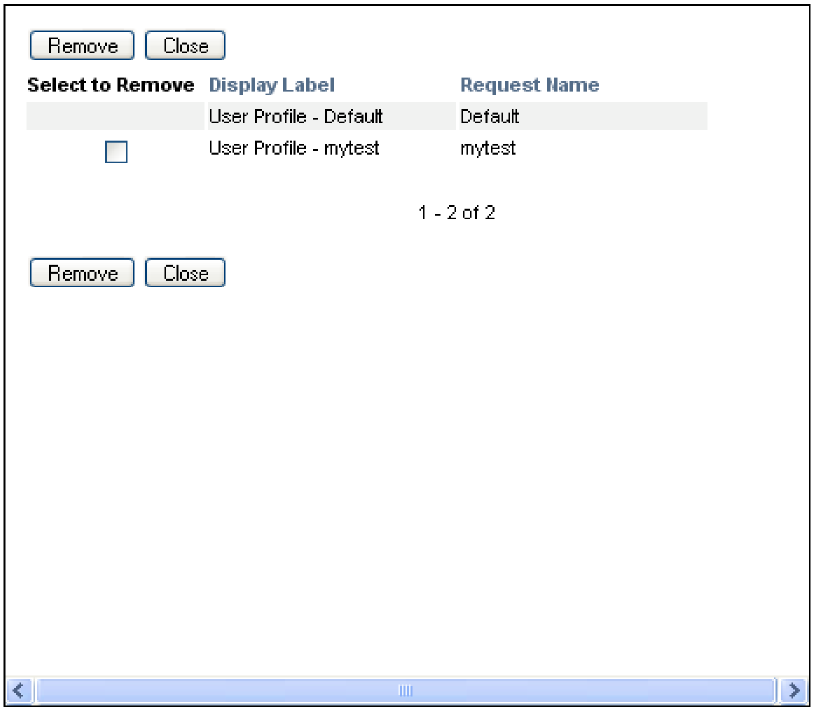
When you’re making an attestation request, you have the option to use details from a previously saved request as the basis for the new request. The saved requests that are available for selection vary depending on the type of attestation process you are requesting. For example, if you are making a user 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.



Select to Remove	Display Label	Request Name
	User Profile - Default	Default
□	User Profile - mytest	mytest

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.

Making Attestation Requests

20

This section provides instructions for making attestation requests. Topics include:

20.1 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.

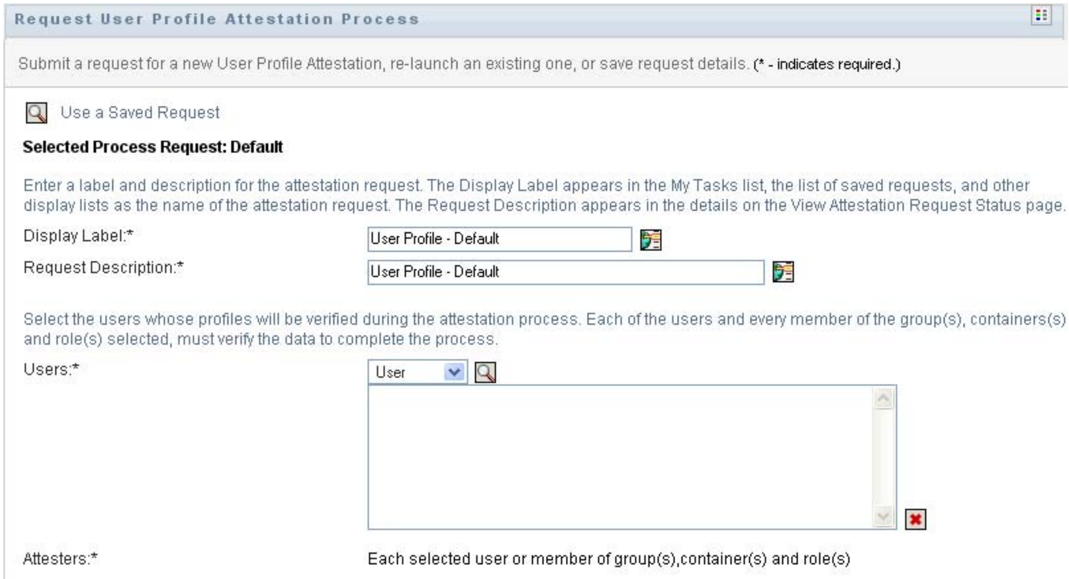
20.2 Requesting User Profile Attestation Processes

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:* User Profile - Default

Request Description:* User Profile - Default

Select the users whose profiles will be verified during the attestation process. Each of the users and every member of the group(s), containers(s) and role(s) selected, must verify the data to complete the process.

Users:* User

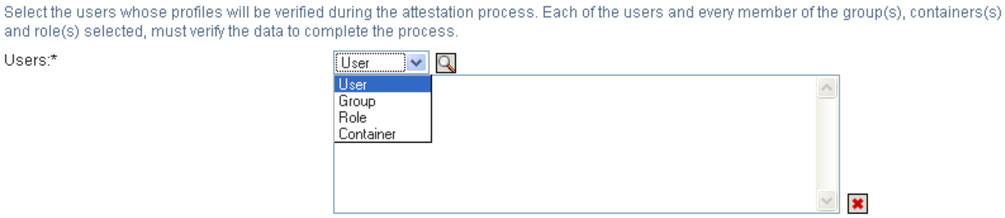
Attesters:* Each selected user or member of group(s),container(s) and role(s)

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 19.6.7, “Using a Saved Request,” on page 279.

3 Specify the display label and description for the request. For more information, see Section 19.6.1, “Specifying the Label and Description for a Request,” on page 274.

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), containers(s) and role(s) selected, must verify the data to complete the process.

Users:* User

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 25.

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 19.6.3, “Specifying the Deadline,” on page 275.

7 Define the details of the attestation form. For more information, see Section 19.6.4, “Defining the Attestation Form,” on page 276.

8. Submit the request. For more information, see Section 19.6.5, “Submitting an Attestation Request,” on page 277.
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 19.6.6, “Saving Request Details,” on page 278.

20.3 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.

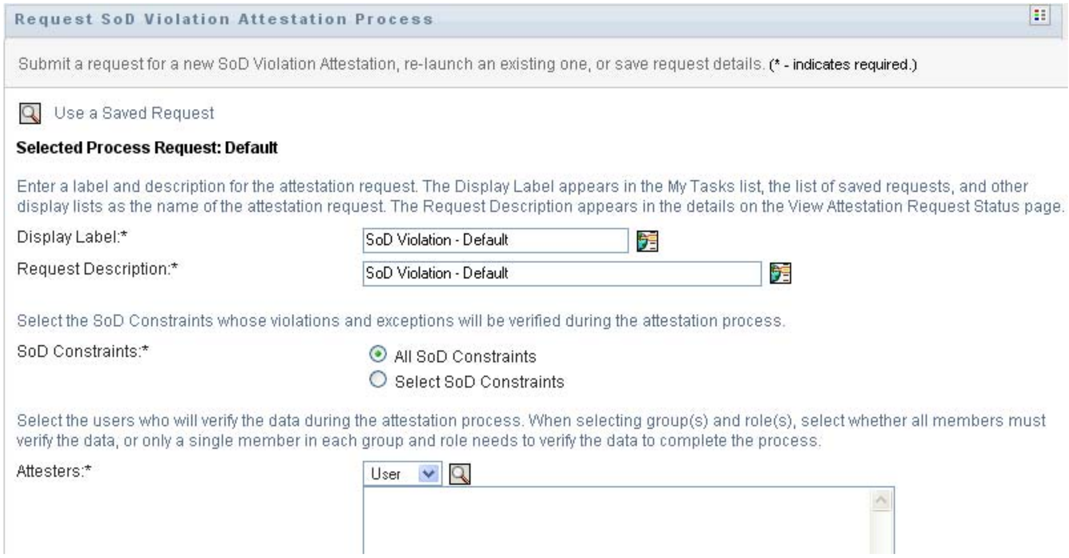
When you initiate an SoD attestation process, the User Application generates a set of localized reports for the attesters to review.

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.



Request SoD Violation Attestation Process

Submit a request for a new SoD Violation 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:* SoD Violation - Default

Request Description:* SoD Violation - Default

Select the SoD Constraints whose violations and exceptions will be verified during the attestation process.

SoD Constraints:* ● All SoD Constraints ○ Select SoD Constraints

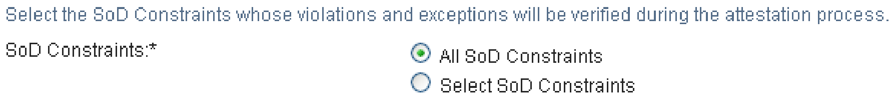
Select the users who will verify the data during the attestation process. When selecting group(s) and role(s), select whether all members must verify the data, or only a single member in each group and role needs to verify the data to complete the process.

Attesters:* User

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 19.6.7, “Using a Saved Request,” on page 279.
3. Specify the display label and description for the request. For more information, see Section 19.6.1, “Specifying the Label and Description for a Request,” on page 274.

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 attestation 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 25.

You must select at least one SoD constraint to launch an attestation 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 attestation process. For details, see Section 19.6.2, “Defining the Attesters,” on page 274.

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 19.6.3, “Specifying the Deadline,” on page 275.

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 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 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 19.6.4, “Defining the Attestation Form,” on page 276.

9 Submit the request. For more information, see Section 19.6.5, “Submitting an Attestation Request,” on page 277.

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 19.6.6, “Saving Request Details,” on page 278.

20.4 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.

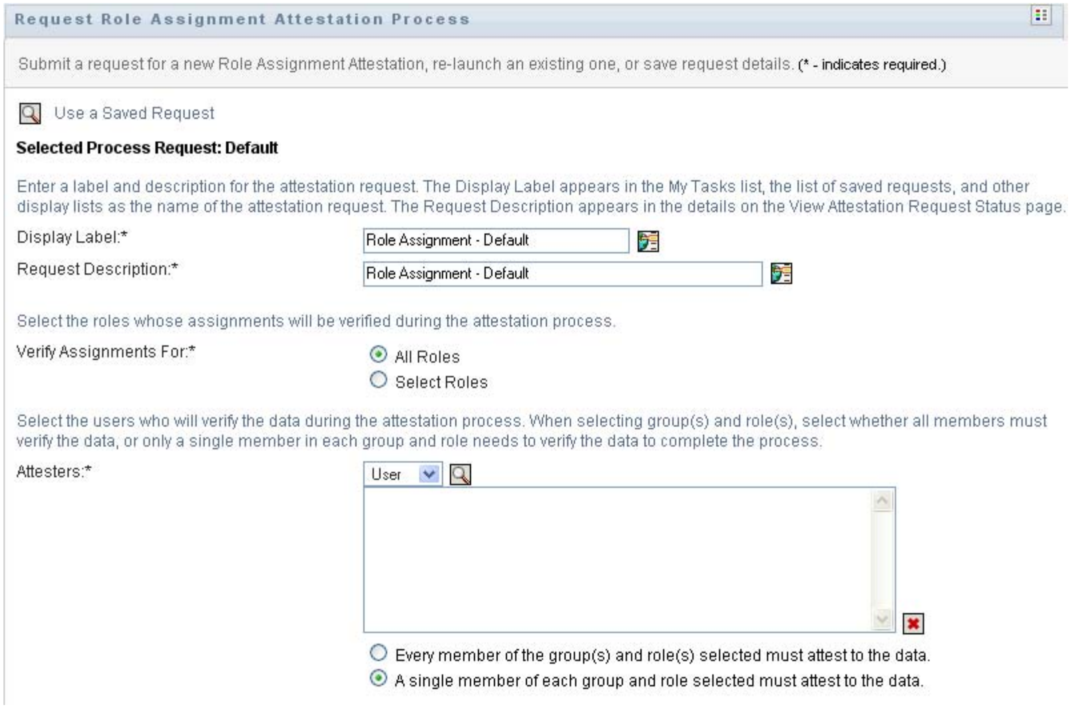
The attesters do not need to have rights for the selected roles to review the reports. If an attester selected for a role assignment attestation process does not have rights to view a particular role, the User Application still allows the attester to view the report showing the role assignments.

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:* Role Assignment - Default

Request Description:* Role Assignment - Default

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:* User

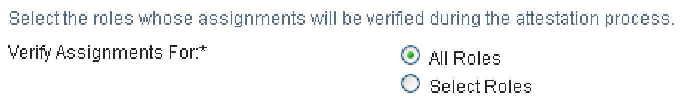
○ Every member of the group(s) and role(s) selected must attest to the data.
● A single member of each group and role selected must attest to the data.

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 19.6.7, “Using a Saved Request,” on page 279.

3 Specify the display label and description for the request. For more information, see Section 19.6.1, “Specifying the Label and Description for a Request,” on page 274.

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 25.

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 19.6.2, “Defining the Attesters,” on page 274.

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 19.6.3, “Specifying the Deadline,” on page 275.

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 19.6.4, “Defining the Attestation Form,” on page 276.

9 Submit the request. For more information, see Section 19.6.5, “Submitting an Attestation Request,” on page 277.

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 19.6.6, “Saving Request Details,” on page 278.

20.5 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.

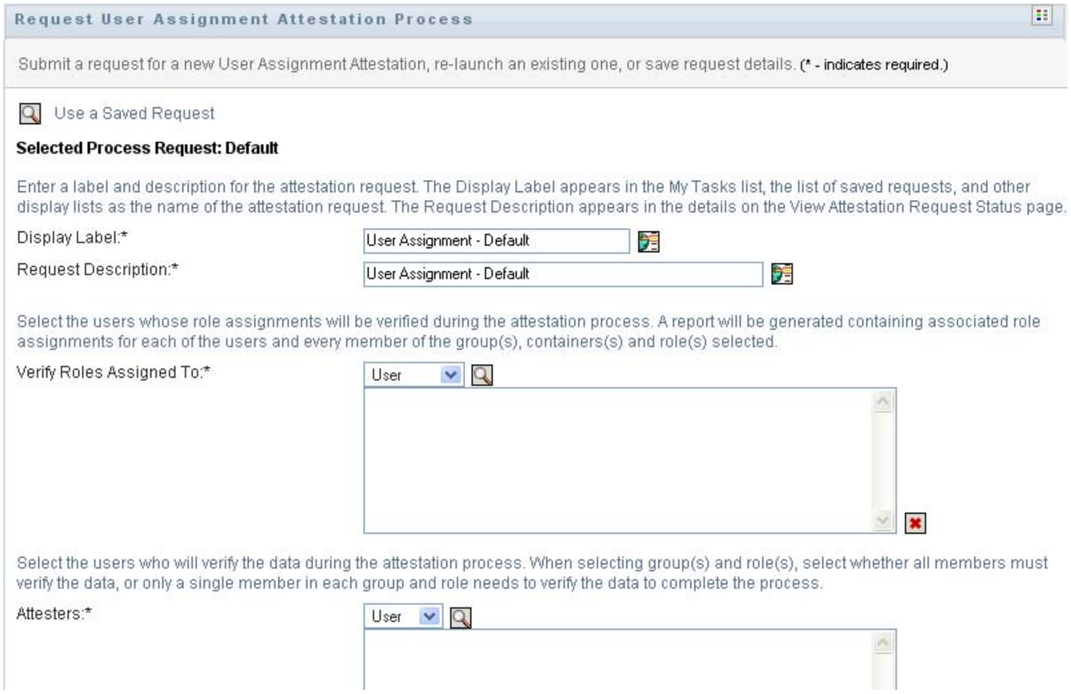
The attesters do not need to have rights for the roles associated with the selected users to review the reports. If an attester selected for a user assignment attestation process does not have rights to view a particular role, the User Application still allows the attester to view the report showing 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:* User Assignment - Default

Request Description:* User Assignment - Default

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

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.

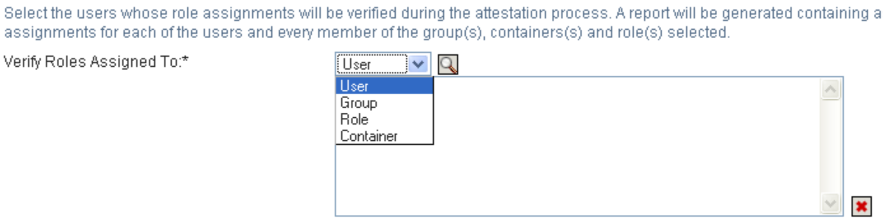
Attesters:* User

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 19.6.7, "Using a Saved Request," on page 279.

3 Specify the display label and description for the request. For more information, see Section 19.6.1, "Specifying the Label and Description for a Request," on page 274.

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

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 25.

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 19.6.2, “Defining the Attesters,” on page 274.

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 19.6.3, “Specifying the Deadline,” on page 275.

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 19.6.4, “Defining the Attestation Form,” on page 276.

9 Submit the request. For more information, see Section 19.6.5, “Submitting an Attestation Request,” on page 277.

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 19.6.6, “Saving Request Details,” on page 278.

20.6 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.

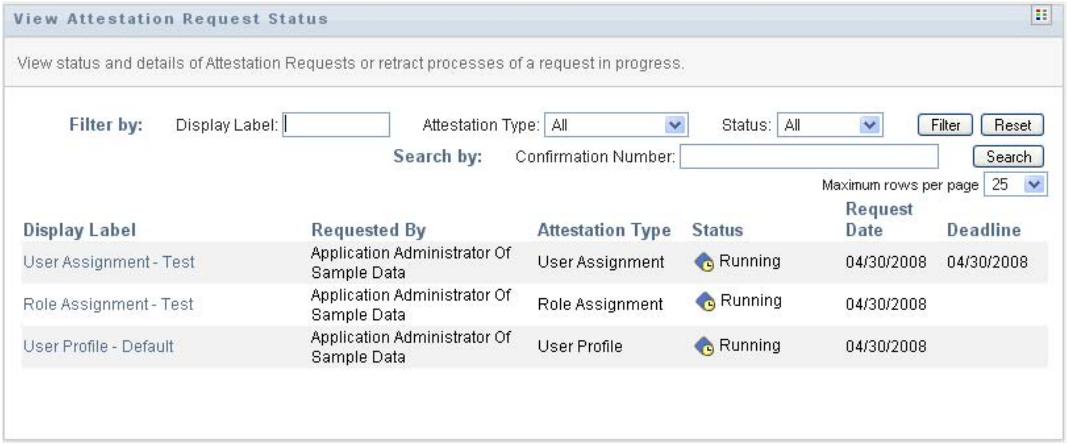
The *View Attestation Request Status* action shows all attestation requests, including those that are initializing, running, completed, or in error.

The User Application does not place any restrictions on what the Compliance Module Administrator and Attestation Manager can see on the View Attestation Request Status page. Both of these roles permit 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.



View Attestation Request Status

View status and details of Attestation Requests or retract processes of a request in progress.

Filter by: Display Label: Attestation Type: All Status: All

Search by: Confirmation Number:

Maximum rows per page 25

Display Label	Requested By	Attestation Type	Status	Request Date	Deadline
User Assignment - Test	Application Administrator Of Sample Data	User Assignment	Running	04/30/2008	04/30/2008
Role Assignment - Test	Application Administrator Of Sample Data	Role Assignment	Running	04/30/2008	
User Profile - Default	Application Administrator Of Sample Data	User Profile	Running	04/30/2008	

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 Module Administrator or Attestation Manager needs to use the *Request User Profile Attestation Process* 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 Module Administrator or Attestation Manager needs to use the *Request SoD Violation Attestation Process* 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 Module Administrator or Attestation Manager needs to use the *Request Role Assignment Attestation Process* 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 Module Administrator or Attestation Manager needs to use the *Request User Assignment Attestation Process* 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 Module Administrator or Attestation Manager) and the request has finished processing.

Status	Description
Error	Indicates that an error occurred during the course of processing. 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* drop-down 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 Module Administrator or Attestation Manager) 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*.

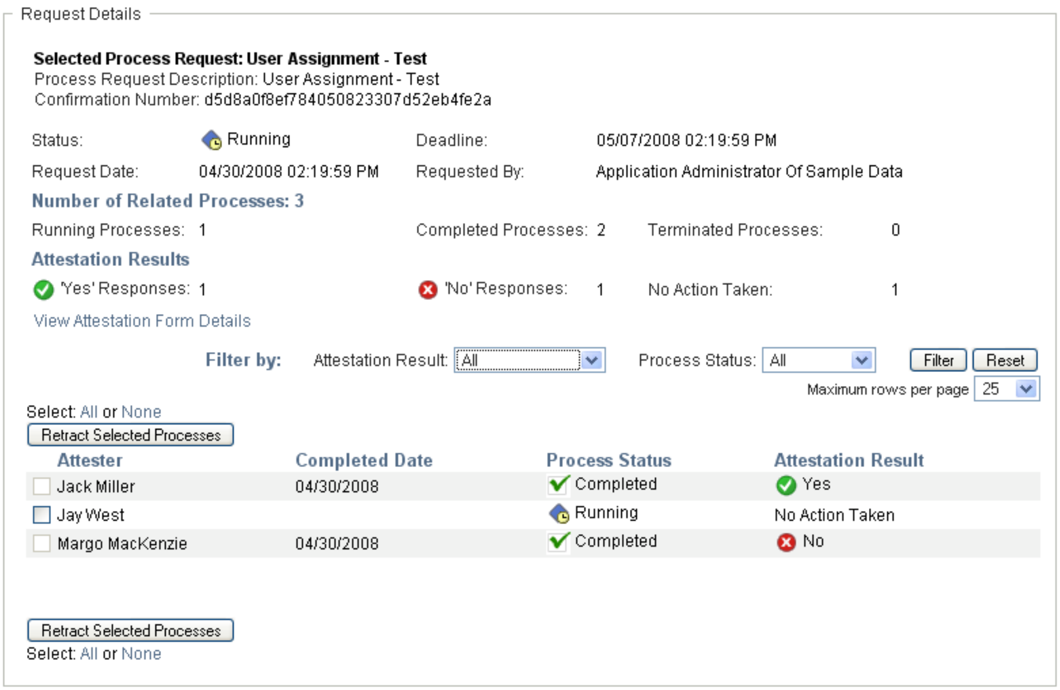
3 To search by the confirmation number that was generated when the request was first submitted, type the number in the *Confirmation Number* field, and click *Search*.

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 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: All   Process Status: All   Filter   Reset

Maximum rows per page 25

Select: All or None

Retract Selected Processes

	Attester	Completed Date	Process Status	Attestation Result
□	Jack Miller	04/30/2008	✓ Completed	✓ Yes
□	Jay West		Running	No Action Taken
□	Margo MacKenzie	04/30/2008	✓ Completed	✗ No

Retract Selected Processes

Select: All or None

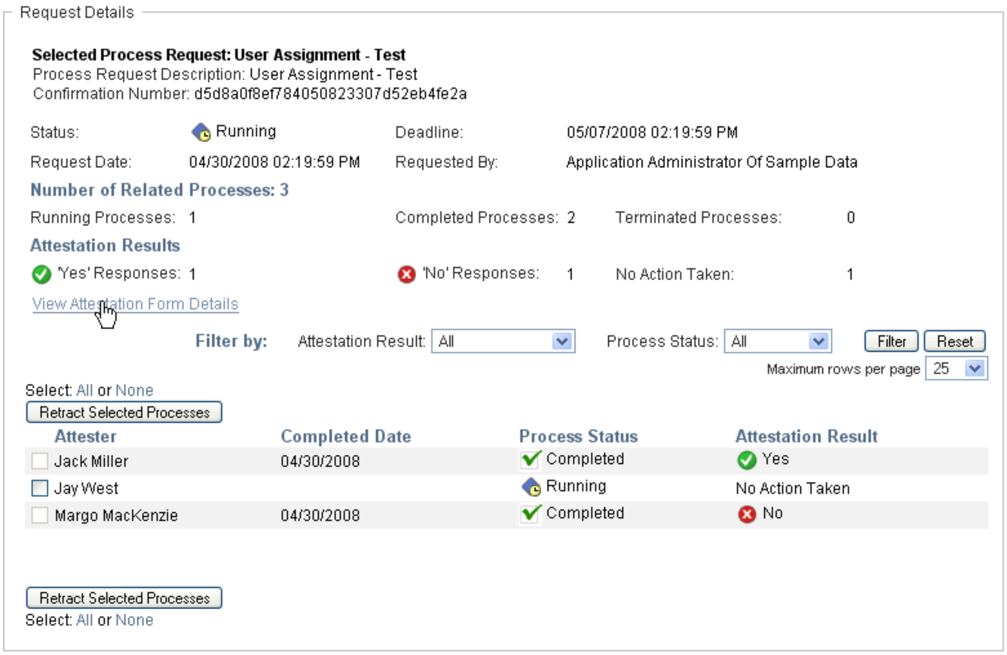
In addition to showing information already displayed in the summary, the *Request Details* group box shows status information for all processes related to the request.

- 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. **NOTE:** The default text for an affirmative answer is *Yes*. 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. **NOTE:** The default text for a negative answer is *No*. 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 Module Administrator or Attestation Manager.

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

	Attester	Completed Date	Process Status	Attestation Result
□	Jack Miller	04/30/2008	✓ Completed	✓ Yes
□	Jay West		Running	No Action Taken
□	Margo MacKenzie	04/30/2008	✓ Completed	✗ No

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 10.2.3, "Claiming a Task," on page 126.

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 Module Administrator or Attestation Manager.

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. 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.