

**User Application: 用户指南**

# **Novell®**

## **Identity Manager 基于角色的供应模块**

**3.6.1**

2008 年 7 月 23 日

[www.novell.com](http://www.novell.com)



## 法律声明

Novell, Inc. 对于本文档的内容或使用不做任何陈述或保证，特别是对用于任何特定目的的适销性或适用性不做任何明示或暗示的保证。另外，Novell, Inc. 保留随时修订本出版物和更改其内容的权利，并且没有义务将这些修订或更改通知任何个人或实体。

另外，Novell, Inc. 对任何软件不做任何声明或保证，特别是对用于任何特定目的的适销性或适用性不做任何明示或暗示的保证。另外，Novell, Inc. 保留随时更改 Novell 软件全部或部分内容的权利，并且没有义务将这些更改通知任何个人或实体。

依据本协议提供的任何产品或技术信息都将受到美国出口控制和其它国家 / 地区的贸易法律的约束。您同意遵守所有出口控制法规，并同意在出口、再出口或进口可交付产品之前取得所有必要的许可证或分类证书。您同意不出口或再出口至当前美国出口排除列表上所列的实体，或者美国出口法律中规定的任何被禁运的国家 / 地区或支持恐怖主义的国家 / 地区。您同意不将可交付产品用于禁止的核武器、导弹或生物化学武器等终端用途。有关出口 Novell 软件的详细信息，请访问 [Novell International Trade Services 万维网页面 \(http://www.novell.com/info/exports/\)](http://www.novell.com/info/exports/)。如果您未能获得任何必要的出口许可，则 Novell 对此概不负责。

版权所有 © 1997-2007 Novell, Inc. 版权所有。未经出版商的明确书面许可，不得复制、影印、传送此出版物的任何部分或将其储存在检索系统上。

Novell, Inc. 拥有与本文档所述产品中包含的技术相关的知识产权。特别是，这些知识产权包括但不限于 [Novell Legal Patents 万维网页面 \(http://www.novell.com/company/legal/patents/\)](http://www.novell.com/company/legal/patents/) 中列出的一项或多项美国专利，以及美国和其它国家 / 地区的一项或多项其它专利或正在申请的专利。

Novell, Inc.  
404 Wyman Street, Suite 500  
Waltham, MA 02451  
U.S.A.  
[www.novell.com](http://www.novell.com)

**联机文档:** 若要访问本产品及其它 Novell 产品的最新联机文档，请参见 [Novell 文档万维网页 \(http://www.novell.com/documentation\)](http://www.novell.com/documentation)。

## **Novell 商标**

有关 Novell 商标，请参见 [Novell 商标和服务标记列表 \(http://www.novell.com/company/legal/trademarks/tmlist.html\)](http://www.novell.com/company/legal/trademarks/tmlist.html)。

## **第三方资料**

所有第三方商标均属其各自所有者的财产。



# 目录

<b>关于本指南</b>	<b>11</b>
<b>I 欢迎使用 Identity Manager</b>	<b>13</b>
<b>1 入门</b>	<b>15</b>
1.1 Identity Manager 和用户	15
1.1.1 Identity Manager User Application 介绍	15
1.1.2 整体流程图	17
1.1.3 典型用途	17
1.2 访问 Identity Manager User Application	19
1.2.1 您的 User Application 看上去可能不一样	20
1.3 登录	20
1.3.1 如果您忘记了口令	21
1.3.2 登录时出现问题	22
1.3.3 提示提供更多信息	22
1.4 浏览 User Application	22
1.4.1 获得帮助	23
1.4.2 首选区域设置	23
1.4.3 注销	24
1.4.4 常用用户操作	24
1.5 下一步	28
<b>II 使用身份自助服务选项卡</b>	<b>29</b>
<b>2 身份自助服务选项卡介绍</b>	<b>31</b>
2.1 关于身份自助服务选项卡	31
2.2 访问“身份自助服务”选项卡	31
2.3 浏览选项卡的功能	32
2.4 可以执行的身份自助服务操作	33
<b>3 使用组织结构图</b>	<b>35</b>
3.1 关于组织结构图	35
3.2 浏览图	38
3.2.1 浏览至下个较高级别	38
3.2.2 重设置关系的根	39
3.2.3 切换默认关系	40
3.2.4 展开或折叠默认图	41
3.2.5 选择要展开或折叠的关系	41
3.2.6 在组织结构图中查找某个用户	43
3.3 显示详细信息	44
3.4 从关系图发送电子邮件	45
3.4.1 用电子邮件发送图中用户的相关信息	45
3.4.2 将新的电子邮件发送给图中的某个用户	46
3.4.3 向经理的小组发送电子邮件	46

<b>4</b>	<b>使用关联报告</b>	<b>49</b>
4.1	关于关联报告	49
4.2	显示关联	50
<b>5</b>	<b>使用我的配置文件</b>	<b>53</b>
5.1	关于我的配置文件	53
5.2	编辑信息	54
5.2.1	隐藏信息	54
5.2.2	使用编辑按钮	55
5.3	用电子邮件发送您的信息	59
5.4	显示组织结构图	60
5.5	链接至其他用户或组	60
5.6	选择首选语言	63
5.6.1	在浏览器中定义首选语言	64
<b>6</b>	<b>使用目录搜索</b>	<b>65</b>
6.1	关于目录搜索	65
6.2	执行基本搜索	67
6.3	执行高级搜索	68
6.3.1	选择表达式	70
6.3.2	为比较运算指定值	71
6.4	处理搜索结果	75
6.4.1	关于搜索结果	76
6.4.2	使用搜索列表	77
6.4.3	可以执行的其它操作	78
6.5	使用保存的搜索	80
6.5.1	要列出保存的搜索, 请执行下列操作:	80
6.5.2	要运行保存的搜索, 请执行下列操作:	81
6.5.3	要编辑保存的搜索, 请执行下列操作:	81
6.5.4	要删除保存的搜索, 请执行下列操作:	81
<b>7</b>	<b>执行口令管理</b>	<b>83</b>
7.1	关于口令管理	83
7.2	口令询问应答	83
7.3	口令提示更改	84
7.4	更改口令	85
7.5	口令策略状态	86
7.6	口令同步状态	87
<b>8</b>	<b>创建用户或组</b>	<b>89</b>
8.1	关于创建用户或组	89
8.2	创建用户	89
8.3	创建组	91
8.4	使用编辑按钮	92
8.4.1	要查找容器, 请执行下列操作:	93
8.4.2	要查找用户, 请执行下列操作:	94
8.4.3	要使用“历史”列表, 请执行下列操作:	95

<b>III 使用请求和批准选项卡</b>	<b>97</b>
<b>9 请求和批准选项卡介绍</b>	<b>99</b>
9.1 关于“请求和批准”选项卡	99
9.2 访问“请求和批准”选项卡	99
9.3 浏览选项卡的功能	100
9.4 可以执行的“请求和批准”操作	101
9.5 了解请求和批准图例	103
<b>10 管理您的工作</b>	<b>107</b>
10.1 关于“我的工作”操作	107
10.2 管理您的任务	107
10.2.1 查看任务	108
10.2.2 选择任务	109
10.2.3 声明任务	112
10.3 请求资源	116
10.4 检查请求的状态	121
<b>11 配置供应设置</b>	<b>125</b>
11.1 关于“我的设置”操作	125
11.1.1 关于代理和委托	125
11.1.2 样本使用场景	125
11.2 担当代理	126
11.3 指定您的可用性	127
11.3.1 设置可用性状态	127
11.3.2 创建或编辑可用性设置	129
11.3.3 删除可用性设置	131
11.4 查看和编辑代理指派	132
11.4.1 显示代理设置	132
11.4.2 创建或编辑代理指派	132
11.4.3 删除代理指派	133
11.5 查看和编辑委托指派	133
11.5.1 显示委托设置	134
11.5.2 创建或编辑委托指派	134
11.5.3 删除委托指派	136
<b>12 管理您的小组工作</b>	<b>137</b>
12.1 关于“我的小组的工作”操作	137
12.1.1 关于小组	137
12.1.2 关于小组请求权限	137
12.2 管理您的小组任务	138
12.2.1 按小组成员查看任务	138
12.2.2 按用户或组查看任务	139
12.2.3 使用任务显示格式	141
12.2.4 选择任务	144
12.2.5 声明任务	147
12.2.6 重指派任务	150
12.2.7 释放任务	151
12.3 执行小组请求	152
12.4 管理您的小组请求	155

<b>13 配置小组供应设置</b>	<b>161</b>
13.1 关于“我的小组的设置”操作	161
13.2 查看和编辑小组的代理指派	161
13.3 查看和编辑小组的委托指派	164
13.4 指定小组的可用性	169
<b>IV 使用“角色”选项卡</b>	<b>173</b>
<b>14 “角色”选项卡简介</b>	<b>175</b>
14.1 关于“角色”选项卡	175
14.1.1 关于角色	175
14.2 访问“角色”选项卡	180
14.3 浏览选项卡的功能	180
14.4 可执行的角色操作	182
14.5 了解角色图例	183
<b>15 查看角色</b>	<b>185</b>
15.1 关于“我的角色”操作	185
15.2 查看已批准的角色请求	185
<b>16 作出角色指派</b>	<b>187</b>
16.1 关于角色指派操作	187
16.2 指派角色	187
16.2.1 将用户、组和容器指派给角色	187
16.2.2 将角色指派给一个用户	189
16.2.3 将角色指派给一个组	191
16.2.4 将角色指派给一个容器	193
16.3 检查请求的状态	195
<b>17 管理角色</b>	<b>203</b>
17.1 浏览“角色编目”	203
17.2 管理角色	204
17.2.1 创建新角色	205
17.2.2 修改或删除现有角色	205
17.2.3 角色属性	206
17.3 管理角色关系	208
17.3.1 创建与去除角色关系	208
17.3.2 管理角色关系属性	210
17.4 管理职责分离限制	210
17.4.1 创建新的职责分离限制	211
17.4.2 修改现有 SoD 限制	211
17.4.3 SoD 限制属性参照	212
17.5 配置角色子系统	214
<b>18 创建并查看角色报告</b>	<b>217</b>
18.1 关于角色报告操作	217
18.2 角色报告	217
18.2.1 角色列表报告	217

18.2.2	角色指派报告	219
18.3	SoD 报告	220
18.3.1	SoD 限制报告	220
18.3.2	SoD 违例和异常报告	221
18.4	用户报告	222
18.4.1	用户角色报告	222
18.4.2	用户权利报告	224
<b>V 使用“合规性”选项卡</b>		<b>227</b>
<b>19 “合规性”选项卡简介</b>		<b>229</b>
19.1	关于“合规性”选项卡	229
19.1.1	关于合规性和证明	229
19.2	访问该选项卡	231
19.3	浏览选项卡的功能	232
19.4	可执行的合规性操作	233
19.5	了解证明请求图例	234
19.6	常用合规性操作	235
19.6.1	指定请求的标签和说明	235
19.6.2	定义证明者	235
19.6.3	指定最后期限	236
19.6.4	定义证明表单	236
19.6.5	提交证明请求	238
19.6.6	保存请求细节	238
19.6.7	使用已保存的请求	239
<b>20 发出证明请求</b>		<b>241</b>
20.1	关于证明请求操作	241
20.2	请求用户简介证明流程	241
20.3	请求 SoD 违反证明进程	242
20.4	请求角色指派证明流程	244
20.5	请求用户指派证明流程	245
20.6	检查证明请求的状态	247



# 关于本指南

本书介绍 Novell® Identity Manager User Application 的用户界面，以及如何使用该应用程序提供的功能，包括：

- ◆ 身份自助服务（用于用户信息、口令和目录）
- ◆ 请求和批准（用于基于工作流程的供应）
- ◆ 角色（用于基于角色的供应操作）
- ◆ 合规性（用于法规合规性和证明）

## 读者

本书中的信息供 Identity Manager 用户界面的终端用户参考。

## 前提条件

本指南假定您使用的是 Identity Manager 用户界面的默认配置。但是，您有可能已自定义用户界面的版本，以便以不同的方式进行查看或操作。

开始使用之前，应该咨询系统管理员，以获取有关可能遇到的任何自定义设置的细节。

## 组织

下面是本书内容的摘要：

部分	说明
“欢迎使用 Identity Manager”（第 13 页）	介绍 Identity Manager 用户界面以及如何开始使用该界面
“使用身份自助服务选项卡”（第 29 页）	如何使用 Identity Manager 用户界面的 <i>身份自助服务</i> 选项卡来显示和处理身份信息，包括： <ul style="list-style-type: none"><li>◆ 组织结构图</li><li>◆ 配置文件（身份详细信息）</li><li>◆ 目录搜索</li><li>◆ 口令</li><li>◆ 用户帐户（及其他）</li></ul>
“使用请求和批准选项卡”（第 97 页）	如何使用 Identity Manager 用户界面的 <i>请求和批准</i> 选项卡执行以下操作： <ul style="list-style-type: none"><li>◆ 管理您自己或小组的供应工作（任务和资源请求）</li><li>◆ 配置您自己或小组的供应设置</li></ul>

部分	说明
“使用“角色”选项卡”（第 173 页）	<p>如何使用 Identity Manager 用户界面的“角色”选项卡实现以下目的：</p> <ul style="list-style-type: none"> <li>◆ 为您自己或贵组织内的其他用户发出角色请求</li> <li>◆ 创建角色以及角色层次结构内的角色关系</li> <li>◆ 创建职责分离 (SoD) 限制以管理角色指派之间的潜在冲突</li> <li>◆ 查看提供有关“角色编目”当前状态和当前指派给用户、组与容器的角色的细节的报告</li> </ul>
“使用“合规性”选项卡”（第 227 页）	<p>如何使用 Identity Manager 用户界面的“合规性”选项卡执行以下操作：</p> <ul style="list-style-type: none"> <li>◆ 发出用户简介证明流程的请求</li> <li>◆ 发出责任分离 (SoD) 证明流程的请求</li> <li>◆ 请求角色指派证明进程</li> <li>◆ 请求用户指派证明进程</li> </ul>

## 反馈

我们希望听到您对本手册和本产品中包含的其他文档的意见和建议。请使用联机文档每页底部的“用户意见”功能，或访问 [www.novell.com/documentation/feedback.html](http://www.novell.com/documentation/feedback.html) 并输入您的意见。

## 文档更新

有关《*IDM User Application: 用户指南*》的最新版本，请访问 [Identity Manager 万维网站点 \(http://www.novell.com/documentation/idmrbpm361/\)](http://www.novell.com/documentation/idmrbpm361/)。

## 文档约定

在 Novell 文档中，使用大于号 (>) 来分隔某个步骤中的各项操作和交叉引用路径中的各个项目。

商标符号（®、™ 等）代表一个 Novell 商标。星号 (\*) 表示第三方商标。

如果某个路径名的书写对某些平台需使用反斜线而对另一些平台需使用正斜线，则使用反斜线表示该路径名。要求使用正斜杠的平台（例如 Linux\* 或 UNIX\*）的用户应根据软件要求使用正斜杠。

# 欢迎使用 Identity Manager

请首先阅读此部分，了解 Identity Manager User Application 以及如何开始使用它。

- ◆ [第 1 章“入门”（第 15 页）](#)



本部分说明如何开始使用 Identity Manager User Application。包括以下主题：

- ◆ 第 1.1 节“Identity Manager 和用户”（第 15 页）
- ◆ 第 1.2 节“访问 Identity Manager User Application”（第 19 页）
- ◆ 第 1.3 节“登录”（第 20 页）
- ◆ 第 1.4 节“浏览 User Application”（第 22 页）
- ◆ 第 1.5 节“下一步”（第 28 页）

## 1.1 Identity Manager 和用户

Novell® Identity Manager 是一种系统软件产品，您的组织可使用它来安全地管理用户团体的访问需求。如果您是用户团体的成员，则可以在很多方面受益于 Identity Manager。例如，组织可以借助 Identity Manager 实现以下功能：

- ◆ 首先为用户指定对所需信息（例如组结构图、部门用户信息数据库或雇员查找）和资源（例如内部系统中的设备或帐户）的访问权限
- ◆ 对于所有系统，只需一次登录，即可同步输入多个口令
- ◆ 必要时（例如某个用户转到不同的组或离开组织时）立即修改或取消访问权限
- ◆ 服从政府法规

为使您及小组能直接受益于这些好处，Identity Manager User Application 提供了一个可通过万维网浏览器使用的用户界面。

### 1.1.1 Identity Manager User Application 介绍

使用 Identity Manager User Application 可以查看 Identity Manager 的信息、资源和功能。在 Identity Manager User Application 中可查看的内容细节和可执行的具体操作由系统管理员确定。通常包括：

- ◆ 身份自助服务，其功能为：
  - ◆ 显示组织结构图
  - ◆ 报告和用户关联的应用程序（如果您是管理员）。（需要使用 Roles Based Provisioning Module for Identity Manager。）
  - ◆ 编辑配置文件中的信息
  - ◆ 搜索目录
  - ◆ 更改口令、口令询问应答和口令提示
  - ◆ 检查您的口令策略状态和口令同步状态
  - ◆ 为新用户或组创建帐户（如果您得到授权）
- ◆ 请求和批准，其功能为：
  - ◆ 请求资源
  - ◆ 查看资源请求的批准状态

- ◆ 处理向您指派的、批准其它资源请求的任务
- ◆ 以其他某人的代理或委托的身份执行请求和批准
- ◆ 将其他用户指派为您的代理或委托（如果您有权限）
- ◆ 为您的小组管理所有这些请求和批准功能（如果您有权限）
- ◆ 可选择为每个请求或批准提供数字签名

---

**注释：**请求和批准需要使用 Roles Based Provisioning Module for Identity Manager。

---

- ◆ 角色，其功能为：
  - ◆ 请求角色指派和管理角色指派请求的批准流程
  - ◆ 检查角色请求的状态
  - ◆ 定义角色和角色关系
  - ◆ 定义职责分离 (SoD) 限制并在用户请求覆盖限制时管理批准流程
  - ◆ 浏览“角色编目”
  - ◆ 查看详细的报告，这些报告列出了角色和编目中定义的职责分离限制，以及角色指派的当前状态、职责异常的分离，以及用户权利

---

**注释：**角色需要使用 Identity Manager 基于角色的供应模块。

---

- ◆ 合规性，其功能为：
  - ◆ 请求用户简介证明流程
  - ◆ 请求责任分离 (SoD) 证明流程
  - ◆ 请求角色指派证明流程
  - ◆ 请求用户指派证明流程

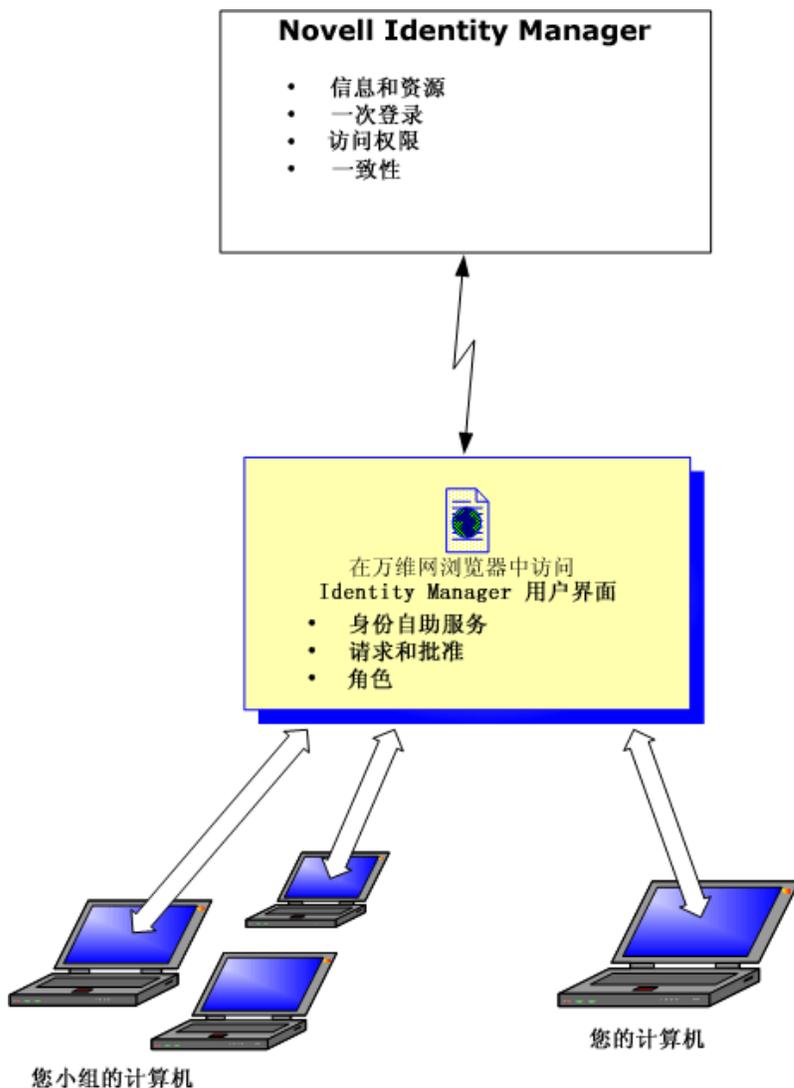
---

**注释：**合规性需要 Identity Manager 基于角色的供应模块。

---

## 1.1.2 整体流程图

图 1-1 IDM User Application 提供 Identity Manager 的用户界面



## 1.1.3 典型用途

下面是用户在组织中使用 Identity Manager User Application 的一些典型示例。

### 使用身份自助服务

- Ella（一个终端用户）在登录后通过身份自助服务功能重新获得她忘记的口令。
- Erik（一个最终用户）执行搜索，查找其所在位置所有说德语的员工。
- Eduardo（一个终端用户）浏览组织结构图、查找 ella，然后单击电子邮件图标向她发送讯息。

## 使用请求和批准

- ◆ Ernie（一个终端用户）浏览可用资源的列表，然后请求访问 Siebel\* 系统。
- ◆ Amy（一个批准者）通过电子邮件（其中包含 URL）接收某个批准请求的通知。她单击链接，随即出现了一个批准表格，然后对此表格进行批准。
- ◆ Ernie 查看上次请求访问 Siebel 的状态（现在该请求已转至另一个用户以待批准）。他看到该请求仍在处理中。
- ◆ Amy 将去度假，所以她表明自己暂时离开。在她离开期间，不会有新的批准任务指派给她。
- ◆ Amy 打开批准任务列表，发现由于任务太多而无法及时回复，因此她将部分任务重指派给同事。
- ◆ Pat（一位行政助理，担任 Amy 的代理用户）打开 Amy 的任务列表，然后替她执行批准任务。
- ◆ Max（一位经理）查看部门中人员的任务列表。他知道 Amy 正在度假，因此他将任务重指派给部门中的其他人。
- ◆ Max 为部门中直接向他汇报的某个用户发出了申请数据库帐户的请求。
- ◆ Max 将 Dan 指派为 Amy 的授权代表。
- ◆ Amy 离开时，Dan（现在为受委托的批准人）接收她的任务。
- ◆ Max 聘用了一个无薪实习员工，不应将该员工输入 HR 系统。系统管理员为该实习员工创建用户记录，然后请求向他授予对 Notes、Active Directory\* 和 Oracle\* 的访问权限。

## 使用角色

- ◆ Maxine（一个角色管理员）创建 Nurse 与 Doctor 业务角色和 Administer Drugs 与 Write Prescriptions IT 角色。
- ◆ Maxine（一个角色管理者）定义 Nurse 与 Administer Drugs 角色之间的关系，并且指定 Nurse 角色包含 Administer Drugs 角色。Max 还定义了 Write Prescriptions 与 Doctor 角色之间的关系，并且指定 Doctor 角色包含 Write Prescriptions 角色。
- ◆ Chester（一个安全专员）定义职责分离限制，该限制指定 Doctor 和 Nurse 角色之间存在潜在冲突。这意味着通常不应将同一用户同时指派给两个角色。在某些情况下，请求角色指派的个人可能希望覆盖此限制。要定义职责分离异常，请求指派的个人必须提供调整。
- ◆ Ernest（一个终端用户）浏览可用角色列表，然后请求指派给 Nurse 角色。
- ◆ Amelia（一个批准者）通过电子邮件（其中包含 URL）接收批准请求的通知。她单击链接，随即出现了一个批准表格，然后对此表格进行批准。
- ◆ Arnold（一个角色管理员）请求将 Ernest 指派给 Doctor 角色。他将收到通知，说明 Doctor 角色与 Nurse 角色之间存在潜在冲突，而 Ernest 已经指派给了后一个角色。他提供有关作出职责分离限制异常的调整。
- ◆ Edward（一个职责分离批准者）通过电子邮件收到有关职责分离冲突的通知。他批准 Arnold 关于覆盖该职责分离限制的请求。
- ◆ Amelia（一个批准者）通过电子邮件收到有关 Doctor 角色的批准请求的通知。她批准 Arnold 关于将 Ernest 指派给 Doctor 角色的请求。
- ◆ Bill（一个角色审计员）查看 SoD 违例和异常报告并了解到将 Ernest 同时指派给了 Doctor 和 Nurse 角色。

## 使用合规性

- ◆ Maxine（一个角色管理员）创建 Nurse 与 Doctor 业务角色和 Administer Drugs 与 Write Prescriptions IT 角色。
- ◆ Maxine（一个角色管理者）定义 Nurse 与 Administer Drugs 角色之间的关系，并且指定 Nurse 角色包含 Administer Drugs 角色。Max 还定义了 Write Prescriptions 与 Doctor 角色之间的关系，并且指定 Doctor 角色包含 Write Prescriptions 角色。
- ◆ Chester（一个安全专员）定义职责分离限制，该限制指定 Doctor 和 Nurse 角色之间存在潜在冲突。这意味着通常不应将同一用户同时指派给两个角色。在某些情况下，请求角色指派的个人可能希望覆盖此限制。要定义职责分离异常，请求指派的个人必须提供调整。
- ◆ Arnold（一个角色管理员）请求将 Ernest 指派给 Doctor 角色。他将收到通知，说明 Doctor 角色与 Nurse 角色之间存在潜在冲突，而 Ernest 已经指派给了后一个角色。他提供有关作出职责分离限制异常的调整。
- ◆ Philip（合规性模块管理员）启动了针对“护士”角色的角色指派证明流程。
- ◆ Fiona（证明者）通过电子邮件（包含 URL）收到证明任务的通知。她单击链接，然后看到一个证明表单。她对证明问题做出肯定回答，因而认同该信息是正确的。
- ◆ Philip（合规性模块管理员）为人力资源组中的用户启动了新的用户简介证明流程的请求。
- ◆ 人力资源组中的每个用户都通过电子邮件（包含 URL）收到了证明任务通知。每个用户都单击链接，然后看到一个证明表单。该表单使用户可以审阅各种用户简介属性的值。审阅信息后，每个用户都回答证明问题。

## 1.2 访问 Identity Manager User Application

做好开始使用 Identity Manager User Application 的准备后，计算机上只需要有万维网浏览器就可以开始了。Identity Manager 支持最常用的浏览器版本；请与系统管理员联系，以获取受支持浏览器的列表或安装浏览器的帮助。

由于 Identity Manager User Application 在浏览器中运行，因此访问该界面就如同访问任何万维网网页那样容易。

---

**注释：**要使用 Identity Manager User Application，请在万维网浏览器中启用 cookie（在 Internet Explorer 中隐私级别至少为 *中*）和 JavaScript\*。

---

要访问 Identity Manager User Application，请打开万维网浏览器，转到 Identity Manager User Application 的地址 (URL)（由您的系统管理员提供），例如 <http://myappserver:8080/IDM>。

默认情况下，执行此操作后，您将会进入 User Application 的用户欢迎页面：

图 1-2 User Application 的用户欢迎页面



可以从这里登录 User Application，以访问其功能。

## 1.2.1 您的 User Application 看上去可能不一样

访问 Identity Manager User Application 时，如果所看到的第一页不同，通常是由于已针对您的组织自定义了应用程序。在工作时，您可能会发现 User Application 的其它功能也已被自定义。

在这种情况下，应该咨询系统管理员，以了解自定义的 User Application 与本指南中介绍的默认配置有哪些差别。

## 1.3 登录

只有已授权用户才能从用户欢迎页面登录 Identity Manager User Application。如需有关如何获取登录时使用的用户名和口令的帮助，请与系统管理员联系。

要登录 Identity Manager User Application，请执行下列操作：

- 1 在“欢迎用户”页面上，单击登录链接（位于页面右上角）。  
User Application 将提示输入用户名和口令：



The image shows the Novell Identity Manager login interface. At the top, the text "Novell® Identity Manager" is displayed in white on a dark blue background. Below this, there are two input fields: "用户名:" (Username) and "口令:" (Password). A link labeled "→ 忘记了口令?" (Forgot password?) is positioned below the password field. At the bottom left, there is a red "N" logo, and at the bottom right, there is a blue button labeled "登录..." (Login...).

2 输入用户名和口令，然后单击 **登录**。

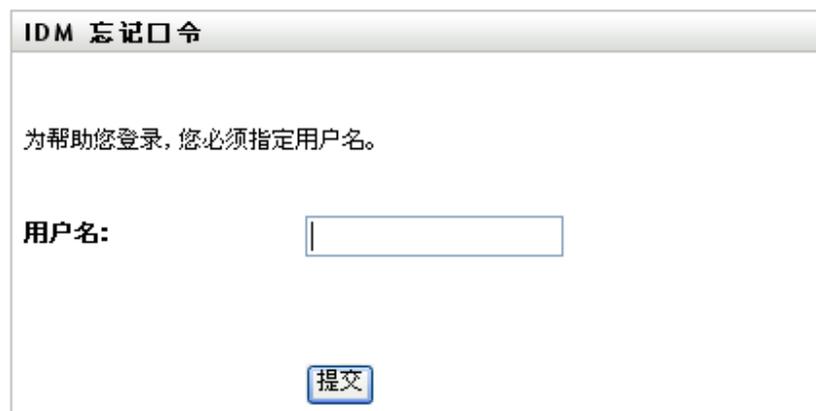
### 1.3.1 如果您忘记了口令

如果忘记了需要键入的口令，可以使用 [忘记了口令?](#) 链接获得帮助。默认情况下，在出现登录提示时，页面上将显示该链接。如果系统管理员为您设置了相应的口令策略，则可以利用该链接。

要使用“忘记口令”功能：

1 出现登录提示时，单击 [忘记了口令?](#) 链接。

然后系统将要求输入用户名：

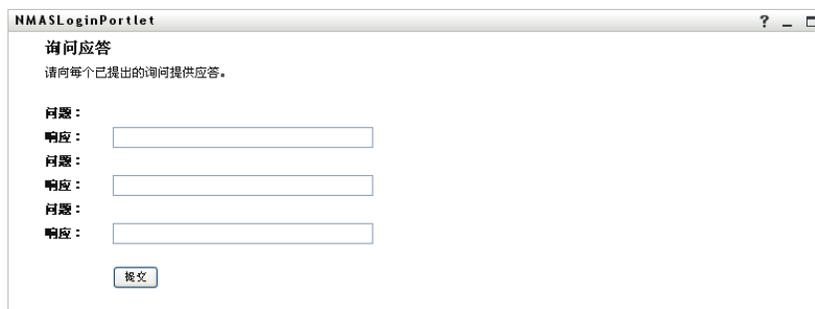


The image shows the "IDM 忘记口令" (IDM Forgot Password) form. The title bar reads "IDM 忘记口令". Below the title bar, the text "为帮助您登录，您必须指定用户名。" (To help you log in, you must specify a username.) is displayed. There is a label "用户名:" (Username) followed by an input field. At the bottom center, there is a blue button labeled "提交" (Submit).

2 键入用户名，然后单击 **提交**。

如果 Identity Manager 回复它无法为您找到口令策略，请咨询系统管理员以获得帮助。

3 回答显示的任何安全询问问题，然后单击 **提交**。例如：



回答询问问题以帮助找到口令。根据系统管理员设置口令策略的方式，您可以：

- ◆ 看到页面上显示的有关口令的提示
- ◆ 收到包含口令或口令提示的电子邮件
- ◆ 收到重设置口令的提示

### 1.3.2 登录时出现问题

如果无法登录 Identity Manager User Application，请确保使用了正确的用户名，并且正确键入了口令（拼写、大小写字母等）。如果仍有问题，请咨询系统管理员。如果能够提供更与所遇问题有关的细节（如错误讯息），则会有助于解决问题。

### 1.3.3 提示提供更多信息

登录 Identity Manager User Application 后，系统可能随即提示您提供其它类型的信息。要提供哪些信息完全取决于系统管理员设置的口令策略（如有）。例如：

- ◆ 如果是第一次登录，系统可能会提示您定义安全询问问题和应答或口令提示
- ◆ 如果口令已失效，系统可能会提示您重设置口令

## 1.4 浏览 User Application

登录后，Identity Manager User Application 将显示您可以使用的选项卡页面：

图 1-3 登录时，您会看到选项卡和组织结构图



在 User Application 的顶部，可以看到下列主选项卡：

- ◆ *身份自助服务*（默认情况下处于打开状态）

要了解该选项卡及其操作方式，请参见“[使用身份自助服务选项卡](#)”（第 29 页）。

- ◆ *请求和批准*

要了解该选项卡及其操作方式，请参见“[使用请求和批准选项卡](#)”（第 97 页）。

---

**注释：**要启用 *请求和批准* 选项卡，贵组织必须具有 Identity Manager 基于角色的供应模块。

---

- ◆ *角色*

要了解该选项卡及其操作方式，请参见“[使用“角色”选项卡](#)”（第 173 页）。

---

**注释：**要启用 *角色* 选项卡，贵组织必须具有 Identity Manager 基于角色的供应模块。

---

- ◆ *合规性*

要了解该选项卡及其操作方式，请参见“[使用“合规性”选项卡](#)”（第 227 页）。

---

**注释：**要启用 *合规性* 选项卡，贵组织必须具有 Identity Manager 基于角色的供应模块。除非您是合规性模块管理员或证明管理者，否则 *合规性* 选项卡将不可用。

---

要切换至其他选项卡，只需单击要使用的选项卡。

## 1.4.1 获得帮助

在 Identity Manager User Application 中执行操作时，可以显示联机帮助，以获取与当前使用的选项卡有关的文档。

- 1 转至您要了解的选项卡（如 *角色* 或 *合规性*）。

- 2 单击 *帮助* 链接（位于页面右上角）。

显示当前选项卡的帮助页。

## 1.4.2 首选区域设置

如果您的管理员没有定义 User Application 的首选区域设置（语言），第一次登录时将提示您选择自己的首选区域设置。

- 1 看到提示时，请打开 *可用区域设置* 列表，选择区域设置并单击 *添加* 来添加区域设置。

更多信息请参见第 5.6 节“[选择首选语言](#)”（第 63 页）。

### 编辑首选区域设置

用户: Margo MacKenzie  
为当前应用程序的用户设定“区域设置自选设置”。

---

按自选设置排列的区域设置

可用区域设置

---

### 1.4.3 注销

如果在 Identity Manager User Application 中执行完操作，并且希望结束会话，则请注销。

- 1 单击[注销](#)链接（位于页面右上角）。

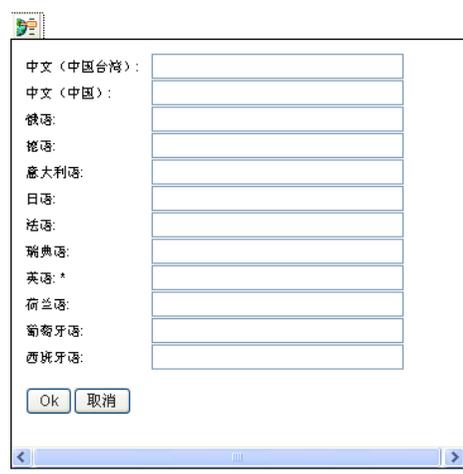
默认情况下，User Application 将感谢您使用 Novell Identity Manager。单击标题为[返回到 Novell Identity Manager](#) 登录的红色链接，返回到登录提示。

### 1.4.4 常用用户操作

User Application 提供了一个统一的用户界面，可执行访问和显示数据等常用用户操作。本部分描述若干常用用户界面元素，并包含下列操作的说明：

- ◆ [使用“对象选择器”按钮进行搜索（第 26 页）](#)
- ◆ [过滤数据（第 27 页）](#)

表 1-1 常用按钮

按钮	说明
	<p><b>对象选择器</b> 提供对“搜索”对话框或弹出式对话框的访问。可以根据您在 User Application 内的位置，为不同类型的对象输入搜索准则。例如，在“身份自助服务”选项卡中，可以搜索用户和组，而在“角色”选项卡中，则可搜索用户、组和角色。</p> 
	<p><b>显示历史</b> 提供指向以前访问的数据的链接。可以选中此链接来显示以前选择的数据。如果知道最近使用过某项，单击“显示历史”可能比执行搜索的速度更快。</p> 
	<p><b>重置</b> 清除当前选择。</p>
	<p><b>本地化</b> 显示一个对话框，用于以 User Application 目前提供的任何区域设置输入通常用于字段名称或说明的文本。</p> 

按钮	说明
	<b>添加</b> 添加新项目或对象。将提示输入特定于要添加的对象类型的更多信息。
	<b>删除</b> 删除当前所选项目。
	<b>“向上”或“向下”箭头</b> 在列表中将当前所选对象上下移动
	

**图例** 提供对 *请求和批准*或*角色*选项卡上所用符号的说明。

## 使用“对象选择器”按钮进行搜索

使用“对象选择器”按钮：

- 1 单击 。将显示“搜索”对话框：



- 2 如下所示指定搜索准则：

**2a** 使用该下拉列表选择要搜索的相关字段。该下拉列表中的字段取决于起动搜索的位置。在本示例中，可以指定 *名称*或*说明*。

**2b** 在下拉列表旁边的文本框中，输入完整或部分搜索准则（如名称或说明）。搜索将查找所搜索对象类型的以输入文本开头的每个实例。也可以在文本中使用星号 (\*) 作为通配符，以代表零个或多个任意字符。例如，以下所有示例都将查找角色

Nurse:

nurse

n

n\*

\*u

\*r

\*e

- 3 单击 *搜索*。

将显示搜索结果。单击列标题可按升序或降序对搜索结果排序。本示例显示一系列角色。



如果希望结果列表包含所需的角色，请转至**步骤 4**。否则，请返回到**步骤 2**。

- 4 从列表中选择所需的项目。查找页面将关闭，并将使用与所选相关联的数据填充此页面。

## 过滤数据

User Application 的“角色”选项卡提供过滤器，用于仅显示有兴趣查看的数据。可以通过使用“每页最大行数”设置进一步限制一个页面上显示的数据量。下面是部分过滤器示例：

- ◆ 按角色指派和来源过滤（“我的角色”操作中可用）：



- ◆ 按角色名称、用户和状态过滤（“查看请求状态”操作中可用）：



- ◆ 按角色级别和编目过滤（“浏览角色编目”操作中可用）：



使用过滤功能：

- 1 如下所示在 *过滤方式* 文本字段中指定一个值：

- 1a 要限制为以特定字符串开始的项目，请在 *过滤方式* 框中输入完整或部分字符串。也可以在文本中使用星号 (\*) 作为通配符，以代表零个或多个任意字符。例如，下面的所有示例都将查找名称为 Nurse 的角色指派：

nurse

n

n\*

\*u

\*r

\*e

---

**注释：**“角色名称”过滤器不限制从身份库中返回的对象数量。只是根据过滤准则限制页面上显示的对象数。其他过滤器（如“状态”）则限制从身份库返回的对象数量。

---

- 1b** 要进一步过滤显示的项，可指定更多过滤准则。User Application 允许根据数据以不同方式选择准则。可以选择复选框或从列表框选择一项或多项（使用平台的多选击键）。准则之间为“与”关系，因此只显示满足所有准则的项目。
  - 1c** 要对显示应用指定的过滤准则，请单击 *过滤器*。
  - 1d** 要清除当前指定的过滤准则，请单击 *重设置*。
- 2** 要设置按准则匹配过滤器的项在每页上显示的最大数量，请在 *每页最大行数* 下拉列表中选择 一个数字。

## 1.5 下一步

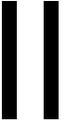
了解 Identity Manager User Application 的基本知识后，就可以开始使用它提供的选项卡来完成工作。

---

要了解	， 请参见
执行身份自助服务的操作	“使用身份自助服务选项卡”（第 29 页）
执行请求和批准的操作	“使用请求和批准选项卡”（第 97 页）
执行角色的工作	“使用“角色”选项卡”（第 173 页）
处理合规性	“使用“合规性”选项卡”（第 227 页）

---

# 使用身份自助服务选项卡



这些部分说明如何使用 Identity Manager User Application 的 *身份自助服务* 选项卡来显示和处理身份信息。

- ◆ 第 2 章“身份自助服务选项卡介绍”（第 31 页）
- ◆ 第 3 章“使用组织结构图”（第 35 页）
- ◆ 第 4 章“使用关联报告”（第 49 页）
- ◆ 第 5 章“使用我的配置文件”（第 53 页）
- ◆ 第 6 章“使用目录搜索”（第 65 页）
- ◆ 第 7 章“执行口令管理”（第 83 页）
- ◆ 第 8 章“创建用户或组”（第 89 页）



# 身份自助服务选项卡介绍

本部分说明如何开始使用 Identity Manager User Application 的 *身份自助服务* 选项卡。包括以下主题：

- ◆ 第 2.1 节“关于身份自助服务选项卡”（第 31 页）
- ◆ 第 2.2 节“访问“身份自助服务”选项卡”（第 31 页）
- ◆ 第 2.3 节“浏览选项卡的功能”（第 32 页）
- ◆ 第 2.4 节“可以执行的身份自助服务操作”（第 33 页）

有关访问和使用 Identity Manager User Application 的更多一般信息，请参见第 1 章“入门”（第 15 页）。

## 2.1 关于身份自助服务选项卡

*身份自助服务* 选项卡让您能方便地自行显示和处理身份信息。它使您能随时访问需要的信息，从而使您的组织更快做出响应。例如，可以使用 *身份自助服务* 选项卡实现以下功能：

- ◆ 直接管理自己的用户帐户
- ◆ 按需查找组织中的其他用户和组
- ◆ 使这些用户和组的相关方式直观化
- ◆ 列出与您关联的应用程序

系统管理员负责为您以及组织中的其他人设置 *身份自助服务* 选项卡的内容。可以查看的内容以及可以执行的操作通常由您的工作需要和权限级别确定。

## 2.2 访问“身份自助服务”选项卡

默认情况下，登录 Identity Manager User Application 后，*身份自助服务* 选项卡将会打开，并显示“组织结构图”页面：

图 2-1 “身份自助服务”选项卡上的“组织结构图”页面



如果要在转至 Identity Manager User Application 中的另一选项卡后返回，则只需单击 *身份自助服务* 选项卡再次将其打开。

## 2.3 浏览选项卡的功能

本节介绍身份自助服务选项卡的默认功能。（您的选项卡外观可能由于为您组织所作的自定义而有所不同；请咨询您的系统管理员。）

身份自助服务选项卡的左侧显示可以执行的操作的菜单。这些操作按以下类别列出 — 信息管理、口令管理和目录搜索（如果已授权）：

图 2-2 身份自助服务操作菜单



如果单击一项操作，其右侧会显示相应的页面。该页面通常包含一个称为 *Portlet* 的特殊窗口，其中显示该操作的细节。例如，“组织结构图”页面上的 *Portlet* 如下所示：

图 2-3 “组织结构图”页面上的 *Portlet*



*Portlet* 标题栏通常显示一组按钮，可单击这些按钮执行标准的操作。例如：



表 2-1 描述了这些按钮的功能：

表 2-1 Portlet 标题栏按钮及其功能

按钮	作用
	显示 Portlet 的帮助
	打印 Portlet 的内容
	最小化 Portlet
	最大化 Portlet

如果看到其它按钮且不知道它们的功能，可以将鼠标指针悬停在这些按钮上以显示说明。

## 2.4 可以执行的身份自助服务操作

表 2-2 总结了默认情况下可以在身份自助服务选项卡上使用的操作：

表 2-2 可通过身份自助服务选项卡执行的操作

类别	操作	说明
信息管理	组织结构图	以交互式组织结构图的形式显示用户和组之间的关系。  有关细节，请参见第 3 章“使用组织结构图”（第 35 页）。
	关联报告	对管理员可用。显示与用户关联的应用程序。  有关细节，请参见第 4 章“使用关联报告”（第 49 页）。
	我的配置文件	显示您的用户帐户细节，并让您处理该信息。  有关细节，请参见第 5 章“使用我的配置文件”（第 53 页）。
	目录搜索	用于通过输入搜索准则或使用以前保存的搜索准则，来搜索用户或组。  有关细节，请参见第 6 章“使用目录搜索”（第 65 页）。

类别	操作	说明
口令管理	口令询问应答	用于设置或更改对管理员定义的安全询问问题的有效应答，以及设置或更改用户定义的安全询问问题和应答。  有关细节，请参见第 7 章“执行口令管理”（第 83 页）。
	口令提示定义	用于设置或更改口令提示。  有关细节，请参见第 7 章“执行口令管理”（第 83 页）。
	更改口令	用于根据系统管理员建立的规则更改（重设置）口令。  有关细节，请参见第 7 章“执行口令管理”（第 83 页）。
	口令策略状态	显示关于您的口令管理有效性的信息。  有关细节，请参见第 7 章“执行口令管理”（第 83 页）。
	口令同步状态	显示与身份库同步的关联应用程序的口令同步状态。  有关细节，请参见第 7 章“执行口令管理”（第 83 页）。
目录管理	创建用户或组	对管理员及授权用户可用。可用来创建新用户或组。  有关细节，请参见第 8 章“创建用户或组”（第 89 页）。

# 使用组织结构图

本部分说明如何使用 Identity Manager User Application 的 *身份自助服务* 选项卡上的“组织结构图”页面。包括以下主题：

- ◆ [第 3.1 节“关于组织结构图”](#)（第 35 页）
- ◆ [第 3.2 节“浏览图”](#)（第 38 页）
- ◆ [第 3.3 节“显示详细信息”](#)（第 44 页）
- ◆ [第 3.4 节“从关系图发送电子邮件”](#)（第 45 页）

---

**注释：**本部分介绍“组织结构图”页面的默认功能。由于您的工作角色和权限级别的不同以及针对组织执行的自定义，您可能会发现某些差异；有关细节，请咨询系统管理员。

---

有关访问和操作 *身份自助服务* 选项卡的更多一般信息，请参见 [第 2 章“身份自助服务选项卡介绍”](#)（第 31 页）。

## 3.1 关于组织结构图

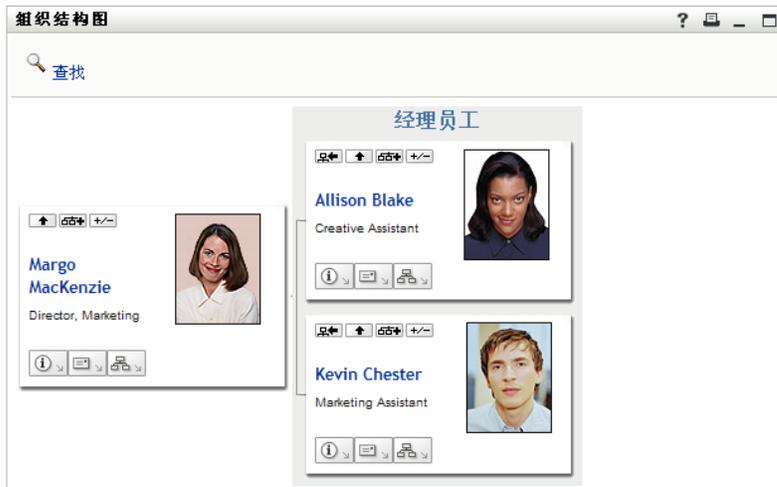
“组织结构图”页面会显示关系。它可以显示公司中的经理、员工和用户组之间的关系，以及您的管理员定义的其他关系类型。这些是以组织结构图的形式显示的。在该图中，每个人、组或其他实体都以类似名片的格式显示。作为组织结构图起点或方向点的名片，是 *根名片*。

组织结构图是交互式的。您可以：

- ◆ 选择并显示关系类型。
- ◆ 设置您的首选默认关系类型，例如经理员工、用户组，或您的管理员提供的其他类型。
- ◆ 设置关系图的默认放置位置在根名片的左边还是右边。
- ◆ 向显示的图的根名片上添加最多两级名片。
- ◆ 将其他用户设定为该图的根。
- ◆ 关闭（折叠）或打开（展开）名片下的图。
- ◆ 查找要在图中显示的用户。
- ◆ 显示选定用户的细节（“配置文件”页面）。
- ◆ 通过电子邮件（以链接的形式）将用户细节发送给某个用户。
- ◆ 将新的电子邮件发送给选定用户或经理的小组。

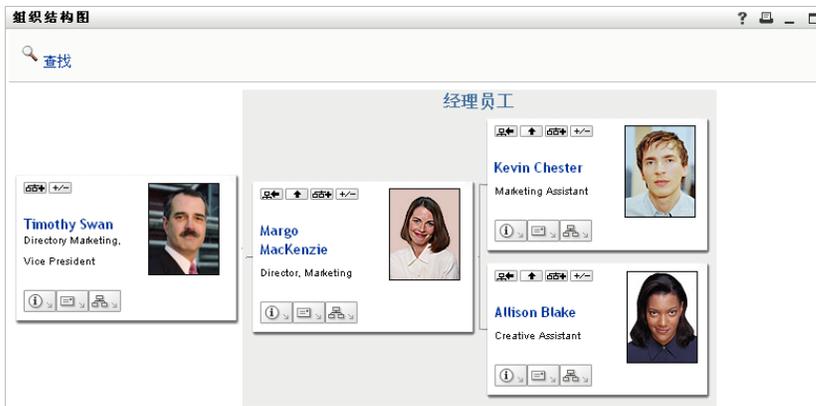
以下示例会向您介绍如何使用组织结构图。首次显示“组织结构图”页面时，该页面将显示您本人的经理员工关系。例如，Margo MacKenzie（市场总监）登录时会看到“组织结构图”页面的以下默认显示：

图 3-1 登录时的默认视图



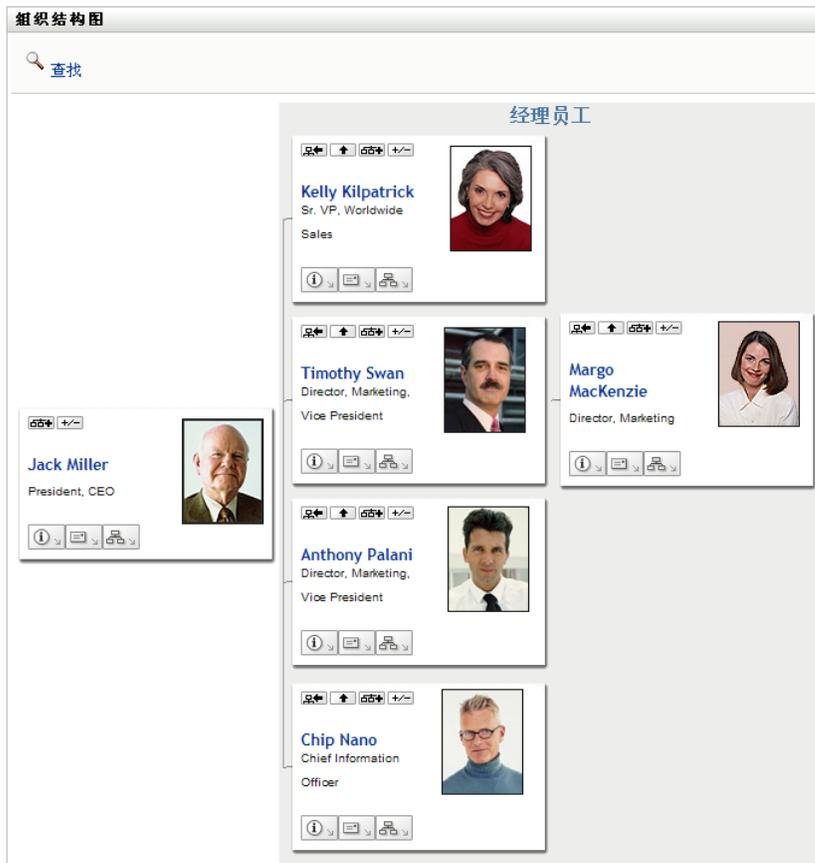
在她的名片中， Margo MacKenzie 单击上升一级  展开该图，显示她的经理：

图 3-2 Margo 单击“上升一级”显示她的经理



Margo 随后在她的经理的名片上单击上升一级 ，显示她的经理的经理：

图 3-3 Margo 再次单击“上升一级”，显示她的经理的经理



Margo 随后在自己的名片中单击 **将此实体设定为新的根**。这样就将她的名片再次设定为显示的根。

图 3-4 Margo 在她的名片中单击“将此实体设定为新的根”



## 3.2 浏览图

本部分说明如何通过以下方式在关系图中移动：

- ◆ 第 3.2.1 节“浏览至下个较高级别”（第 38 页）
- ◆ 第 3.2.2 节“重置关系的根”（第 39 页）
- ◆ 第 3.2.3 节“切换默认关系”（第 40 页）
- ◆ 第 3.2.4 节“展开或折叠默认图”（第 41 页）
- ◆ 第 3.2.5 节“选择要展开或折叠的关系”（第 41 页）
- ◆ 第 3.2.6 节“在组织结构图中查找某个用户”（第 43 页）

### 3.2.1 浏览至下个较高级别

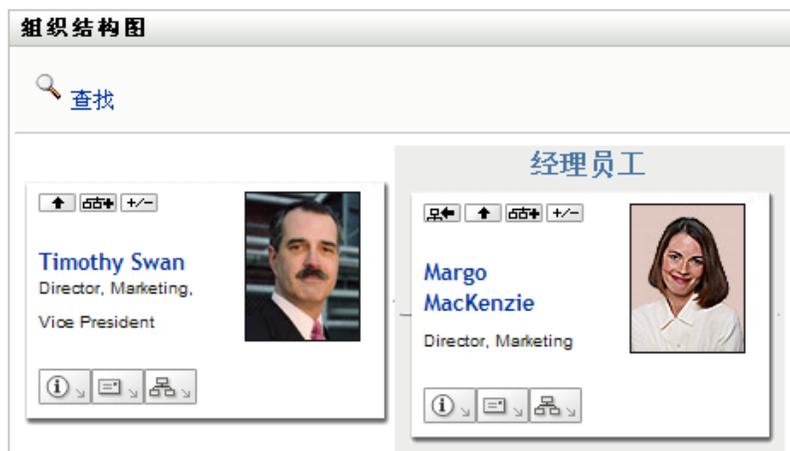
要浏览并展开至关系树中的下个较高级别：

- 1 在当前顶级名片中单击 **上升一级** 。

例如，假定 Margo 在该视图中单击 **上升一级**：



她的视图将展开为包含其上一级：



上升一级仅当将名片中的用户指派为经理时可用。如果该功能对您不可用，请咨询您的管理员。

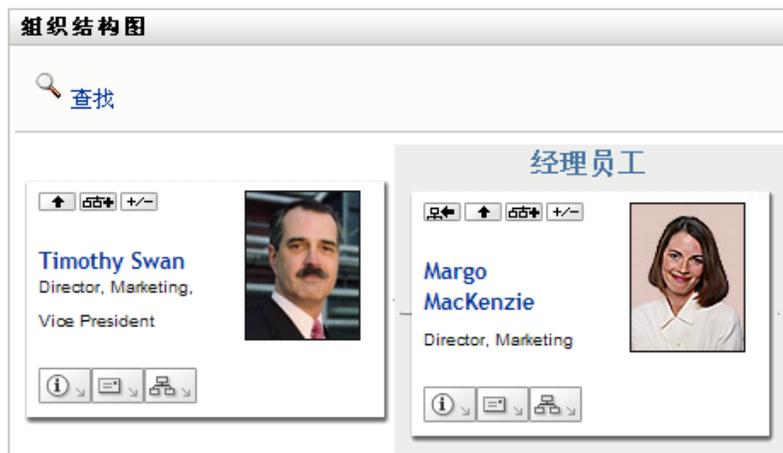
一张名片可以操作“上升一级”两次。

### 3.2.2 重设置关系的根

要重设置您的关系图视图的根：

- 1 找到要用作新根的用户的名片。
- 2 单击 **将此实体设定为新的根** ，或单击该名片上该用户的姓名（链接）。所选名片将成为组织结构图的根。

例如，假定 Margo Mackenzie 在该视图中她自己的名片上单击“将此实体设定为新的根”：



她的名片已成为新的根，现在位于她的组织结构图的顶部：



### 3.2.3 切换默认关系

- 1 单击 *切换到某个组织结构图*  更改您的默认关系。
- 2 选择要显示的关系类型。您的管理员可使用 Novell 提供的关系（请参见 [表 3-1](#)），也可以自定义关系。

表 3-1 Novell 提供的组织结构图关系的类型

组织结构图类型	说明
经理员工	显示经理和下属之间的报告结构。
用户组	显示用户及其所在的组。

Margo Mackenzie 将她的默认关系显示更改为用户组：

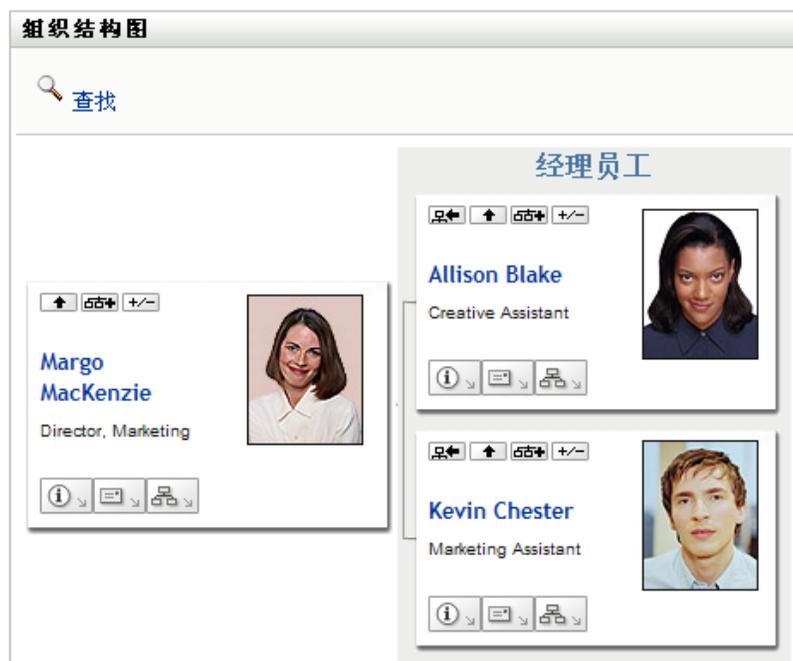


### 3.2.4 展开或折叠默认图

默认关系图是经理员工，除非您或您的管理员将它设置为其他类型。要展开或折叠默认图：

- 1 找到要展开或折叠默认关系显示的名片。
- 2 单击**展开/折叠当前关系**  切换按钮。

该图展开或折叠（即显示或隐藏）与所选名片相关的补充名片。例如，以下两个视图显示“展开”视图和“折叠”视图。



### 3.2.5 选择要展开或折叠的关系

- 1 确定要查看关系的名片。
- 2 在该名片中单击**选择要展开/折叠的关系** 。将打开一个下拉列表。
- 3 从下拉列表中选择关系和操作：

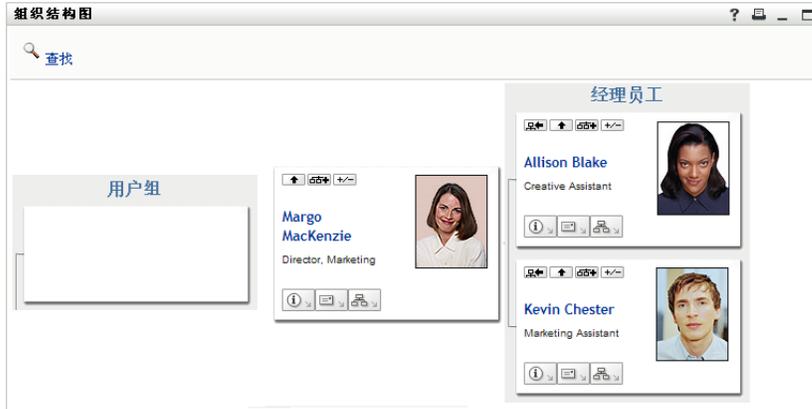
操作	说明
展开经理员工	选择此选项以打开管理者员工图。该图关闭时可用。
展开用户组	选择此选项以打开用户组。用户组关闭时可用。
折叠经理员工	选择此选项以折叠名片的管理者员工图。该图打开时可用。
折叠用户组	选择此选项以折叠名片的用户组。该图打开时可用。

如果您的管理员定义了其他关系，则它们也显示在该列表中。

在以下示例中，Margo MacKenzie 单击 *选择要展开/折叠的关系*，然后选择 *展开用户组*。



然后她单击 *向左* 并看到：



### 3.2.6 在组织结构图中查找某个用户

您可以在组织结构图中查找某个用户。这是查找不在您当前视图或关系图中的用户的快速搜索方法。找到的用户成为您视图的新的根。

- 1 单击位于图左上角的 *查找* 链接。

将显示“查找”页面：



- 2 针对需要查找的用户指定搜索准则：

**2a** 使用下拉列表选择是按 *名字* 还是按 *姓氏* 搜索。

**2b** 在下拉列表旁边的文本框中，键入要搜索的完整或部分姓名。

搜索操作将查找以键入的文本开头的 *所有* 姓名。该操作不区分大小写。也可以在文本中使用星号 (\*) 作为通配符，以代表零个或多个任意字符。

例如，以下所有示例都将查找名字 **Chip**：

Chip

chip

c

c\*

\*p

\*h\*

- 3 单击 *搜索*。

“查找”页面将显示搜索结果：



如果看到包含所需用户的用户列表，请转至**步骤 4**。否则，请返回到**步骤 2**。  
单击列标题可按升序或降序对搜索结果排序。

#### 4 从列表中选择所需的用户。

“查找”页面关闭，将该用户设定为该图的视图中新的根。

### 3.3 显示详细信息

可以在图中显示选定用户的细节（“配置文件”页面）。

- 1 找到要显示细节的用户的名片。
- 2 在该名片上单击**身份操作** ：  
将显示一个下拉列表。
- 3 在下拉列表中单击**显示信息**。如果您的管理员定义了其他选项，也将列出。  
出现“配置文件”页面，其中显示选定用户的详细信息：



该页面和 *身份自助服务* 选项卡上您自己的“我的配置文件”页面相似。但是，当您查看其他用户的细节时，可能没有权限在该页面上查看某些数据或执行某些操作。请咨询系统管理员以获得帮助。

要了解如何使用“配置文件”页面的功能，请参见第 5 章“使用我的配置文件”（第 53 页）。

- 4 使用完“配置文件”页面后，可以关闭该页面的窗口。

## 3.4 从关系图发送电子邮件

本部分将说明：

- ◆ 第 3.4.1 节“用电子邮件发送图中用户的相关信息”（第 45 页）
- ◆ 第 3.4.2 节“将新的电子邮件发送给图中的某个用户”（第 46 页）
- ◆ 第 3.4.3 节“向经理的小组发送电子邮件”（第 46 页）

### 3.4.1 用电子邮件发送图中用户的相关信息

- 1 找到要将其细节以电子邮件发送给某人的用户的名片。

- 2 在该名片上单击电子邮件图标 

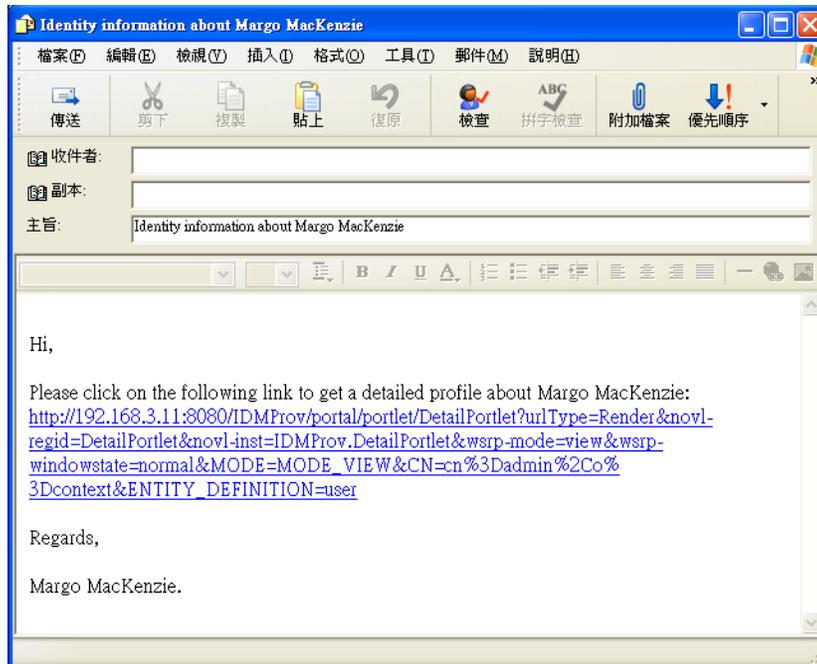
将显示一个弹出菜单。

- 3 选择 *电子邮件信息*。

将在默认的电子邮件客户程序中创建新邮件。邮件的以下部分已事先填写：

邮件各部分	包含
主题	文本：  <code>Identity Information for user-name</code>
正文	问候、讯息、链接和发件人姓名。  一个链接 (URL)，指向显示所选用户详细信息的“配置文件”页面。  在 Identity Manager User Application 显示任何信息之前，该链接将提示收件人先登录。收件人必须具有查看或编辑数据的相应权限。  要了解如何使用“配置文件”页面的功能，请参见第 5 章“使用我的配置文件”（第 53 页）。

例如：



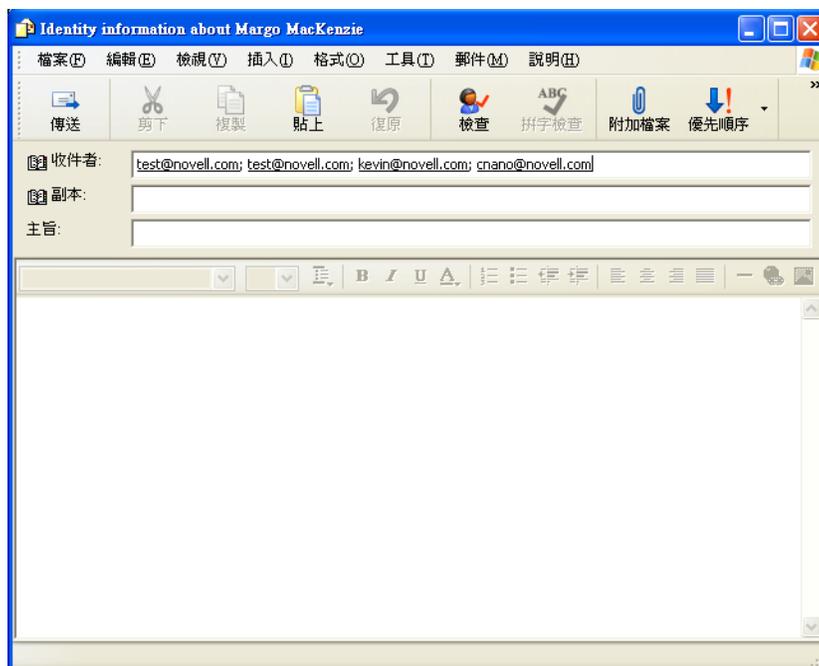
- 4 指定邮件的收件人（以及所需的其它内容）。
- 5 发送邮件。

### 3.4.2 将新的电子邮件发送给图中的某个用户

- 1 找到要向其发送电子邮件的用户的名片。
- 2 单击该名片上的电子邮件图标。  
将显示一个弹出菜单。
- 3 选择 *新建电子邮件*。  
将在默认的电子邮件客户程序中创建新邮件。该邮件除 *收件人* 列表（将所选用户指定为收件人）外，其它部分均是空白的。
- 4 填写邮件内容。
- 5 发送邮件。

### 3.4.3 向经理的小组发送电子邮件

- 1 找到用户的名片，该用户管理要向其发送电子邮件的小组。
- 2 在该名片上单击电子邮件图标。  
将显示一个弹出菜单。
- 3 选择 *向小组发送电子邮件*。  
将在默认的电子邮件客户程序中创建新邮件。该邮件除 *收件人* 列表外其它部分均是空白的，“收件人”列表将所选用户（经理）的每个直接下属指定为收件人。



- 4 填写邮件内容。
- 5 发送邮件。



# 使用关联报告

本部分说明如何使用 Identity Manager User Application 的 *身份自助服务* 选项卡上的“关联报告”页面。包括以下主题

- ◆ 第 4.1 节“关于关联报告”（第 49 页）
- ◆ 第 4.2 节“显示关联”（第 50 页）

**注释：**本部分将说明“关联报告”页面的默认功能。由于您的工作角色和权限级别的不同以及针对组织执行的自定义，您可能会发现某些差异；有关细节，请咨询系统管理员。

有关访问和操作 *身份自助服务* 选项卡的更多一般信息，请参见第 2 章“*身份自助服务选项卡介绍*”（第 31 页）。

## 4.1 关于关联报告

作为管理员，您可以用“关联报告”页面列出或诊断已供应给用户的某些关联。应用程序表显示：

- ◆ 用户在身份库的 DirXML- 关联表中有关联的应用程序或系统名称。（身份库通过策略或权利将用户帐户与已连接系统同步时，将填充关联表。）
- ◆ 关联的实例。
- ◆ 关联的状态。有关状态的说明请参见表 4-1。

表 4-1 关联状态表

状态	指示
已处理	驱动程序可识别驱动程序的目标应用程序的用户。用户可能想知道，是否需要对其关联列表之外的应用程序或系统发出供应请求。或者，如果某个应用程序在他们的列表中，但无法访问，用户可能希望咨询应用程序管理员来确定该问题。
禁用	该应用程序可能对该用户不可用。
待发	关联正在等待中。
手动	要实现该关联，手动处理是必需的。
迁移	迁移是必需的。
任意	各类状态。

并非所有已提供资源都表示在身份库中。

图 4-1 在第 50 页显示了“关联报告”页面的示例。

图 4-1 “关联报告” 页面



## 4.2 显示关联

单击*关联报告*时，首先显示的是您自己的关联。要显示其他用户的关联：

- 1 在*身份自助服务*选项卡上的*信息管理*下，单击*关联报告*。
- 2 在关联表上，单击*查找*。



- 3 在“对象查找”窗口中，从下拉菜单选择*名字或姓氏*，并指定搜索字符串。“对象查找”窗口将同时显示*名字*和*姓氏*。



- 4 选择姓名。关联表将显示该姓名的关联。

关联报告		
查找		
Jack Miller		
名称	实例	省/州
权利服务驱动程序	Entitlements Service Driver	已处理



# 使用我的配置文件

本部分说明如何使用 Identity Manager User Application 的 *身份自助服务* 选项卡上的“我的配置文件”页面。包括以下主题：

- ◆ 第 5.1 节“关于我的配置文件”（第 53 页）
- ◆ 第 5.2 节“编辑信息”（第 54 页）
- ◆ 第 5.3 节“用电子邮件发送您的信息”（第 59 页）
- ◆ 第 5.4 节“显示组织结构图”（第 60 页）
- ◆ 第 5.5 节“链接至其他用户或组”（第 60 页）

**注释：**本部分说明“我的配置文件”页面的默认功能。由于您的工作角色和权限级别的不同以及针对组织执行的自定义，您可能会发现某些差异；有关细节，请咨询系统管理员。

有关访问和操作 *身份自助服务* 选项卡的更多一般信息，请参见第 2 章“*身份自助服务选项卡介绍*”（第 31 页）。

## 5.1 关于我的配置文件

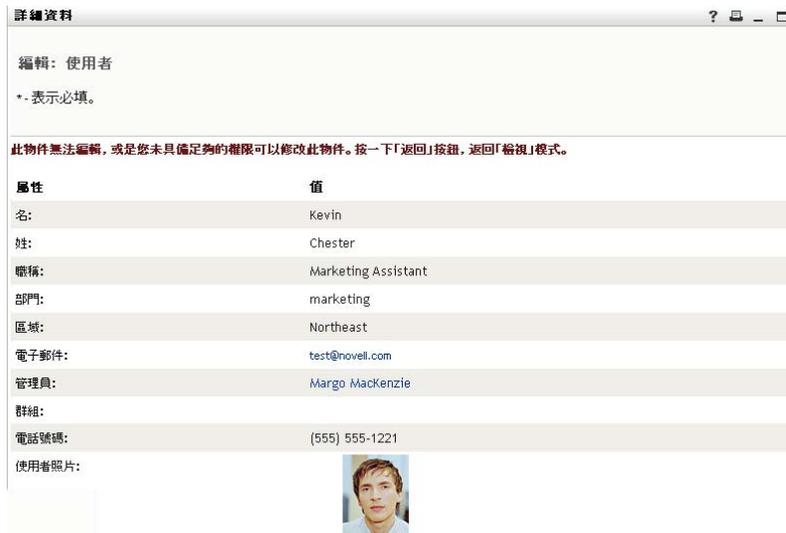
可以使用“我的配置文件”页面显示用户帐户的细节，并按需处理这些信息。例如，以下是 Kevin Chester（市场助理）进入“我的配置文件”页面时会看到的内容：

图 5-1 “我的配置文件细节”页面



如果要更改某些细节，可以编辑信息（尽管有权编辑的内容完全由系统管理员确定）。例如，假定 Kevin Chester 单击 *编辑您的信息*。在管理员授予他执行该操作的特权之后，他会看到可以编辑配置文件信息的页面：

图 5-2 “编辑配置文件” 页面



返回到主页（查看页）后，“我的配置文件”将提供可针对信息执行其它有用操作的链接。您可以：

- ◆ 通过电子邮件（以链接的形式）将细节发送给某个用户
- ◆ 切换为显示组织结构图（而不是细节）
- ◆ 如果已授权，可在组织结构图中选择要显示其细节的其他用户或组
- ◆ 单击一个电子邮件地址以将邮件发送给该帐户
- ◆ 为您使用的 User Application 实例指定区域设置（语言）。

## 5.2 编辑信息

“我的配置文件”提供了编辑页，如果需要进行更改，可切换到该页。

某些值可能无法编辑。不可编辑的值在编辑页面上显示为只读文本或链接。如果存在与有权编辑的内容相关的问题，请咨询系统管理员。

要编辑信息，请执行下列操作：

- 1 单击位于“我的配置文件”页顶部的 *编辑您的信息* 链接。
- 2 显示编辑页时，按需要进行更改。使用表 5-1 中的编辑按钮。
- 3 完成编辑后，请单击 *保存更改*，然后单击 *返回*。

### 5.2.1 隐藏信息

如果隐藏一项信息，则除了您本人和系统管理员以外，其他使用 Identity Manager User Application 的任何用户都看不到该信息。

- 1 单击位于“我的配置文件”页面顶部的 *编辑您的信息* 链接。
- 2 在编辑页面上，找到需要隐藏的项目。
- 3 单击该项目旁的 *隐藏*。

隐藏对某些项目可能已禁用。系统管理员可对特定项目启用该功能。

## 5.2.2 使用编辑按钮

表 5-1 列出了您可用于编辑配置文件细节的编辑按钮。

表 5-1 编辑按钮

按钮	作用
	查找需要在某个项中使用的值
	显示项中使用的值的 <i>历史</i> 列表
	添加其他项
	显示该属性的所有项
	删除现有项及其值
	用于编辑（以及指定和显示）图像

**注释：**以单独的编辑操作添加和删除组。如果在同一编辑操作中去除和添加组，则当单击 +（添加）按钮时，被删除的组名会重新出现。

以下各部分介绍有关使用其中某些编辑按钮的更多信息：

- ◆ [查找用户（第 55 页）](#)
- ◆ [查找组（第 56 页）](#)
- ◆ [使用历史列表（第 58 页）](#)
- ◆ [编辑图像（第 58 页）](#)

### 查找用户

1 在要查找其用户的项右侧，单击 [查找](#) 。

将显示“查找”页面：



2 针对需要查找的用户指定搜索准则：

**2a** 用下拉列表按 *名字*或*姓氏*指定搜索。

**2b** 在下拉列表旁边的文本框中，键入要搜索的完整或部分姓名。

搜索将查找以键入的文本开头的所有姓名。该操作不区分大小写。也可以在文本中使用星号 (\*) 作为通配符，以代表零个或多个任意字符。

例如，以下所有示例都将查找名字 Chip:

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

经理查找只会搜索身份为经理的用户。

### 3 单击 *搜索*。

“查找”页面将显示搜索结果:



如果看到包含所需用户的用户列表，请转至 **步骤 4**。否则，请返回到 **步骤 2**。

单击列标题可按升序或降序对搜索结果排序。

### 4 从列表中选择所需的用户。

“查找”页面将会关闭，同时将该用户的姓名插入到编辑页面上的相应项中。

## 查找组

#### 1 在要查找组的项右侧，单击 *查找* .

将显示“查找”页面:



## 2 针对需要查找的组指定搜索准则：

**2a** 在下拉列表中，只能按 *说明* 搜索。

**2b** 在下拉列表旁边的文本框中，键入要搜索的完整或部分说明。

搜索将查找以键入的文本开头的说明。该操作不区分大小写。也可以在文本中使用星号 (\*) 作为通配符，以代表零个或多个任意字符。

例如，以下所有示例都将查找说明 Marketing：

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

## 3 单击 *搜索*。

“查找”页面将显示搜索结果：



如果看到包含所需组的组列表，请转至 **步骤 4**。否则，请返回到 **步骤 2**。

单击列标题可按升序或降序对搜索结果排序。

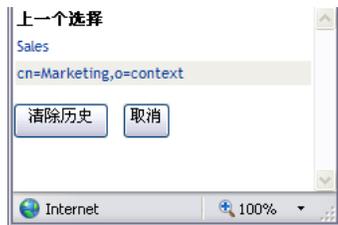
4 从列表中选择所需的组。

“查找”页面将会关闭，同时将该组插入到编辑页面上的相应项中。

### 使用历史列表

1 在要查看其以前值的项右侧，单击 **历史** 。

将显示 **历史** 列表。值按字母顺序显示。



2 执行以下步骤之一：

如果要	操作
从 <b>历史</b> 列表中选择	从列表中选择所需的值。  <i>历史</i> 列表将会关闭，同时将该值插入到编辑页面上的相应项中。
清除 <b>历史</b> 列表	单击 <b>清除历史</b> 。  <i>历史</i> 列表将会关闭，同时删除该项的历史值。清除 <b>历史</b> 列表不会更改编辑页面上的项的当前值。

### 编辑图像

编辑信息可能涉及到添加、替换或显示图像。

1 在编辑页面上单击 **显示** 以显示图像。

2 单击加号图标  **添加图像** 添加图像。

如果图像已存在，可以单击铅笔图标  **替换或删除图像** 替换或删除它。

3 单击该按钮以显示“文件上传”页面：



如果该项目已具有图像，则该图像会显示在此处。

- 4 要添加图像或替换当前图像：
  - 4a 单击“浏览”并选择适当的图像文件（如 GIF 或 JPG）。
  - 4b 单击 *保存更改*，将所选图像文件上传到服务器。
- 5 单击 *关闭窗口* 可返回到编辑页面。

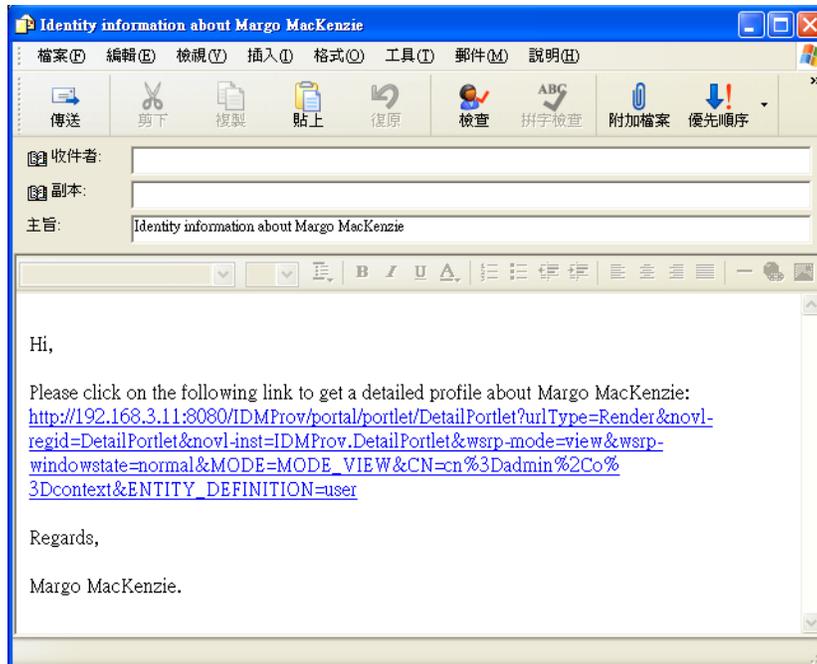
## 5.3 用电子邮件发送您的信息

“我的配置文件”页面可用电子邮件细节作为链接：

- 1 单击“我的配置文件”页面顶部的 *发送身份信息* 链接。  
将在默认的电子邮件客户程序中创建新邮件。邮件的以下部分已事先填写：

邮件各部分	包含
主题	文本：  Identity Information for <i>your-user-id</i>
正文	问候、讯息、链接和您的姓名。  一个链接 (URL) 指向显示您详细信息的“配置文件”页面。  在 Identity Manager User Application 显示任何信息之前，该链接将提示收件人先登录。收件人必须具有查看或编辑数据的相应权限。

例如：



- 2 指定邮件的收件人（以及所需的其它内容）。
- 3 发送邮件。

## 5.4 显示组织结构图

要从“我的配置文件”切换到“组织结构图”，请单击“我的配置文件”页面中间的 *显示组织结构图* 链接。

将显示组织结构图。例如：



要了解如何使用该页面的功能，请参见第 3 章“使用组织结构图”（第 35 页）。

## 5.5 链接至其他用户或组

您配置文件的“细节”页面可包含其他用户或组的链接。可以显示在细节中作为链接列出的其他用户或组的细节（“配置文件”页面）。

要显示有关另一用户或组的详细信息，请执行下列操作：

- 1 在“我的配置文件”页面上查看或编辑信息的同时，查找指向用户名或组名的链接。将鼠标指针移动到文本上，显示出表示链接的下划线。
- 2 单击一个链接（在单独的窗口中）显示该用户或组的细节。
- 3 使用该细节窗口后，可以关闭该窗口。

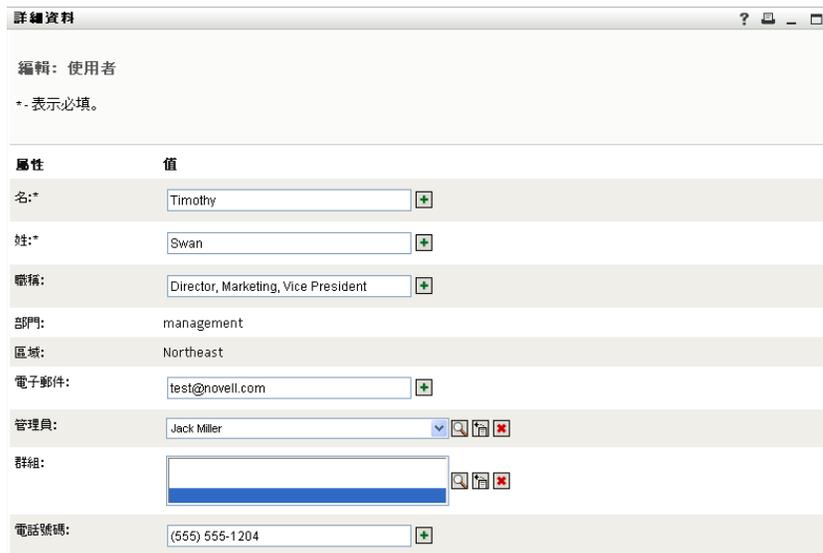
以下场景显示某个用户如何链接到另一用户和组细节。Timothy Swan（市场营销部副总经理）登录 Identity Manager User Application，然后进入“我的配置文件”页面：

图 5-3 “我的配置文件” 页面显示配置文件细节，并列出了配置文件操作



他单击 [編輯您的信息](#)。

图 5-4 “编辑细节” 页面



他注意到显示为链接的用户名 (Terry Mellon) 和组名 (行政管理、市场营销、改进客户服务工作小组)。于是他单击 [市场营销](#)，随即出现了一个新窗口：

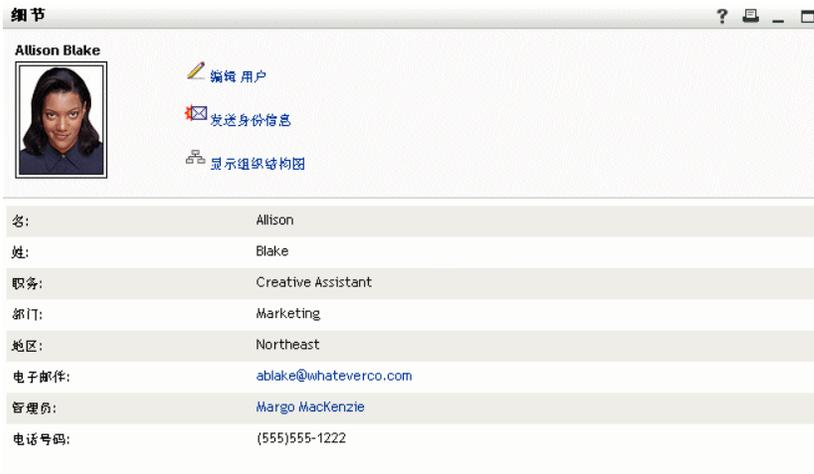
图 5-5 “组细节”页面



上面是有关“市场营销”组的详细信息。如果他有权限，则可以单击 *编辑组*，用 *编辑组* 页面从组中添加或去除成员、更改组说明或删除组。

“市场营销”组成员的姓名也是链接。他单击 *Allison Blake*，随即出现：

图 5-6 组成员配置文件的“组细节页面”链接

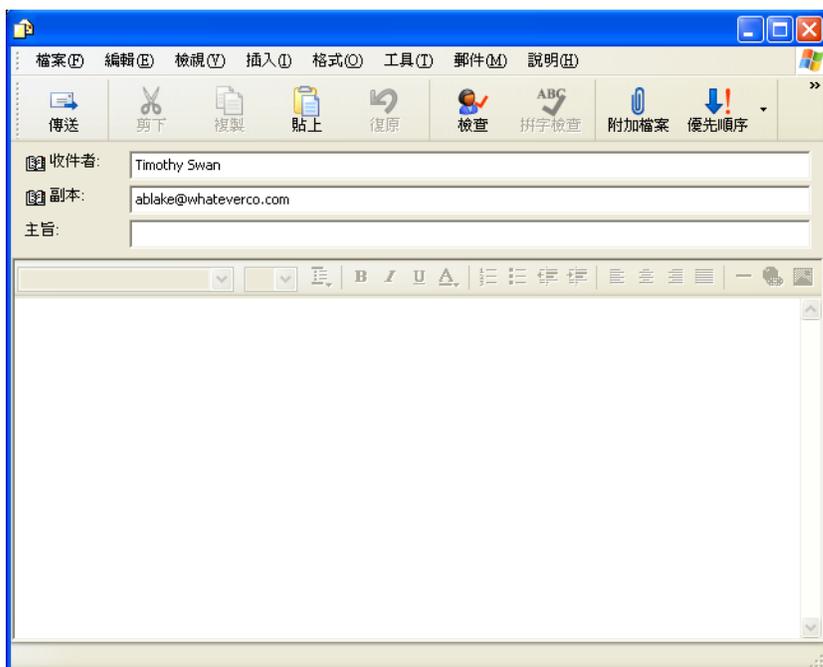


这是有关用户 Allison Blake（Timothy 的一个员工）的详细信息。

他可以单击 *编辑: 用户*（如果系统管理员允许），还可以编辑该用户的细节（除了部门和地区属性外）或删除该用户。

Allison 的电子邮件地址是一个链接。如果 Timothy 单击该链接，他的电子邮件客户程序会创建发送给 Allison 的新邮件：

图 5-7 用电子邮件将消息从用户的“配置文件”页面发送至用户



他现在可以键入消息内容，然后发送该消息。

## 5.6 选择首选语言

您可以选择要在 Identity Manager User Application 中使用的区域设置（语言）。您可以随时在*我的配置文件*中设置首选区域设置。

- 1 单击身份自助服务 > 信息管理 > 我的配置文件 > 编辑首选区域设置。将打开编辑首选区域设置页面。
- 2 可打开可用区域设置下拉列表，选择区域设置并单击添加，来添加区域设置。
- 3 可从按自选设置顺序排列区域设置列表选择区域设置，并选择上移、下移或删除，来更改自选设置顺序。
- 4 单击保存更改。

### 编辑首选区域设置

用户: Margo MacKenzie  
为当前应用程序的用户设定“区域设置自选设置”。

---

按自选设置排列的区域设置

上移下移去除

可用区域设置

▼ 添加

---

保存更改关闭

Identity Manager User Application 页面根据以下规则，以一种或多种首选语言（区域设置）显示：

1. User Application 按照首选区域设置列表中的顺序，使用 User Application 中定义的区域设置。
2. 如果没有为 User Application 定义首选区域设置，User Application 将按列出的顺序使用首选浏览器语言。
3. 如果没有为 User Application 或浏览器定义首选区域设置，将使用 User Application 默认设置。

### 5.6.1 在浏览器中定义首选语言

在 Firefox\* 中，通过 *工具 > 一般 > 语言 > 语言* 来添加语言。将您的首选语言放在列表顶部。在 Internet Explorer 中，通过 *查看 > 编码设置语言*。

# 使用目录搜索

本部分说明如何使用 Identity Manager User Application 的 *身份自助服务* 选项卡上的“目录搜索”页面。包括以下主题：

- ◆ 第 6.1 节“关于目录搜索”（第 65 页）
- ◆ 第 6.2 节“执行基本搜索”（第 67 页）
- ◆ 第 6.3 节“执行高级搜索”（第 68 页）
- ◆ 第 6.4 节“处理搜索结果”（第 75 页）
- ◆ 第 6.5 节“使用保存的搜索”（第 80 页）

**注释：**本部分说明“目录搜索”页面的默认功能。由于您的工作角色和权限级别的不同以及针对组织执行的自定义，您可能会发现某些差异；有关细节，请咨询系统管理员。

有关访问和操作 *身份自助服务* 选项卡的更多一般信息，请参见第 2 章“身份自助服务选项卡介绍”（第 31 页）。

## 6.1 关于目录搜索

可以使用“目录搜索”页面，通过输入搜索准则或使用以前保存的搜索准则来搜索用户、组或小组。

例如，假设 Timothy Swan（市场营销部主管）需要搜索组织中某个人的有关信息。他转至“目录搜索”页面，默认情况下他将看到以下内容：

图 6-1 “目录搜索”页面



他还没有任何已保存的搜索可选择，因此他选择 *新搜索*。

有位用户想联系一个名字以字母 C 开头的人，但想不起全名。因此，他只需指定一个具有以下准则的基本搜索：

图 6-2 在“搜索列表”页面上指定搜索准则



将显示搜索结果，而 Timothy 可使用这些结果查看和处理请求的信息。默认情况下，会显示身份选项卡信息：

图 6-3 搜索结果



Timothy 在搜索结果中单击组织选项卡，获得该信息的另一个视图。他想起要查找的这个人是在 Kip Keller 手下工作，于是将搜索范围缩小到 Cal Central：

图 6-4 使用选项卡更改搜索结果的视图



除了用于切换不同视图的选项卡外，搜索结果页面还提供用于对信息执行操作的链接和按钮。您可以：

- ◆ 通过单击列标题对信息行排序
- ◆ 通过单击用户或组的行显示细节（“配置文件”页面）
- ◆ 通过单击某个用户行中的电子邮件图标来向该用户发送新的电子邮件
- ◆ 保存搜索以供以后复用
- ◆ 将结果导出到文本文件
- ◆ 通过更改搜索准则来修改搜索

生成搜索结果时，有时需要指定一个比基本搜索更具体的搜索，以描述所需的信息。可以使用高级搜索指定复杂准则。

如果以后需要再次执行某个高级搜索，则可以保存该搜索。甚至可以将已保存搜索方便地用作经常运行的基本搜索。例如， Timothy Swan 添加了一组经常使用的已保存搜索：

图 6-5 搜索列表页面上已保存的搜索

搜索列表		
我保存的搜索，单击搜索进行搜索。		
修改	去除	搜索名称
 编辑	 删除	Marketing
 编辑	 删除	Search on B
 编辑	 删除	search a

 新搜索

## 6.2 执行基本搜索

- 1 转到“目录搜索”页面，并单击 *新搜索*。默认情况下将显示“基本搜索”页面：



- 2 在 *搜索* 下拉列表中，通过选择 *组* 或 *用户* 指定要查找的信息类型。
- 3 在 *项目类别* 下拉列表中，选择要搜索的属性。例如：  
Last Name  
可用属性的列表由搜索内容（用户或组）确定。
- 4 在 *表达式* 下拉列表中，根据您所选属性选择要执行的比较运算。例如：  
equals  
更多信息请参见第 6.3.1 节“选择表达式”（第 70 页）。
- 5 在 *搜索术语* 输入框中，根据选定属性指定要比较的值。例如：  
Smith  
更多信息请参见第 6.3.2 节“为比较运算指定值”（第 71 页）。
- 6 单击 *搜索*。  
将显示搜索结果。  
要了解下一步操作，请参见第 6.4 节“处理搜索结果”（第 75 页）。

## 6.3 执行高级搜索

搜索用户或组时，如果需要指定多个准则，则可以使用高级搜索。例如：

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

如果指定多个准则分组（用于控制评估准则时遵循的顺序），则还将使用相同的逻辑运算来连接各分组。例如，要使用以下准则执行高级搜索（用一个“or”运算符连接两个准则分组）：

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

指定图 6-6 在第 68 页中显示的以下选项：

图 6-6 在“搜索列表”页面上指定高级搜索

The screenshot shows the 'Search List' (搜索列表) window with the following configuration:

- Search scope: 用户 (User)
- Criteria 1: Operator: 和 (AND), Item Category: 姓 (Last Name), Expression: 等于 (equals), Search Term: (empty)
- Criteria 2: Operator: 和 (AND), Item Category: 职务 (Title), Expression: 开始于 (starts with), Search Term: (empty)
- Buttons: 添加/去除条件 (Add/Remove Condition), 添加/去除条件分组 (Add/Remove Condition Group), 搜索 (Search), 我保存的搜索 (My Saved Searches), 基本搜索 (Basic Search)

此搜索的结果在图 6-7 在第 68 页中显示。

图 6-7 高级搜索结果

The screenshot shows the search results for the criteria defined in Figure 6-6. The search criteria are: 用户: (姓 等于 Smith 和 职务 包含 rep) -或- (名 开始于 k 和 部门 等于 sales). The results are sorted by 部门 (Department) and show 4 matches.

身份	位置	组织	姓名	职务	部门	管理员	电子邮件
Jane	Smith	HR, Representative	hr				
Kate	Smith	Sales Representative	sales	Sally South			
Kevin	Chester	Marketing Assistant	sales	Margo MacKenzie			
Kip	Keller	VP, North American Sales	sales	Kelly Kilpatrick			

1 - 4 / 4

Buttons: 我保存的搜索 (My Saved Searches), 保存搜索 (Save Search), 导出结果 (Export Results), 修改搜索 (Modify Search), 新搜索 (New Search)

要执行高级搜索，请执行下列操作：

- 1 转到“目录搜索”页面，并单击新搜索。默认情况下将显示“基本搜索”页面。
- 2 单击高级搜索。将显示“高级搜索”页面：



3 在 *搜索* 下拉列表中，通过选择下列选项之一，指定要查找的信息类型：

- ◆ 组
- ◆ 用户

现在可以填写 *搜索准则* 区域。

4 指定准则分组的标准：

4a 使用 *项目类别* 下拉列表选择要搜索的属性。例如：

Last Name

可用属性的列表由搜索内容（用户或组）确定。

4b 使用 *表达式* 下拉列表，根据您选择的属性选择要执行的比较运算。例如：

equals

更多信息请参见第 6.3.1 节“选择表达式”（第 70 页）。

4c 使用 *搜索术语* 项，根据您选择的属性指定要比较的值。例如：

Smith

更多信息请参见第 6.3.2 节“为比较运算指定值”（第 71 页）。

5 如果要指定准则分组的另一个标准，请执行下列操作：

5a 单击准则分组右侧的 *添加准则*：



5b 在新准则的左侧，使用 *准则逻辑运算符* 下拉列表将此准则与前一个准则相连接；选择 *and* 或 *or*。在任一准则分组中，只能使用两种逻辑运算符中的一种。

5c 从步骤 4 开始重复该过程。

要删除准则，请单击准则右侧的 *去除准则*：

6 如果要指定另一个准则分组，请执行下列操作：

6a 单击 *添加准则分组*：



6b 在新准则分组的上方，使用 *准则分组逻辑运算符* 下拉列表将此分组与前一个分组相连接；选择 *and* 或 *or*。

6c 从步骤 4 开始重复该过程。

要删除准则分组，请单击其上的 *去除准则分组*： *去除条件分组*

7 单击 *搜索*。

将显示搜索结果。

要了解下一步操作，请参见第 6.4 节“处理搜索结果”（第 75 页）。

### 6.3.1 选择表达式

单击 *表达式* 为您的搜索选择比较准则。准则中可用的比较（关系）运算的列表由该准则中指定的属性类型确定：

表 6-1 用于搜索的比较运算

如果属性为	您可以选择以下比较运算之一
字符串（文本）	<ul style="list-style-type: none"><li>◆ 起始字符</li><li>◆ 包含</li><li>◆ 等于</li><li>◆ 结束字符</li><li>◆ 存在</li><li>◆ 起始字符不是</li><li>◆ 不包含</li><li>◆ 不等于</li><li>◆ 结束字符不是</li><li>◆ 不存在</li></ul>
具有预先确定的选项列表的字符串（文本）	<ul style="list-style-type: none"><li>◆ 等于</li></ul>
用户或组（或 DN 标识的其它对象）	<ul style="list-style-type: none"><li>◆ 存在</li></ul>
布尔值（true 或 false）	<ul style="list-style-type: none"><li>◆ 不等于</li><li>◆ 不存在</li></ul>
用户（项目类别：管理员、组或直接报告）	<ul style="list-style-type: none"><li>◆ 等于</li><li>◆ 存在</li><li>◆ 不等于</li><li>◆ 不存在</li></ul>
组（项目类别：成员）	<ul style="list-style-type: none"><li>◆ 等于</li><li>◆ 存在</li><li>◆ 不等于</li><li>◆ 不存在</li></ul>

如果属性为	您可以选择以下比较运算之一
时间（格式为日期 - 时间或仅有日期）	<ul style="list-style-type: none"> <li>◆ 等于</li> </ul>
数字（整数）	<ul style="list-style-type: none"> <li>◆ 大于</li> <li>◆ 大于等于</li> <li>◆ 小于</li> <li>◆ 小于等于</li> <li>◆ 存在</li> <li>◆ 不等于</li> <li>◆ 不大于</li> <li>◆ 不大于等于</li> <li>◆ 不小于</li> <li>◆ 不小于等于</li> <li>◆ 不存在</li> </ul>

### 6.3.2 为比较运算指定值

准则中指定的属性类型还确定如何为准则中的比较运算指定值：

**表 6-2** 输入比较值的方法

如果属性为	执行此操作来指定值
字符串（文本）	在右侧显示的文本框中键入文本。
具有预先确定的选项列表的字符串（文本）	从右侧显示的下拉列表中选择一个选项。
用户或组（或 DN 标识的其它对象）	使用右侧显示的 <i>查找</i> 、 <i>历史</i> 和 <i>重设置</i> 按钮。
时间（格式为日期 - 时间或仅有日期）	使用右侧显示的 <i>日历</i> 和 <i>重设置</i> 按钮。
数字（整数）	在右侧显示的文本框中键入数字。
布尔值（true 或 false）	在右侧显示的文本框中键入 true 或 false。

如果比较运算为下列情况之一，则不需要指定值：

- ◆ 存在
- ◆ 不存在

#### 文本的大小写

文本搜索不区分大小写。无论输入的值是大写还是小写的，都将得到相同的结果。例如，以下所有输入都是等效的：

McDonald  
mcdonald  
MCDONALD

## 文本中的通配符

也可以在文本中使用星号 (\*) 作为通配符，以代表零个或多个任意字符。例如：

Mc\*

\*Donald

\*Don\*

McD\*d

## 使用“查找”、“历史”和“重置”按钮

有些搜索准则会显示“查找”、“历史”和“重置”按钮。本部分介绍如何使用这些按钮：

**表 6-3** 搜索准则中的“查找”、“历史”和“重置”按钮。

按钮	作用
	查找比较运算中使用的值
	显示用于比较运算的值的 <i>历史</i> 列表
	重置比较运算中使用的值

要查找用户，请执行下列操作：

- 1 在要查找其用户的项右侧，单击 *查找* 按钮：



将显示“查找”页面：



- 2 针对需要查找的用户指定搜索准则：

**2a** 用下拉列表按 *名字* 或 *姓氏* 选择搜索。

**2b** 在下拉列表旁边的文本框中，键入要搜索的完整或部分姓名。

搜索将查找以键入的文本开头的所有姓名。该操作不区分大小写。也可以根据需要在文本中使用星号 (\*) 作为通配符，以代表零个或多个任意字符。

例如，以下所有示例都将查找名字 Chip：

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

**3** 单击 *搜索*。

“查找”页面将显示搜索结果：



如果看到包含所需用户的用户列表，请转至 **步骤 4**。否则，请返回到 **步骤 2**。

单击列标题可按升序或降序对搜索结果排序。

**4** 从列表中选择所需的用户。

“查找”页面将会关闭，同时将该用户的姓名插入到相应项中，以用作比较运算中的值。

要以用户搜索准则查找某组：

**1** 将 *组* 添加为搜索准则，然后单击 *查找* （位于 *搜索术语* 字段右边）：



“查找”页面将显示搜索结果：



**2** 针对需要查找的组指定搜索准则:

**2a** 在下拉列表中, 只能按 *说明* 搜索。

**2b** 在下拉列表旁边的文本框中, 键入要搜索的完整或部分说明。

搜索将查找以键入的文本开头的所有说明。该操作不区分大小写。也可以在文本中使用星号 (\*) 作为通配符, 以代表零个或多个任意字符。

例如, 以下所有示例都将查找说明 **Marketing**:

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

**3** 单击 *搜索*。

“查找”页面将显示搜索结果:



如果看到包含所需组的组列表, 请转至 **步骤 4**。否则, 请返回到 **步骤 2**。

单击列标题可按升序或降序对搜索结果排序。

4 从列表中选择所需的组。

“查找”页面将会关闭，同时将该组的说明插入到相应项中，以用作比较运算中的值。

要使用 *历史* 列表，请执行下列操作：

1 单击某个项（要查看该项以前的值）右侧的 *历史* ：

*历史* 列表以字母顺序显示该准则以前的值：



2 执行以下步骤之一：

如果要	操作
从 <i>历史</i> 列表中做出选择	从列表中选择所需的值。 <i>历史</i> 列表将会关闭，同时将该值插入到相应项中，以用作比较运算中的值。
清除 <i>历史</i> 列表	单击 <i>清除历史</i> 。 <i>历史</i> 列表将会关闭，同时删除该项的历史值。清除 <i>历史</i> 列表不会更改比较运算中的项的当前值。

## 6.4 处理搜索结果

本部分说明如何处理成功搜索后显示的结果：

- ◆ 第 6.4.1 节“关于搜索结果”（第 76 页）
- ◆ 第 6.4.2 节“使用搜索列表”（第 77 页）
- ◆ 第 6.4.3 节“可以执行的其它操作”（第 78 页）

## 6.4.1 关于搜索结果

搜索结果的内容取决于所执行搜索的类型：

- ◆ 对于用户搜索（第 76 页）
- ◆ 对于组搜索（第 76 页）

在任何搜索结果页面上，您都可以选择

- ◆ 查看我保存的搜索
- ◆ 保存搜索
- ◆ 修改搜索
- ◆ 导出结果
- ◆ 开始新搜索

### 对于用户搜索

在用户搜索的结果中，用户列表提供了三个信息视图选项卡：

- ◆ 身份（联系信息）
- ◆ 位置（地理信息）
- ◆ 组织（组织信息）

图 6-8 用户搜索结果

身份	位置	组织	姓名	职务	部门	管理员	电子邮件
Bill	Bender	Technical Account Manager	Bill	Burke	Sales manager, Central		
Margo	MacKenzie	Director, Marketing				Timothy Swan	
Jane	Smith	HR, Representative			hr		
Timothy	Swan	Director, Marketing, Vice President			management	Jack Miller	
Allison	Blake	Creative Assistant			marketing	Margo MacKenzie	
Cal	Central	VP, North American Sales			sales		
Kevin	Chester	Marketing Assistant			sales	Margo MacKenzie	

### 对于组搜索

组搜索的结果只提供该信息的“组织”视图：

图 6-9 组搜索结果



## 6.4.2 使用搜索列表

对于显示的、用于表示结果的行列表，可以执行下列操作：

- ◆ 要切换到其它视图，请执行下列操作：（第 77 页）
- ◆ 要对信息行排序，请执行下列操作：（第 77 页）
- ◆ 要显示用户或组的细节，请执行下列操作：（第 77 页）
- ◆ 要将电子邮件发送给搜索列表中的某个用户，请执行下列操作：（第 78 页）

**要切换到其它视图，请执行下列操作：**

- 1 单击要显示的视图的选项卡。

**要对信息行排序，请执行下列操作：**

- 1 单击要排序的列的标题。  
最初按升序排序。
- 2 再次单击列标题可以在升序和降序之间切换（随意切换）。

**要显示用户或组的细节，请执行下列操作：**

- 1 单击要查看细节的用户或组的行（但除非要发送邮件，否则不要直接单击电子邮件图标）。  
将出现“配置文件”页面，其中显示选定用户或组的详细信息：



该页面类似于 *身份自助服务* 选项卡上的“我的配置文件”页面。唯一区别在于，在查看另一用户或组（即除您本人以外）的细节时，您将无权在页面上查看某些数据或执行某些操作。请咨询系统管理员以获得帮助。

要了解如何使用“配置文件”页面的功能，请参见第 5 章“使用我的配置文件”（第 53 页）。

2 完成“配置文件”页面的操作后，可以关闭该页面的窗口。

**要将电子邮件发送给搜索列表中的某个用户，请执行下列操作：**

1 找到要向其发送电子邮件的用户所在行。

2 在该用户的行中单击 *发送电子邮件* ：

将在默认的电子邮件客户程序中创建新邮件。该邮件除 *收件人列表*（将所选用户指定为收件人）外，其它部分均是空白的。

3 填写邮件内容。

4 发送邮件。

### 6.4.3 可以执行的其它操作

显示搜索结果时，还可以：

- ◆ [保存搜索](#)（第 78 页）
- ◆ [导出搜索结果](#)（第 79 页）
- ◆ [修改搜索准则](#)（第 80 页）

#### 保存搜索

要保存当前的搜索准则集以供将来复用，请执行下列操作：

1 单击 *保存搜索*（位于页面底部）。

2 出现提示时，为该搜索指定名称。

如果正在查看现有已保存搜索的结果，则该搜索名称将显示为默认值。这样，便可以使用所做的任何准则更改来更新保存的搜索。

否则，如果键入的搜索名称与现有已保存搜索的名称相冲突，则在保存新的搜索时，系统会自动将版本号添加到名称的末尾。

**3** 单击 *确定* 保存搜索。

“搜索列表”页面将显示“我保存的搜索”列表。

要了解如何处理保存的搜索，请参见第 6.5 节“使用保存的搜索”（第 80 页）。

## 导出搜索结果

要将搜索结果导出到文本文件，请执行下列操作：

**1** 单击 *导出结果*（位于页面底部）。

将显示“导出”页面：



默认情况下，将选择在 *屏幕上查看*，并在格式下拉列表中选择 *CSV*。因此，“导出”页面将以 *CSV*（逗号分隔值）格式显示当前的搜索结果。

**2** 如果要查看这些搜索结果以制表符分隔格式显示的效果，请选择下拉列表中的 *制表符分隔*，然后单击 *继续*。

**3** 如果已准备好将当前搜索结果导出到文本文件，请选择 *导出到磁盘*。

将显示“导出”页面：



**4** 用 *格式* 下拉列表选择搜索结果所用的导出格式：

导出格式	生成的文件的默认名称
CSV	SearchListResult. <i>date</i> . <i>time</i> .csv  例如：  SearchListResult.27-Sep-05.11.21.47.csv
制表符分隔	SearchListResult. <i>date</i> . <i>time</i> .txt  例如：  SearchListResult.27-Sep-05.11.20.51.txt
XML（如果导出至磁盘则可用）	SearchListResult. <i>date</i> . <i>time</i> .xml  例如：  SearchListResult.27-Sep-05.11.22.51.xml

- 5 单击 *导出*。
- 6 出现提示时，指定保存导出的搜索结果文件的位置。
- 7 完成导出后，单击 *关闭窗口*。

### 修改搜索准则

- 1 单击 *修改搜索*（位于页面底部）。  
您会回到上个搜索页面，可编辑搜索准则。
- 2 根据下列部分中的指导修改搜索准则：
  - ◆ [第 6.2 节“执行基本搜索”（第 67 页）](#)
  - ◆ [第 6.3 节“执行高级搜索”（第 68 页）](#)

## 6.5 使用保存的搜索

进入“目录搜索”后，默认情况下会显示“我保存的搜索”页面。本部分说明可对已保存搜索执行的操作：

- ◆ [第 6.5.1 节“要列出保存的搜索，请执行下列操作：”（第 80 页）](#)
- ◆ [第 6.5.2 节“要运行保存的搜索，请执行下列操作：”（第 81 页）](#)
- ◆ [第 6.5.3 节“要编辑保存的搜索，请执行下列操作：”（第 81 页）](#)
- ◆ [第 6.5.4 节“要删除保存的搜索，请执行下列操作：”（第 81 页）](#)

### 6.5.1 要列出保存的搜索，请执行下列操作：

- 1 单击“目录搜索”页面底部的 *我保存的搜索* 按钮。将显示“我保存的搜索”页面。[图 6-10 在第 81 页](#) 显示了一个示例。

图 6-10 “我保存的搜索”页面

搜索列表		
我保存的搜索。单击搜索进行搜索。		
修改	去除	搜索名称
 编辑	 删除	Marketing
 编辑	 删除	Search on B
 编辑	 删除	search a
 新搜索		

## 6.5.2 要运行保存的搜索，请执行下列操作：

- 1 在*我保存的搜索*列表中，找到需要执行的已保存搜索。
- 2 单击已保存搜索的名称（或单击该行的开始处）。  
将显示搜索结果。  
要了解下一步操作，请参见第 6.4 节“处理搜索结果”（第 75 页）。

## 6.5.3 要编辑保存的搜索，请执行下列操作：

- 1 在*我保存的搜索*列表中，找到需要修改的已保存搜索。
- 2 在该已保存搜索的行中单击*编辑*。  
您将进入可编辑搜索准则的搜索页面。
- 3 根据下列部分中的指导修改搜索准则：
  - ◆ 第 6.2 节“执行基本搜索”（第 67 页）
  - ◆ 第 6.3 节“执行高级搜索”（第 68 页）
- 4 要保存对搜索所做的更改，请参见第 6.4 节“处理搜索结果”（第 75 页）。

## 6.5.4 要删除保存的搜索，请执行下列操作：

- 1 在*我保存的搜索*列表中，找到要删除的已保存搜索。
- 2 在该保存的搜索的行中单击“删除”。
- 3 出现提示时，单击“确定”*确认删除*。



# 执行口令管理

本部分说明如何使用 Identity Manager User Application 的 *身份自助服务* 选项卡上的“口令管理”页面。包括以下主题：

- ◆ 第 7.1 节“关于口令管理”（第 83 页）
- ◆ 第 7.2 节“口令询问应答”（第 83 页）
- ◆ 第 7.3 节“口令提示更改”（第 84 页）
- ◆ 第 7.4 节“更改口令”（第 85 页）
- ◆ 第 7.5 节“口令策略状态”（第 86 页）
- ◆ 第 7.6 节“口令同步状态”（第 87 页）

**注释：**本部分说明“口令管理”页面的默认功能。由于您的工作角色和权限级别的不同以及针对组织执行的自定义，您可能会发现某些差异；有关细节，请咨询系统管理员。

有关访问和操作 *身份自助服务* 选项卡的更多一般信息，请参见第 2 章“*身份自助服务选项卡介绍*”（第 31 页）。

## 7.1 关于口令管理

可以视需要使用“口令管理”页执行表 7-1 中列出的任一功能：

表 7-1 口令管理功能

“口令管理”页面	功能
口令询问应答	设置或更改下列项目之一： <ul style="list-style-type: none"> <li>◆ 对管理员定义的询问问题的有效应答</li> <li>◆ 用户定义的询问问题和应答</li> </ul>
口令提示更改	设置或更改口令提示
更改口令	根据系统管理员设置的规则更改（重置）口令
口令策略状态	检查您的口令策略要求。您可以更改标为 <b>有效</b> 的要求
口令同步状态	显示应用程序口令与身份库的同步状态

**注释：**在同步完成前访问应用程序会导致应用程序访问出现问题。

## 7.2 口令询问应答

在登录期间如果您忘记了口令，系统可使用安全询问问题校验您的身份。如果系统管理员设置了为您启用此功能的口令策略，则您可以使用“口令询问应答”页执行下列操作：

- ◆ 指定回答管理员定义的问题时，对您有效的应答
- ◆ 指定您自己的问题和这些问题的有效应答（如果您的口令策略启用了此功能）

要使用“口令询问应答”页面，请执行下列操作：

- 1 在身份自助服务选项卡上，单击菜单中的口令询问应答（在口令管理下方）。  
将显示“口令询问应答”页面。例如：



应答文本框将显示为空白（即使您以前定义过应答）。

- 2 在每个应答文本框（它们都是必填的）中键入适当应答，或者使用您以前保存的应答。  
请确保指定今后可以记住的应答。
- 3 指定或更改任何必需的用户定义的问题。不能多次使用同一问题。
- 4 单击提交。

将显示请求的状态。例如：



## 7.3 口令提示更改

在登录期间如果忘记了口令，则可以使用口令提示帮助记起口令。可以使用“口令提示更改”页面设置或更改口令提示。

- 1 在身份自助服务选项卡上，单击菜单中的口令提示更改（在口令管理下方）。  
将显示“口令提示定义”页面：



- 2 为提示键入新文本。

口令不能出现在提示文本中。

### 3 单击提交。

将显示请求的状态。例如：



## 7.4 更改口令

不论何时需要更改口令，都可以使用此页面（前提是系统管理员允许您更改口令）。

### 1 在身份自助服务选项卡上，单击菜单中的更改口令（在口令管理下方）。

将显示“更改口令”页面。如果系统管理员已为您设置了口令策略，则“更改口令”页面通常会提供与如何指定符合策略要求的口令有关的信息。例如：



如果没有适用的口令策略，将显示基本的“更改口令”页面：



- 2 在 *旧* 口令文本框中键入当前口令。
- 3 在 *新* 口令文本框中键入新口令。
- 4 在 *重键入口* 口令文本框中再次键入新口令。
- 5 单击 *提交*。
- 6 如果管理员将您的安全策略配置为要提供口令提示，则可能会提示您提供提供口令提示。如果出现提示，请参见第 7.3 节“口令提示更改”（第 84 页）。
- 7 将显示您的请求的状态。例如：



## 7.5 口令策略状态

管理员会指派给您一个口令策略。该策略决定了与您的口令相关的安全措施。您可以通过以下操作检查您的口令策略要求：

- 1 在 *身份自助服务* 选项卡上，单击菜单中的 *口令策略状态*（在 *口令管理* 下方）。将显示 *口令策略状态* 页面。例如：



您不能更改标为无效的项目。

## 7.6 口令同步状态

用“口令同步状态”页面确定您的口令是否已在应用程序间同步。请在您的口令同步后，再访问其他应用程序。在同步完成前访问应用程序可能导致应用程序访问问题。

- 1 在身份自助服务选项卡上，单击菜单中的口令同步状态（在口令管理下方）。将显示口令同步状态页面。彩色图标表示口令已同步的应用程序。暗淡的图标表示尚未同步的应用程序。例如：





# 创建用户或组

本部分说明如何使用 Identity Manager User Application 的 *身份自助服务* 选项卡上的“创建用户或组”页面。包括以下主题：

- ◆ 第 8.1 节“关于创建用户或组”（第 89 页）
- ◆ 第 8.2 节“创建用户”（第 89 页）
- ◆ 第 8.3 节“创建组”（第 91 页）
- ◆ 第 8.4 节“使用编辑按钮”（第 92 页）

有关访问和操作 *身份自助服务* 选项卡的一般信息，请参见第 2 章“*身份自助服务选项卡介绍*”（第 31 页）。

## 8.1 关于创建用户或组

系统管理员可使用“创建用户或组”页面创建用户和组。系统管理员可允许其他人（通常是行政或管理职位上选定的人）访问该页面。

由于您的工作角色和权限级别的不同以及针对组织执行的自定义，您可能会发现与本部分中描述的功能有些差异。请咨询系统管理员以了解细节。

有关允许访问“创建用户或组”页面的细节位于《*Identity Manager User Application: 管理指南* (<http://www.novell.com/documentation/idmr bpm361/index.html>)》的“页面管理”部分。要允许访问，请打开 iManager，将用户添加为“受托者”，将名为“创建”的已指派权限添加给“受托者”。

要查看哪些用户或组已存在，可使用“目录搜索”页面。请参见第 6 章“*使用目录搜索*”（第 65 页）。

## 8.2 创建用户

- 1 在 *身份自助服务* 选项卡上，单击菜单中的 *创建用户或组*（如果已显示 *目录管理*，则在其下方）。

将显示 *选择要创建的对象* 面板。



- 2 使用 *对象类型* 下拉列表选择 *用户*，然后单击 *继续*。

将显示 *用户 - 设置属性* 面板：

### 3 指定以下必需属性的值：

属性	指定的内容
用户 ID	该新用户的用户名。
容器	<p>需要在其中储存新用户的身份库中的组织单元（例如名称为 users 的组织单元）。例如：</p> <p><code>ou=users,ou=MyUnit,o=MyOrg</code></p> <p>要了解如何使用为指定容器而提供的按钮，请参见第 8.4 节“使用编辑按钮”（第 92 页）。</p> <p>如果系统管理员已经为此类型的对象建立了默认的创作容器，则系统不会提示您提供容器。</p>
名字	用户的名字。
姓氏	用户的姓氏。

4 指定该新用户的可选细节，例如头衔、部门、地区、电子邮件地址、经理或电话号码。要了解有关使用为指定某些属性的值而提供的按钮，请参见第 8.2 节“创建用户”（第 89 页）。

5 单击 *继续*。

将显示 *创建* 对话框：

如果口令策略对目标容器有效，则此面板将提供与如何指定符合策略要求的口令有关的信息。还会针对该策略验证口令。

- 在 *口令* 和 *确认口令* 文本框中键入新用户的口令，然后单击 *继续*。

这将设置新用户的初始口令。该用户首次登录时，Identity Manager User Application 将提示该用户更改该口令。

至此已创建用户和口令，随后将显示用于汇总结果的 *审阅* 面板：

*审阅* 面板提供了便利的可选链接：

- 单击新用户的名称，以显示列出该用户细节的“配置文件”页面。您可以在“配置文件”页面中编辑用户细节，进行更改或删除该用户。
- 单击 *创建另一个* 返回到“创建用户或组”页面的初始面板

## 8.3 创建组

- 在 *身份自助服务* 选项卡上，单击菜单中的 *创建用户或组*（如果已显示 *目录管理*，则在其下方）。

将显示 *选择要创建的对象* 面板。

- 使用 *对象类型* 下拉列表选择 *组*，然后单击 *继续*。

将显示 *设置该组的属性* 面板：

- 指定以下必需属性的值：

属性	指定的内容
组 ID	该新组的组名。
容器	<p>需要在其中储存新组的身份库中的组织单元（例如名称为 groups 的组织单元）。例如：</p> <pre>ou=groups,ou=MyUnit,o=MyOrg</pre> <p>要了解如何使用为指定容器而提供的按钮，请参见第 8.2 节“创建用户”（第 89 页）。</p> <hr/> <p><b>注释：</b>如果系统管理员已经为此类型的对象建立了默认的建立容器，则系统不会提示您提供容器。</p>
说明	该新组的说明。

#### 4 单击继续。

至此已创建组，随后将显示用于汇总结果的 *审阅* 面板：



*审阅* 面板提供了一组便利的可选链接。

- 单击新组的名称，以显示列出该组细节的“配置文件”页面  
您可以从“配置文件”页面编辑该组的细节，进行更改或删除该组。
- 单击 *创建另一个* 返回到“创建用户或组”页面的初始面板

## 8.4 使用编辑按钮

表 8-1 列出了您可以用于指定属性值的编辑按钮。

表 8-1 用于指定用户和组的编辑按钮

按钮	作用
	查找需要在某个项中使用的值
	显示项中使用的值的 <i>历史</i> 列表
	重设置所选项的值
	添加新项。您可以添加多个项。
	指示存在多个项。
	删除选定项及其值

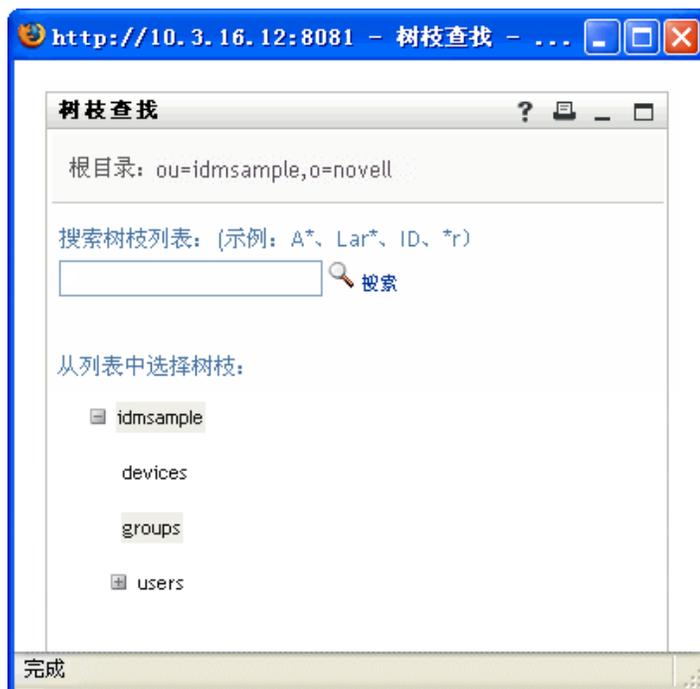
**重要：**可使用身份自助服务选项卡的“编辑用户”页面，解除分层报告结构。例如，您可以向管理员添加直接报告（即使直接报告具有指派的另一个经理），也可以让经理向他/她组织中的某个人报告。

## 8.4.1 要查找容器，请执行下列操作：

- 1 单击要查找容器的某个项右侧的 *查找*：

■

“查找”页面将显示容器树：



可以展开或折叠该树中的节点（通过单击 + 或 - 按钮），以查找所需的容器。

- 2 必要时针对所需的容器指定搜索准则。

在文本框中键入要搜索的完整或部分容器名称。搜索将查找以键入的文本开头的所有容器名称。该操作不区分大小写。也可以根据需要在文本中使用星号 (\*) 作为通配符，以代表零个或多个任意字符。

例如，以下所有示例都将查找名称为 users 的容器：

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

- 3 单击 *搜索*。

“查找”页面将显示搜索结果：



4 从树中选择所需的容器。

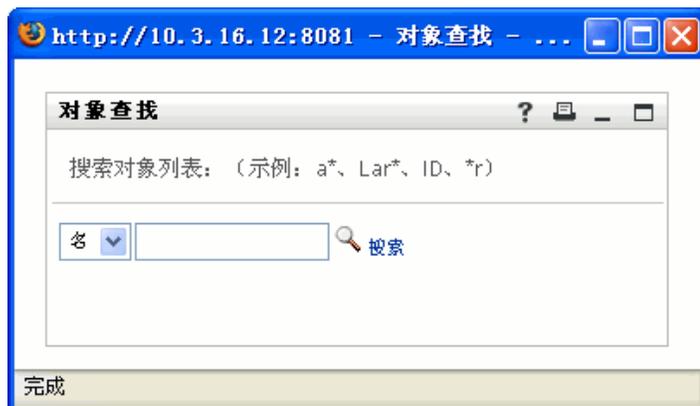
“查找”页面将会关闭，同时将该容器的名称插入到相应项中。

## 8.4.2 要查找用户，请执行下列操作：

1 在要查找其用户的项右侧，单击 *查找*：



将显示“查找”页面：



2 针对需要查找的用户指定搜索准则：

**2a** 用下拉列表按 *名字*或*姓氏*选择搜索。

**2b** 在下拉列表旁边的文本框中，键入要搜索的完整或部分姓名。

搜索将查找以键入的文本开头的所有姓名。该操作不区分大小写。也可以在文本中使用星号(\*)作为通配符，以代表零个或多个任意字符。

例如，以下所有示例都将查找名字 Chip：

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

经理查找只会搜索身份为经理的用户。

### 3 单击 *搜索*。

“查找”页面将显示搜索结果：



如果看到包含所需用户的用户列表，请转至 **步骤 4**。否则，请返回到 **步骤 2**。

单击列标题可按升序或降序对搜索结果排序。

### 4 从列表中选择所需的用户。

“查找”页面将会关闭，同时将该用户的姓名插入到相应项中。

## 8.4.3 要使用“历史”列表，请执行下列操作：

### 1 单击某个项（要查看该项以前的值）右侧的 *历史*：

而

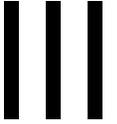
将显示 *历史* 列表，其中的值以字母顺序排列：



## 2 执行以下步骤之一：

如果要	操作
从 <i>历史</i> 列表中做出选择	从列表中选择所需的值。 <i>历史</i> 列表将会关闭，同时将该值插入到相应项中。
清除 <i>历史</i> 列表	单击 <i>清除历史</i> 。 <i>历史</i> 列表将会关闭，同时删除该项的历史值。清除 <i>历史</i> 列表不会更改项的当前值。

# 使用请求和批准选项卡



以下部分说明如何使用 Identity Manager User Application 的 *请求和批准* 选项卡。

- ◆ 第 9 章“请求和批准选项卡介绍”（第 99 页）
- ◆ 第 10 章“管理您的工作”（第 107 页）
- ◆ 第 11 章“配置供应设置”（第 125 页）
- ◆ 第 12 章“管理您的小组工作”（第 137 页）
- ◆ 第 13 章“配置小组供应设置”（第 161 页）



# 请求和批准选项卡介绍

本部分概述 *请求和批准* 选项卡。包括以下主题：

- ◆ 第 9.1 节“关于“请求和批准”选项卡”（第 99 页）
- ◆ 第 9.2 节“访问“请求和批准”选项卡”（第 99 页）
- ◆ 第 9.3 节“浏览选项卡的功能”（第 100 页）
- ◆ 第 9.4 节“可以执行的“请求和批准”操作”（第 101 页）
- ◆ 第 9.5 节“了解请求和批准图例”（第 103 页）

有关访问和操作 Identity Manager 用户界面的更多一般信息，请参见第 1 章“入门”（第 15 页）。

## 9.1 关于“请求和批准”选项卡

*请求和批准* 选项卡用于使您方便地执行基于工作流程的供应操作。可通过这些操作管理对组织中安全资源的用户访问。这些资源可以包含诸如用户帐户、计算机和数据库之类的数字实体。例如，可以使用 *请求和批准* 选项卡执行以下操作：

- ◆ 发出供应请求
- ◆ 管理供应工作（与资源请求以及角色和证明请求相关联的工作流程任务）
- ◆ 配置您自己或小组的供应设置

供应请求需要从组织中的一个或多个人中获得许可权限时，此请求将启动工作流程。工作流程可协调完成请求所需的批准。有些请求需要一个人批准，而另一些请求则需要多个人批准。在某些实例中，可以不经任何批准完成请求。

初始化供应请求时，供应系统将跟踪发起人和收件人。发起人是指发出请求的用户。收件人是请求的接收用户。

工作流程设计者和系统管理员负责为您以及组织中的其他用户设置 *请求和批准* 选项卡的内容。供应工作流程的控制流程以及表单外观可能随 Designer for Identity Manager 中供应请求定义的不同而不同。此外，可以查看的内容以及可以执行的操作通常由您的工作要求和权限级别确定。

有关自定义供应工作流程设计的细节，请参见《*Identity Manager User Application: 设计指南* (<http://www.novell.com/documentation/idmrbpm361/index.html>)》。有关工作流程管理的细节，请参见《*Identity Manager User Application: 管理指南* (<http://www.novell.com/documentation/idmrbpm361/index.html>)》。

## 9.2 访问“请求和批准”选项卡

默认情况下，登录 Identity Manager 用户界面后，*请求和批准* 选项卡将会打开，并显示“我的任务”页面：



如果要在转至 Identity Manager 用户界面中的另一选项卡后返回，则只需单击 *请求和批准* 选项卡再次将其打开。

### 9.3 浏览选项卡的功能

本节介绍 *请求和批准* 选项卡的默认功能。（选项卡的外观可能由于针对您组织所作的自定义而不同；请咨询系统管理员或工作流程设计者。）

*请求和批准* 选项卡的左侧显示可以执行的操作的菜单。这些操作按类别（*我的工作*、*我的设置*、*我的小组的工作*和*我的小组的设置*）列出：



仅当您是小组经理时，才会显示 *我的小组的工作* 和 *我的小组的设置* 操作。

单击一项操作时，其右侧会显示相应的页面。该页面通常包含一个窗口，其中显示该操作的细节。例如，该窗口可能会显示一个可以在其中输入数据或进行选择的列表或表格，如下图所示：

图 9-1 为某操作显示的页面



在 *请求和批准* 选项卡中操作的大多数页面的右上角都包含一个按钮，可以使用该按钮显示 *请求和批准* 图例：



有关 *请求和批准* 图例的细节，请参见第 9.5 节“了解请求和批准图例”（第 103 页）。

## 9.4 可以执行的“请求和批准”操作

下面是默认情况下可以在 *请求和批准* 选项卡中使用的操作的摘要：

表 9-1 “请求和批准”操作

类别	操作	说明
我的工作	我的任务	<p>显示工作流程队列中当前指派给您的批准任务。这些任务可能与资源请求相关联，也可能与角色和证明请求相关联。</p> <p>如果某任务需要数字签名，“我的任务”操作将提供根据数字签名批准或不批准任务的途径。</p> <hr/> <p><b>警告：</b>必须使用 Novell Audit（或 Sentinel）保留数字签名的文档。数字签名文档不是随工作流程数据储存在 User Application 数据库中，而是储存在日志记录数据库中。必须启用日志记录，才能保留这些文档。</p> <hr/> <p>如果将某任务指派给多个接收人，“我的任务”操作将提供查看该任务批准要求以及接收人列表、批准状态的途径。</p> <p>有关细节，请参见第 10 章“管理您的工作”（第 107 页）。</p>
	请求资源	<p>用于发出资源请求。</p> <p>如果某资源要求数字签名，“请求资源”操作提供将数字签名与请求关联的途径。</p> <p>有关细节，请参见第 10 章“管理您的工作”（第 107 页）。</p>
	我的请求	<p>显示由您发出或向您发出的请求的状态。因此请求列表包含您发出的请求，或者以您为接收者并授予接收者查看特权的请求。</p> <p>有关细节，请参见第 10 章“管理您的工作”（第 107 页）。</p>
我的设置	进入代理方式	<p>使您担当另一用户的代理。</p> <p>有关细节，请参见第 11 章“配置供应设置”（第 125 页）。</p>
	编辑可用性	<p>允许您指定您可以处理哪些请求，以及您指派的委托可以处理哪些请求。</p> <p>有关细节，请参见第 11 章“配置供应设置”（第 125 页）。</p>
	我的代理指派	<p>用于查看或编辑代理指派。要编辑代理指派，您必须具有必需的授权。</p> <p>有关细节，请参见第 11 章“配置供应设置”（第 125 页）。</p>
	我的委托指派	<p>用于查看或编辑委托指派。要编辑委托指派，您必须具有必需的授权。</p> <p>有关细节，请参见第 11 章“配置供应设置”（第 125 页）。</p>

类别	操作	说明
我的小组的工作	小组任务	<p>显示向小组成员指派的批准任务。</p> <p>根据为小组定义的权限，该操作也可以让您声明和 / 或重指派任务。</p> <p>如果某任务需要数字签名，“小组任务”操作将提供根据数字签名批准或不批准任务的途径。</p> <p>如果某任务指派给了多个接收人，“小组任务”操作将提供查看该任务批准要求以及接收人列表的途径。</p> <p>有关细节，请参见第 12 章“管理您的小组工作”（第 137 页）。</p>
	请求小组资源	<p>用于向小组成员发出资源请求。</p> <p>如果某资源要求数字签名，“请求小组资源”操作提供将数字签名与请求关联的途径。</p> <p>有关细节，请参见第 12 章“管理您的小组工作”（第 137 页）。</p>
	小组请求	<p>显示由小组成员发出的或向小组成员发出的请求的状态。</p> <p>有关细节，请参见第 12 章“管理您的小组工作”（第 137 页）。</p>
我的小组的设置	小组代理指派	<p>用于为小组成员指定代理指派。</p> <p>该功能必须在小组定义中启用。该功能禁用时，不允许该操作。</p> <p>有关细节，请参见第 13 章“配置小组供应设置”（第 161 页）。</p>
	小组委托指派	<p>用于为小组成员指定委托指派。</p> <p>该功能必须在小组权限定义中启用。如果小组权限允许经理让某小组成员委托代理其他小组成员的供应请求，就允许对这些请求执行该操作。该功能在小组权限定义中禁用时，不允许该操作。</p> <p>有关细节，请参见第 13 章“配置小组供应设置”（第 161 页）。</p>
	小组可用性	<p>允许您指定小组成员及其委托可以处理哪些请求。</p> <p>该功能必须在小组定义中启用。该功能禁用时，不允许该操作。</p> <p>有关细节，请参见第 13 章“配置小组供应设置”（第 161 页）。</p>

## 9.5 了解请求和批准图例

在 *请求和批准* 选项卡中操作的大多数页面的右上角都包含一个按钮，可以使用该按钮显示 *请求和批准* 图例。要显示图例，请单击图 9-2 中显示的“图例”按钮。

图 9-2 “图例”按钮



图例可简要说明整个请求和批准选项卡中使用的图标。图 9-3 在第 104 页显示该图例。

图 9-3 “请求和批准”图例



下表详细说明图例中的图标:

表 9-2 “图例”图标

图标	说明
已声明	表示特定的工作流程任务是否已被某个用户声明。 在“我的任务”页面上显示。
正在运行: 处理中	表示特定的请求仍在处理中。 在“我的请求”和“小组请求”页面上显示。
已完成: 已批准	表示已完成处理且已批准特定的请求。 在“我的请求”和“小组请求”页面上显示。
已完成: 已拒绝	表示已完成处理且已拒绝特定的请求。 在“我的请求”和“小组请求”页面上显示。
已终止: 已取消	表示某个用户（提交请求的用户、小组管理者或供应应用程序管理员）已收回特定的请求。 在“我的请求”和“小组请求”页面上显示。
已终止: 错误	表示特定的请求由于出错而终止。 在“我的请求”和“小组请求”页面上显示。
编辑	用于编辑代理指派或委托指派。要编辑指派，请选择它并单击编辑图标。 在“我的代理指派”、“我的委托指派”、“小组代理指派”、“小组委托指派”、“编辑可用性”和“小组可用性”页面上显示。

图标	说明
删除	<p>用于删除代理指派或委托指派。要删除指派，请选择它并单击<i>删除</i>图标。</p> <p>在“我的代理指派”、“我的委托指派”、“小组代理指派”、“小组委托指派”、“编辑可用性”和“小组可用性”页面上显示。</p>
允许多个收件人	<p>表示该资源可为多个收件人提供支持。如果资源支持多个收件人，则可以使用<i>请求小组资源</i>操作将多个用户选择为收件人。</p> <p>在“请求小组资源”页面上显示。</p>
指派给委托	<p>表示另一用户委托了特定的工作流程任务。由于原始受托人声明不在位，因此该任务将显示在当前用户的队列中。由于当前用户是原始受托人的委托，因此该用户可以看到该任务。</p> <p>在“我的任务”和“小组任务”页面上显示。</p>
指派给用户	<p>表示已将特定的工作流程任务指派给了某个用户。</p> <p>在“我的任务”和“小组任务”页面上显示。</p>
指派给组	<p>表示已将特定的工作流程任务指派给了某个组。</p> <p>在“我的任务”和“小组任务”页面上显示。</p>
已指派给角色	<p>表示已将特定的工作流程任务指派给某个角色。</p> <p>在“我的任务”和“小组任务”页面上显示。</p>
指派给多个批准者	<p>表示已将特定的工作流程任务指派给了多个用户。</p> <p>在以下情况下会应用该图标：</p> <ul style="list-style-type: none"> <li>◆ 该任务已指派给一组接收人，但只有一个接收人可以声明并批准任务。批准后，就认为任务已完成执行。</li> <li>◆ 该任务已指派给多个接收人，他们都必须声明并批准任务，才能认为活动已完成。</li> <li>◆ 该任务已指派给多个接收人，选定数量的用户都必须声明并批准任务，才能认为活动已完成。选定用户数的定义由管理员配置。要定义选定用户数，管理员将指定批准条件，该条件指定批准的精确数量或需要批准的百分比。</li> </ul> <p>在“我的任务”和“小组任务”页面上显示。</p>
可用于所有请求	<p>表示特定的用户可用于所有类型的请求。该设置适用于委托。</p> <p>在“编辑可用性”和“小组可用性”页面上显示。</p>
不可用于指定的请求	<p>表示在特定的时段内，特定的用户对某些类型的请求不可用。该设置适用于委托。在特定用户不可用于这些请求的时间段内，受委托处理这些请求的用户可以对其进行处理。</p> <p>在“编辑可用性”和“小组可用性”页面上显示。</p>
不可用于任何请求	<p>表示特定的用户对当前系统中的所有请求都不可用。该设置适用于委托。在特定用户不可用于某个请求的时间段内，受委托处理该请求的用户可以对其进行处理。</p> <p>在“编辑可用性”和“小组可用性”页面上显示。</p>



# 管理您的工作

本部分提供与管理供应工作有关的指导。包括以下主题：

- ◆ 第 10.1 节“关于“我的工作”操作”（第 107 页）
- ◆ 第 10.2 节“管理您的任务”（第 107 页）
- ◆ 第 10.3 节“请求资源”（第 116 页）
- ◆ 第 10.4 节“检查请求的状态”（第 121 页）

## 10.1 关于“我的工作”操作

Identity Manager User Application 中的 *请求和批准* 选项卡包括一组称为 *我的工作* 的操作。使用 *我的工作* 操作可以发出资源请求、检查所发出请求的状态，以及执行指派给您或您所属组的任务。这些任务可能与资源请求相关联，也可能与角色和证明请求相关联。

使用 *我的工作* 操作还能以另一用户的委托的身份执行任务。如果任务的原始受托人已声明不在位，并且已将您指派为委托，则委托的任务将显示在您的队列中。

---

**注释：** 供应工作流程的控制流程以及表单外观可能随 Designer for Identity Manager 中供应请求定义的不同而不同。有关自定义供应工作流程设计的细节，请参见《*Identity Manager User Application: 设计指南* (<http://www.novell.com/documentation/idmrbpm361/index.html>)》。

---

## 10.2 管理您的任务

使用 *我的任务* 操作，可以检查向您指派的的任务的工作流程队列。任务出现在队列中时，需要执行下列操作之一：

- ◆ 声明任务，以便可以开始处理该任务
- ◆ 将任务重指派给另一用户

---

**注释：** 必须具有相应的授权才能重指派任务。要重指派任务，您必须是在小组权限定义中被赋予此许可权限的供应应用程序管理员或小组经理。

---

使用 *我的任务* 操作，您可处理与资源请求、角色请求和证明请求相关联的工作流程任务。在有些情况下，用户界面可能根据您选择处理的工作流程任务类型而异。对于证明请求，*我的任务* 操作仅显示已将您指定为证明者的那些任务。

声明与某个资源请求或角色请求相关联的任务时，您可以采取将工作项转发给工作流程中的下一个活动的操作。您可执行的操作如下所述：

**表 10-1** 转发操作

“转发”操作	说明
批准	用于批准任务。批准任务时，工作项目将转发到工作流程中的下一活动。

“转发”操作	说明
拒绝	用于明确拒绝对任务的批准。拒绝任务时，工作项目将转发到工作流程中的下一活动，同时将拒绝请求。通常，拒绝请求后，工作流程进程将会终止。
拒收	可用于明确拒收任务。拒收任务后，该工作项目将转发到工作流程中被拒收操作的下一个活动。

声明与某个证明请求相关联的任务时，您需要审阅证明表单中显示的信息。此外，您还需要回答必需的证明问题，这些证明问题指示您是否证明数据的正确性，而且在某些情况下，需要响应一个或多个调查问题。对于用户简介证明流程，表单包括您的用户属性数据（您需要校验其是否准确）。对于角色指派、用户指派和 SoD 证明流程，表单包括显示您需要校验的角色指派、用户指派或 SoD 数据的报告。

## 10.2.1 查看任务

要查看向您指派的任务，请执行下列操作：

- 1 在*我的工作*操作组中单击*我的任务*。

将显示队列中的任务列表。



对于资源和角色请求，任务列表中的*收件人*列指定（在获得所需批准的情况下）将接收资源或角色的用户或组。对于证明请求，*收件人*列指定证明者的姓名（与当前登录到 User Application 的人员姓名相同）。

任务列表中的*类型*列包括表示该任务当前是指派给用户、组、委托还是多个批准者的图标。类型*指派给多个批准者*适用于以下情形：

- ◆ 该任务已指派给一组接收人，但只有一个接收人可以声明并批准任务。批准后，就认为任务已完成执行。
- ◆ 该任务已指派给多个接收人，他们都必须声明并批准任务，才能认为活动已完成。
- ◆ 该任务已指派给多个接收人，选定数量的用户都必须声明并批准任务，才能认为活动已完成。选定用户数的定义由管理员配置。要定义选定用户数，管理员将指定批准条件，该条件指定批准的精确数量或需要批准的百分比。

工作流程系统将执行*短路评估*，以优化选定用户数。每当选定用户数批准条件达到无法满足最低选定用户数的临界点时，活动将被拒绝，任务将从所有接收人的队列中去除。

*优先级*列显示高优先级任务的标志。您可以通过单击*优先级*列，按优先级排列任务列表。

与证明请求相关联的工作流程任务显示任务名称*证明批准*，如下所示：

图 10-1 证明请求的工作流程任务

任务	请求	收件人	类型	已声明	超时	优先级
证明批准	用户配置文件 - 默认值 (2008/06/13)	main administrator			6天 19小时 55分钟	
证明批准	用户指派 - 默认值 (2008/06/13)	main administrator			从不	
证明批准	角色指派 - 默认值 (2008/06/13)	main administrator			从不	
批准角色请求 (序列)	角色批准 - Conflict1	main administrator			从不	

1 - 4 / 4

刷新

## 10.2.2 选择任务

要选择队列列表中的任务，请执行下列操作：

- 1 单击队列中任务的名称。



将显示“任务细节”表格。



将一项任务指派给多个批准者时，“任务细节”表格将显示多个批准者图标（在指派至字段旁），并在该图标下显示文字，表示需要多个批准者。



2 要显示关于指派给多个批准者的任务的更多信息，请单击 *多个批准者* 图标下的文字：



将显示弹出窗口，它会指出需要的批准数量，当前接收人以及当前的批准状态。



任务的要求取决于您的管理员如何配置任务：

- 如果您的批准类型是 *组*，则任务已指派给组内若干用户，但只应有一个用户声明并批准任务。
- 如果您的批准类型是 *角色*，则该任务已指派给角色内若干用户，但只应有一个用户声明并批准该任务。
- 如果批准类型是 *多个批准者*，则该任务已指派给若干接收人，所有接收人都必须声明并批准任务。
- 如果批准类型是 *选定用户数*，则该任务已指派给若干接收人，选定数量的接收人就足以批准任务。选定用户数的定义由管理员配置。要定义选定用户数，管理员将指定批准条件，该条件指定批准的精确数量或需要批准的百分比。

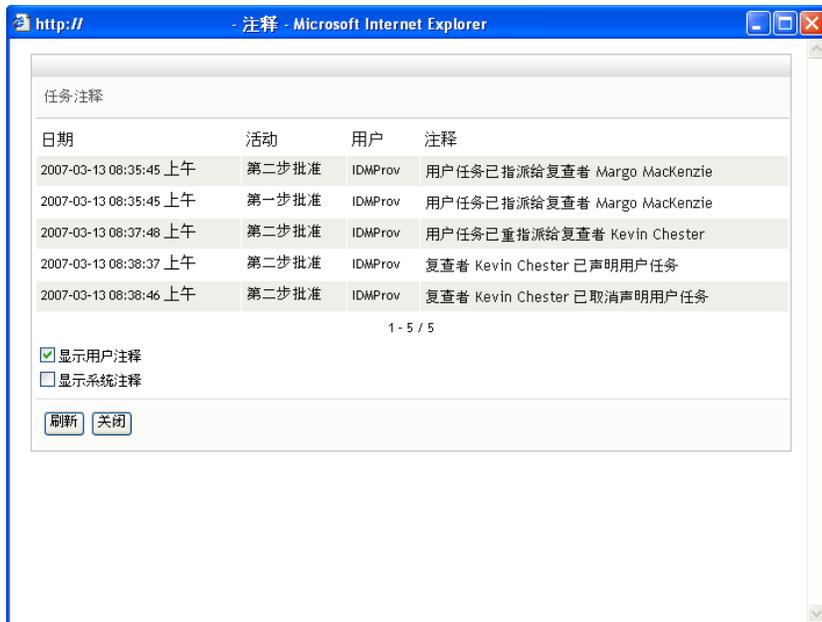
工作流程系统将执行 *短路评估*，以优化选定用户数。每当选定用户批准条件达到无法满足最低选定用户数的临界点时，活动将被拒绝，任务将从所有接收人的队列中去除。

3 要声明一个任务，请遵循第 10.2.3 节“*声明任务*”（第 112 页）中的指导。

4 要查看该任务的注释历史，请单击 *查看注释历史*。

可在弹出窗口中查看用户和系统注释。注释显示的顺序由和每条注释关联的时戳决定。先输入的注释先显示。对于并行批准流程，并行处理的活动顺序可能是不可预测的。

4a 要显示用户注释，请单击 *显示用户注释*。



用户注释包含以下类型的信息：

- ◆ 添加每条注释的日期和时间。
- ◆ 应用每条注释的活动名称。显示的活动列表包含已处理或当前正在处理的用户和供应活动。
- ◆ 作出注释的用户名称。如果注释由工作流程系统生成，应用程序的名称（例如 IDMProv）就是用户名。工作流程系统生成的注释会被自动本地化。
- ◆ 注释文本，包含作为每个活动当前受托人的用户的名称。

工作流程设计者可以禁止某个工作流程生成用户注释。有关更多信息，请参见《*Identity Manager User Application: 设计指南* (<http://www.novell.com/documentation/idmrbpm361/index.html>)》。

**4b** 要显示系统注释，请单击 *显示系统注释*。



系统注释包含以下类型的信息：

- ◆ 添加每条注释的日期和时间。
- ◆ 应用每条注释的活动的名称。显示系统注释时，将列出工作流程中的所有活动。活动列表包含已处理或当前正在处理的活动。
- ◆ 作出注释的用户名称。如果注释由工作流程系统生成，应用程序的名称（例如 IDMProv）就是用户名。工作流程系统生成的注释将被自动本地化。
- ◆ 注释文本，表示对该活动采用的操作。

系统注释主要用于调试。多数业务用户无需查看工作流程的系统注释。

- 4c** 要在很长的注释列表中滚动，请单击屏幕底部的箭头。例如，要滚动到下一页，请单击 *下一页* 箭头。



- 4d** 单击 *关闭* 可关闭此窗口。

- 5** 要返回到任务列表，请单击 *后退*。

### 10.2.3 声明任务

要声明一个待处理的任務，請執行下列操作：

- 1** 单击 *声明*。

**小组任务**

任务细节

\* - 表示必需。

---

资源: Provisioning Request 收件人: Kevin Chester  
 请求者: Margo MacKenzie 任务: 第一步批准  
 进入队列的时间: 2007-03-15 06:05:55 上午 超时: 2007-03-17 06:05:55 上午  
 指派给: Margo MacKenzie 声明者:

表格细节

**第一步批准**

请选择相应的按钮以批准或拒绝请求。

请求人: Margo MacKenzie 收件人: Kevin Chester  
 请求日期: 2007-03-15  
 原因:   
 注释:

对于资源请求和角色请求，本页面的**表单细节**部分将更新，以包含**拒绝**和**批准**按钮，以及流程定义包含的其他操作按钮，相应字段将变为可编辑的。

对于证明请求，本页面的**表单细节**部分将更新为包含证明表单。表单的外观因证明类型而异。对于用户简介证明流程，表单显示您需要审阅的用户简介数据：

表格细节

**属性列表**

名:	main
姓:	administrator
职务:	
电话号码:	

转到您的配置文件

---

**证明问题**

要证明您已查看过用户配置文件上的细节并根据需要进行更新吗？ \*

注释:

对于角色指派、用户指派和 SoD 证明流程，该表单包含显示您需要审阅的数据的报告：

证明表单细节	
报告:	角色指派证明报告
报告日期:	2008年6月13日 下午2:30
<b>业务角色 (总计: 1)</b>	
角色名称:	Conflict1 (业务角色)
容器:	Conflict1.Level30.RoleDefs
角色类别:	
说明:	Conflict1
此角色的指派	批准者 main administrator (已批准, 08-6-13 下午2:27)
<b>IT 角色 (总计: 2)</b>	
角色名称:	合规性模块管理员 (IT 角色)
容器:	合规性模块管理员.Level20.RoleDefs
角色类别:	系统角色
说明:	合规性管理员
此角色的指派	批准者 main administrator (用户)
角色名称:	角色模块管理员 (IT 角色)
容器:	角色模块管理员.Level20.RoleDefs
角色类别:	系统角色
说明:	角色模块管理员
此角色的指派	批准者 main administrator (用户)

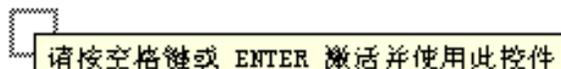
对于所有证明类型，表单显示一些控件，允许您回答必需的证明问题以及证明流程中包含的其他调查问题：

<b>调查问题</b>	
Test	注释: <input type="text"/>
<b>证明问题</b>	
是否证明该角色指派报告中的角色指派是有效且恰当的? *	注释: <input type="text"/>
<input type="button" value="提交证明"/>	

如果是资源请求，并且任务要求数字签名，将在页面右上角显示 *需要数字签名* 图标。



此外，在 Internet Explorer 上将显示讯息，表示您必须按空格键或 Enter 键激活数字签名小程序。



- 2 如果您要处理需要数字签名的任务，请执行以下步骤：
  - 2a 如果您使用智能卡，请将智能卡插入智能卡读卡器。
  - 2b 在 Internet Explorer 上，按空格键或 Enter 键激活小程序。  
此时您的浏览器可能会显示安全警告讯息。



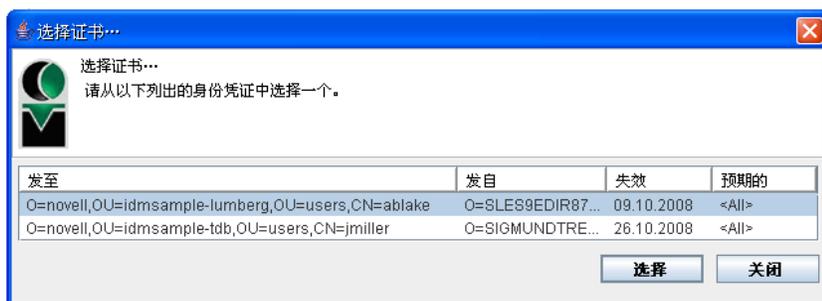
2c 单击 *运行* 继续。

2d 填充批准表格中的字段。表格中的字段可能随请求资源的不同而不同。

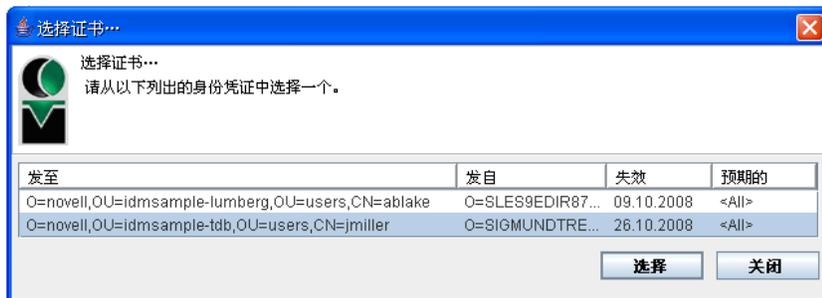
2e 单击数字签名确认讯息旁的复选框，表示您即将签名。

数字签名确认讯息可能随管理员配置供应资源方式的不同而不同。

小程序随即显示弹出窗口，您可以通过它选择证书。弹出窗口将列出导入浏览器的证书及导入智能卡的证书（如果当前已连接智能卡）。



2f 选择要使用的证书并单击 *选择*。



2g 如果选择已导入浏览器的证书，则在请求表单的 *口令* 字段键入证书口令。

2h 如果选择已导入智能卡的证书，请键入您的智能卡的 PIN，并单击 *确定*。

如果您使用智能卡，则无需键入证书口令，因为证书口令已传送到智能卡。



如果您的管理员启用了预览用户协议功能，则将启用 *预览* 按钮。

2i 单击 *预览* 查看用户协议。

如果数字签名类型设置为“表格”，则将显示 PDF 文档。

如果数字签名类型设置为数据，则将显示 XML 文档。

3 要拒绝资源或角色请求，请单击 *拒绝*。



4 要批准资源或角色请求，请单击 *批准*。



User Application 将显示一条讯息，指示操作是否成功。

## 10.3 请求资源

可使用 *请求资源* 操作发出资源请求。启动请求时，User Application 将显示初始请求表单。可使用该表单指定请求所需的所有信息。

**注释：**请求资源操作不允许您请求角色指派或启动证明请求。要请求角色指派，您需要使用角色选项卡上的角色指派操作。要启动证明请求，您需要使用合规性选项卡上证明请求下列出的任何操作。

提交资源请求时，该请求将启动工作流程。工作流程可协调完成请求所需的批准。有些资源请求需要一个人批准，而另一些请求则需要多个人批准。在某些实例中，可以不经任何批准完成请求。

要请求资源，请执行下列操作：

- 1 在我的工作操作组中单击请求资源。  
将显示“请求资源”页面。



- 2 在请求类型下拉列表中选择请求的类别。选择全部以包含来自所有可用类别的请求。
- 3 单击继续。  
“请求资源”页将显示当前用户可用的资源的列表。

User Application 将实施安全限制，以确保您只能看到有权访问的那些请求类型。

- 4 通过单击资源名称选择所需的资源。



“请求资源”页面显示初始请求表格。



如果您请求的资源要求数字签名，该页面右上角将显示 **要求数字签名** 图标。此外，在 Internet Explorer 上将显示讯息，表示您必须按空格键或 Enter 键激活数字签名小程序。

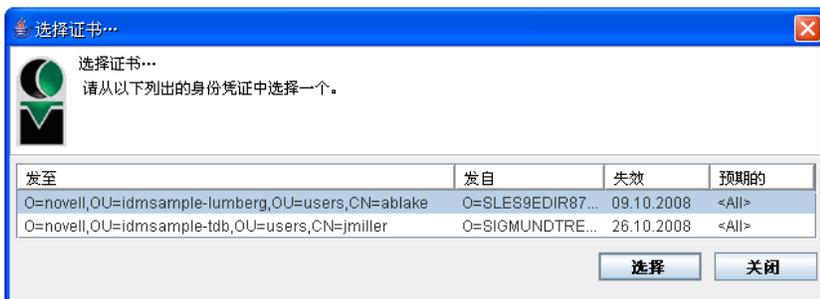


5 如果您的请求需要数字签名，请执行以下步骤：

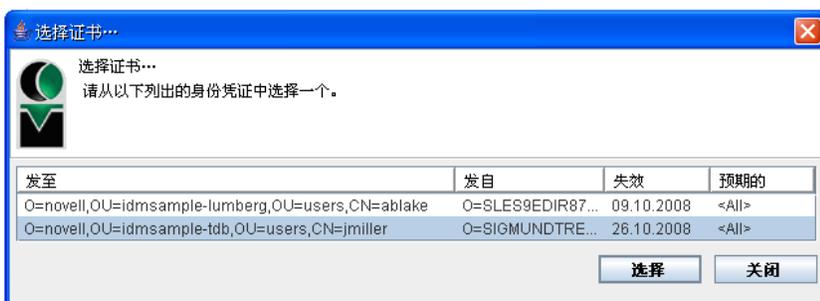
- 5a 如果您使用智能卡，请将智能卡插入智能卡读卡器。
- 5b 在 Internet Explorer 上，按空格键或 Enter 键激活小程序。  
此时您的浏览器可能会显示安全警告讯息。



- 5c 单击 **运行** 继续。
- 5d 填写初始请求表格中的字段。表格中的字段可能随请求资源的不同而不同。
- 5e 单击数字签名确认讯息旁的复选框，表示您即将签名。  
数字签名确认讯息可能随管理员配置供应资源方式的不同而不同。  
小程序随即显示弹出窗口，您可以通过它选择证书。弹出窗口将列出导入浏览器的证书及导入智能卡的证书（如果当前已连接智能卡）。



5f 选择您要用的证书并单击 *选择*。



5g 如果选择已导入浏览器中的证书，则需要在请求表格的 *口令* 字段键入证书口令。

5h 如果选择已导入智能卡的证书，请键入您的智能卡的 PIN，并单击 *确定*。

如果您使用智能卡，则无需键入证书口令，因为证书口令已传送到智能卡。

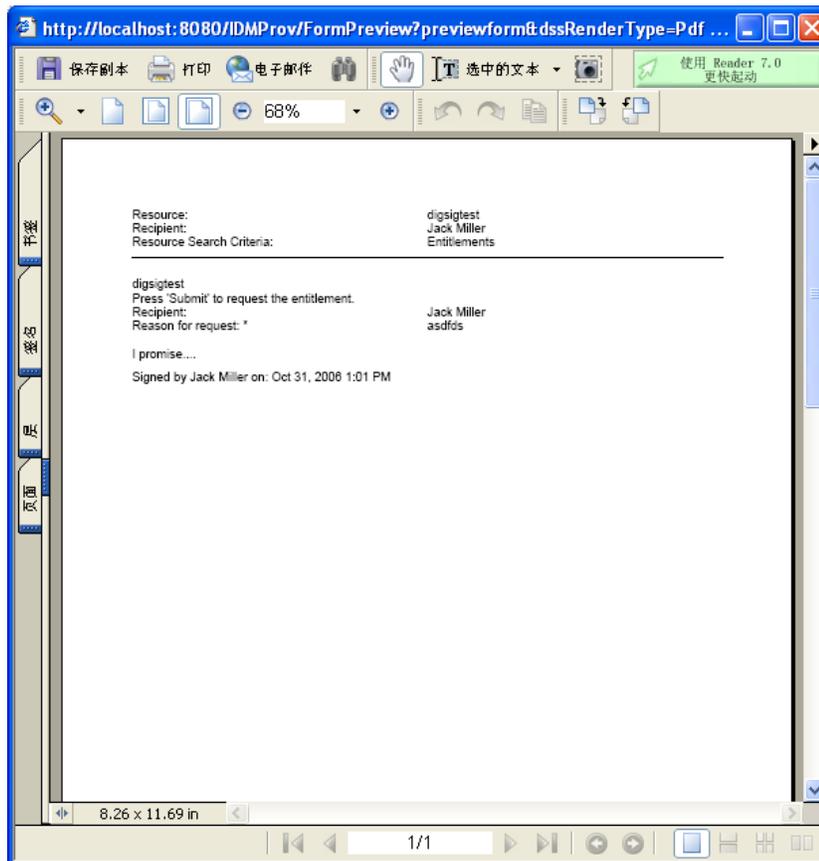


如果您的管理员启用了预览用户协议功能，将启用 *预览* 按钮。



5i 单击 *预览* 按钮查看用户协议。

如果数字签名类型设置为“表格”，将显示 PDF 文档。



如果数字签名类型设置为数据，将显示 XML 文档。



6 如果您的请求无需数字签名，则只需填充初始请求表格中的字段。表格中的字段根据请求资源的不同而不同。

7 单击提交。

“请求资源”页面将显示状态讯息，指明是否已成功提交请求。



## 10.4 检查请求的状态

使用我的请求操作，您可查看发出的请求的状态。可通过该操作查看每个请求的历史和当前状态。此外，如果您改变主意且不需要完成请求，则可通过该操作选择收回正在处理的请求。

**注释：**我的请求操作不显示角色或证明请求。要查看角色请求的状态，您需要使用角色选项卡上的查看请求状态操作。要查看证明请求的状态，您需要使用合规性选项卡上的查看证明请求状态操作。

要查看请求列表，请执行下列操作：

- 1 在我的工作操作组中单击我的请求。



- 2 在请求类型下拉列表中选择请求的类别。选择全部以包含来自所有可用类别的请求。
- 3 可通过选择在、早于或晚于并填充请求日期字段，按日期过滤请求列表。要包含选定类别的所有请求，请将请求日期字段保留为空白。
- 4 单击继续。

“请求资源”页面将显示您的请求。列表中包含活动的请求，以及已批准或拒绝的请求。管理员可控制保留工作流程结果的时间长度。默认情况下，工作流程系统保留工作流程结果 120 天。
- 5 要查看特定请求的细节，请单击名称来选择请求：



“我的请求”页将显示请求的启动时间、工作流程的当前状态等细节。

您可审阅状态以确定某个工作流程是仍在运行还是已遇到错误。例如，如果某个请求显示 *正在运行*：正在处理状态的时间段长得异常，则您可能希望联系管理员以确保不存在问题。

我的请求

请求细节

资源: QuorumApprover

收件人: Margo MacKenzie

活动状态: 正在处理

请求者: Margo MacKenzie

请求日期: 2007-03-14 08:49:08 上午

注释: [查看注释和流程历史](#)

[返回](#) [收回](#)

6 要收回请求，请单击 *收回*。

7 要查看请求的注释历史，请单击 *查看注释和流程历史*。

可通过弹出窗口查看用户和系统注释。注释显示的顺序由和每条注释关联的时戳决定。先输入的注释先显示。对于并行批准流程，并行处理的活动顺序可能是不可预测的。

7a 要显示用户注释，请单击 *显示用户注释*。

任务注释

日期	活动	用户	注释
2007-03-13 08:35:45 上午	第二步批准	IDMProv	用户任务已指派给复查者 Margo MacKenzie
2007-03-13 08:35:45 上午	第一步批准	IDMProv	用户任务已指派给复查者 Margo MacKenzie
2007-03-13 08:37:48 上午	第二步批准	IDMProv	用户任务已重指派给复查者 Kevin Chester
2007-03-13 08:38:37 上午	第二步批准	IDMProv	复查者 Kevin Chester 已声明用户任务
2007-03-13 08:38:46 上午	第二步批准	IDMProv	复查者 Kevin Chester 已取消声明用户任务

1 - 5 / 5

显示用户注释

显示系统注释

[刷新](#) [关闭](#)

用户注释包含以下类型的信息：

- ◆ 添加每条注释的日期和时间。
- ◆ 应用每条注释的活动名称。显示的活动列表包含已处理或当前正在处理的用户和供应活动。
- ◆ 作出注释的用户名称。如果注释由工作流程系统生成，应用程序的名称（例如 IDMProv）就是用户名。工作流程系统生成的注释会被自动本地化。
- ◆ 注释文本，包含作为每个活动当前受托人的用户的名称。

工作流程设计者可以禁止某个工作流程生成用户注释。有关更多信息，请参见《*Identity Manager User Application: 设计指南*》(<http://www.novell.com/documentation/idmr361/index.html>)。

**7b** 要显示系统注释，请单击 *显示系统注释*。



系统注释包含以下类型的信息：

- ◆ 添加每条注释的日期和时间。
- ◆ 应用每条注释的活动的名称。显示系统注释时，将列出工作流程中的所有活动。活动列表包含已处理或当前正在处理的活动。
- ◆ 作出注释的用户名称。如果注释由工作流程系统生成，应用程序的名称（例如 IDMProv）就是用户名。工作流程系统生成的注释将被自动本地化。
- ◆ 注释文本，表示对该活动采用的操作。

系统注释主要用于调试。多数业务用户无需查看工作流程的系统注释。

**7c** 要在很长的注释列表中滚动，请单击屏幕底部的箭头。例如，要滚动到下一页，请单击 *下一页* 箭头。



**7d** 单击 *关闭* 可关闭此窗口。

# 配置供应设置

本部分提供有关配置供应设置的指导。包括以下主题：

- ◆ 第 11.1 节“关于“我的设置”操作”（第 125 页）
- ◆ 第 11.2 节“担当代理”（第 126 页）
- ◆ 第 11.3 节“指定您的可用性”（第 127 页）
- ◆ 第 11.4 节“查看和编辑代理指派”（第 132 页）
- ◆ 第 11.5 节“查看和编辑委托指派”（第 133 页）

## 11.1 关于“我的设置”操作

Identity Manager User Application 中的 *请求和批准* 选项卡包含一组称为 *我的设置* 的操作。您可以通过 *我的设置* 操作成为另一用户的代理。此外，还可以使用这些操作查看代理指派和委托指派。如果您是小组管理者或供应应用程序管理员，您也可以定义代理指派、委托指派及小组可用性设置。

### 11.1.1 关于代理和委托

*委托*是指有权为另一用户执行工作的用户。委托指派适用于特定类型的请求。

*代理*是指有权为一个或多个用户、组或者容器执行任一和所有工作（以及定义供应设置）的用户。与委托指派不同，代理指派与资源请求无关，因此它适用于所有工作和设置操作。

**代理指派和委托指派具有时间段：**代理指派和委托指派都与时间段关联。代理指派或委托指派可以具有任意长短的时间段。时间段还可以没有失效日期。

**将会记录代理和委托操作：**如果启用了日志记录，则代理或委托执行的任何操作都将和其他用户执行的操作一起记录。代理或委托执行了某个操作后，日志讯息将明确指出该操作是由代理或委托为其他用户执行的。另外，每次定义一个新的代理指派或委托指派时，都会记录此事件。

**角色为批准者时的委托指派：**当工作流程批准者是角色时，User Application 不执行委托处理。角色中的任何用户都可执行指派给角色的批准，因此无需委托。

**角色为批准者时的代理指派：**进行代理指派时，User Application 将对已由用户持有的角色执行任何检查。有可能已将用户指派给与正在充当代理的人相同的所有角色。也有可能他们与将充当代理的人的角色存在冲突。

### 11.1.2 样本使用场景

本部分介绍两个可能会用到代理和委托的业务场景。

- ◆ 代理使用场景（第 126 页）
- ◆ 委托使用场景（第 126 页）

## 代理使用场景

假设您是一位经理，负责每天批准（或拒绝）大量的工作流程任务。此外，您还负责为组织中的众多用户编辑供应设置。在这种情况下，您可能需要指派一位代理，以便将您的一部分工作负荷转给小组中的受信任成员。

## 委托使用场景

假设您是一位经理，负责批准或拒绝对十种不同类型的提供资源的请求。所有十种请求类型都只需要常规受理，但您希望组织中有另一个人可以受理其中的六种。在这种情况下，可以为这六种资源请求类型指定一个委托。必要时，可以将此委托关系限制在几个小时、几天或几周的时段内。或者不为此委托关系指定时限，从而将此关系建立在更长久的安排之上。

## 11.2 担当代理

您可以通过 *进入代理方式* 操作担当另一用户的代理。

### 1 在我的设置操作组中单击 *进入代理方式*。

如果您有权担当其他至少一个用户的代理，则 User Application 将显示用户列表。



如果您无权担当其他任何用户的代理，则 User Application 将显示以下讯息：



### 2 选择要代理的用户，然后单击 *继续*。

如果您已被指定为某个组或容器的代理，则只有在选择该组或容器后才能选择用户。User Application 提供了一个下拉列表，使您能够选择组或容器。

User Application 将刷新显示，并使您返回到 *我的任务* 操作，即登录后的默认操作。任务列表将显示指派给你作为代理的用户的任务。*我的工作组* 上方（以及标题栏中）将显示一条讯息，指明现在您正担当另一用户的代理。



此时，您作为代理的用户可以执行的任何操作，您都可以执行。可用操作列表随您的权限和您作为代理的用户的权限而变化。

## 11.3 指定您的可用性

使用 *编辑可用性* 操作可以指定在指派委托的情况下，您在特定时间段内无法处理的那些请求。在您没空处理特定请求的时间段内，受委托的用户可处理该请求。

如果您不想单独地为每个请求定义指定可用性，则可以使用 *编辑可用性* 操作建立与委托有关的全局设置。

---

**提示：**在使用 *编辑可用性* 操作之前，至少需要有一个用于操作的委托指派。您必须让您的小组管理者（或供应应用程序管理员）为您创建委托指派。

---

- ◆ [第 11.3.1 节“设置可用性状态”](#)（第 127 页）
- ◆ [第 11.3.2 节“创建或编辑可用性设置”](#)（第 129 页）
- ◆ [第 11.3.3 节“删除可用性设置”](#)（第 131 页）

### 11.3.1 设置可用性状态

- 1 在 *我的设置* 操作组中单击 *编辑可用性*。

User Application 将显示“编辑可用性”页。如果当前没有任何可用性设置，则显示列表为空：



如果没有为您指派委托，User Application 将显示一条讯息，指示您不能在“编辑可用性”页上更改状态。

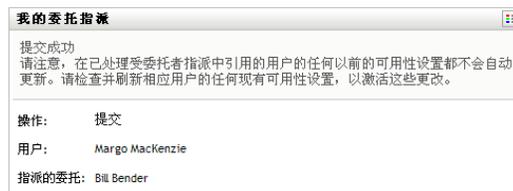
如果您有一个或多个可用性设置，显示列表将显示这些设置：



2 要查看和可用性指派关联的特定资源，请单击该资源的名称：



该页面随即显示弹出窗口，提供关于委托指派的信息：



在同一资源名称多次出现在可用性设置列表中的情况下，该信息特别有帮助。

3 通过在更改状态下拉列表中选择下列选项之一来指定状态：

状态	说明
可用于所有请求	<p>这是默认状态。它表示您全局可用。如果该状态有效，则向您指派请求不会被委托，即使已为您指派了委托，也是如此。</p> <p>使用 <i>可用于所有请求</i> 状态将覆盖其它设置。如果将状态更改为其它设置之一，然后又重新更改为 <i>可用于所有请求</i>，则会去除以前定义的任何 <i>选择性可用</i> 设置。</p>
不可用于任何请求	<p>指定您对当前系统中的任何请求定义全局地不可用。</p> <p>选择 <i>不可用于任何请求</i> 状态表示您不可用于现有的每个委托指派，并且会将当前状态更改为 <i>不可用于指定的请求</i>。这些指派可立即生效，并且在委托指派失效前保持有效。此设置不影响在此时间点后创建的新指派的可用性。</p>
不可用于指定的请求	<p>指定您不可用于特定的资源请求定义。在您没空处理特定请求的时间段内，受委托的用户可处理该请求。</p> <p>选择 <i>不可用于指定的请求</i> 后，您将进入“编辑可用性”页面。该操作相当于单击 <i>新建</i> 按钮。</p>

### 11.3.2 创建或编辑可用性设置

- 1 要创建新的可用性设置，请单击 *新建*（或者，在 *更改状态*”下拉列表中选择 *不可用于指定的请求*）。
- 2 要编辑现有设置，请单击要修改的设置旁边的 *编辑*：

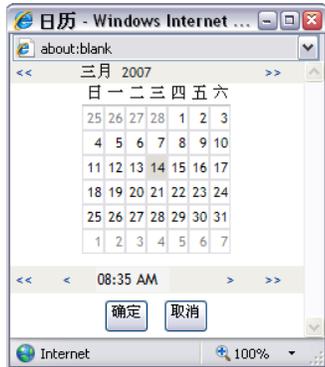


User Application 将显示一组控件，可使用这些控件指定您处于不可用状态的时间段，以及选择该设置适用的请求。

显示请求列表中只包含那些已指派委托的请求。

3 指定您处于不可用状态的时间段：

3a 指定该时间段的开始时间，方法是在“不可用的开始日期”框中键入开始日期和时间；或者单击日历按钮，然后选择日期和时间。



3b 通过单击下列按钮之一来指定该时间段的结束时间：

按钮	说明
持续时间	用于以周、天或小时为单位指定时间段。
结束日期	用于指定结束日期和时间。可以键入日期和时间；或者单击日历按钮，然后从日历中选择日期和时间。
不失效	表示该不可用性设置不会失效。

指定的结束日期必须在委托指派允许的时间段内。例如，如果委托指派在 2007 年 10 月 31 日失效，则不能对可用性设置指定失效日期 2007 年 11 月 15 日。如果您指定失效日期为 2007 年 11 月 15 日，则在 2007 年 10 月 31 日提交失效时会自动调整该日期。

4 通过填充以下字段，指定是否要向其他用户发送电子邮件通知：

字段	说明
将这些更改通知给其他用户	表示是否要发送电子邮件讯息，将该可用性指派通知给一个或多个用户。
接收人	指定应收到电子邮件通知的用户： <b>选定的：</b> 允许您向选择的任何用户发送电子邮件通知。

5 在请求类型列表选择一个或多个请求，然后单击添加。

在此页面上选择您不在位时不接受的请求类型。结果是将这些请求委托给其他用户。

**请求类型选择**  
选择您人不在时不接受的请求类型。只有带有委托指派请求的请求可用于下面的选择。

请求的类型:

digsigtest  
 Enable Active Directoy Account  
 Provisioning Request  
 Provisioning Request with digi signature  
 .....

在指定期间谢绝:\*

添加的每个请求将包含在在指定期间拒绝列表中。

**请求类型选择**  
选择您人不在时不接受的请求类型。只有带有委托指派请求的请求可用于下面的选择。

请求的类型:

digsigtest  
 Provisioning Request  
 Provisioning Request with digi signature  
 .....

在指定期间谢绝:\*

Enable Active Directoy Account  
 .....

- 6 要表示该可用性设置应用于所有请求类型，请单击*所有请求类型*，而不是分别选择请求类型。

**所有请求类型**

*所有请求类型*复选框仅当委托指派的请求类型设置为*全部*时才可用。

- 7 要从列表中去掉一个请求，请单击*去除*。
- 8 单击*提交*可提交更改。

### 11.3.3 删除可用性设置

要删除一个现有的可用性设置，请执行下列操作：

- 1 单击该设置旁的*去除*：



## 11.4 查看和编辑代理指派

可使用 *我的代理指派* 操作查看代理指派。如果您是供应应用程序管理员，也可以用此操作编辑代理指派。

只有供应应用程序管理员和小组管理者可以指派代理，如下所述：

- ◆ 供应应用程序管理员可以定义组织中任何用户的代理指派。
- ◆ 根据小组定义，小组管理者可能可以定义该小组中用户的代理设置。代理必须也在小组内。要定义代理，小组管理者必须使用 *小组代理指派* 操作。

如果小组管理者需要选择小组外的代理，他必须请求供应应用程序管理员定义代理关系。

### 11.4.1 显示代理设置

- 1 在 *我的设置* 操作组中单击 *我的代理指派*。

User Application 将显示当前设置。显示的代理指派包括将您指定为其他人的代理的指派，以及将其他人指定为您的代理的指派。

如果您不是供应应用程序管理员，您会看到代理指派视图是只读的：



如果您具有管理特权，则会为您提供可用于创建和编辑代理指派的按钮。

- 2 要刷新列表，请单击 *刷新*。

### 11.4.2 创建或编辑代理指派

- 1 要创建新的代理指派，请单击 *新建*。
- 2 要编辑一个现有的代理指派，请单击该指派旁边的 *编辑*：



如果您是供应应用程序管理员，则 User Application 将显示以下用于定义代理指派的界面：



- 3 如果您是供应应用程序管理员，请选择一个或多个要定义代理的用户、组和容器。使用 *对象选择器* 或 *显示历史* 工具选择用户、组或容器。
- 4 如果您是小组管理者，请选择一个或多个要定义代理的用户。
- 5 在 *指派的代理* 字段中指定要作为代理的用户。
- 6 通过单击下列单选按钮之一来指定该时间段的结束时间：

按钮	说明
不失效	表示该代理指派不会失效。
指定失效	用于指定结束日期和时间。可以键入日期和时间；或者单击日历按钮，然后从日历中选择日期和时间。

- 7 单击 *提交* 可提交更改。

### 11.4.3 删除代理指派

要删除一个现有的代理指派，请执行下列操作：

- 1 单击该指派旁的 *去除*：



## 11.5 查看和编辑委托指派

可使用 *我的委托指派* 操作查看委托指派。如果您是供应应用程序管理员，也可以用此操作编辑委托指派。

只有供应应用程序管理员和小组管理者可以指派委托，如下所述：

- ◆ 供应应用程序管理员可以定义组织中任何用户的委托指派。
- ◆ 根据小组权限的定义，小组管理者可能可以定义其小组中用户的委托设置。委托必须也在小组内。要定义委托，小组管理者必须使用 *小组委托指派* 操作。

如果小组管理者需要为不在其权限范围内的用户定义委托关系，则必须请求供应应用程序管理员定义委托关系。

**提示：**在使用 *编辑可用性* 操作之前，至少需要有一个用于操作的委托指派。

## 11.5.1 显示委托设置

- 1 在 *我的设置* 操作组中单击 *我的委托指派*。

User Application 将显示当前设置。

如果您不是供应应用程序管理员，则会看到委托指派视图是只读的：



如果您具有管理特权，则会为您提供可用于创建和编辑委托指派的按钮。



- 2 要刷新列表，请单击 *刷新*。

## 11.5.2 创建或编辑委托指派

- 1 要编辑一个现有的委托指派，请单击该指派旁边的 *编辑*：



或者，要创建新的委托指派，请单击 *新建*。

如果您是供应应用程序管理员，则 User Application 将显示以下用于定义委托指派的界面：



- 2 选择要定义委托的一个或多个用户、组和容器。  
使用对象选择器或显示历史工具选择用户、组或容器。
- 3 单击指派委托。在指派的委托字段中指定作为委托的用户。也可以单击按关系指派，然后在委托关系字段中选择关系。
- 4 通过单击下列按钮之一来指定该时间段的结束时间：

按钮	说明
不失效	表示该委托指派不会失效。
指定失效	用于指定结束日期和时间。可以键入日期和时间；或者单击日历按钮，然后从日历中选择日期和时间。

- 5 在请求类型字段中选择资源请求的类别。选择全部以包含来自所有可用类别的请求。
- 6 从选定类别中可用的请求列表选择一个或多个要委托的请求，然后单击添加。



添加的每个请求将包含在选定的请求列表中。

**请求类型选择**  
 选择您人不在时不接受的请求类型。只有带有委托指派请求可用于下面的选择。

请求的类型:

在指定期间谢绝:\*

Enable Active Directory Account  


---

如果添加了多个请求，则每个请求都视为可以单独编辑的独立对象。

7 要从列表中去掉一个请求，请单击去除。

8 单击提交可提交更改。

User Application 将显示一条确认讯息，指示是否已成功提交委托指派：

**我的委托指派**

提交成功  
 请注意，在已处理受委托者指派中引用的用户的任何以前的可用性设置都不会自动更新。请检查并刷新相应用户的任何现有可用性设置，以激活这些更改。

操作:     提交

用户:       Margo MacKenzie

指派的委托: Timothy Swan

### 11.5.3 删除委托指派

要删除一个现有的委托指派，请执行下列操作：

1 单击该指派旁的去除：



# 管理您的小组工作

本部分说明如何使用 *请求和批准* 选项卡管理小组的供应工作。包括以下主题：

- ◆ 第 12.1 节“关于“我的小组的工作”操作”（第 137 页）
- ◆ 第 12.2 节“管理您的小组任务”（第 138 页）
- ◆ 第 12.3 节“执行小组请求”（第 152 页）
- ◆ 第 12.4 节“管理您的小组请求”（第 155 页）

## 12.1 关于“我的小组的工作”操作

Identity Manager User Application 中的 *请求和批准* 选项卡包含一组称为 *我的小组的工作* 的操作。可以使用 *我的小组的工作* 操作处理工作流程中的小组成员任务和请求。某些操作与第 10 章“管理您的工作”（第 107 页）中介绍的操作相同。您可以执行的操作由小组定义及小组请求权限决定。*请求和批准* 选项卡可处理现有的用户和小组。要添加新的用户和小组，请参考第 8 章“创建用户或组”（第 89 页）。

---

**注释：** 供应工作流程的控制流程以及表单外观可能随 Designer for Identity Manager 中供应请求定义的不同而不同。有关自定义供应工作流程设计的细节，请参见《*Identity Manager User Application：设计指南* (<http://www.novell.com/documentation/idmrbpm361/index.html>)》。

---

### 12.1.1 关于小组

*小组* 标识一组用户。它决定可以管理供应请求及批准与该小组相关的任务的 *用户*。小组定义由小组经理、小组成员和小组选项的列表组成，如下所述：

- ◆ *小组经理* 是可以管理小组成员的请求和任务的 *用户*。小组经理也可以被授予为小组成员设置代理和委托的许可权限。小组经理可以是用户或组。
- ◆ *小组成员* 是可以参与小组的 *用户*。小组成员可以是用户、组或者目录上的容器。它们也可以通过目录关系得到。例如，成员列表可以通过组织内的经理员工关系得到。在这种情况下，小组成员就是向小组经理报告的所有用户。

---

**注释：** 供应应用程序管理员可配置目录提取层以支持级联关系，在这种情况下组织内的若干级可能包含在一个小组内。包含的级数可由管理员配置。

---

- ◆ *小组选项* 决定供应请求的范围，它指定小组可对单个供应请求、一个或多个请求类别还是所有请求执行操作。小组选项还决定小组经理能否为小组成员设置代理和 / 或针对委托设置小组成员的可用性。

供应应用程序管理员可执行所有小组管理功能。

小组定义本身由一个或多个经理在 iManager 内管理。

### 12.1.2 关于小组请求权限

*小组请求权限* 指定小组范围内的请求列表，以及小组经理可对供应请求和任务执行的操作。

小组请求权限由一个或多个经理在 iManager 内管理。不允许小组经理设置那些权限。

您的管理员可以根据特定小组的业务需要定义小组经理的控制范围。由于您作为管理者管理的小组不同，您对请求和任务的权限也可能不同。如果您对特定小组的访问权限有疑问，请联系管理员。

## 12.2 管理您的小组任务

当某个任务处于工作流程队列中时，可以执行下列操作：

- ◆ 第 12.2.1 节“按小组成员查看任务”（第 138 页）
- ◆ 第 12.2.2 节“按用户或组查看任务”（第 139 页）
- ◆ 第 12.2.3 节“使用任务显示格式”（第 141 页）
- ◆ 第 12.2.4 节“选择任务”（第 144 页）
- ◆ 第 12.2.5 节“声明任务”（第 147 页）
- ◆ 第 12.2.6 节“重指派任务”（第 150 页）
- ◆ 第 12.2.7 节“释放任务”（第 151 页）

### 12.2.1 按小组成员查看任务

小组管理者可以查看小组成员的任务。仅小组可用的任务可在任务列表中列出。

- 1 在 *我的小组的工作* 操作组中单击 *小组任务*，可显示“小组任务”窗口。



- 2 单击 *选择小组* 向下箭头显示小组。选择已指派小组管理者的组。

- 3 选择用户。

如果 *用户* 选择框包含姓名，则单击 *用户* 向下箭头可显示选定小组的所有成员。单击要显示其任务的人员姓名。

如果 *用户* 选择框为空，则单击 *对象选择器* 图标打开“对象查找”窗口。指定小组成员的搜索准则，单击 *搜索*，然后选择小组成员。

您的管理员定义您的小组，并定义您可以看到的是一个自动填充的选择列表还是一个空白列表，该选择框旁边有个 *对象选择器* 图标 。

- 4（可选）指定 *超时* 间隔，查找在所选时间内失效的任务。指定一位或多位的数字，例如 10。

如果指定 *超时* 间隔，请选择该间隔单位为天、周还是月。

- 5 使用 *过滤方式* 选择要查看的某个小组成员的部分任务。要查看为小组成员授予或撤消资源的任务，请选择 *收件人*。要查看小组成员负责的任务，请选择 *指派给*。可以同时选择这两种任务。
- 6 在 *任务列表列* 选择框中，选择要显示的一个或多个任务列，并单击向右箭头将它们添加到任务列表中。选择这些列的顺序即是它们显示的顺序。可以包括以下列：

任务（必需。）  
 请求  
 收件人  
 请求日期  
 类型  
 指派给  
 请求者  
 已声明  
 超时  
 优先级  
 数字签名

- 7 单击 *搜索* 列出选定用户的任务。
- 8 要查看另一个小组成员的任务或另一个小组的任务，请返回到 **步骤 2** 并定义新的搜索。

## 12.2.2 按用户或组查看任务

供应应用程序管理员可以按用户或组查看任务。

- 1 在 *我的小组的工作* 操作组中单击 *小组任务*，可显示“小组任务”窗口。
- 2 在 *选择类型* 中，选择 *用户* 或 *组*。



- 3 要查找一个名称，请单击 *对象选择器* 图标 ，指定搜索准则，并单击 *搜索*。  
 单击一个用户名或组名以将其选中。以下对象查找页面示例是对所有组的查找：



- 4 (可选) 指定一个*超时*间隔，查找在该间隔内失效的任务。指定一位或多位的数字。  
如果指定*超时*间隔，请选择该间隔单位为天、周还是月。
- 5 使用*过滤*方式选择任务的子集。要查看对用户或组授予或撤消资源的任务，请选择*收件人*。要查看用户或组负责的任务，请选择*指派给*。可以同时选择这两种任务。
- 6 在*任务列表*选择框中，选择要显示的一个或多个任务说明，然后单击向右箭头将说明添加到任务列表中。您添加这些说明的顺序即是它们在任务列表作为列标题显示的顺序。您的选项包括：  
任务。(必需。)  
请求  
收件人  
请求日期  
类型  
指派给  
请求者  
已声明  
超时  
优先级  
数字签名
- 7 单击*搜索*显示这些任务。  
显示的组任务是明确指派给组的任务，而不是指派给组中每个成员的任务。要查看指派给每个成员的任务，请查看该成员的任务。
- 8 要查看另一个用户或组的任务，请返回到**步骤 2**并定义新的搜索。

## 12.2.3 使用任务显示格式

任务列表以“模板显示”或“展示显示”格式显示。您的显示格式由管理员选择。

### 模板显示格式

“模板显示”是默认显示格式。图 12-1 显示了一个示例：

图 12-1 模板显示格式的任务列表示例

任务	请求	收件人	类型	指派至	已索取	超时
单个批准	授予医疗保险	Kevin Chester	👤	Margo MacKenzie		1 天 23 小时 39 分钟
单个批准	授予支出系统访问权限	Margo MacKenzie	👤	Timothy Swan		1 天 23 小时 43 分钟
单个批准	启用 Active Directory Account (管理器批准无超时)	Kevin Chester	👤	Margo MacKenzie		1 天 23 小时 35 分钟
单个批准	启用 Active Directory Account (管理器批准无超时)	Margo MacKenzie	👤	Timothy Swan		1 天 23 小时 42 分钟
单个批准	启用 Active Directory Account (管理器批准无超时)	Allison Blake	👤	Margo MacKenzie		1 天 23 小时 40 分钟
单个批准	授予智能卡	Margo MacKenzie	👤	Timothy Swan		1 天 23 小时 44 分钟
单个批准	授予健身	Kevin Chester	👤	Margo MacKenzie		1 天 23 小时 39 分钟
单个批准	授予工作簿 7x24	Kevin Chester	👤	Margo MacKenzie		1 天 23 小时 36 分钟
单个批准	授予牙科保险	Kevin Chester	👤	Margo MacKenzie		1 天 23 小时 37 分钟
单个批准	授予医疗保险	Allison Blake	👤	Margo MacKenzie		1 天 23 小时 41 分钟

1 - 10 项 (共 16 项)

模板显示格式使您可以将列按值排序，设置每页的任务数以及对任务列表分页。

### 将列按值排序

- 1 单击列标题可对该列中的值排序。
- 2 再次单击标题可反转排序顺序。

### 设置每页的任务数

- 1 单击任务列表上方右侧的每页的任务数选择框的向下箭头。
- 2 选择每页 5 个任务、10 个任务或 25 个任务。

### 对任务列表分页

- 1 单击第一个、上一个、下一个和最后一个对任务列表分页。

任务	请求	收件人	指派至	超时	优先级
单个批准	启用 Active Directory Account (管理器批准无超时)	Margo MacKenzie	Timothy Swan	1 天 22 小时 8 分钟	
单个批准	授予自助餐	Kevin Chester	Margo MacKenzie	1 天 22 小时 14 分钟	
单个批准	授予依赖性护理	Allison Blake	Margo MacKenzie	1 天 22 小时 12 分钟	
单个批准	启用 Active Directory Account (管理器批准无超时)	Kevin Chester	Margo MacKenzie	1 天 22 小时 13 分钟	
单个批准	授予工作簿 7x24	Margo MacKenzie	Timothy Swan	1 天 22 小时 8 分钟	

6 - 10 项 (共 18 项)

### 展示显示格式

展示显示格式使您可以过滤检索到的数据。图 12-2 显示了展示显示格式的示例：

图 12-2 展示显示格式的任务列表示例



## 将列按值排序

- 1 单击列标题可对该列中的值排序。
- 2 再次单击标题可反转排序顺序。

## 过滤数据视图

展示显示格式显示由搜索返回的整个数据集。可以使用过滤器过滤数据集。这些过滤器在显示格式的右侧，从搜索中获取列标题的名称。可以按任务、请求、指派给和请求者列值来过滤数据。仅当显示中包含相应的列时，才显示过滤器。

**注释：**展示显示格式将过滤器称为方面。

图 12-3 显示了具有“请求”过滤器和“指派给”过滤器的示例。

图 12-3 展示显示格式的两个过滤器



在每个过滤器参数旁边是一个数字和选中标记（可选）。该数字表示当前过滤器集合中与该参数匹配的任务数。选中标记表示是否已选中该过滤器参数。初始情况下，所有过滤器参数都是选中的，使您可以查看搜索的所有数据。如果一个过滤器仅有一个参数，则会自动选中该参数。

- 1 要查看数据的子集，请单击一个或多个过滤器框中的一个或多个参数。

**注释：**选择一个过滤器的一个参数可以更改其他过滤器中可用的参数。

例如，如果在“指派到”过滤器中单击 Margo 的姓名，在“请求者”过滤器中单击 Kevin 的姓名，则将只看到同时指派到 Margo Mackenzie 并由 Kevin Chester 请求的任务，如图 12-4 所示：

图 12-4 应用两个过滤器的任务列表示例



## 导出显示中的数据

- 1 要导出在显示中看到的数据，请单击 *将列表复制到剪贴板*（显示的顶部）。
- 2 选择 *制表符分隔的值*或*此视图生成的HTML*。展示显示格式会生成一个编码文本文件。
- 3 将这些内容复制到剪贴板。
- 4 从剪贴板粘贴到目标文件。
- 5 单击*关闭*或*ESC*关闭编码文本的窗口。

## 了解显示图标

模板视图和展示视图都显示表示结果集中每个任务的状态的图标。本部分说明任务列表中出现的显示图标：

- ◆ “类型”列（第 144 页）
- ◆ “优先级”列（第 144 页）
- ◆ “已声明”列（第 144 页）
- ◆ “数字签名”列（第 144 页）

## “类型”列

在类型列下显示状态标志。标志是在图例中定义的。要访问图例，请单击“小组任务”标题栏右侧的彩色图标。图 12-5 在第 144 页 显示该图例。

图 12-5 在“小组任务”显示格式中显示的图标



## “优先级”列

红色标志表示高优先级任务。此优先级是在您的管理员创建的“供应请求定义”中设置的。

## “已声明”列

已声明列中的已声明图标  表示已声明该任务。

## “数字签名”列

数字签名列中的数字签名图标  表示批准或拒绝该任务需要数字签名。

## 12.2.4 选择任务

要选择并打开任务列表中的任务，请执行下列操作：

- 1 单击任务名称。  
将显示“小组任务细节”表单。



将一项任务指派给多个批准者时，“任务细节”表格将显示 *多个批准者* 图标（在 *指派至* 字段旁），并在该图标下显示文字，表示需要多个批准者。



2 要显示关于指派给多个批准者的任务的更多信息，请单击 *多个批准者* 图标下的文本：



将显示弹出窗口，指出需要的批准数量，当前接收人以及当前的批准状态。

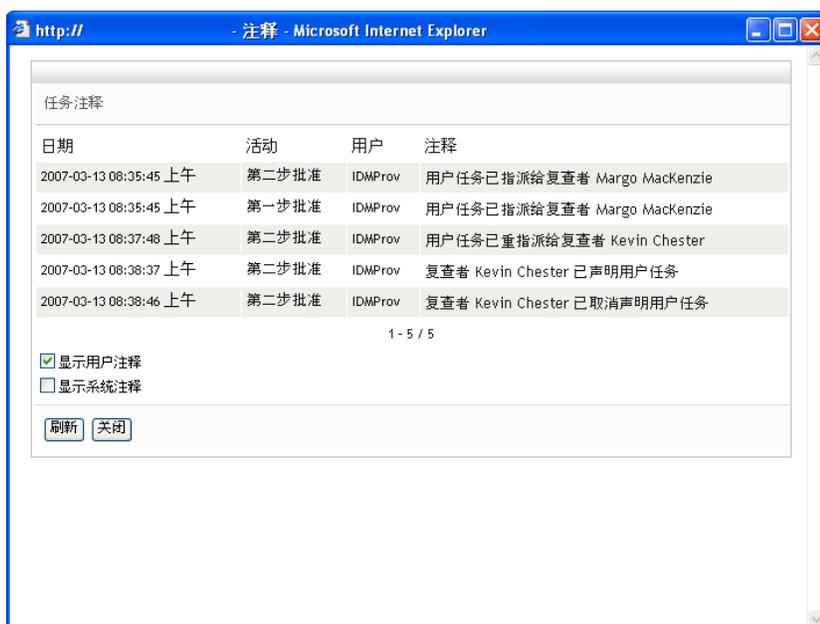


任务的要求取决于您的管理员如何配置任务：

- ◆ 如果您的批准类型是**组**，则任务已指派给组内若干用户，但只应有一个用户声明并批准任务。
  - ◆ 如果批准类型是**多个批准者**，则该任务已指派给若干接收人，所有接收人都必须声明并批准任务。
  - ◆ 如果批准类型是**选定用户数**，则该任务已指派给若干接收人，选定数量的接收人就足以批准任务。选定用户数的定义由管理员配置。要定义选定用户数，管理员将指定批准条件，该条件指定批准的精确数量或需要批准的百分比。
- 3 要声明一个任务，请遵循第 12.2.5 节“**声明任务**”（第 147 页）中的指导。
  - 4 要重指派一个任务，请遵循第 12.2.6 节“**重指派任务**”（第 150 页）中的指导。
  - 5 要查看该任务的注释历史，请单击**查看注释历史**。

可在弹出窗口中查看用户和系统注释。注释显示的顺序由和每条注释关联的时戳决定。先输入的注释先显示。对于并行批准流程，并行处理的活动顺序可能是不可预测的。

**5a** 要显示用户注释，请单击**显示用户注释**。



用户注释包含以下类型的信息：

- ◆ 添加每条注释的日期和时间。
- ◆ 应用每条注释的活动名称。显示的活动列表包含已处理或当前正在处理的用户和供应活动。
- ◆ 作出注释的用户名称。如果注释由工作流程系统生成，应用程序的名称（例如 IDMProv）就是用户名。工作流程系统生成的注释会被自动本地化。
- ◆ 注释文本，包含作为每个活动当前受托人的用户的名称。

---

**注释：**工作流程设计者可以禁止某个工作流程生成用户注释。有关更多信息，请参见《*Identity Manager User Application: 设计指南*》(<http://www.novell.com/documentation/idmr/bpm361/index.html>)。

---

**5b** 要显示系统注释，请单击**显示系统注释**。



系统注释包含以下类型的信息：

- ◆ 添加每条注释的日期和时间。
- ◆ 应用每条注释的活动的名称。显示系统注释时，将列出工作流程中的所有活动。活动列表包含已处理或当前正在处理的活动。
- ◆ 作出注释的用户名称。如果注释由工作流程系统生成，应用程序的名称（例如 IDMProv）就是用户名。工作流程系统生成的注释将被自动本地化。
- ◆ 注释文本，表示对该活动采用的操作。

系统注释主要用于调试。多数业务用户无需查看工作流程的系统注释。

- 5c** 要在很长的注释列表中滚动，请单击屏幕底部的箭头。例如，要滚动到下一页，请单击 *下一页* 箭头。



- 5d** 单击 *关闭* 可关闭此窗口。

- 6** 要返回到任务列表，请单击 *后退*。

---

**注释：** *声明* 和 *重指派* 按钮仅在小组请求权限允许这些操作时可见。

---

## 12.2.5 声明任务

要声明处理的小组成员任务：

- 1** 单击 *声明*。

**小组任务**

任务细节

\*-表示必需。

资源: Enable Active Directory account 收件人: Margo MacKenzie

请求者: Margo MacKenzie 任务: 单一批准

进入队列的时间: 2007-03-15 08:03:25 上午 超时: 2007-03-17 08:03:25 上午

指派给: Marketing group 声明者:

声明 释放 重指派 返回

表格细节

**单一批准**

请选择相应的按钮以批准或拒绝请求。

请求人: Margo MacKenzie 收件人: Margo MacKenzie

请求日期: 2007-03-15

原因:

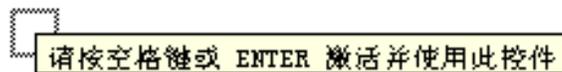
注释:

本页面的表格细节部分将更新，以包含拒绝和批准按钮，以及流程定义包含的其他操作按钮，相应字段将变为可编辑的。

如果您请求的资源要求数字签名，本页面右上角将显示“要求数字签名”图标。



此外，在 Internet Explorer 上将显示讯息，表示您必须按空格键或 Enter 键激活数字签名小程序。



- 2 如果您要处理需要数字签名的任务，请执行以下步骤：
  - 2a 如果您使用智能卡，请将智能卡插入智能卡读卡器。
  - 2b 在 Internet Explorer 上，按空格键或 Enter 键激活小程序。  
此时您的浏览器可能会显示安全警告讯息。



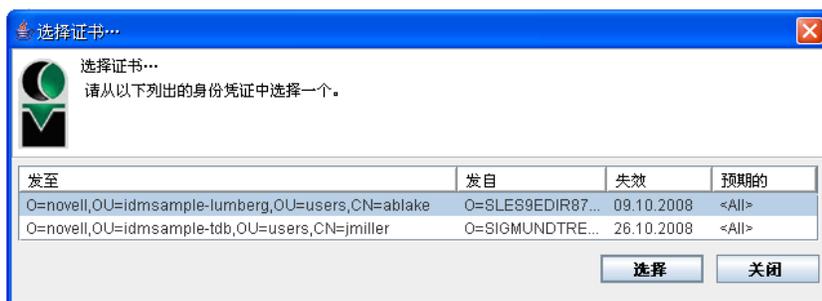
2c 单击 *运行* 继续。

2d 填充批准表格中的字段。表格中的字段可能随请求资源的不同而不同。

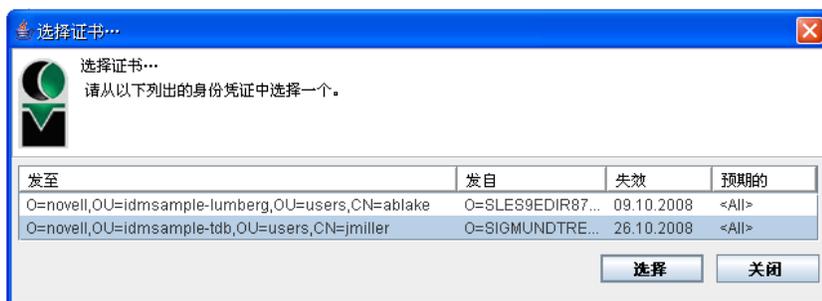
2e 单击数字签名确认讯息旁的复选框，表示您即将签名。

数字签名确认讯息可能随管理员配置供应资源方式的不同而不同。

小程序随即显示弹出窗口，您可以通过它选择证书。弹出窗口将列出导入浏览器的证书及导入智能卡的证书（如果当前已连接智能卡）。



2f 选择您要用的证书并单击 *选择*。



2g 如果选择已导入浏览器中的证书，则需要在请求表格的 *口令* 字段键入证书口令。

2h 如果选择已导入智能卡的证书，请键入您的智能卡的 PIN，并单击 *确定*。

如果您使用智能卡，则无需键入证书口令，因为证书口令已传送到智能卡。



如果您的管理员启用了预览用户协议功能，则将启用 *预览* 按钮。

2i 单击 *预览* 查看用户协议。

如果数字签名类型设置为“表格”，则将显示 PDF 文档。

如果数字签名类型设置为数据，则将显示 XML 文档。

3 要拒绝请求，请单击 *拒绝*。



4 要批准请求，请单击 *批准*。



User Application 将显示一条讯息，指示操作是否成功。

## 12.2.6 重指派任务

要重指派小组成员的任务，请执行以下操作：

1 在“小组任务”任务细节窗口中单击 *重指派*。

**小组任务**

任务细节

\* - 表示必需。

---

资源: Enable Active Directory account 收件人: Margo MacKenzie  
 请求者: Margo MacKenzie 任务: 单一批准  
 进入队列的时间: 2007-03-15 08:03:25 上午 超时: 2007-03-17 08:03:25 上午  
 指派给: Marketing group 声明者:

声明 释放 重指派 返回

---

表格细节

**单一批准**

请选择相应的按钮以批准或拒绝请求。

请求人: Margo MacKenzie 收件人: Margo MacKenzie  
 请求日期: 2007-03-15  
 原因: dfg  
 注释:

- 2 单击 **对象选择器** 图标  (在您选择的输入框旁)。
- 3 在 **新指派** 至下拉列表中选择要向其重指派该任务的用户。

**小组任务**

选择将向其重新指派任务的用户，可以选择添加注释。

\* - 表示必需。

---

资源: Enable Active Directory account 收件人: Margo MacKenzie  
 请求者: Margo MacKenzie 任务: 单一批准  
 进入队列的时间: 2007-03-15 08:03:25 上午 超时: 2007-03-17 08:03:25 上午  
 指派给: Marketing group 声明者: Kevin Chester

**新的指派对象**

请选择以下指派选项之一，并指定要重新为其指派该任务的用户或组。

指派类型: \*  指派: 用户

用户: Allison Blake  
 指派: Allison Blake  
 指派: Kevin Chester

注释:

提交 取消

- 4 (可选) 在 **注释** 字段中输入注释以说明再指派的原因。
- 5 单击 **提交**。

User Application 将显示一条讯息，指示操作是否成功。

## 12.2.7 释放任务

释放任务，以便将该任务指派给另一小组成员或由其声明。

- 1 在“小组任务”任务细节窗口中单击 **释放**。

**小组任务**

任务细节

\* - 表示必需。

---

资源: Enable Active Directory account 收件人: Margo MacKenzie  
 请求者: Margo MacKenzie 任务: 单一批准  
 进入队列的时间: 2007-03-15 08:03:25 上午 超时: 2007-03-17 08:03:25 上午  
 指派给: Marketing group 声明者: Kevin Chester

声明 释放 重指派 返回

表格细节

---

**单一批准**

请选择相应的按钮以批准或拒绝请求。

请求人: Margo MacKenzie 收件人: Margo MacKenzie  
 请求日期: 2007-03-15  
 原因: dfg  
 注释:

## 12.3 执行小组请求

可使用 *请求小组资源* 操作为小组成员请求资源:

- 1 在 *我的小组的工作* 操作组中单击 *请求小组资源*。  
将显示“请求小组资源”页面。

- 2 单击 *选择小组* 选择指定您作为小组经理的小组。然后单击 *继续*。  
应用程序将显示可用来选择类别的页面。
- 3 在 *请求类型* 下拉列表中选择请求的类别。选择 *全部* 以包含来自所有可用类别的请求。  
可用类别的列表取决于小组请求权限。如果小组的供应请求范围不包括资源类别，则不显示类别列表。在这种情况下，跳至下一步，选择资源。
- 4 单击 *继续*。  
“请求小组资源”页面将显示可以请求的资源的列表。该列表只包含小组经理可发起请求的那些资源。



5 单击资源名可选择该资源。

6 单击收件人名称即可将其选定。您选择的小组成员是该请求的收件人。

根据小组的定义，您可能会看到对象选择器图标（位于收件人选择框旁），而不是小组成员列表。在这种情况下，单击该图标打开“对象查找”窗口。指定小组成员的搜索准则，单击搜索，然后选择小组成员。

如果该工作流程的**流程策略**已定义为支持多个收件人，则应用程序允许选择组、容器或小组作为收件人。根据工作流程的配置方式，**User Application** 可能对每个收件人生成单独的工作流程（从而可以对每个收件人独立批准或拒绝请求），也可能生成包含多个供应步骤（每个收件人一步）的单个工作流程。对于后一种情况，请求的批准或拒绝将应用至所有收件人。

7 单击继续。

8 “请求小组资源”页面将显示请求表格。填写请求表格中的字段。在以下示例中，唯一必填的字段为**请求原因**。

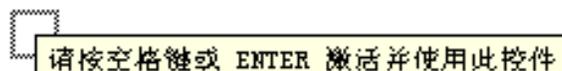
表格中的字段可能随请求资源的不同而不同。



如果您请求的资源要求数字签名，本页面右上角将显示**要求数字签名**图标。



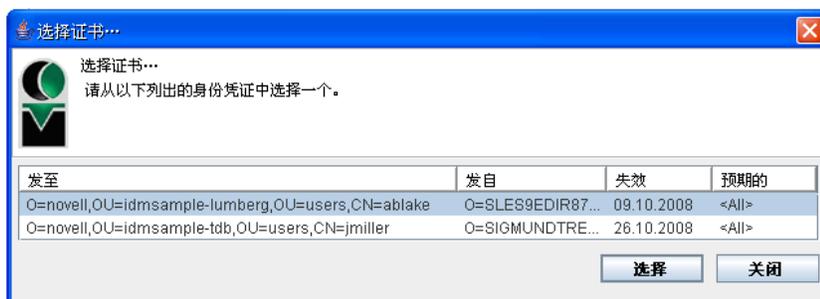
此外，在 Internet Explorer 上将显示讯息，表示您必须按空格键或 Enter 键激活数字签名小程序。



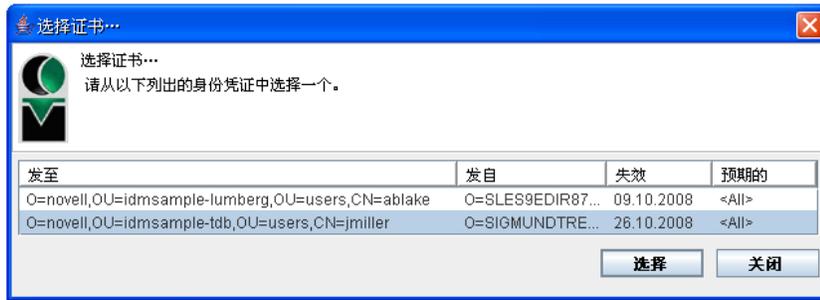
- 9 如果您的请求需要数字签名，请执行以下步骤：
  - 9a 如果您使用智能卡，请将智能卡插入智能卡读卡器。
  - 9b 在 Internet Explorer 上，按空格键或 Enter 键激活小程序。  
此时您的浏览器可能会显示安全警告讯息。



- 9c 单击运行继续。
- 9d 填写初始请求表格中的字段。表格中的字段可能随请求资源的不同而不同。
- 9e 单击数字签名确认讯息旁的复选框，表示您即将签名。  
数字签名确认讯息可能随管理员配置供应资源方式的不同而不同。  
小程序随即显示弹出窗口，您可以通过它选择证书。弹出窗口将列出导入浏览器的证书及导入智能卡的证书（如果当前已连接智能卡）。



9f 选择您要用的证书并单击 *选择*。



9g 如果选择已导入浏览器中的证书，则需要在请求表格的 *口令* 字段键入证书口令。

9h 如果选择已导入智能卡的证书，请键入您的智能卡的 PIN，并单击 *确定*。

如果您使用智能卡，则无需键入证书口令，因为证书口令已传送到智能卡。



如果您的管理员启用了预览用户协议功能，将启用 *预览* 按钮。



9i 单击 *预览* 按钮查看用户协议。

如果数字签名类型设置为“表格”，将显示 PDF 文档。如果数字签名类型设置为数据，将显示 XML 文档。

10 单击 *提交*。

将为用户启动一个工作流程。

“请求小组资源”页面将显示状态讯息，指明是否已成功提交请求。

如果请求需要组织中一个或多个人的许可，则该请求将启动一个或多个工作流程以获取这些批准。

## 12.4 管理您的小组请求

使用“小组请求”操作，小组管理者和供应应用程序管理员可查看资源请求的状态和历史，并可收回资源请求。

**注释：**小组请求操作不显示角色或证明请求。要查看角色请求的状态，您需要使用角色选项卡上的查看请求状态操作。要查看证明请求的状态，您需要使用合规性选项卡上的查看证明请求状态操作。

1 在我的小组的工作操作组中单击小组请求。

2 单击选择小组选择指定您作为小组经理的小组。

如果您是供应应用程序管理员，则不会看到选择小组框。

供应应用程序管理员不能按容器或组过滤小组请求列表。他必须分别选择小组成员。



3 单击继续。

“请求小组资源”页面提示您选择小组成员、请求类型（类别）和请求日期过滤器。

4 单击小组成员名称选择它。

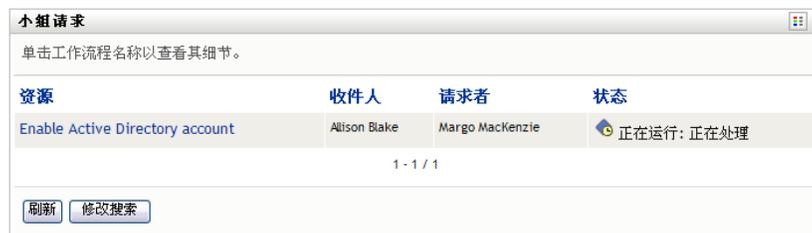
根据小组的定义，您可能会看到对象选择器图标（位于小组成员选择框旁），而不是小组成员列表。在这种情况下，单击该图标打开“对象查找”窗口。指定小组成员的搜索准则，单击搜索，然后选择小组成员。

5 选择小组成员后，可以选择请求类型（类别）和请求日期过滤器。单击继续。

“小组请求”页将列出：

- ◆ 请求的每个资源
- ◆ 资源的接收者
- ◆ 资源的请求者
- ◆ 请求的状态

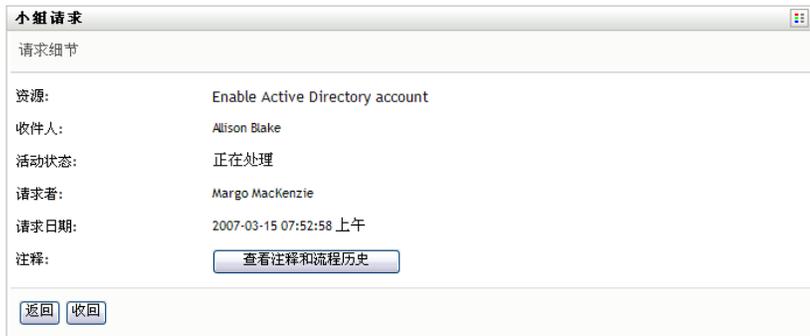
将显示小组请求。请求列表只包含对该小组可用的请求。



**6** 要查看请求的细节，请单击列表中的请求名称。

“请求细节”页将显示细节，例如：

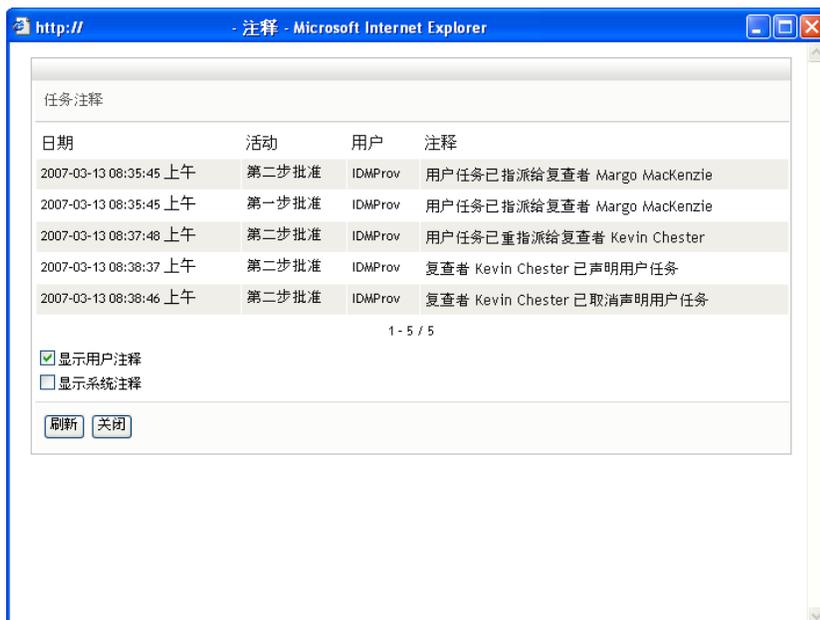
- ◆ 资源名称
- ◆ 资源收件人
- ◆ 支持请求的活动的状态
- ◆ 资源的请求者
- ◆ 请求的发出时间
- ◆ 注释



**7** 要查看请求的注释历史，请单击 *查看注释和流程历史*。

可通过弹出窗口查看用户和系统注释。注释显示的顺序由和每条注释关联的时戳决定。先输入的注释先显示。对于并行批准流程，并行处理的活动顺序可能是不可预测的。

**7a** 要显示用户注释，请单击 *显示用户注释*。



用户注释包含以下类型的信息：

- ◆ 添加每条注释的日期和时间。

- ◆ 应用每条注释的活动名称。显示的活动列表包含已处理或当前正在处理的用户和供应活动。
- ◆ 作出注释的用户名称。如果注释由工作流程系统生成，应用程序的名称（例如 IDMProv）就是用户名。工作流程系统生成的注释会被自动本地化。
- ◆ 注释文本，包含作为每个活动当前受托人的用户的名称。

工作流程设计者可以禁止某个工作流程生成用户注释。有关更多信息，请参见《*Identity Manager User Application: 设计指南* (<http://www.novell.com/documentation/idmrbpm361/index.html>)》。

**7b** 要显示系统注释，请单击 **显示系统注释**。



系统注释包含以下类型的信息：

- ◆ 添加每条注释的日期和时间。
- ◆ 应用每条注释的活动的名称。显示系统注释时，将列出工作流程中的所有活动。活动列表包含已处理或当前正在处理的活动。
- ◆ 作出注释的用户名称。如果注释由工作流程系统生成，应用程序的名称（例如 IDMProv）就是用户名。工作流程系统生成的注释将被自动本地化。
- ◆ 注释文本，表示对该活动采用的操作。

系统注释主要用于调试。多数业务用户无需查看工作流程的系统注释。

**7c** 要在很长的注释列表中滚动，请单击屏幕底部的箭头。例如，要滚动到下一页，请单击 **下一页**。



**7d** 单击 **关闭** 可关闭此窗口。

**8** 要收回请求，请在“请求细节”页面中单击 **收回**。**收回**是为运行中的进程启用的。在不再运行的进程中，将禁用 **收回**。

收回按钮仅当小组经理在小组请求权限中被赋予收回请求的权限时，才会显示。



## 配置小组供应设置

本部分说明如何使用 Identity Manager 用户界面的 *请求和批准* 选项卡上的 *我的小组的设置* 操作。包括以下主题：

- ◆ 第 13.1 节“关于“我的小组的设置”操作”（第 161 页）
- ◆ 第 13.2 节“查看和编辑小组的代理指派”（第 161 页）
- ◆ 第 13.3 节“查看和编辑小组的委托指派”（第 164 页）
- ◆ 第 13.4 节“指定小组的可用性”（第 169 页）

### 13.1 关于“我的小组的设置”操作

Identity Manager User Application 中的 *请求和批准* 选项卡包含一组称为 *我的小组的设置* 的操作。*我的小组的设置* 操作可用于：

- ◆ 创建、查看和修改小组当前的代理指派。
- ◆ 创建、查看和修改小组当前的委托指派。
- ◆ 定义和查看小组成员对委托指派的可用性。

### 13.2 查看和编辑小组的代理指派

*小组代理指派* 操作可用于管理任一小组成员的代理指派。定义代理的规则为：

- ◆ 如果您是小组管理者，则可能有权为您小组的成员定义代理。定义代理的权限由小组定义决定。
- ◆ 指定为代理的人员也必须在您的小组中。
- ◆ 供应应用程序管理员可为组织中的任何用户、组或容器设置代理。

要为小组成员指派代理，请执行下列操作：

- 1 在 *我的小组的设置* 操作组中单击 *小组代理指派*。



- 2 单击 *选择小组* 选择指定您作为小组经理的小组。  
如果您是供应应用程序管理员，则不会看到 *选择小组* 框。

小组列表包含允许小组经理为其设置代理的小组以及禁止为其设置代理的小组。如果特定小组定义不允许小组经理设置代理，他仍可以查看管理员或这些用户所属小组的经理为小组成员定义的代理设置。但是，小组经理无法编辑这些设置，不能查看这些设置的细节，也不能创建新的代理指派。

3 单击 *继续*。

4 单击 *小组成员* 名称选择它。

根据小组的定义，您可能会看到 *对象选择器* 图标  (位于 *小组成员* 选择框旁)，而不是小组成员列表。在这种情况下，单击该图标打开“对象查找”窗口。指定小组成员的搜索准则，单击 *搜索*，然后选择小组成员。



5 单击 *继续*。

将显示所选小组成员的代理指派（如有）。您可以单击 *指派的代理* 字段排列代理指派。

6 单击 *新建*。

*新建* 按钮仅用于小组经理可为其成员设置代理的小组。

7 如下填充字段：

字段	说明
<i>用户</i>	选择要指派代理的小组成员。可以选择多个用户。
<i>指派的代理</i>	选择将要担当代理的小组成员。
<i>将这些更改通知给其他用户</i>	表示是否要发送电子邮件讯息，将该代理指派通知给一个或多个用户。
<i>接收人</i>	指定哪些用户应收到电子邮件通知：  <b>所有：</b> 指定指派为代理的用户以及要指派代理的小组成员会收到电子邮件通知。  <b>指派自：</b> 指定只有要指派代理的小组成员会收到电子邮件通知。  <b>指派至：</b> 指定只有担当代理的小组成员会收到电子邮件通知。  <b>选定的：</b> 允许您向选择的任何用户发送电子邮件通知，包括不在小组内的用户。
<i>失效</i>	<b>不失效：</b> 如果希望代理指派在被去除或修改之前保持有效，请选择 <b>不失效</b> 。  <b>指定失效：</b> 选择 <i>指定失效</i> 定义 <i>结束日期</i> 。单击“日历”，然后选择代理指派的失效日期和时间。

8 单击 *提交* 保存选择。

如果指派成功，将显示如下所示的讯息：

Submission was successful  
Changes will be reflected upon the assigned's next login.

- 9 单击“Back to Team Proxy Assignments（返回小组代理指派）”可创建新的代理指派，或编辑现有的代理指派。

要更改现有的代理指派，请执行下列操作：

- 1 在我的小组的设置操作组中单击小组代理指派。
- 2 单击选择小组选择指定您作为小组经理的小组。

小组列表包含允许小组经理为其设置代理的小组以及禁止为其设置代理的小组。如果特定小组定义不允许小组经理设置代理，他仍可以查看管理员或这些用户所属小组的经理为小组成员定义的代理设置。但是，小组经理无法编辑这些设置，不能查看这些设置的细节，也不能创建新的代理指派。

如果您是供应应用程序管理员，则不会看到选择小组框。

- 3 单击继续。
- 4 单击小组成员名称选择它。

根据小组的定义，您可能会看到对象选择器图标（位于小组成员选择框旁），而不是小组成员列表。在这种情况下，单击该图标打开“对象查找”窗口。指定小组成员的搜索准则，单击搜索，然后选择小组成员。

- 5 单击继续。

将显示所选小组成员的代理指派（如有）。

- 6 要更改一个代理指派，请单击要修改的指派旁边的编辑按钮。



如果小组定义不允许小组经理设置代理，该编辑按钮将被禁用。

- 7 如下填充字段：

字段	说明
用户	选择要指派代理的小组成员。可以选择多个用户。
指派的代理	选择将要担当代理的小组成员。
将这些更改通知给其他用户	表示是否要发送电子邮件讯息，将该代理指派通知给一个或多个用户。
接收人	指定哪些用户应收到电子邮件通知：  <b>所有：</b> 指定指派为代理的用户以及要指派代理的小组成员会收到电子邮件通知。  <b>指派自：</b> 指定只有要指派代理的小组成员会收到电子邮件通知。  <b>指派至：</b> 指定只有担当代理的小组成员会收到电子邮件通知。  <b>选定的：</b> 允许您向选择的任何用户发送电子邮件通知，包括不在小组内的用户。
失效	<b>不失效：</b> 如果希望代理指派在被去除或修改之前保持有效，请选择 <b>不失效</b> 。  <b>指定失效：</b> 选择 <i>指定失效定义结束日期</i> 。单击“日历”，然后选择代理指派的失效日期和时间。

## 8 单击 *提交* 保存选择。

如果更改成功，将显示如下所示的讯息：

```
Submission was successful
Changes will be reflected upon the assigned's next login.
```

要删除代理指派，请执行下列操作：

- 1 在 *我的小组的设置* 操作组中单击 *小组代理指派*。
- 2 要去掉代理设置，请单击 *删除*。



系统将提示您确认删除。删除完成后，将显示如下所示的确认讯息：

```
Submission was successful.Changes will be reflected upon the assigned's next
login.
```

**注释：** 也可以在编辑代理指派的过程中删除代理指派。

## 13.3 查看和编辑小组的委托指派

可使用 *小组委托指派* 操作来管理小组成员的委托指派。定义委托的规则如下：

- ◆ 您可以为指定您作为小组经理的小组的成员定义委托，只要小组定义赋予您该许可权限。
- ◆ 指定为委托的人员也必须在您的小组中。
- ◆ 供应应用程序管理员可为组织中的任何用户、组或容器定义委托指派。

要定义委托指派，请执行下列操作：

- 1 在 **小组设置** 操作组中单击 **小组委托指派**。
- 2 单击 **选择小组** 选择指定您作为小组经理的小组。



小组列表包含小组经理有权定义委托的小组（在小组请求权限中指定）以及禁止设置委托的小组。如果小组请求权限不允许小组经理定义委托，他仍可以查看管理员或这些用户所属小组的经理为小组成员定义的委托设置。但是，小组经理无法编辑或删除这些设置，不能查看这些设置的细节，也不能创建新的委托指派。

如果您是供应应用程序管理员，则不会看到 **选择小组** 框。

- 3 单击 **继续**。
- 4 单击 **小组成员** 名称选择它。



根据小组的定义，您可能会看到 **对象选择器** 图标 （位于 **小组成员** 选择框旁），而不是小组成员列表。在这种情况下，单击该图标打开“对象查找”窗口。指定小组成员的搜索准则，单击 **搜索**，然后选择小组成员。

- 5 从列表中选择小组成员，然后单击 **继续**。  
将显示该小组成员的任何现有指派。
- 6 单击 **新建**。  
**新建**按钮仅用于小组经理可为其成员定义委托的小组。
- 7 如下填充字段：

字段	说明
用户	选择您要委托其工作的一个或多个用户。
指派类型	通过选择下列选项之一，指派可以执行受委托工作的用户： <ul style="list-style-type: none"> <li>◆ <b>指派委托</b>：在表中选择用户。</li> <li>◆ <b>按关系指派</b>：从下拉列表中选择委托关系。</li> </ul>
将这些更改通知给其他用户	指示是否要发送电子邮件讯息，将该委托指派通知给一个或多个用户。
接收人	指定哪些用户应收到电子邮件通知： <p><b>所有</b>：指定指派为委托的用户以及要指派委托的小组成员会收到电子邮件通知。</p> <p><b>指派自</b>：指定只有要指派委托的小组成员会收到电子邮件通知。</p> <p><b>指派至</b>：指定只有担当委托的小组成员会收到电子邮件通知。</p> <p><b>选定的</b>：允许您向选择的任何用户发送电子邮件通知，包括不在小组内的用户。</p>
失效	<p><b>不失效</b>：如果希望委托在被去除或修改之前保持有效，请选择<b>不失效</b>。如果此选项有效，则委托永久有效。</p> <p><b>指定失效</b>：选择<b>指定失效定义结束日期</b>。单击“日历”，然后选择委托指派的失效日期和时间。</p>
请求类型	从列表选择一个类别。
所选类别中的可用请求	这会填充 <b>所选类别</b> 中的 <b>可用请求</b> 列表。
选定的请求	从该列表选择一个或多个资源请求，然后单击 <b>添加</b> 。
选定的请求	该列表显示已被委托的资源请求类型。要去除一个请求类型，请从列表中选择它，然后单击 <b>去除</b> 。

## 8 单击“提交”可保存指派。

如果保存成功，将显示如下所示的讯息：

```
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.
```

要修改委托指派，请执行下列操作：

- 1 在**小组设置**操作组中单击**小组委托指派**。
- 2 单击**选择小组**选择指定您作为小组经理的小组。

小组列表包含小组经理有权定义委托的小组（在小组请求权限中指定）以及禁止设置委托的小组。如果小组请求权限不允许小组经理定义委托，他仍可以查看管理员或这些用户所属小组的经理为小组成员定义的委托设置。但是，小组经理无法编辑或删除这些设置，不能查看这些设置的细节，也不能创建新的委托指派。

如果您是供应应用程序管理员，则不会看到**选择小组**框。

**3** 单击*继续*。

**4** 单击*小组成员*名称选择它。

根据小组的定义，您可能会看到*对象选择器*图标（位于*小组成员*选择框旁），而不是小组成员列表。在这种情况下，单击该图标打开“对象查找”窗口。指定小组成员的搜索准则，单击*搜索*，然后选择小组成员。

将显示所选小组成员的委托指派（如有）。

**5** 从列表中选择小组成员，然后单击*继续*。

将显示该小组成员的任何现有指派。

**6** 要编辑委托指派，请在要修改的指派所在行中单击编辑按钮。



如果小组请求权限不允许小组经理定义委托，该编辑按钮将被禁用。

**7** 如下填充字段：

字段	说明
用户	选择您要委托其工作的一个或多个用户。
指派类型	<p>通过选择下列选项之一，指派可以执行受委托工作的用户：</p> <ul style="list-style-type: none"> <li>◆ <b>指派委托</b>：在表中选择用户。</li> <li>◆ <b>按关系指派</b>：从下拉列表中选择委托关系。</li> </ul>
将这些更改通知给其他用户	指示是否要发送电子邮件讯息，将该委托指派通知给一个或多个用户。
接收人	<p>指定哪些用户应收到电子邮件通知：</p> <p><b>所有</b>：指定指派为委托的用户以及要指派委托的小组成员会收到电子邮件通知。</p> <p><b>指派自</b>：指定只有要指派委托的小组成员会收到电子邮件通知。</p> <p><b>指派至</b>：指定只有担当委托的小组成员会收到电子邮件通知。</p> <p><b>选定的</b>：允许您向选择的任何用户发送电子邮件通知，包括不在小组内的用户。</p>
失效	<p><b>不失效</b>：如果希望委托在被去除或修改之前保持有效，请选择<b>不失效</b>。如果此选项有效，则委托永久有效。</p> <p><b>指定失效</b>：选择<b>指定失效定义结束日期</b>。单击“日历”，然后选择委托指派的失效日期和时间。</p>
请求类型	<p>从列表中选择一个类别。</p> <p>这会填充<b>所选类别</b>中的<b>可用请求</b>列表。</p> <p>要指定该委托指派适用于所有类别，请将该委托指派的请求类型设置为<b>全部</b>。</p> <div data-bbox="690 1234 1367 1375" data-label="Image"> </div>
	<p><b>注释</b>：“全部”选项仅当供应管理员为您的应用程序启用“允许所有请求”选项时可用。</p>
所选类别中的可用请求	<p>从该列表中选择一个或多个资源请求，然后单击<b>添加</b>。</p> <p>供应请求列表只包含小组范围内的那些请求。如果小组请求权限不允许小组经理定义委托，和该小组相关的供应请求不会包含在该列表中。</p>
选定的请求	该列表显示已被委托的资源请求类型。要去除请求类型，请从列表中选择该请求类型，然后单击 <b>去除</b> 。

8 单击 **提交** 保存选择。

要删除委托指派，请执行下列操作：

- 1 在 *小组设置* 操作组中单击 *小组委托指派*，查看委托给该小组成员的指派和该小组成员委托给别人的指派。
- 2 要去除委托指派，请在要修改的指派所在行中单击删除按钮。



系统将提示您确认删除。删除完成后，将显示一条确认讯息。

## 13.4 指定小组的可用性

可使用 *小组可用性* 操作指定您的小组成员没空处理的资源请求。在您或者小组成员没空的时间段内，该类型的资源请求都将转发到委托的队列。

可以单独或全局地指定对每个资源请求的可用性。只能为已指派委托的用户指定可用性。

- 1 在 *我的小组的设置* 操作组中单击 *小组可用性*。
- 2 单击 *选择小组* 选择指定您作为小组经理的小组。



小组列表包含小组经理有权定义可用性的小组（在小组定义中指定）以及禁止定义可用性的小组。如果小组定义不允许小组经理定义可用性，他仍可以查看管理员或这些用户所属小组的经理为小组成员定义的可用性设置。但是，小组经理无法编辑或删除这些设置，不能查看这些设置的细节，也不能创建新的可用性指派。

如果您是供应应用程序管理员，则不会看到 *选择小组* 框。

- 3 单击 *继续*。
- 4 单击 *小组成员* 名称选择它，然后单击 *继续*。

根据小组的定义，您可能会看到 *对象选择器* 图标 （位于 *小组成员* 选择框旁），而不是小组成员列表。在这种情况下，单击该图标打开“对象查找”窗口。指定小组成员的搜索准则，单击 *搜索*，然后选择小组成员。



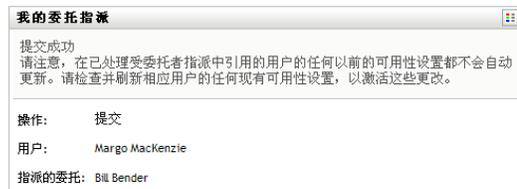
将显示所选小组成员的可用性设置（如有）。

- 5 要查看和可用性指派关联的特定资源，请单击该资源的名称：

### 资源

[Enable Active Directory Account](#)

该页面随即显示弹出窗口，提供关于委托指派的信息：



在同一资源名称多次出现在可用性设置列表中的情况下，该信息特别有帮助。

- 6 单击 **新建**。

**新建**按钮仅可用于小组管理者可为其成员定义可用性设置的那些小组。

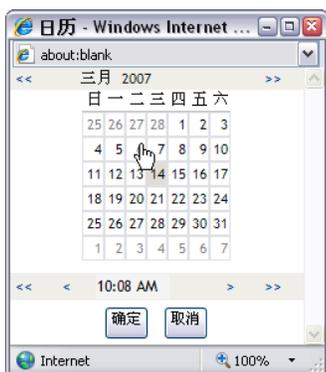
- 7 通过在 **更改状态** 下拉列表中选择下列选项之一来指定状态：

状态	说明
可用于所有请求	<p>这是默认状态。它表示小组成员全局可用。如果该状态有效，则向该小组成员指派请求不会被委托，即使已为其指派了委托，也是如此。</p> <p><b>注释：</b>如果更改了状态，然后又重新更改为 <i>可用于所有请求</i>，则会去除以前定义的任何 <i>选择性可用</i> 设置。</p>
不可用于任何请求	<p>指定小组成员对当前系统中的所有资源请求都不可用。（这又称为“全局不可用”。）</p> <p>选择该状态表示小组成员不可用于现有的每个委托指派，并且会将当前状态更改为 <i>不可用于指定的请求</i>。</p> <p>这些指派可立即生效，并且在委托指派失效前保持有效。</p> <p><b>注释：</b>此设置不影响在此时间点后新建的指派的可用性。</p>

状态	说明
不可用于指定的请求	<p>如果选择该选项，系统将提示您指定小组成员的可用性。（该操作相当于单击 <b>新建</b> 按钮。）系统将提示您指定：</p> <ul style="list-style-type: none"> <li>◆ 小组成员没空处理的请求类型。</li> <li>◆ 小组成员没空的时间段。</li> </ul> <p>在小组成员没空处理特定请求的时间段内，受委托的用户可处理该请求。</p>

**8** 指定小组成员没空的时间段：

**8a** 指定该时间段的开始时间，方法是在“不可用的开始日期”框中键入开始日期和时间；或者单击日历，然后选择日期和时间。



**8b** 通过单击下列按钮之一来指定该时间段的结束时间：

按钮	说明
不失效	表示该不可用性设置不会失效。
指定持续时间	用于以周、天或小时为单位指定时间段。
指定结束日期	用于指定结束日期和时间。可以键入日期和时间；或者单击日历，然后从日历中选择日期和时间。

**9** 通过填充以下字段，指定是否要向其他用户发送电子邮件通知：

字段	说明
将这些更改通知给其他用户	表示是否要发送电子邮件讯息，将该可用性指派通知给一个或多个用户。
接收人	<p>指定应收到电子邮件通知的用户：</p> <p><b>选定的：</b> 允许您向选择的任何用户发送电子邮件通知，包括不在小组内的用户。</p>

**10** 在 *请求类型* 列表框中选择一个或多个请求，然后单击 **添加**。

在此页面上选择小组成员不在位的时段内不接受的请求类型。结果是把这些请求委托给其他用户。

添加的每个请求将包含在在*在指定期间拒绝*列表框中。

如果为该时间段添加了多个请求，则将每个请求都视为可以单独编辑的独立对象。

- 11 要表示该可用性设置应用于所有请求类型，请单击*所有请求类型*，而不是分别选择请求类型。

**所有请求类型**

*所有请求类型*复选框仅当委托指派请求类型设置为*全部*时才可用。

- 12 要从列表中去掉一个请求，请单击*去除*。
- 13 单击*提交*可保存更改。

# 使用“角色”选项卡

# IV

以下部分说明如何使用 Identity Manager User Application 的 *角色* 选项卡。

- ◆ 第 14 章““角色”选项卡简介”（第 175 页）
- ◆ 第 15 章“查看角色”（第 185 页）
- ◆ 第 16 章“作出角色指派”（第 187 页）
- ◆ 第 17 章“管理角色”（第 203 页）
- ◆ 第 18 章“创建并查看角色报告”（第 217 页）



# “角色”选项卡简介

本部分概述 *角色* 选项卡。包括以下主题：

- ◆ 第 14.1 节“关于“角色”选项卡”（第 175 页）
- ◆ 第 14.2 节“访问“角色”选项卡”（第 180 页）
- ◆ 第 14.3 节“浏览选项卡的功能”（第 180 页）
- ◆ 第 14.4 节“可执行的角色操作”（第 182 页）
- ◆ 第 14.5 节“了解角色图例”（第 183 页）

有关访问和操作 Identity Manager 用户界面的更多一般信息，请参见第 1 章“入门”（第 15 页）。

## 14.1 关于“角色”选项卡

*角色* 选项卡用于使您方便地执行基于角色的供应操作。这些操作允许用户管理贵组织内的角色定义和角色指派。角色指派可以映射到公司内的资源，如用户帐户、计算机和数据库。例如，可以使用 *角色* 选项卡执行以下操作：

- ◆ 为您自己或贵组织内的其他用户发出角色请求
- ◆ 创建角色以及角色层次结构内的角色关系
- ◆ 创建职责分离 (SoD) 限制以管理角色指派之间的潜在冲突
- ◆ 查看提供有关“角色编目”当前状态和当前指派给用户、组与容器的角色的细节的报告

如果角色指派请求需要从组织中的一个或多个人获得许可权限，则该请求将启动工作流程。工作流程可协调完成请求所需的批准。有些角色请求需要一个人批准，而另一些请求则需要多人批准。在某些实例中，可以不经任何批准完成请求。

如果角色指派请求可能产生职责分离冲突，发起人可以覆盖职责分离限制，并且对产生限制异常提供调整。在某些情况下，职责分离冲突可能导致工作流程启动。工作流程协调允许职责分离异常生效所需的批准。

工作流程设计者和系统管理员负责为您以及组织中的其他用户设置 *角色* 选项卡的内容。基于角色的工作流程或职责分离工作流程的控制流程以及表单外观可能有所不同，具体取决于工作流程的批准定义在 Designer for Identity Manager 中的定义方式。此外，可以查看的内容以及可以执行的操作通常由您的工作要求和权限级别确定。

### 角色和代理方式

代理方式仅在 *请求* 和 *批准* 选项卡上起作用，在 *角色* 选项卡上不受支持。如果在 *请求* 和 *批准* 选项卡上进入代理模式，然后切换到 *角色* 选项卡，则代理模式在这两个选项卡上都将关闭。

### 14.1.1 关于角色

本部分概述 *角色* 选项卡中所用的术语和概念：

- ◆ *角色与角色指派*（第 176 页）

- ◆ [角色编目与角色层次结构](#)（第 176 页）
- ◆ [职责分离](#)（第 178 页）
- ◆ [角色报告与审计](#)（第 178 页）
- ◆ [角色安全性](#)（第 178 页）
- ◆ [角色服务驱动程序](#)（第 180 页）

## 角色与角色指派

*角色*定义与一个或多个目标系统或应用程序相关的一组许可权限。*角色*选项卡允许用户请求*角色指派*，角色指派是角色与用户、组或容器之间的关联。*角色*选项卡还允许用户定义*角色*关系，用于在角色层次结构中建立角色之间的关联。

可以将角色直接指派给用户，在这种情况下，这些*直接指派*使用户可以显式访问与该角色关联的许可权限。也可以定义*间接指派*，从而允许用户通过角色层次结构中的组、容器或相关角色中的成员资格获取角色。

请求角色指派时，可以选择定义*角色指派有效日期*，用于指定指派生效的日期和时间。如果将该字段保留为空，则表示指派立即生效。

也可以定义*角色指派失效日期*，用于指定自动去除指派的日期和时间。

用户请求角色指派时，角色子系统将管理角色请求的生命周期。要了解用户或角色子系统对请求采取了哪些操作，可以在“查看请求状态”页面上查看请求状态。

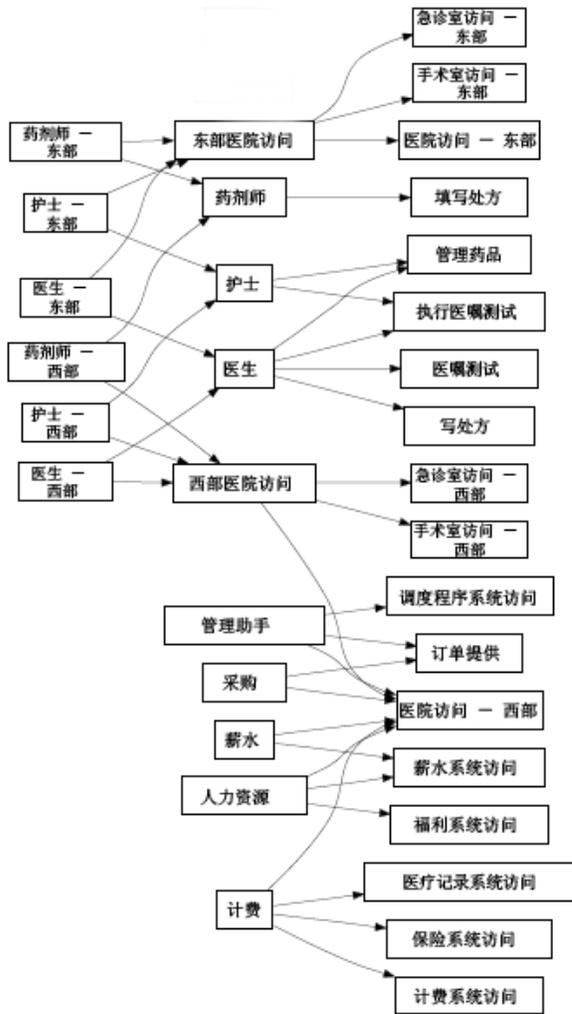
## 角色编目与角色层次结构

必须首先在“角色编目”中定义角色，然后用户才能开始指派这些角色。“角色编目”是所有角色定义与角色子系统所需支持数据的储存库。要设置“角色编目”，“角色模块管理员”（或“角色管理者”）应定义角色与角色层次结构。

*角色层次结构*建立编目中角色之间的关系。通过定义角色关系，可以简化通过角色指派授予许可权限的任务。例如，可以定义一个 **Doctor** 角色并指定这个 **Doctor** 角色与每个医疗角色之间的关系，而无需只要有医生加入贵组织，就指派 50 个不同的医疗角色。通过向用户指派 **Doctor** 角色，可以向这些用户提供为每个相关医疗角色定义的许可权限。

角色层次结构支持三个级别。最高级别定义的角色（称为“业务角色”）定义组织内具有业务意义的操作。中级角色（称为“IT 角色”）支持技术功能。层次结构最低级别定义的角色（称为“许可权限角色”）定义较低级别的特权。以下示例显示一家医疗组织的样本角色层次结构，其中包含三个级别。层次结构的最高级别位于左侧，最低级别位于右侧：

图 14-1 样本角色层次结构



较高级别的角色自动包含其包含的较低级别角色的特权。例如，一个“业务角色”自动包含该角色下包含的“IT 角色”的特权。同样，一个“IT 角色”自动包含该角色下包含的“许可权限角色”的特权。

层次结构中对等角色之间不允许存在角色关系。此外，较低级别的角色不能包含较高级别的角色。

定义角色时，可以选择为该角色指定一个或多个拥有者。*角色拥有者*是指定为角色定义的拥有者的一个用户。针对“角色编目”生成报告时，可以基于角色拥有者过滤这些报告。角色拥有者不会自动具备管理角色定义更改的授权。在某些情况下，拥有者必须要求角色管理员对角色执行任何管理操作。

定义角色时，也可以将该角色与一个或多个角色类别相关联。*角色类别*允许用户对角色分类，以便组织角色系统。将角色与类别关联之后，可以在浏览“角色编目”时将该类别用作过滤器。

如果角色指派请求需要批准，则角色定义将指定用于协调批准的工作流程细节以及批准者列表。批准者是可以批准或拒绝角色指派请求的个人。

## 职责分离

角色子系统的一个关键功能是定义*职责分离 (SoD) 限制*。职责分离 (SoD) 限制是定义认为存在冲突的两个角色的规则。安全专员负责为组织创建职责分离限制。通过定义 SoD 限制，这些专员可以防止将用户指派给冲突的角色，或是维护审计追踪，以便跟踪允许冲突的情况。在职责分离限制中，冲突的角色在角色层次结构中的级别必须相同。

某些职责分离限制不经批准即可被覆盖，而其他的则需批准。无需批准即允许的冲突称为*职责分离违例*。已经批准的冲突称为*已批准的职责分离异常*。角色子系统无需批准源自间接指派（例如组或容器中的成员资格或角色关系）的 SoD 违例。

如果职责分离冲突需要批准，则该限制定义将指定用于协调批准的工作流程细节以及批准者列表。批准者是可以批准或拒绝 SoD 异常的个人。将定义一个默认列表，充当角色子系统配置的组成部分。但是，可以在 SoD 限制的定义中覆盖该列表。

## 角色报告与审计

角色子系统提供了一套丰富的报告工具，帮助审计员分析“角色编目”，以及角色指派与 SoD 限制、违例和异常的当前状态。这个角色报告工具允许角色审计员和角色模块管理员以 PDF 格式显示下列类型的报告：

- ◆ 角色列表报告
- ◆ 角色细节报告
- ◆ 角色指派报告
- ◆ SoD 限制报告
- ◆ SoD 违例与异常报告
- ◆ 用户角色报告
- ◆ 用户权利报告

除通过报告工具提供信息之外，还可以将角色子系统配置为把事件记录到 Novell® Audit 中。

## 角色安全性

角色子系统使用一组系统角色来保护对*角色选项卡*内的功能的访问。*角色选项卡*中的每个菜单操作都映射到一个或多个系统角色。如果用户不是与某个操作关联的一个角色的成员，则*角色选项卡*上将不显示相应的菜单项。

*系统角色*是在安装时由系统自动定义的管理角色，用于执行委派管理。这些更改包括以下几点：

- ◆ 角色模块管理员
- ◆ 角色管理者
- ◆ 角色审计员
- ◆ 安全专员

下文将详细说明这些系统角色。

表 14-1 系统角色

职能	说明
角色模块管理员	<p>这是一个系统角色，它允许成员创建、去除或修改所有角色，以及授予或撤销对任何用户、组或容器的任何角色指派。此角色还允许成员为任何用户运行任何报告。此角色的人员可以不受限制地执行 User Application 中的下列功能：</p> <ul style="list-style-type: none"> <li>◆ 创建、去除和修改角色。</li> <li>◆ 修改角色的角色关系。</li> <li>◆ 请求将用户、组或容器指派给角色。</li> <li>◆ 创建、去除和修改 SoD 限制。</li> <li>◆ 浏览“角色编目”。</li> <li>◆ 配置角色子系统。</li> <li>◆ 查看所有请求的状态。</li> <li>◆ 收回角色指派请求。</li> <li>◆ 运行任何或全部报告。</li> </ul>
角色管理者	<p>这是一个系统角色，允许成员修改角色和角色关系，以及为用户授予或撤销角色指派。此角色的人员可以执行 User Application 中的下列功能，但对角色对象的目录浏览权限范围受到限制：</p> <ul style="list-style-type: none"> <li>◆ 创建新的角色和修改用户具有浏览权限的现有角色。</li> <li>◆ 修改用户具有浏览权限的角色的角色关系。</li> <li>◆ 请求将用户、组或容器指派给用户具有浏览权限的角色。</li> <li>◆ 浏览“角色编目”（范围受浏览权限的限制）。</li> <li>◆ 浏览对用户、组和容器的角色指派请求（范围受对角色、用户、组和容器对象的目录浏览权限的限制）。</li> <li>◆ 收回对用户、组和容器的角色指派请求（范围受对角色、用户、组和容器对象的目录浏览权限的限制）。</li> </ul>
角色审计员	<p>这是一个系统角色，允许成员对具有目录浏览权限的对象运行任何报告。</p>
安全专员	<p>这是一个系统角色，允许成员创建、去除或修改 SoD 限制。安全专员必须具有 SoD 限制的浏览权限。</p>

### 已鉴定用户

除支持这些系统角色之外，角色子系统还允许已鉴定的用户进行访问。已鉴定用户是已登录 User Application，但不具备系统角色中的成员资格所享有的任何特殊特权的用户。典型的已鉴定用户可以执行下面的任何功能：

- ◆ 查看已指派给该用户的所有角色。
- ◆ 请求对具有浏览权限的角色的指派（仅针对该用户）。
- ◆ 查看该用户充当请求者或收件人的请求的状态。
- ◆ 收回该用户同时充当请求者和收件人的请求的角色指派请求。

## 角色服务驱动程序

角色子系统使用角色服务驱动程序管理角色的后端处理。例如，管理所有角色指派，启动需要批准的角色指派请求和 SoD 冲突的工作流程，以及根据组和容器成员资格及相关角色中的成员资格维护间接角色指派。该驱动程序还根据用户的角色成员资格为其授予和撤销权利，并且执行已完成请求的清理过程。

有关角色服务驱动程序的细节，请参见《*Identity Manager User Application: 管理指南* (<http://www.novell.com/documentation/idmrbpm361/index.html>)》。

## 14.2 访问“角色”选项卡

要访问角色选项卡：

- 1 请在 User Application 中单击角色。

默认情况下，角色选项卡将打开，并显示“我的角色”页面。



如果转至用户界面中的另一个选项卡，但是又希望返回前一个选项卡，则仅需单击角色选项卡，即可将其再次打开。

## 14.3 浏览选项卡的功能

本部分介绍角色选项卡的默认功能。（选项卡的外观可能由于针对您组织所作的自定义而不同；请咨询系统管理员或工作流程设计者。）

角色选项卡的左侧显示可以执行的操作的菜单。这些操作按类别排列（我的角色、角色指派、角色管理和角色报告）：



仅当用户为“角色模块管理员”或“角色管理者”时，才显示角色管理操作。仅当用户为“角色模块管理员”或“安全专员”时，才显示角色管理内的管理职责分离操作。仅当用户为“角色模块管理员”或“角色审计员”时，才显示角色报告操作。

单击一项操作时，其右侧会显示相应的页面。该页面通常包含一个窗口，其中显示该操作的细节。例如，该窗口可能会显示一个可以在其中输入数据或进行选择的列表或表格，如下图所示：

图 14-2 为某操作显示的页面



在角色选项卡中使用的大多数页面的右上角都包含一个按钮，可以使用该按钮显示角色图例：



有关角色图例的细节，请参见第 14.5 节“了解角色图例”（第 183 页）。

## 14.4 可执行的角色操作

下面是默认情况下可以在角色选项卡中使用的操作的摘要：

表 14-2 角色操作

类别	操作	说明
我的角色	我的角色	可用于查看已批准角色的状态和细节。显示状态为“已供应”或“待发激活”的角色，而非尚未批准的角色。  有关细节，请参见第 15 章“查看角色”（第 185 页）。
职能指派	职能指派	<i>角色指派</i> 操作使用户可请求角色指派。“角色模块管理员”、“角色管理者”和不是特别指派给任何已安装系统角色的其他已鉴定用户可执行此操作。 <ul style="list-style-type: none"><li>“角色模块管理员”可以请求将用户、组和容器指派给角色。“角色模块管理员”在该目录内不受范围限制。</li><li>“角色管理者”可以请求将用户、组和容器指派给具有浏览权限的角色。</li><li>其他已鉴定用户可以请求将自己指派给具有浏览权限的角色。</li></ul> 有关细节，请参见第 16.2 节“指派角色”（第 187 页）。
	查看请求状态	允许用户查看自己的角色请求（包括明确发出的请求以及所属组或容器的角色指派请求）状态。可通过该操作查看每个请求的当前状态。此外，如果改变主意且不需要完成请求，则可通过该操作选择收回尚未完成或终止的请求。  有关细节，请参见第 16.3 节“检查请求的状态”（第 195 页）。
职能管理	浏览“角色编目”	可用于查看“角色编目”中的现有角色。您还可删除角色、访问 <i>管理角色关系</i> 和 <i>职能指派</i> 操作。  有关细节，请参见第 17.1 节“浏览“角色编目””（第 203 页）。
	管理角色	允许用户创建、修改或删除角色。  有关细节，请参见 <i>管理角色</i> （第 204 页）。
	管理角色关系	可用于定义角色在较低与较高角色包容层次结构中的关系。此层次结构使用户可将较低级别角色包含的许可权限或资源分组进较高级别的角色，从而使许可权限的指派更加容易。  有关细节，请参见 <i>管理角色关系</i> （第 208 页）。
	管理职责分离	允许用户定义职责分离 (SoD) 限制。SoD 限制表示使两个角色相互排斥的一种规则。如果用户已是一个角色，则不能为第二个角色，除非允许该限制存在异常。可以定义是始终允许对该限制的异常，还是仅通过批准流程允许。  有关细节，请参见 <i>管理职责分离限制</i> （第 210 页）。
	配置角色子系统	允许用户为角色子系统指定管理设置。  有关细节，请参见 <i>配置角色子系统</i> （第 214 页）。

类别	操作	说明
角色报告	角色报告	使用户可创建和查看说明角色与角色指派当前状态的报告。 有关细节，请参见第 18.2 节“角色报告”（第 217 页）。
	SoD 报告	使用户可创建和查看说明职责分离限制、冲突与已批准异常的当前状态的报告。 有关细节，请参见第 18.3 节“SoD 报告”（第 220 页）。
	用户报告	使用户可创建和查看说明用户的角色成员资格与权利的当前状态的报告。 有关细节，请参见第 18.4 节“用户报告”（第 222 页）。

## 14.5 了解角色图例

在角色选项卡中使用的大多数页面的右上角都包含一个按钮，可以使用该按钮显示角色图例。要显示图例，请单击图 9-2 显示的图例按钮：

图 14-3 “图例”按钮



图例可简要说明整个角色选项卡中使用的图标。下图显示图例。

图 14-4 角色图例



下表详细说明图例中的图标：

表 14-3 “图例”图标

图标	说明
正在运行：处理中	表示一个角色请求仍在处理中。 在“查看请求状态”页面上显示。
待发批准	表示一个（职责分离异常或角色指派本身的）角色请求正在等待批准。 在“查看请求状态”页面上显示。

图标	说明
<i>已批准</i>	<p>表示一个角色请求已批准。如果检测到职责分离异常，也可将该状态用于表示已批准该异常。</p> <p>在“查看请求状态”页面上显示。</p>
<i>已完成：已供应</i>	<p>表示一个角色请求已批准且该角色已指派给收件人（用户、组或容器）。</p> <p>在“我的角色”、“角色指派”和“查看请求状态”页面上显示。</p>
<i>拒绝</i>	<p>表示一个角色请求已拒绝。如果检测到职责分离异常，也可将该状态用于表示已拒绝该异常。</p> <p>在“查看请求状态”页面上显示。</p>
<i>已终止</i>	<p>表示一个角色请求在完成之前即终止，原因是用户取消了请求或处理过程中出错。</p> <p>在“查看请求状态”页面上显示。</p>
<i>职能</i>	<p>表示对象为角色。</p> <p>在“我的角色”、“角色指派”和“查看请求状态”页面上显示。</p>
<i>较高级别关系</i>	<p>表示一个角色具有比当前所选角色更高的级别，这意味着该角色包含当前所选角色。</p> <p>在“管理角色关系”页面上显示。</p>
<i>较低级别关系</i>	<p>表示一个角色具有比当前所选角色更低的级别，这意味着当前所选角色包含该角色。</p> <p>在“管理角色关系”页面上显示。</p>
<i>用户</i>	<p>表示对象为用户。</p> <p>在“我的角色”和“角色指派”页面上显示。</p>
<i>组</i>	<p>表示对象为组。</p> <p>在“我的角色”和“角色指派”页面上显示。</p>
<i>容器</i>	<p>表示对象为容器。</p> <p>在“我的角色”和“角色指派”页面上显示。</p>
<i>直接指派</i>	<p>表示角色是直接指派给当前所选用户、组或容器的。</p> <p>在“我的角色”和“角色指派”页面上显示。</p>
<i>待发激活</i>	<p>表示一个角色请求已完成处理且得到批准，但其激活日期尚未来到。</p> <p>在“我的角色”和“查看请求状态”页面上显示。</p>

# 查看角色

本部分提供查看角色的说明。包括以下主题：

- ◆ 第 15.1 节“关于“我的角色”操作”（第 185 页）
- ◆ 第 15.2 节“查看已批准的角色请求”（第 185 页）

## 15.1 关于“我的角色”操作

Identity Manager User Application 中的角色选项卡包含一组称为我的角色的操作。我的角色操作可用于查看角色。

## 15.2 查看已批准的角色请求

我的角色操作可用于查看已批准角色的状态和细节。显示状态为“已供应”或“待发激活”的角色，而非尚未批准的角色请求。

要查看已批准的角色：

- 1 请单击我的角色操作列表中的我的角色。

User Application 将显示当前已鉴定用户的角色指派的当前状态。



下面说明了指派列表中的列：

- ◆ 指派列提供指派给当前用户的角色名称。
- ◆ 源列指示为用户进行角色指派的方式，如下所示：

源	说明
直接指派	表示此角色是直接指派给当前用户的。
角色 角色名称中的成员资格	表示用户是作为相关角色中的成员而收到此角色的。
组 组名中的成员资格	表示用户是作为组中的成员而收到此角色的。
容器 容器名称中的成员资格	表示用户是作为容器中的成员而收到此角色的。

- ◆ 有效日期列显示指派生效的日期。如果未显示任何日期，则指派一经请求即立即生效。

- ◆ *失效日期*列显示指派失效的日期。如果未显示任何日期，则指派保持有效的时间无限期。
- ◆ *状态*列显示指派是否已授予：

状态	说明
已供应	已批准（如果需要）且已激活。
待发激活	已批准（如果需要）但尚未激活，因为该角色指派的有效日期尚未到来。

2 可以如下所示过滤指派列表：

- 2a** 要仅查看以特定字符串开始的指派，请参见*过滤数据*（第 27 页），以获取有关在*指派*框中输入的内容的信息。
- 2b** 要仅查看直接指派给该用户的角色，请选中*直接*框。
- 2c** 要仅查看用户通过角色关系或者作为组或容器的成员收到的已指派角色，请选中*间接*框。
- 2d** 要对显示应用指定的过滤准则，请单击*过滤器*。

**注释：**过滤不会自动执行。必须单击*过滤器*按钮，才能应用准则。

**2e** 要清除当前指定的过滤准则，请单击*重设置*。

- 3** 要设置每页显示的指派的最大数量，请在*每页最大行数*下拉列表中选择一个数字。
- 4** 要查看特定角色指派的细节，请在*指派*列中单击指派名称并向下滚动，直到显示“指派细节”组框。

**指派细节**

**所选角色:** 护士

**初始请求说明:** adasd

**有效日期:** 2008-01-18 08:21:58 上午

**失效日期:** 不失效

# 作出角色指派

本部分提供作出角色指派的说明。包括以下主题：

- ◆ 第 16.1 节“关于角色指派操作”（第 187 页）
- ◆ 第 16.2 节“指派角色”（第 187 页）
- ◆ 第 16.3 节“检查请求的状态”（第 195 页）

## 16.1 关于角色指派操作

Identity Manager User Application 中的角色选项卡包含一组称为角色指派的操作。角色指派操作使用户能够作出角色指派请求和检查所作请求的状态。

## 16.2 指派角色

角色指派操作使用户可请求角色指派。“角色模块管理员”、“角色管理者”和不是特别指派给任何已安装系统角色的其他已鉴定用户可执行此操作。

- ◆ “角色模块管理员”可以请求将用户、组和容器指派给角色。“角色模块管理员”在该目录内不受范围限制。
- ◆ “角色管理者”可以请求将用户、组和容器指派给具有浏览权限的角色。
- ◆ 其他已鉴定用户可以请求指派给具有浏览权限的角色。

### 16.2.1 将用户、组和容器指派给角色

要请求将一个或多个用户、组或容器指派给一个角色：

- 1 单击角色指派操作列表中的角色指派。
- 2 单击希望如何查看指派？下的角色图标。



- 3 选择要将用户、组或容器指派到的角色。

使用对象选择器或显示历史工具选择角色。有关使用对象选择器和显示历史工具的细节，请参见第 1.4.4 节“常用用户操作”（第 24 页）。

User Application 将显示所选角色指派的当前状态。



下面说明了指派列表中的列：

- ◆ *指派*列提供指派给当前所选角色的对象名称。
- ◆ *角色来源*列表示将对象指派给角色的方式，如下所示：

源	说明
角色关系	表示此指派提供角色关系。“指派”列中的名称为相关角色的名称。
指派给角色的用户	表示“指派”列中指定的用户之前已指派给当前所选角色。
指派给角色的组	表示“指派”列中指定的组之前已指派给当前所选角色。
指派给角色的容器	表示“指派”列中指定的容器之前已指派给当前所选角色。

- ◆ *有效日期*列显示指派生效的日期。如果未显示任何日期，则指派一经请求即立即生效。
- ◆ *失效日期*列显示指派失效的日期。如果未显示任何日期，则指派保持有效的时间无限期。
- ◆ *状态*列显示指派是否已授予：

状态	说明
已供应	已批准（如果需要）且已激活。

4 可以如下所示过滤指派列表：

- 4a 要仅查看这些指派，请参见[过滤数据（第 27 页）](#)以获取有关在*指派*框中输入的信息。
- 4b 要仅查看用户指派，请选中*用户*框。
- 4c 要仅查看组指派，请选中*组*框。
- 4d 要仅查看容器指派，请选中*容器*框。

- 4e 要仅查看角色关系，请选中 *角色框*。
  - 4f 要对显示应用指定的过滤准则，请单击 *过滤器*。
  - 4g 要清除当前指定的过滤准则，请单击 *重设置*。
  - 5 要设置每页显示的指派的最大数量，请在 *每页最大行数* 下拉列表中选择 一个数字。
  - 6 要创建新的指派，请单击 *新指派*。
- 在 *指派细节* 组框中指定指派的细节。

- ◆ 在 *指派类型* 下拉列表中，选择 *用户*、*组* 或 *容器*，表示要将何种类型的对象指派给当前所选角色。
- ◆ 在 *选择用户* 字段中，指定要指派的用户。

---

**注释：**如果选择 *组* 作为指派类型，则用户界面将显示 *选择组* 字段。如果选择 *容器*，则显示 *选择容器* 字段。

---

- ◆ 在 *初始请求说明* 字段中，输入说明指派请求的理由的文本。
- ◆ 在 *有效日期* 字段中，指定希望指派生效的日期。可以使用“日历”控件来选择日期。
- ◆ 在 *失效日期* 字段中，表示是否希望指派具有失效日期。如果想让指派无限期保持有效，请选择 *不失效*。如果要定义失效日期，请选择 *指定失效* 并使用“日历”控件来选择日期。
- ◆ 单击 *提交* 以提交角色指派请求。

---

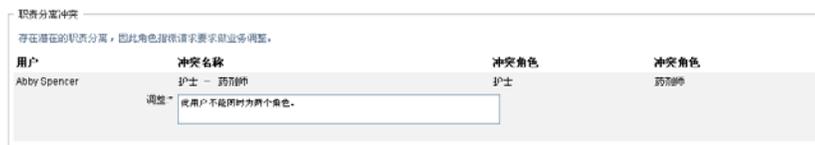
**注释：***角色指派* 操作可用于查看与当前所选角色有关的角色，但不允许创建角色关系。要创建角色关系，需使用 *管理角色关系* 操作。

---

如果将一个角色指派给一个或多个用户时将发生职责分离冲突，用户界面将在页面底部显示 *职责分离冲突* 框。在这种情况下，需要为角色指派提供业务调整。

提供调整：

- 1 在 *调整* 字段中输入说明，解释这种情况下需要职责分离限制异常的原因。




---

**注释：**以下情况无需提供调整：新角色指派与用户通过角色关系或组或容器中的成员资格间接获得的现有指派之间的冲突。如果已将用户间接添加到一个角色，但是检测到存在潜在的职责分离冲突，则 *User Application* 允许添加新指派，并记录该违例以进行报告和审计。如果需要，角色管理员可通过重新定义角色来更正违例。

---

## 16.2.2 将角色指派给一个用户

要请求将一个或多个角色指派给一个用户：

- 1 单击 *角色指派* 操作列表中的 *角色指派*。
- 2 单击 *希望如何查看指派？* 下的 *用户* 图标。



### 3 选择要指派一个或多个角色的用户。

使用 *对象选择器* 或 *显示历史* 工具选择用户。有关使用 *对象选择器* 和 *显示历史* 工具的细节，请参见 [使用“对象选择器”按钮进行搜索（第 26 页）](#)。

User Application 将显示所选用户指派的当前状态。



下面说明了指派列表中的列：

- ◆ *指派*列提供指派给当前所选用户的角色名称。
- ◆ *来源*列表示角色是如何指派给用户的，如下所示：

源	说明
直接指派	表示此角色是直接指派给当前所选用户的。
角色 <i>角色名称</i> 中的成员资格	表示用户是作为相关角色中的成员而收到此角色的。
组 <i>组名</i> 中的成员资格	表示用户是作为组中的成员而收到此角色的。
容器 <i>容器名称</i> 中的成员资格	表示用户是作为容器中的成员而收到此角色的。

- ◆ *有效日期*列显示指派生效的日期。如果未显示任何日期，则指派一经请求即立即生效。
- ◆ *失效日期*列显示指派失效的日期。如果未显示任何日期，则指派保持有效的时间无限期。
- ◆ *状态*列显示指派是否已授予和供应：

状态	说明
已供应	已批准（如果需要）且已激活。

4 可以如下所示过滤指派列表：

- 4a 要仅查看以特定字符串开始的指派，请参见[过滤数据（第 27 页）](#)，以获取有关在指派框中输入的内容的信息。
- 4b 要仅查看直接指派给该用户的指派，请选中 *直接框*。
- 4c 要仅查看间接指派的指派，请选中 *间接框*。间接指派是用户通过角色关系或作为组或容器中的成员而收到的指派。
- 4d 要对显示应用指定的过滤准则，请单击 *过滤器*。
- 4e 要清除当前指定的过滤准则，请单击 *重置*。

5 要设置每页显示的指派的最大数量，请在 *每页最大行数* 下拉列表中选择 一个数字。

6 要创建新的指派，请单击 *新指派*。

在 *指派细节* 组框中指定指派的细节。

- ◆ 在 *选择角色* 字段中，指定要指派的角色。
- ◆ 在 *初始请求说明* 字段中，输入说明指派请求的理由的文本。
- ◆ 在 *有效日期* 字段中，指定希望指派生效的日期。可以使用“日历”控件来选择日期。
- ◆ 在 *失效日期* 字段中，表示是否希望指派具有失效日期。如果想让指派无限期保持有效，请选择 *不失效*。如果要定义失效日期，请选择 *指定失效* 并使用“日历”控件来选择日期。
- ◆ 单击 *提交* 以提交角色指派请求。

如果将一个角色指派给当前所选用户时将发生职责分离冲突，用户界面将在页面底部显示 *职责分离冲突框*。在这种情况下，需要为角色指派提供业务调整。

提供调整：

1 在 *调整* 字段中输入说明，解释这种情况下需要职责分离限制异常的原因。

**间接角色指派与 SoD 冲突** 以下情况无需提供调整：新角色指派与用户通过角色关系或组或容器中的成员资格间接获得的现有指派之间的冲突。如果已将用户间接添加到一个角色，但是检测到存在潜在的职责分离冲突，则 User Application 允许添加新指派，并记录该违例以进行报告和审计。如果需要，角色管理员可通过重新定义角色来更正违例。

### 16.2.3 将角色指派给一个组

请求将一个或多个角色指派给一个组：

- 1 单击 *角色指派* 操作列表中的 *角色指派*。
- 2 单击 *希望如何查看指派？* 下的 *组* 图标。

### 3 选择要指派一个或多个角色的组。

使用 *对象选择器* 或 *显示历史* 工具选择组。有关使用 *对象选择器* 和 *显示历史* 工具的细节，请参见使用“*对象选择器*”按钮进行搜索（第 26 页）。

User Application 将显示所选组指派的当前状态。



下面说明了指派列表中的列：

- ◆ *指派*列提供指派给当前所选组的角色名称。
- ◆ *来源*列表示角色是如何指派给组的，如下所示：

源	说明
直接指派	表示此角色是直接指派给当前所选组的。
角色 <i>角色名称</i> 中的成员资格	表示为组提供此角色是由于该组已指派给相关角色。

- ◆ *有效日期*列显示指派生效的日期。如果未显示任何日期，则指派一经请求即立即生效。
- ◆ *失效日期*列显示指派失效的日期。如果未显示任何日期，则指派保持有效的时间无限期。
- ◆ *状态*列显示指派是否已授予和供应：

状态	说明
已供应	已批准（如果需要）且已激活。

### 4 可以如下所示过滤指派列表：

- 4a 要仅查看以特定字符串开始的指派，请参见 *过滤数据*（第 27 页），以获取有关在 *指派* 框中输入的内容的信息。
- 4b 要仅查看直接指派给该组的指派，请选中 *直接* 框。

- 4c 要仅查看间接指派的指派，请选中 *间接框*。间接指派是组通过角色关系收到的指派。
- 4d 要对显示应用指定的过滤准则，请单击 *过滤器*。
- 4e 要清除当前指定的过滤准则，请单击 *重设置*。
- 5 要设置每页显示的指派的最大数量，请在 *每页最大行数* 下拉列表中选择 一个数字。
- 6 要创建新的指派，请单击 *新指派*。  
在 *指派细节* 组框中指定指派的细节。
  - ◆ 在 *选择角色* 字段中，指定要指派的角色。
  - ◆ 在 *初始请求说明* 字段中，输入说明指派请求的理由的文本。
  - ◆ 在 *有效日期* 字段中，指定希望指派生效的日期。可以使用“日历”控件来选择日期。
  - ◆ 在 *失效日期* 字段中，表示是否希望指派具有失效日期。如果想让指派无限期保持有效，请选择 *不失效*。如果要定义失效日期，请选择 *指定失效* 并使用“日历”控件来选择日期。
  - ◆ 单击 *提交* 以提交角色指派请求。

## 16.2.4 将角色指派给一个容器

请求将一个或多个角色指派给一个容器：

- 1 单击 *角色指派* 操作列表中的 *角色指派*。
- 2 单击 *希望如何查看指派?* 下的 *容器* 图标。



- 3 选择要指派一个或多个角色的容器。  
使用 *对象选择器* 或 *显示历史* 工具选择容器。有关使用 *对象选择器* 和 *显示历史* 工具的细节，请参见 [使用“对象选择器”按钮进行搜索（第 26 页）](#)。  
User Application 将显示所选容器指派的当前状态。



下面说明了指派列表中的列：

- ◆ *指派*列提供指派给当前所选容器的角色名称。
- ◆ *来源*列表示角色是如何指派给容器的，如下所示：

源	说明
直接指派	表示此角色是直接指派给当前所选容器的。
角色 <i>角色名称</i> 中的成员资格	表示为容器提供此角色是由于该容器已指派给相关角色。
容器 <i>容器名称</i> 中的成员资格	表示为容器指派此角色是由于该容器已嵌套到一个更高级别的容器内。

- ◆ *有效日期*列显示指派生效的日期。如果未显示任何日期，则指派一经请求即立即生效。
- ◆ *失效日期*列显示指派失效的日期。如果未显示任何日期，则指派保持有效的时间无限期。
- ◆ *状态*列显示指派是否已授予和供应：

状态	说明
已供应	已批准（如果需要）且已激活。

4 可以如下所示过滤指派列表：

- 4a 要仅查看以特定字符串开始的指派，请参见 [过滤数据](#)（第 27 页），以获取有关在 *指派* 框中输入的内容的信息。
- 4b 要仅查看直接指派给容器的指派，请选择 *直接* 框。
- 4c 要仅查看间接指派的指派，请选中 *间接* 框。间接指派是指容器通过角色关系接收到的指派。
- 4d 要对显示应用指定的过滤准则，请单击 *过滤器*。
- 4e 要清除当前指定的过滤准则，请单击 *重置*。

5 要设置每页显示的指派的最大数量，请在 *每页最大行数* 下拉列表中选择 一个数字。

6 要创建新的指派，请单击 *新指派*。

在 *指派细节* 组框中指定指派的细节。

- ◆ 在 *选择角色* 字段中，指定要指派的角色。
- ◆ 在 *初始请求说明* 字段中，输入说明指派请求的理由的文本。
- ◆ 在 *有效日期* 字段中，指定希望指派生效的日期。可以使用“日历”控件来选择日期。
- ◆ 在 *失效日期* 字段中，表示是否希望指派具有失效日期。如果想让指派无限期保持有效，请选择 *不失效*。如果要定义失效日期，请选择 *指定失效* 并使用“日历”控件来选择日期。
- ◆ 要将此角色指派传送给所有子容器中的用户，请选择 *将角色指派应用到子容器*。
- ◆ 单击 *提交* 以提交角色指派请求。

## 16.3 检查请求的状态

通过 *查看请求状态* 操作，可以查看角色请求的状态，包括已直接发出的请求和您所属容器组的角色指派请求。可通过该操作查看每个请求的当前状态。此外，如果改变主意且不需要完成请求，则可通过该操作选择收回尚未完成或终止的请求。

*查看请求状态* 操作将显示所有角色指派请求，包括正在运行、待发批准、已批准、完成、拒绝或终止的请求。*查看请求状态* 操作还将显示要通过 *管理角色关系* 操作创建角色关系的请求。

在“查看请求状态”页面上的所见及所为取决于您的安全角色，如下所示：

**表 16-1** 每个安全角色的功能

安全角色	功能
角色模块管理员	“角色模块管理员”可在“查看请求状态”页面上执行以下功能： <ul style="list-style-type: none"><li>◆ 查看所有角色指派请求。</li><li>◆ 对基于状态和用户的请求进行过滤。当“角色模块管理员”根据“用户”过滤请求时，结果将显示指定用户为请求者或收件人的请求。“角色模块管理员”不能使用基于请求者或收件人的过滤请求控件。</li><li>◆ 如果角色指派请求仍然处于可收回状态（尚未批准、拒绝、完成或终止），则可以收回所有这些请求。</li></ul>

安全角色	功能
角色管理者	<p>角色管理者可在“查看请求状态”页面上执行以下功能：</p> <ul style="list-style-type: none"> <li>◆ 查看要求用户具有角色浏览权限、以及用户为请求者或收件人的请求的状态。</li> <li>◆ 对基于状态和用户的请求进行过滤。当“角色管理者”根据“用户”过滤请求时，结果将显示指定用户为请求者或收件人的请求。“角色管理者”不能使用基于请求者或收件人的过滤请求控件。</li> <li>◆ 收回用户、组和容器的用户具有角色和目标（用户、组或容器）对象目录浏览权限的请求。这些请求必须仍处于可收回状态（尚未批准、拒绝、完成或终止）。</li> </ul>
已鉴定用户	<p>登录到 User Application 的非系统角色成员的典型用户可以在“查看请求状态”页面上执行以下任何功能：</p> <ul style="list-style-type: none"> <li>◆ 查看用户为请求者或收件人的请求的状态。</li> <li>◆ 对基于状态以及请求者或收件人的请求进行过滤。由于已鉴定用户仅能查看对其自身的请求，因此已鉴定用户不能使用基于用户的过滤请求控件。</li> <li>◆ 收回用户既是请求者又是收件人的请求。该请求必须仍处于可收回状态（尚未批准、拒绝、完成或终止），且用户必须具有角色浏览权限。</li> </ul>

**大结果集** 默认情况下，“查看请求状态”页最多可检索 10,000 个请求对象。如果尝试检索一个大结果集，您将看到一条提示已达到限值的讯息。在这种情况下，应缩小搜索范围（例如，通过指定某个特定用户或状态）以限制返回到结果集中的对象数。请注意，在将过滤器应用到一个角色名称中时，该过滤器将限制您所看到的内容及其顺序，而非返回的对象数。

查看角色请求：

- 1 单击 *角色指派* 操作列表中的 *查看请求状态*。

User Application 将显示当前已鉴定用户的角色请求的当前状态。



角色请求列表中的列如下所示：

- ◆ *角色名称*列提供了为该请求指定的角色名称。
- ◆ *请求者*列标识发出请求的用户。
- ◆ *收件人*列标识批准请求时，将接收角色的用户、组或容器。在角色关系中，*收件人*列显示了与在*角色名称*列中指定的角色相关的角色名称。
- ◆ *状态*列显示了该请求的详细状态和表示状态摘要的图标。“状态摘要”显示了该请求的一般状态，可从“过滤器”菜单中选择，以在搜索处于特定状态的请求时缩小结果的范围：

状态摘要图标	详细状态	说明
	新请求	表明这是一个当前正在处理的新请求。  此状态下的请求可以收回。
	SoD 批准开始 - 待发	表明角色服务驱动程序正在随“SoD 批准开始 - 暂停”条件尝试重启职责分离请求批准进程。  此状态下的请求可以收回。

状态摘要图标	详细状态	说明
 正在运行：正在处理	SoD 批准开始 - 暂停	<p>表明角色服务驱动程序无法启动职责分离批准进程且该进程已暂时停止。</p> <p>当角色服务驱动程序尝试启动一个工作流程却又无法进行时（例如，在 User Application 已关闭或不可用时），请求将先转换到待发重试状态并等待至少一分钟，然后才会转换到将触发驱动程序以便重新尝试启动该工作流程的重试状态（SoD 批准开始 - 待发状态）。对于那些不依赖于工作流程的请求，这些状态可以防止它们处于由无法启动的工作流程阻止的请求之后时被备份。</p> <p>如果请求显示此状态超过一定时间段，请确保 User Application 仍在运行。如果它正在运行，请检查指定给角色服务驱动程序的连接参数是否正确。</p> <p>此状态下的请求可以收回。</p>
 正在运行：正在处理	批准开始 - 待发	<p>表明角色服务驱动程序正在随“批准开始 - 暂停”条件尝试重新启动请求批准进程。</p> <p>此状态下的请求可以收回。</p>
 正在运行：正在处理	批准开始 - 暂停	<p>表明已为请求启动批准进程，但该进程已暂停。</p> <p>当角色服务驱动程序尝试启动一个工作流程却又无法进行时（例如，在 User Application 已关闭或不可用时），请求将先转换到待发重试状态并等待至少一分钟，然后才会转换到将触发驱动程序以便重新尝试启动该工作流程的重试状态（批准开始 - 待发状态）。对于那些不依赖于工作流程的请求，这些状态可以防止它们处于由无法启动的工作流程阻止的请求之后时被备份。</p> <p>如果请求显示此状态超过一定时间段，请确保 User Application 仍在运行。如果它正在运行，请检查指定给角色服务驱动程序的连接参数是否正确。</p> <p>此状态下的请求可以收回。</p>
 待发批准	SoD 异常 - 批准待发	<p>表明职责分离批准进程已开始，正在等待一个或多个批准。</p> <p>此状态下的请求可以收回。</p>

状态摘要图标	详细状态	说明
 待发批准	批准待发	<p>表明请求的批准进程已开始，正在等待一个或多个批准。</p> <p>此状态下的请求可以收回。</p>
 已批准	SoD 异常 - 已批准	<p>表明此请求的职责分离异常已批准。</p> <p>此状态下的请求可以收回。</p>
 已批准	已批准	<p>表明请求已批准。</p> <p>此状态下的请求可以收回。</p>
 已批准	供应	<p>表明请求已批准（如果要求批准），且已达到角色指派的激活时间。角色服务驱动程序正在授权进行角色指派。</p> <p>您不能收回此状态下的请求。</p>
 待发激活	待发激活	<p>指示已批准请求，但角色指派的激活时间仍未到达。待发激活没有聚集类别或摘要状态图标。这表示您不能按待发激活状态来过滤请求列表。</p> <p>此状态下的请求可以收回。</p>
 已拒绝	SoD 异常 - 已拒绝	<p>表明此请求的职责分离异常已被拒绝。</p> <p>您不能收回此状态下的请求。</p>
 已拒绝	拒绝	<p>表明此请求已被拒绝。</p> <p>您不能收回此状态下的请求。</p>
 已完成：已供应	已供应	<p>表明请求已批准（如果要求批准），且已授权进行角色指派。</p> <p>您不能收回此状态下的请求。</p>
 已完成：已供应	清理	<p>表明请求已处理，角色服务驱动程序正在去除为该请求创建的内部对象。</p> <p>您不能收回此状态下的请求。</p>
 已终止	正在取消	<p>表明角色服务驱动程序由于用户操作正在取消请求。</p> <p>您不能收回此状态下的请求。</p>
 已终止	已取消	<p>表明请求已由用户操作取消。</p> <p>您不能收回此状态下的请求。</p>

状态摘要图标	详细状态	说明
 已终止	供应错误	<p>表明在供应（授予）或取回（撤销）角色指派过程中出现了错误。</p> <p>如果其中任何一项处于活动状态，则供应错误的准确错误讯息将写入跟踪或审计日志中。如果出现供应错误，请检查跟踪或审计日志以查看该错误讯息是否指明一个严重问题必须得到修复。</p> <p>您不能收回此状态下的请求。</p>

**注释：**如果角色服务驱动程序所在服务器上的系统时钟与正在运行 User Application 的服务器上的系统时钟不同步，“查看请求状态”和“角色指派”页面上的请求状态可能会不同。例如，如果请求了一个不需要批准的角色指派，可能将看到“查看请求状态”页面上的状态显示为“已供应”，但“角色指派”页面上的状态显示“待发激活”。如果等待一分钟左右，可能将看到“角色指派”页面上的状态更改为“已供应”。要确保整个 User Application 正确显示状态，请检查系统时钟以确保同步正确。

- ◆ *请求日期*列显示了发出请求的日期。
- ◆ *初始请求说明*列显示了请求者在发出请求时提供的说明。

2 您可以对请求列表进行过滤，如下所示：

- 2a 要仅查看以特定字符串开始的指派，请参见[过滤数据（第 27 页）](#)以获得有关应在角色名称框中键入的内容的信息。
- 2b 要仅查看应用于特定用户的请求，请使用 *对象选择器*或 *显示历史*工具来选中该用户。要查看您自己的请求，需从“用户”列表中将自已选中。有关使用 *对象选择器*和 *显示历史*工具的细节，请参见[使用“对象选择器”按钮进行搜索（第 26 页）](#)。

**注释：**如果登录的用户不是角色模块管理员或角色管理者，则“用户”控件将不可用。

2c 要查看带有特定状态摘要的角色请求，请在 *状态*下拉列表中选择该状态。

状态	说明
所有	包含所有请求。
正在运行	包含已经开始且当前正在处理的请求。
待发批准	包含正在等待职责分离异常或角色指派本身批准的请求。
已批准	包含已批准的请求和已检测到并已批准职责分离异常的请求。
已完成	包含已批准的请求和将角色指派给收件人（用户、组或容器）的位置。
拒绝	包含已拒绝的请求和已检测到并已拒绝职责分离异常的请求。

状态	说明
已终止	包含在完成之前由于用户取消操作或处理过程中出现错误而终止的请求。

**2d** 要仅查看您作为请求者的请求，请选中 *请求者* 框。

**注释：**如果当前用户是角色模块管理员或角色管理者，*请求者* 控件将不可用。

**2e** 要仅查看您作为收件人的请求，请选中 *收件人* 框。

**注释：**如果登录的用户是角色模块管理员或角色管理者，*收件人* 控件将不可用。

**2f** 要对显示应用指定的过滤准则，请单击 *过滤器*。

**2g** 要清除当前指定的过滤准则，请单击 *重设置*。

**3** 要设置每个页面上显示的指派的最大数量，请在 *每页最大行数* 下拉列表中选择一个数字。

**4** 要对请求列表排序，请单击包含想要排序的数据的列标题。

如果多个角色指派请求共享一个 *通用请求 ID*，您可能希望按照“初始请求说明”对数据进行排序以同时查看相关的请求集。“通用请求 ID”是一个与同时请求的角色指派集相关联的内部标识符（仅在“请求细节”组框中显示）。以下是角色指派集共享“通用请求 ID”的一些情况：

- ◆ 单个请求将多个角色指派给单个用户。
- ◆ 单个请求将单个角色指派给多个用户。当请求者将一个角色指派给一个组或容器时，可能出现这种情况。

当角色指派集共享一个“通用请求 ID”时，用户可以单独收回每一个指派。此外，还可独立地批准或拒绝每一个角色指派。

**5** 要查看特定请求的细节，请单击 *状态* 列中的“状态”并向下滑动，直到显示“请求细节”组框。

请求细节

状态:	🟢 待发激活	请求操作:	将角色添加到用户
角色:	医生	收件人:	chjp.nano
请求者:	主要	请求日期:	2008-01-16
有效日期:	2008-01-28	失效日期:	
初始请求说明:	trrw	通用请求 ID:	b49f6a6b3a843318439c84cdeb9c269

“状态”字段显示了请求的状态以及状态摘要图标和说明该图标的文本。该图标（及相关文本）提供了快速查看状态的便捷方法。下表显示了各种状态代码映射到状态图标的方式：

状态图标	相关状态编码
正在运行：正在处理	<ul style="list-style-type: none"> <li>◆ 新请求</li> <li>◆ SoD 批准开始 - 待发</li> <li>◆ SoD 批准开始 - 暂停</li> <li>◆ 批准开始 - 待发</li> <li>◆ 批准开始 - 暂停</li> </ul>
待发批准	<ul style="list-style-type: none"> <li>◆ SoD 异常 - 批准待发</li> <li>◆ 批准待发</li> </ul>
已批准	<ul style="list-style-type: none"> <li>◆ SoD 异常 - 已批准</li> <li>◆ 已批准</li> <li>◆ 待发激活</li> <li>◆ 供应</li> </ul>
待发激活	<ul style="list-style-type: none"> <li>◆ 待发激活</li> </ul>
拒绝	<ul style="list-style-type: none"> <li>◆ SoD 异常 - 已拒绝</li> <li>◆ 拒绝</li> </ul>
已完成：已供应	<ul style="list-style-type: none"> <li>◆ 已供应</li> <li>◆ 清理</li> </ul>
已终止	<ul style="list-style-type: none"> <li>◆ 正在取消</li> <li>◆ 已取消</li> <li>◆ 供应错误</li> </ul>

**6** 要收回请求，请单击 *收回请求*。

如果该请求已完成或终止，*收回请求*按钮将禁用。

如果某个请求与一组相关请求共享一个“通用请求 ID”，则可以单独收回每一个角色指派。

# 管理角色

此部分介绍了角色管理分类操作的使用方法。它包含以下部分：

- ◆ 第 17.1 节“浏览“角色编目””（第 203 页）
- ◆ 第 17.2 节“管理角色”（第 204 页）
- ◆ 第 17.3 节“管理角色关系”（第 208 页）
- ◆ 第 17.4 节“管理职责分离限制”（第 210 页）
- ◆ 第 17.5 节“配置角色子系统”（第 214 页）

## 17.1 浏览“角色编目”

浏览“角色编目”：

- 1 请单击角色管理操作列表中的浏览角色编目。

User Application 将在“角色编目”中显示当前角色列表。



下面说明了指派列表中的列：

- ◆ **角色名称**列提供了编目中每个角色的名称。
- ◆ **级别**列指出了编目中角色的级别。默认情况下，此编目支持带以下名称的三个级别：

级别	说明
业务角色	角色层次结构中的最高级别。
IT 角色	角色层次结构中的中间级别。
许可权限角色	角色层次结构中的最低级别。

- ◆ **类别列**列出了与该角色相关联的类别。通过“类别”，一项业务可对“角色编目”中的角色进行组织。在角色与类别关联之后，可在浏览编目时将其用作过滤器。
- ◆ 通过 **操作列**可快速访问其他页面。
  - 单击  可转至 **管理角色关系**页。
  - 单击  可转至 **角色指派**页。
  - 单击  可转至 **管理角色**页。
  - 单击  可删除相应行中的角色。

2 可以过滤角色列表，如下所示：

- 2a** 要仅查看以特殊字符串开始的指派，请参见 **过滤数据**（第 27 页）以获得有关应在 **角色名称**框中输入的内容的信息。
- 2b** 要查看层次结构中特定级别的角色，请在 **级别**框中选择所需级别。
- 2c** 要查看已与某个特定类别相关联的角色，请在 **类别**框中选择所需类别。
- 2d** 要对显示应用指定的过滤准则，请单击 **过滤器**。
- 2e** 要清除当前指定的过滤准则，请单击 **重设置**。

3 要设置每页显示的指派的**最大数量**，请在 **每页最大行数**下拉列表中选择**一个数字**。

4 要查看某个特定角色的**细节**，请在 **角色名称**列中单击该角色名称。

User Application 将转至 **管理角色**页，可在此页面查看该角色的**细节**或进行更改。

## 17.2 管理角色

可以通过 Identity Manager 用户界面的 **角色**选项卡上的 **管理角色**操作创建新角色或者修改或删除现有角色。

- ◆ [第 17.2.1 节“创建新角色”](#)（第 205 页）
- ◆ [第 17.2.2 节“修改或删除现有角色”](#)（第 205 页）
- ◆ [第 17.2.3 节“角色属性”](#)（第 206 页）

---

**注释：**不能使用此操作创建新的或删除现有的系统角色。但可将其用于修改系统角色。

---

在此页面上的所见及所为取决于您的安全角色，如 [表 17-1](#) 所示。

**表 17-1** 安全角色功能

安全角色	功能
角色模块管理员	角色模块管理员可以： <ul style="list-style-type: none"> <li>◆ 在所有容器中创建新角色。</li> <li>◆ 修改所有现有角色。</li> <li>◆ 删除所有现有角色（系统角色除外）。</li> </ul>

安全角色	功能
角色管理者	<p>角色管理者可以：</p> <ul style="list-style-type: none"> <li>◆ 在所有容器（包括不具有浏览权限的容器）中创建新角色。在角色创建时将把所有必需权限授予用户。</li> <li>◆ 仅修改其具有浏览权限的角色。</li> <li>◆ 仅删除其具有浏览权限的角色。</li> </ul> <p>该用户界面仅显示角色管理者具有浏览权限的级别和容器。如果管理者对某一特定级别没有浏览权限，但对子容器具有权限，则该界面将显示该级别。如果管理者对子容器具有浏览权限，但对父容器没有浏览权限，则父容器可见，但是不可选择。</p> <p>角色管理者尝试创建新角色时，用户界面将校验管理者是否对所选级别和容器具有权限。如果用户不具有必需的权限，该界面将禁用“新建”按钮并显示一条错误讯息。</p>

## 17.2.1 创建新角色

- 1 单击 *角色管理* 操作列表中的 *管理角色*。
- 2 单击“新建”。

User Application 将提示您在“管理角色”页面的 *新建角色细节* 部分提供 *角色名称*。有关该部分中每个字段的详细信息，请参见表 17-2“*角色细节*”在第 207 页。

新建角色细节

输入新的角色细节。角色容器是在储存新角色的角色级别下的可选目录容器，角色容器可用于确保有权使用角色。

角色名称：\*

角色说明：\*

角色级别：业务角色

角色容器：

角色拥有者：

角色类别：系统角色 默认值

- 3 浏览到 *批准细节*，并按照表 17-3“*批准细节*”在第 207 页 中所述的方法完成这些字段。
- 4 单击 *保存* 以永久保存更改。

## 17.2.2 修改或删除现有角色

- 1 单击 *角色管理* 操作列表中的 *管理角色*。



- 2 要找到想要修改其细节的角色，请使用 *对象选择器* 或 *显示历史* 工具来选择限制。有关使用 *对象选择器* 和 *显示历史* 工具的细节，请参见 [常用用户操作（第 24 页）](#)。
- 3 在从列表中选择所需角色时，查找页面将关闭并显示所选角色的 *角色细节* 和 *批准细节*。“管理角色”页面将显示当前在 *角色细节* 部分所选角色的名称。




---

**提示：**通过 *管理角色关系* 链接可以快速访问 *管理角色关系* 页面。如果选择了一个角色，将显示所选角色的内容，以便进行编辑。

---

- 4 要删除当前所选角色，请单击 *去除*。  
有关可以修改的角色细节的详细信息，请参见 [表 17-2“角色细节”](#) 在第 207 页。  
有关可以修改的批准细节的详细信息，请参见 [表 17-3“批准细节”](#) 在第 207 页。
- 5 完成更改后，请单击 *保存*。

### 17.2.3 角色属性

- ◆ [角色细节属性（第 207 页）](#)
- ◆ [批准细节属性（第 207 页）](#)

## 角色细节属性

表 17-2 角色细节

字段	说明
职能名称	<p>当角色名称显示在 User Application 中时使用的文本。创建角色时，不得在角色名称中包含以下字符：</p> <p>&lt; &gt; , ; \ " + # = /   &amp; *</p> <p>可以将此名称翻译为 User Application 所支持的任意一种语言。有关详细信息，请参见表 1-1“常用按钮”在第 25 页。</p>
角色说明	<p>当角色说明显示在 User Application 中时使用的文本。与“角色名称”一样，可以将其翻译为 User Application 所支持的任意一种语言。有关详细信息，请参见表 1-1“常用按钮”在第 25 页。</p>
角色级别	<p>（修改角色时为只读。）从下拉列表中选择一个角色级别。</p> <p>使用 Designer for Identity Manager 角色配置编辑器定义角色级别。有关“角色级别”的详细信息，请参见第 14.1 节“关于“角色”选项卡”（第 175 页）。</p>
角色容器	<p>（修改角色时为只读。）驱动程序中角色对象的位置。角色容器处于角色级别中。User application 仅显示所选的角色级别中的角色容器。可以在角色级别中直接创建角色，也可以在角色级别内部的容器中创建角色。可以选择指定角色容器。</p>
角色拥有者	<p>指派为角色定义拥有者的用户。在对“角色编目”生成报告时，可以根据角色拥有者对报告进行过滤。角色拥有者不会自动具备管理角色定义的更改的授权。</p>
角色类别	<p>可用于为角色组织对角色进行分类。类别用于对角色列表进行过滤。类别是多选的。</p>

## 批准细节属性

表 17-3 批准细节

字段	说明
必需批准	<p>如果角色在请求时需要批准，且您希望批准过程执行标准角色指派批准定义，请选择是。</p> <p>如果角色在请求时不需要批准，请选择否。</p>
使用标准批准	<p>如果此角色使用了在角色子系统中指定的标准角色指派批准定义，请选择是。批准定义的名称将以只读方式显示在下面的角色指派批准定义中。</p> <p>必须选择批准类型（序列或规定数）以及有效批准者。</p> <p>如果选择否，将提示您输入自定义的“角色指派批准定义”的名称。</p>
角色指派批准定义	<p>请求角色时执行的供应请求定义的名称。如果使用标准批准的值为是，那么该值将从角色子系统配置设置中获得。如果该值为否，则必须选择要使用的自定义供应请求定义的名称。</p>

字段	说明
批准类型	<p>如果希望 <i>批准者</i> 列表中的所有用户都批准该角色，请选择 <i>序列</i>。将按照列表中显示的顺序对批准者进行逐个处理。</p> <p>如果希望 <i>批准者</i> 列表中一定百分比的用户批准该角色，请选择 <i>规定数</i>。当达到指定的用户百分比时，该批准完成。</p> <p>例如，如果希望列表中四个用户中的其中一个批准该条件，应指定“规定数”和“25%”。此外，如果四个批准者必须同时批准，也可以指定 100%。该值必须是介于 1 和 100 之间的整数。</p> <hr/> <p><b>提示：</b>“序列”和“规定数”字段中的悬浮文本对其行为进行了介绍。</p>
批准者	<p>如果应将角色批准任务指派给一个或多个用户，请选择 <i>用户</i>。如果应将角色批准任务指派给一个组，请选择 <i>组</i>。如果应将角色批准任务指派给一个角色，请选择 <i>角色</i>。</p> <p>要查找特定用户、组或角色，请使用 <i>对象选择器</i> 或 <i>历史</i> 按钮。要更改列表中的批准者顺序或去除某个批准者，请参见 <a href="#">第 1.4.4 节“常用用户操作”</a>（第 24 页）。</p>

## 17.3 管理角色关系

通过 Identity Manager 用户界面的 *角色* 选项卡上的 *管理角色关系* 操作，可以定义各个角色在较高和较低角色包容层次结构中的关联方式。通过此层次结构，可以将较低级别角色所包含的许可权限或资源分组进更容易指派许可权限的较高级别角色中。允许的关系为：

- ◆ 顶层级别角色（业务角色）可以包含较低级别角色。但不能由其他角色包含。如果选择了一个顶层级别角色，您只能在“角色关系”页面上添加一个“新建较低级别角色”关系。
- ◆ 中层级别角色（IT 角色）可以包含较低级别角色，并且它们也可以由较高级别角色包含。“角色关系”页面可用于添加“新建较低级别角色”或“新建较高级别角色”。
- ◆ 底层级别角色（许可权限角色）可以由较高级别角色包含，但它们不能包含其他底层级别角色。“角色关系”页面可用于仅添加一个“新建较高级别角色”。

### 17.3.1 创建与去除角色关系

- 1 单击 *角色管理* 操作组中的 *管理角色关系*。



**提示：**通过 [编辑角色细节](#) 链接可以快速访问 [管理角色](#) 页面。如果选择了一个角色，将显示所选角色的内容，以便进行编辑。

- 2 要找到想要添加或去除关系的角色，请按照第 1.4.4 节“常用用户操作”（第 24 页）中所述的方法使用 [对象选择器](#) 或 [显示历史](#) 工具。
- 3 选择角色。

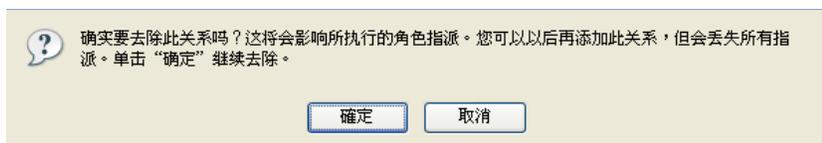
在本示例中，“角色”为 Nurse (West Campus)。由于此角色在角色层次结构中处于最高级别，用户界面将在 [所选角色的包含依据](#) 部分显示一条讯息。



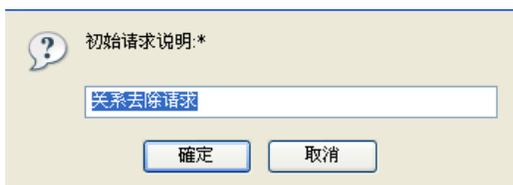
根据所选择的角色级别，您会看到其中一个按钮，或两个按钮均看到：

- ◆ [新建高级关系](#)
  - ◆ [新建低级关系](#)
- 4 要添加关系，请单击其中一个按钮并按照表 17-4 在第 210 页中所述的方法填写低级关系或高级关系细节。
  - 5 可以对高级和低级关系列表进行过滤，如下所示：
    - 5a 要仅查看以特定字符串开始的关系，请参见 [过滤数据](#)（第 27 页）以获得有关要在 [角色名称](#) 字段中输入的信息。
    - 5b 要查看特定级别的角色，请从 [级别](#) 列表框中选择。
    - 5c 要查看特定类别的角色，请从 [类别](#) 列表框中选择。
    - 5d 要对显示应用指定的过滤准则，请单击 [过滤器](#)。
    - 5e 要清除当前指定的过滤准则，请单击 [重设置](#)。
  - 6 单击 [提交](#) 以创建添加角色关系的请求。

转至 [查看请求状态](#) 页面可以检查该请求的状态。当状态为 [已供应](#) 时，角色关系已添加。
  - 7 去除关系：
    - 7a 请浏览到要去除的关系，然后单击 。将要求您确认是否要去除该关系。



**7b** 请单击 *确定* 继续执行去除操作，或单击 *取消* 返回到 *管理角色关系* 页面。将提示输入 *初始请求说明*。



默认文本为 *关系去除请求*，但可以根据需要进行修改。该文本在 *查看请求状态* 页面上显示。

**7c** 单击 *确定* 以提交去除请求。可以在 *查看请求状态* 页面上查看该请求的状态。*已供应* 状态表明关系已去除。

## 17.3.2 管理角色关系属性

表 17-4 角色关系属性

字段	说明
初始请求说明	该值出现在 <i>查看请求状态</i> 中。  可以使用该选项将由一个用户交互创建的多个请求分组，因为这些请求共享同一个通用请求 ID。
将角色添加到所选角色	单击 <i>新建低级关系</i> 时可用。  使用“对象选择器”或“历史”按钮可查找要添加到所选角色的较低级别角色。请参见 <a href="#">使用“对象选择器”按钮进行搜索（第 26 页）</a> 。
将所选角色添加到角色	单击 <i>新建高级关系</i> 时可用。  使用“对象选择器”或“历史”按钮可查找要添加到当前角色的较高级别角色。请参见 <a href="#">使用“对象选择器”按钮进行搜索（第 26 页）</a> 。

## 17.4 管理职责分离限制

Identity Manager 用户界面的 *角色* 选项卡上的 *管理职责分离* 允许您：

- ◆ 定义职责分离 (SoD) 限制（或规则）。
- ◆ 定义如何处理限制异常的请求。

SoD 限制表示一个使得两个同一级别的角色互斥的规则。如果用户已是一个角色，则不能为第二个角色，除非允许该限制存在异常。可以定义是始终允许对该限制的异常，还是仅通过批准流程允许。

- ◆ 第 17.4.1 节“创建新的职责分离限制”（第 211 页）
- ◆ 第 17.4.2 节“修改现有 SoD 限制”（第 211 页）
- ◆ 第 17.4.3 节“SoD 限制属性参照”（第 212 页）

页面访问“管理职责分离”页面可由角色管理员或安全专员访问。安全专员需要身份库中 SoDDef 容器的浏览权限，但不需要角色的浏览权限。

## 17.4.1 创建新的职责分离限制

- 1 单击角色管理操作列表中的管理职责分离。
- 2 单击“新建”。



- 3 浏览到新建职责分离限制细节。有关完成字段设置的信息，请参见表 17-5 在第 213 页。
- 4 浏览到批准细节部分。有关完成字段设置的信息，请参见表 17-6 在第 213 页。
- 5 单击保存以永久保存更改。

## 17.4.2 修改现有 SoD 限制

- 1 单击角色管理操作组中的管理职责分离。



- 2 要查看或修改现有 SoD 限制，请使用 *对象选择器* 或 *显示历史* 工具来选择限制。有关使用 *对象选择器* 和 *显示历史* 工具的细节，请参见使用“对象选择器”按钮进行搜索（第 26 页）。
- 3 从列表中选择所需的 SoD。查找页面关闭，并将显示所选 SoD 的 *职责分离限制细节* 和 *批准细节*。



- 4 有关填写字段的信息，请参见表 17-5“职责分离限制细节”在第 213 页 和表 17-6“批准细节”在第 213 页。
- 5 单击 *保存* 以永久保存更改。

### 17.4.3 SoD 限制属性参照

- ◆ 表 17-5“职责分离限制细节”在第 213 页
- ◆ 表 17-6“批准细节”在第 213 页

表 17-5 职责分离限制细节

字段	说明
SoD 限制名称	<p>限制的名称。它在报告中显示，且当用户请求限制例外时显示。创建限制时，不得在 <i>SoD 限制名称</i> 中包含以下字符：</p> <p>&lt; &gt; , ; \ " + # = /   &amp; *</p> <p>您可以用所支持的任意语言将其本地化，方法是单击 。</p> <p>此名称也可以在 Designer for Identity Manager 中的“SoD 编辑器”内提供。</p>
SoD 限制说明	<p>限制的说明。</p> <p>您可以用所支持的任意语言将其本地化，方法是单击 。</p> <p>此名称可以在 Designer for Identity Manager 中的“SoD 编辑器”内提供。</p>
冲突角色	<p>要定义限制的角色名称。角色定义了一组与一个或多个目标系统或应用程序相关的特权。</p> <p>在修改操作的过程中，该字段是只读的。</p>
冲突角色	<p>冲突角色的名称。单击 <i>浏览</i> 从可用角色中查找现有角色。</p> <p>在修改操作的过程中，该字段是只读的。</p>

**注释：**指定冲突的两个角色十分重要。而指定冲突角色的顺序则无关紧要。

表 17-6 批准细节

字段	说明
必需批准	<p>当用户对 SoD 限制请求异常时，如果要起动工作流程，请选择“是”。</p> <hr/> <p><b>注释：</b>如果该 SoD 异常来自于隐含指派，如通过组或容器成员资格，则选择“是”不会导致批准工作流程启动。SoD 异常始终得到授权，并同样登录。</p> <hr/> <p>如果用户可以对 SoD 限制请求异常且不需要任何批准，请选择否。这种情况下，将始终批准该异常。</p>
SoD 批准定义	<p>显示用户请求 SoD 限制异常时执行的供应请求定义的只读名称。该值源自“角色配置”对象。仅当 <i>必需批准</i> 为是时才执行。</p>
批准类型	<p>显示以上所显示供应请求定义的处理类型的只读字段。该值源自“角色配置”对象。</p>

字段	说明
使用默认批准者	<p>如果在角色子系统中指定批准者，请选择 <i>是</i>。</p> <p>如果 SoD 批准任务应该指派给一个或多个用户，则选择 <i>用户</i>。如果 SoD 批准任务应该指派给组，请选择 <i>组</i>。如果应将 SoD 批准任务指派给角色，请选择 <i>角色</i>。</p> <p>要查找特定用户、组或角色，请使用第 1.4.4 节“常用用户操作”（第 24 页）中所述的“对象选择器”或“历史”按钮。</p> <p>要更改批准者在列表中的顺序或删除批准者，请使用第 1.4.4 节“常用用户操作”（第 24 页）中所述的按钮。</p>

## 17.5 配置角色子系统

Identity Manager 用户界面的角色选项卡上的配置角色子系统操作可用于指定角色子系统的管理设置。

定义角色子系统管理设置：

- 1 单击角色管理操作组中的配置角色子系统。



- 2 指定角色指派去除宽限期（以秒为单位）。

该值指定了角色指派从“角色编目”中去除之前的时间量（以秒为单位，默认为 0）。宽限期为零表示从角色指派中去除某人时，去除将立即发生，且随后立即开始撤消权利。可以使用宽限期来推迟去除随后将重新添加的帐户（例如，如果人员在容器间移动）。权利可以禁用帐户（此为默认设置），而不是将其去除。

- 3 当发出 SoD 异常请求时，请选择要运行的供应请求定义。您可以为每个 User Application 驱动程序指定一个定义。

**3a** 要查找供应请求定义，请使用第 1.4.4 节“常用用户操作”（第 24 页）中所述的“对象选择器”或“历史”按钮。

- 4 选择序列或规定数作为默认 SoD 批准类型。

字段	说明
串行	如果希望批准者列表中的所有用户都批准该角色，请选择“序列”。将按照列表中显示的顺序对批准者进行逐个处理。

字段	说明
规定数	<p>如果希望 <i>批准者</i> 列表中一定百分比的用户批准该角色，请选择 <i>规定数</i>。当达到指定的用户百分比时，该批准完成。</p> <p>例如，如果希望列表中四个用户中的其中一个批准该条件，应指定“规定数”和“25%”。此外，如果四个批准者必须同时批准，也可以指定 100%。该值必须是介于 1 和 100 之间的整数。</p>

## 5 修改默认 SoD 批准者。

字段	说明
默认 SoD 批准者	<p>如果角色批准任务应该指派给一个或多个用户，则选择 <i>用户</i>。如果角色批准任务应该指派给组，则选择 <i>组</i>。仅组中的一个成员需要批准。如果应将角色批准任务指派给角色，请选择 <i>角色</i>。与组相同，仅角色中的一个成员需要批准。</p> <p>要查找特定用户、组或角色，请使用“对象选择器”或“历史”按钮。要更改批准者在列表中的顺序或删除一个批准者，请参见 <a href="#">第 1.4.4 节“常用用户操作”</a>（第 24 页）</p>

## 6 单击 *保存* 以永久保存所选内容。



# 创建并查看角色报告

本部分说明角色报告以及如何创建并查看角色报告。每个导出都是有关生成报告时角色编目当前状态的只读 PDF 数据显示。一个报告不能反映一段时期内的数据更改。要跟踪角色信息以达到一致，请使用审计日志。

本部分主题包括：

- ◆ 第 18.1 节“关于角色报告操作”（第 217 页）
- ◆ 第 18.2 节“角色报告”（第 217 页）
- ◆ 第 18.3 节“SoD 报告”（第 220 页）
- ◆ 第 18.4 节“用户报告”（第 222 页）

## 18.1 关于角色报告操作

通过“角色”选项卡，您可以创建并查看说明角色当前状态的报告。这些报告可帮助您监视、添加、修改和删除角色或职责分离。

必须是角色管理员或角色审计员才能创建和查看角色报告。默认情况下，User Application 管理员具有角色管理员的权限。

## 18.2 角色报告

角色报告有两种：

- ◆ 角色列表报告
- ◆ 角色指派报告

### 18.2.1 角色列表报告

“角色列表报告”显示：

- ◆ 所有角色，按角色级别分组
- ◆ 每个角色的业务名称
- ◆ 每个角色的容器和说明
- ◆ 可选显示项：规定数百分比、所包含的角色、包含的角色、将角色间接指派给的组和容器以及绑定给每个角色的权利

创建和查看“角色列表报告”：

- 1 打开 User Application，然后选择角色 > 角色报告。
- 2 在选择报告下拉菜单中选择角色列表报告，然后单击选择。“角色报告”页面将提示选择报告中包含的参数。



- 3 选中 *显示每个角色的全部管理细节* 来查看以下信息（如果合适且可用）：
  - ◆ 规定数百分比
  - ◆ 所包含角色
  - ◆ 包含角色
  - ◆ 间接将该角色指派给的组
  - ◆ 间接将该角色指派给的容器
  - ◆ 与角色绑定的权利
- 4 选择显示所有角色还是显示所选拥有者拥有的角色。如果选中 *选择角色拥有者*，拥有者选择框将激活。使用这些图标进行选择：



打开对象选择对话框。

要选择一个人，请选择“名”或“姓”，然后输入名称的一个或多个字符来检索选择列表。从选择列表中选择。

要选择用户组，请从组的“说明”列表中选择，或在“说明”框中输入字符来选择较短的组列表。从选择列表中选择。

要选择用户的容器，请在目录树中单击一个容器。



打开历史选择对话框。从对象的“说明”列表中选择，或在“说明”框中输入字符来过滤搜索并检索较短的对象列表。



将当前选择重设置为无选择。

- 5 选择是显示所有安全级别的角色，还是显示一个或多个级别。要选择一个级别，请在选择下拉框中单击该级别。要选择多个级别，请在单击时按下 **Shift** 键或 **Ctrl** 键。
- 6 选择显示所有类别的角色，还是显示一个或多个类别。要选择一个类别，请在选择下拉框中单击该类别。要选择多个类别，请在单击时按下 **Shift** 键或 **Ctrl** 键。
- 7 单击 *运行报告* 将创建一个与图 18-1 中的示例类似的 PDF 报告，并可查看该报告。

图 18-1 样本角色列表报告

Novell		报告日期:	2008年1月17日 下午4:00
<b>角色列表报告</b>			
业务角色 (总计: 2)			
角色名称:	医生 (业务角色)		
容器:	医生_Level30.RoleDef		
说明:	医生		
角色名称:	测试1 (业务角色)		
容器:	测试1_Level30.RoleDef		
说明:	测试		
IT角色 (总计: 0)			
角色名称:	审计员 (IT角色)		
容器:	审计员_Level20.RoleDef		
说明:	角色审计员		
许可权限角色 (总计: 3)			
角色名称:	管理药品 (许可权限角色)		
容器:	管理药品_Level10.RoleDef		
说明:	管理药品		
角色名称:	Charles Sorenson (许可权限角色)		

8 要保存报告，请选择 Adobe Reader 窗口中的文件 > 保存副本。指定保存该文件的目录，然后指定报告的文件名。

## 18.2.2 角色指派报告

“角色指派报告”显示：

- ◆ 按角色级别分组的角色
- ◆ 每个角色的业务名称、容器、类别和说明
- ◆ 指派给角色的用户和批准这些指派的人员名称

创建和查看“角色指派报告”：

- 1 打开 User Application，然后选择角色 > 角色报告。
- 2 选择选择报告下拉菜单中的角色指派报告，然后单击选择。“角色报告”页面将提示选择报告中包含的参数。

- 3 选择显示所有角色指派或显示所选角色的指派。如果选择 *选择角色*，选择框将激活，并出现 **步骤 4（第 218 页）** 中所述的选择图标。
- 4 选择显示所有角色拥有者拥有的角色，还是所选角色拥有者拥有的角色。如果选择 *选择角色拥有者*，选择框将激活，并出现 **步骤 4（第 218 页）** 中所述的选择图标。
- 5 选择显示所有角色级别的角色，还是选择显示一个或多个角色级别的角色。要选择一个级别，请在选择下拉框中单击该级别。要选择多个级别，请在单击每个级别时按下 Shift 键或 Ctrl 键。
- 6 选择显示所有角色类别的角色，还是选择显示一个或多个角色类别的角色。要选择一个类别，请在选择下拉框中单击该类别。要选择多个类别，请在单击每个类别时按下 Shift 键或 Ctrl 键。
- 7 单击 *仅显示有指派的角色*，将报告过滤为仅包含已指派的角色。
- 8 如果选择显示所有角色而不是仅一个角色的指派，请在 *排序和分组* 下选择按名称或按类别对角色分组。
- 9 单击 *运行报告* 将创建一个与 **图 18-2** 中的示例类似的 PDF 报告，并可查看该报告。

**图 18-2** 样本角色指派报告

Novell		报告日期:	2008年1月17日 下午3:37
<b>角色指派报告</b>			
IT 角色 (总计: 0)			
角色名称:	审计员 (IT 角色)		
	审计员_Level20.RoleDefs		
	system		
	角色审计员		
角色名称:	护士 (IT 角色)		
	护士_Level20.RoleDefs		
	护士		
此角色的指派		批准者	
Abby Spencer (用户)			
角色名称:	药剂师 (IT 角色)		

- 10 要保存报告，请选择 Adobe Reader 窗口中的 *文件 > 保存副本*。指定保存该文件的目录，然后指定报告的文件名。

## 18.3 SoD 报告

下面的两个报告说明职责分离的当前状态：

- ◆ SoD 限制报告
- ◆ SoD 违例和异常报告

### 18.3.1 SoD 限制报告

“SoD 限制报告”显示：

- ◆ 当前按名称定义的职责分离限制
- ◆ 职责分离的说明

- ◆ 冲突角色列表
- ◆ 具有批准职责分离违例异常许可权限的人员列表

创建和查看“SoD 限制报告”：

- 1 打开 User Application，然后选择 **角色 > SoD 报告**。
- 2 在 **选择报告** 下拉菜单中选择 **SoD 限制报告**，然后单击 **选择**。“角色报告”页面将提示选择报告中包含的参数。



- 3 选择要列出所有 SoD 限制，还是选择一个 SoD 限制。如果选择 **选择 SoD 限制**，选择框将激活。请查看 **步骤 4（第 218 页）** 的选择框图标说明。
- 4 选择列出所有角色，还是选择一个角色。如果选择 **选择角色**，选择框将激活。请查看 **步骤 4（第 218 页）** 的选择框图标说明。
- 5 单击 **运行报告** 将创建一个与 **图 18-3** 中的示例类似的 PDF 报告，并可查看该报告。

**图 18-3** 样本 SoD 限制报告

Novell		报告日期:	2008年1月18日 上午8:14
<b>SoD 限制报告</b>			
SoD 限制名称:	医生 - 护士		
SoD 限制说明	医生 - 护士		
冲突角色	null		
批准者	主要管理		
<hr/>			
SoD 限制名称:	护士 - 药剂师		
SoD 限制说明	护士 - 药剂师		
冲突角色	护士 - 药剂师		
批准者	invoy primus, 测试用户 2, 测试用户 1		

- 6 要保存报告，请选择 Adobe Reader 窗口中的 **文件 > 保存副本**。指定保存该文件的目录，然后指定报告的文件名。

## 18.3.2 SoD 违例和异常报告

“SoD 违例和异常报告”显示：

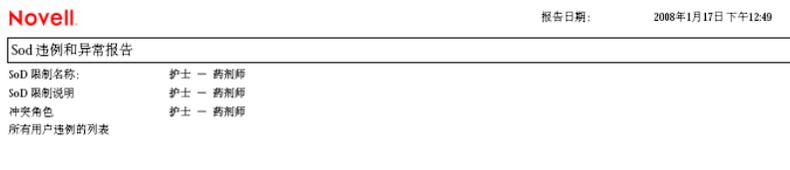
- ◆ 每个职责分离限制的名称，其说明和冲突角色
- ◆ 限制违例的用户，包括已批准的异常和未批准的违例。用户可以通过成为授予其冲突角色的组或容器的成员而存在违例中。
- ◆ 已批准的异常。这些是作为职责分离的异常已批准的违例。
- ◆ 批准或拒绝异常的人员名称以及批准或拒绝的日期和时间。

创建和查看“SoD 违例和异常报告”：

- 1 打开 User Application，然后选择角色 > SoD 报告。
- 2 选择选择报告下拉菜单中的 SoD 违例和异常报告，然后单击选择。“角色报告”页面将提示选择报告中包含的参数。



- 3 选择所有 SoD 限制来显示所有 SoD 限制中任何未解决的违例和异常。或者，选择选择 SoD 限制以将报告集中在单个 SoD 限制的违例上。
- 4 单击运行报告将创建如下例所示的 PDF 报告，并可查看该报告。



- 5 要保存报告，请选择 Adobe Reader 窗口中的文件 > 保存副本。指定保存该文件的目录，然后指定报告的文件名。

## 18.4 用户报告

用户报告有两种：

- ◆ 用户角色报告
- ◆ 用户权利报告

### 18.4.1 用户角色报告

“用户角色报告”显示：

- ◆ 所选的用户、用户组或用户容器
- ◆ 每个用户都保留其成员资格的角色
- ◆ 角色中的成员资格已生效或将生效的日期
- ◆ 角色成员资格的失效日期
- ◆ 角色中成员资格的来源（可选）

创建和查看“用户角色报告”：

- 1 打开 User Application，然后选择角色 > 用户报告。

2 选择 *选择报告* 下拉菜单中的 *用户角色报告*，然后单击 *选择*。

3 在 *用户* 窗格中选择希望为其查看角色的用户、组或容器。请查看 [步骤 4（第 218 页）](#) 的选择框功能说明。

4 在 *报告细节* 窗格中，选择要报告的一种或多种细节类型：

细节	含义
<i>仅显示直接指派的角色。</i>	“用户角色报告”显示直接指派给所选用户的任何角色（如有）。该报告不显示从组或容器的成员资格中继承的角色。
<i>包括直接指派角色的批准信息。</i>	“用户角色报告”显示批准每个用户的每个直接指派角色的人员。
<i>仅显示指派了角色的用户。</i>	“用户角色报告”显示已指派角色的所选用户。该报告不显示未直接或间接指派角色的用户。

5 在 *排序和分组* 窗格中，选择按名还是姓对用户进行排序。

6 在 *排序和分组* 窗格中，选择按级别还是名称来对每个用户的角色进行排序。

7 单击 *运行报告* 将创建如下例所示的报告，并可查看该报告。

用户角色报告			
用户:	Abby Spencer		
角色:	来源	有效日期	失效日期
护士	直接指派	08-1-16 下午5:02	
用户:	主要管理		
角色:	来源	有效日期	失效日期
角色模块管理员	直接指派	08-1-7 上午10:45	
用户:	测试用户 1		
角色:	来源	有效日期	失效日期
管理药品	直接指派	08-1-16 下午12:26	

8 要保存报告，请选择 Adobe Reader 窗口中的文件 > 保存副本。指定保存该文件的目录，然后指定报告的文件名。

## 18.4.2 用户权利报告

“用户权利报告”显示：

- ◆ 按其判别名排列的所有权利
- ◆ 拥有每个权利的用户
- ◆ 用户权利生效的日期
- ◆ 用户权利失效的日期
- ◆ 用户拥有的授予权利的角色

创建和查看“用户权利报告”：

- 1 打开 User Application，然后选择角色 > 用户报告。
- 2 选择选择报告下拉菜单中的用户权利报告，然后单击选择。



3 在用户选择窗格中，选择以下类型的用户：单个用户、组或容器。选择图标的说明位于步骤 4（第 218 页）。

4 在排序和分组窗格中选择下面的一项：

- ◆ 列出每个用户的权利细节
- ◆ 列出每个权利的用户细节

5 选择运行报告以查看与图 18-4 和图 18-5 中的示例类似的 PDF 报告。

图 18-4 样本用户权利报告：每个用户的权利细节

Novell 报告日期：11 月 16日 星期五 15:35:58 (美国) 东部时间

用户权利报告			
用户：Bill Bender			
权利 cn=MedSecureAccess,cn=HajenDriver,cn=TestDrivers,ou=Novell	源 (角色中的成员资格) 医生	有效日期 11/16/2007	失效日期 12/29/2007
用户：Kate Smith			
权利 cn=MedSecureAccess,cn=HajenDriver,cn=TestDrivers,ou=Novell	源 (角色中的成员资格) 医生	有效日期 11/16/2007	失效日期 12/30/2007
用户：Chip Nano			
权利 cn=MedSecureAccess,cn=HajenDriver,cn=TestDrivers,ou=Novell	源 (角色中的成员资格) 医生	有效日期 11/16/2007	失效日期 11/25/2007

图 18-5 样本用户权利报告：每个权利的用户细节

Novell 报告日期：11 月 16日 星期五 15:36:25 (美国) 东部时间

User Entitlements Report			
权利：cn=MedSecureAccess,cn=HajenDriver,cn=TestDrivers,ou=Novell			
用户：	源 (角色中的成员资格)	有效日期	失效日期
Bill Bender	医生	11/16/2007	12/29/2007
Kate Smith	医生	11/16/2007	12/30/2007
Chip Nano	医生	11/16/2007	11/25/2007

6 要保存报告，请选择 Adobe Reader 窗口中的文件 > 保存副本。指定保存该文件的目录，然后指定报告的文件名。



# 使用“合规性”选项卡



以下各节说明如何使用 Identity Manager User Application 的 *合规性* 选项卡。

- ◆ 第 19 章““合规性”选项卡简介”（第 229 页）
- ◆ 第 20 章“发出证明请求”（第 241 页）



# “合规性”选项卡简介

本节概述“合规性”选项卡。包括以下主题：

- ◆ 第 19.1 节“关于“合规性”选项卡”（第 229 页）
- ◆ 第 19.2 节“访问该选项卡”（第 231 页）
- ◆ 第 19.3 节“浏览选项卡的功能”（第 232 页）
- ◆ 第 19.4 节“可执行的合规性操作”（第 233 页）
- ◆ 第 19.5 节“了解证明请求图例”（第 234 页）
- ◆ 第 19.6 节“常用合规性操作”（第 235 页）

有关访问和操作 Identity Manager 用户界面的更多一般信息，请参见第 1 章“入门”（第 15 页）。

## 19.1 关于“合规性”选项卡

*合规性*选项卡提供了一种简便方法来执行基于合规性的操作。

使用 *合规性*选项卡，您可启动证明流程并检查这些流程的状态。您可使用 *合规性*选项卡执行以下操作：

- ◆ 启动证明流程以允许用户确认其用户简介包含准确的信息
- ◆ 启动证明流程以校验一组责任分离 (SoD) 限制的违反和批准的例外
- ◆ 启动证明流程以校验一组角色的指派
- ◆ 启动证明流程以校验一组用户的指派
- ◆ 查看证明请求的状态以分析每个流程的结果

### 合规性和代理方式

代理方式仅在 *请求和批准*选项卡上起作用，在 *合规性*选项卡上不受支持。如果在 *请求和批准*选项卡上进入代理方式，然后切换到 *合规性*选项卡，则在这两个选项卡上都将关闭代理方式。

### 19.1.1 关于合规性和证明

*合规性*是确保组织遵从相关商业法律和法规的过程。合规性的关键元素之一是证明。*证明*为组织提供了一种方法，来校验全体人员是否已完全了解组织策略，并确保采取了步骤来符合这些策略。通过请求员工或管理员定期证明数据的准确性，管理层可确保全体人员的信息（如用户简介、角色指派和已批准的责任分离 (SoD) 例外）最新且符合规定。

### 证明请求和流程

要允许组织中的个人校验企业数据的准确性，用户可发出*证明请求*。该请求将依次启动一个或多个工作流程。*工作流程*使*证明者*可以证明数据的正确性。将为每个证明者分别启动一个工作流程。将把证明者指派到*请求和批准*选项卡上*我的任务*列表中的工作流程任务中。要完成该工作流程，证明者需打开任务、审阅数据并证明该数据是正确还是不正确。

基于角色的供应模块支持四种类型的证明：

- ◆ 用户简介
- ◆ SoD 违反
- ◆ 角色指派
- ◆ 用户指派

如果是用户简介证明流程，每个用户必须是各自简介的证明者，任何其他人都不能是证明者。如果是 SoD 违反、角色指派和用户指派证明，则证明者可以是任何用户、组或角色。证明请求的发起者指定是每个成员还是仅单个成员必须为组或角色证明。如果是用户证明流程，则每个成员必须都为选定组或角色证明。

为简化发出证明请求的流程，基于角色的供应模块安装了一组默认的请求定义，一种定义适用于一种证明类型：

- ◆ 用户简介 — 默认
- ◆ SoD 违反 — 默认
- ◆ 角色指派 — 默认
- ◆ 用户指派 — 默认

可将这些请求定义用作发出您自身的请求的基础。提供新请求的细节后，您即可保存这些细节以备将来之用。

## 证明表单

每个工作流程都具有一个相关联的 *证明表单*。证明者必须审阅并填写该表单以证实数据的正确性。该表单由合规性模块管理员或证明管理者定义。

每个证明表单都包含一个必需的 *证明问题* 和一组可选的 *调查问题*。证明问题为是非题，用于证明或拒绝整个数据。可设置调查问题以收集其他数据或询问限定性问题。

用户简介证明表单还包含一组 *用户属性*，这些属性带有证明者必须审阅的值。SoD 违反、角色指派或用户指派流程的证明表单包含 *证明报告*。

## 证明报告

SoD 违反、角色指派或用户指派流程的证明报告提供了证明者应审阅的详细信息。报告在证明流程启动时生成，可确保所有用户都在审阅相同信息。可用多种语言生成报告，具体取决于为证明流程指定的报告语言设置。

## 证明请求状态

启动证明请求后，可轻松地跟踪它的整个生命周期。User Application 提供了一种简便方法来查看请求的整体状态，以及与请求关联的单个工作流程的详细状态。请求的高级别状态使用户可以查看请求是正在运行、已完成、正在初始化还是发生错误。详细状态提供了有关工作流程处理数量和各个工作流程的状态的信息。此外，它还显示 *证明结果*，指示证明问题的肯定回答和否定回答的数量。证明结果还显示哪些证明者尚未对指派给他们的工作流程任务采取任何操作。

## 合规性安全

“合规性”选项卡使用一组系统角色来保护对合规性功能的访问。*合规性*选项卡中的每个菜单操作都映射到一个或多个系统角色。如果用户不是为合规性定义的安全角色之一的成员，则*合规性*选项卡不可用。

合规性的系统角色由系统在安装时自动定义。包括以下角色：

- ◆ 合规性模块管理员
- ◆ 证明管理者

合规性模块管理员在安装时指定。安装后，角色模块管理员可将其他用户指派给合规性模块管理员角色和证明管理者角色。要进行其他角色指派，角色模块管理员需使用 User Application 中的 *角色 > 角色指派* 页。

下文将详细说明这些系统角色。

表 19-1 系统角色

职能	说明
合规性模块管理员	<p>一种系统角色，允许成员执行“合规性”选项卡上的所有功能（包括证明管理者可执行的功能）。</p> <hr/> <p><b>注释：</b>在基于角色的供应模块的 3.6.1 版本中，合规性模块管理员的功能与授予证明管理者的功能完全相同。在将来的版本中，随着不断向<i>合规性</i>选项卡中添加新功能，因此可能为合规性模块管理员授予其他功能。</p>
证明管理者	<p>一种系统角色，允许成员执行所有证明功能。下面列出了这些功能：</p> <ul style="list-style-type: none"><li>◆ 请求用户简介证明流程。</li><li>◆ 请求 SoD 违反证明进程。</li><li>◆ 请求角色指派证明流程。</li><li>◆ 请求用户指派证明流程。</li><li>◆ 查看已提交的所有证明请求的状态。</li></ul> <hr/> <p><b>注释：</b>可将任意用户定义为证明流程的证明者。证明者不需要属于“证明管理者”或“合规性模块管理员”角色。</p>

如果已鉴定用户不具有上列任一系统角色的成员资格，则这些用户不能访问 *合规性* 选项卡。

## 19.2 访问该选项卡

访问 *合规性* 选项卡：

- 1 在 User Application 中单击 *合规性*。  
默认情况下，*合规性* 选项卡将显示“请求用户简介证明流程”页。



如果转至用户界面中的另一个选项卡，然后又希望返回前一个选项卡，则仅需单击 *合规性* 选项卡，即可将其再次打开。

## 19.3 浏览选项卡的功能

本节介绍 *合规性* 选项卡的默认功能。（您的选项卡外观可能由于为您组织所作的自定义而有所不同；请咨询您的系统管理员。）

*合规性* 选项卡的左侧显示可以执行的操作的菜单。操作列在 *证明请求* 类别中：

图 19-1 “合规性”选项卡菜单



仅当您是 *合规性* 模块管理员或证明管理者时，才会显示 *证明请求* 操作。

单击一项操作时，其右侧会显示相应的页面。该页面通常包含一个窗口，其中显示该操作的细节。例如，该窗口可能会显示一个可以在其中输入数据或进行选择的列表或表格，如下图所示：

图 19-2 为某操作显示的页面



在 **合规性** 选项卡中使用的大多数页面的右上角都包含一个按钮，可以使用该按钮显示 **合规性** 图例：



有关 **合规性** 图例的细节，请参见第 19.5 节“了解证明请求图例”（第 234 页）。

## 19.4 可执行的合规性操作

下面是默认情况下可以在 **合规性** 选项卡中使用的操作的摘要：

表 19-2 合规性操作

类别	操作	说明
证明请求	请求用户简介证明流程	提交证明流程的请求以校验用户简介信息。  有关细节，请参见第 20.2 节“请求用户简介证明流程”（第 241 页）。
	请求 SoD 违反证明进程	提交证明流程的请求以校验一组 SoD 限制的违反和例外。  有关细节，请参见第 20.3 节“请求 SoD 违反证明进程”（第 242 页）。
	请求角色指派证明流程	提交证明流程的请求以校验选定角色的指派。  有关细节，请参见第 20.4 节“请求角色指派证明流程”（第 244 页）。
	请求用户指派证明流程	提交证明流程的请求以校验选定用户的指派。  有关细节，请参见第 20.5 节“请求用户指派证明流程”（第 245 页）。
	查看证明请求状态	允许您查看证明请求的状态。此外，还使您可以查看为某个请求启动的各个工作流程的详细状态并可选择收回工作流程。  有关细节，请参见第 20.6 节“检查证明请求的状态”（第 247 页）。

## 19.5 了解证明请求图例

在*合规性*选项卡中使用的大多数页面的右上角都包含一个按钮，可以使用该按钮显示*合规性*图例。要显示图例，请单击图 9-2 显示的*图例*按钮：

图 19-3 “图例”按钮



该图例简要说明整个*合规性*选项卡中使用的图标。下图显示该图例。

图 19-4 合规性图例



下表详细说明图例中的图标：

表 19-3 “图例”图标

图标	说明
正在初始化	表示证明请求已启动。 在“查看证明请求状态”页上显示。注意：您不能在“查看证明请求状态”页上查看正在初始化的请求的细节。
正在运行	表示证明请求仍在处理中。 在“查看证明请求状态”页上显示。
已完成	表示证明请求已完成处理。 在“查看证明请求状态”页上显示。
错误	表示在处理期间发生了错误。 在“查看证明请求状态”页上显示。
是	表示证明者校验了证明流程的信息是正确的。 在“查看证明请求状态”页上显示。
否	表示证明者已将证明流程的信息视为无效。 在“查看证明请求状态”页上显示。
已终止	表示证明请求的工作流程在完成前即已终止，原因是用户收回了工作流程或是在处理过程中发生了错误。 在“查看证明请求状态”页上显示。

## 19.6 常用合规性操作

“合规性”选项卡提供了一个一致的用户界面，带有可用于访问和显示数据的各种常用工具。本节说明若干常用用户界面元素，并包含下列操作的说明：

- ◆ 第 19.6.1 节“指定请求的标签和说明”（第 235 页）
- ◆ 第 19.6.2 节“定义证明者”（第 235 页）
- ◆ 第 19.6.3 节“指定最后期限”（第 236 页）
- ◆ 第 19.6.4 节“定义证明表单”（第 236 页）
- ◆ 第 19.6.5 节“提交证明请求”（第 238 页）
- ◆ 第 19.6.6 节“保存请求细节”（第 238 页）
- ◆ 第 19.6.7 节“使用已保存的请求”（第 239 页）

### 19.6.1 指定请求的标签和说明

需要为所有证明请求类型定义显示标签和说明。*合规性*选项卡提供了一个一致的界面来进行此操作。

定义显示标签和请求说明：

- 1 在*合规性*选项卡上的左导航菜单中，在*证明请求*下选择要执行的操作。
- 2 在*显示标签*字段中键入标签。  
“显示标签”在“我的任务”列表、已保存请求的列表和其他显示列表中显示为证明流程的名称。  
要提供标签的本地化文本，请单击*添加语言*按钮。然后，在目标语言的右侧键入本地化的文本，并单击*确定*。
- 3 在*请求说明*字段中键入说明。  
在“查看证明请求状态”页上审阅请求状态时，“请求说明”显示在请求的细节中。  
要提供说明的本地化文本，请单击*添加语言*按钮。然后，在目标语言的右侧键入本地化的文本，并单击*确定*。

### 19.6.2 定义证明者

*请求 SoD 违反证明进程*、*请求角色指派证明流程*和*请求用户指派证明流程*操作提供了一个用于定义证明者的一致界面。

定义 SoD、角色指派或用户指派证明流程的证明者：

- 1 在*合规性*选项卡上的左导航菜单中，在*证明请求*下选择要执行的操作。
- 2 在*证明者*字段中，指定将作为证明流程的证明者的用户、组和角色：
  - 2a 要向列表中添加一个或多个用户，请在下拉列表中选择*用户*。

选择将在证明进程中校验数据的用户。选择组和角色时，请选择是所有成员都必须校验数据，还是仅每个组和角色中的单个成员需要校验数据以完成此进程。

证明者：\*

使用 *对象选择器* 选择用户。在 *对象选择器* 中，您可通过单击各项的复选框然后单击 *选择* 来包含多个用户。

有关使用 *对象选择器* 的细节，请参见第 1.4.4 节“常用用户操作”（第 24 页）。

**2b** 要向列表中添加一个或多个组，请在下拉列表中选择 *组*。

使用 *对象选择器* 选择组。在 *对象选择器* 中，您可通过单击各项的复选框然后单击 *选择* 来包含多个组。

**2c** 要向列表中添加一个或多个角色，请在下拉列表中选择 *角色*。

使用 *对象选择器* 选择角色。在 *对象选择器* 中，您可通过单击各项的复选框然后单击 *选择* 来包含多个角色。

**2d** 要删除某项，请选择该项然后单击 *删除* 按钮。您可选择多个项，然后再单击 *删除* 按钮。

**2e** 对于组和角色证明者，指定是所有成员都必须证明数据还是仅每个组和角色中的单个成员必须证明数据，方法是选择以下按钮之一：

- ◆ *选定组和角色的每一位成员都必须证明数据。*
- ◆ *选定各组和角色的单个成员必须证明数据。*

如果是用户简介证明流程，则选定组或角色的每个成员都必须证明。

### 19.6.3 指定最后期限

每个证明流程都具有一个相关联的最后期限。最后期限表示您希望流程继续运行的时长。

最后期限对于启动证明流程是必需的，但对于已保存的请求则不是必需的。

指定证明流程的最后期限：

- 1** 在 *合规性* 选项卡上的左导航菜单中，在 *证明请求* 下选择要执行的操作。
- 2** 在 *最后期限* 字段中，指示您希望证明流程继续运行的时长。如果希望以周、日或小时指定流程的持续时间，请在 *持续时间* 字段中键入一个数字，然后选择 *周*、*天* 或 *小时* 作为度量单位。如果希望定义失效日期，请选择 *指定结束日期* 并使用“日历”控件来选择日期和时间。如果该流程将无限期运行，请选择 *不失效*。

在“最后期限”字段中指定的值不与已保存请求的细节一起储存。

### 19.6.4 定义证明表单

需要为所有证明类型定义证明表单。*合规性* 选项卡提供了一个一致的界面来进行此操作。

定义证明流程的表单：

- 1 在*合规性*选项卡上的左导航菜单中，在*证明请求*下选择要执行的操作。
- 2 定义证明表单的细节，如下所示：
  - 2a 单击 *编辑*按钮。



- 2b 在*证明问题*字段中键入证明问题。



证明问题是所有证明流程都必需的问题。此问题允许证明者证明数据或使数据无效。问题的答案必须为简单的“是”或“否”。启动证明流程时，必须定义证明问题，且每个证明者都必须回答此问题才能完成其应答。

要提供证明问题的本地化文本，请单击*添加语言*按钮。然后，在目标语言的右侧键入本地化的文本，并单击*确定*。

- 2c 对于用户简介证明流程，需要指示要校验的用户属性。在*用户属性*字段中，选择要包含的每个属性。

可选择的属性列表包含目录提取层中标记为可查看的所有属性（二进制或计算出的属性除外）。

- 2d（可选）在*调查问题*字段中，可包含证明者可在证明流程的执行期间回答的一个或多个问题。不要求证明流程包含调查问题。但是，如果包含调查问题，证明者可以选择回答这些问题。

请遵照以下步骤来定义和组织调查问题的列表：

- 2d1 单击*添加项目*按钮以添加调查问题。



在目标语言的右侧键入问题的本地化文本，并单击*确定*。

- 2d2 要向上移动列表中的问题，请选择该问题，然后单击*上移*按钮。

- 2d3 要向下移动列表中的问题，请选择该问题，然后单击*下移*按钮。

**2d4** 要删除某个问题，请选择该问题，然后单击 *删除* 按钮。

**2d5** 要编辑现有问题的本地化文本，请选择该问题，然后单击 *添加语言* 按钮。然后，在目标语言的右侧键入本地化的文本，并单击 *确定*。

**2e** 完成对表单的更改后，单击 *查看* 按钮。

可通过单击 *查看* 或 *编辑* 按钮在只读和可编辑视图之间来回切换。

## 19.6.5 提交证明请求

定义证明请求的细节后，需要提交请求以启动流程。提交请求时，User Application 将显示您的请求的确认编号。

以下是启动请求所必需的字段：

**表 19-4** 启动请求所需的字段

证明类型	必需的字段
用户简介	显示标签、请求说明、用户、最后期限、证明问题
SoD 违反	显示标签、请求说明、SoD 限制、证明者、最后期限、报告区域设置、证明问题
角色指派	显示标签、请求说明、为以下角色校验指派、证明者、最后期限、报告区域设置、证明问题
用户指派	显示标签、请求说明、校验指派给以下用户的角色、证明者、最后期限、报告区域设置、证明问题

提交证明请求：

- 1 在 *合规性* 选项卡上的左导航菜单中，在 *证明请求* 下选择要执行的操作。
- 2 单击 *提交* 以启动证明流程。

请求的 *确认编号* 显示在页面的顶部。记录下此编号，以便在“查看证明请求状态”页上轻松地跟踪请求的进度。如果不记录此编号，可始终通过使用“显示标签”来跟踪请求。

## 19.6.6 保存请求细节

定义证明请求的细节时，可选择保存这些细节以备将来之用。例如，您可能希望保存指定的参数和表单值，这样便可在将来的请求中再次使用它们。

单击 *使用已保存的请求* 时，为已保存请求指定的名称和显示标签将显示在已保存请求的列表中。

以下是已保存请求所必需的字段：

表 19-5 已保存请求所必需的字段

证明类型	必需的字段
用户简介	显示标签、请求说明、证明问题
SoD 违反	显示标签、请求说明、SoD 限制、报告区域设置、证明问题
角色指派	显示标签、请求说明、角色、报告区域设置、证明问题
用户指派	显示标签、请求说明、报告区域设置、证明问题

保存请求细节：

- 1 在 *合规性* 选项卡上的左导航菜单中，在 *证明请求* 下选择要执行的操作。
- 2 单击 *保存请求细节*。

键入要使用的名称以标识已保存流程请求，然后单击 *确定*。



已保存请求的名称中不允许使用以下字符：<>, ; \ " + # = / | & \*

将自动删除名称开头或结尾的空格。

如果该流程请求已存在，User Application 将提示您是否重写现有定义。

## 19.6.7 使用已保存的请求

发出证明请求时，可选择使用先前保存的请求中的细节作为新请求的基础。可供选择的已保存请求根据您正在请求的证明流程类型而异。例如，如果您正在发出用户简介证明请求（如下所示），则您将仅看到适用于用户简介证明流程的已保存请求。

使用已保存的请求：

- 1 在 *合规性* 选项卡上的左导航菜单中，在 *证明请求* 下选择要执行的操作。
- 2 单击 *使用已保存的请求*。

User Application 将显示一个弹出窗口，使您可以选择已保存的请求。



- 2a** 要选择请求，请单击显示标签或请求名称。请求名称是已保存请求定义的常用名 (CN)。
- 2b** 要去除某个已保存的请求，请单击显示标签左侧的复选框，然后单击 **去除**。可通过一次单击而去除多个已保存的请求。
- 无法去除随产品安装的任何默认请求定义。因此，默认请求定义不显示复选框。单击 **去除** 按钮时， **User Application** 将在去除已保存请求前显示一个确认窗口。

# 发出证明请求

本节提供发出证明请求的说明。包括以下主题：

- ◆ 第 20.1 节“关于证明请求操作”（第 241 页）
- ◆ 第 20.2 节“请求用户简介证明流程”（第 241 页）
- ◆ 第 20.3 节“请求 SoD 违反证明进程”（第 242 页）
- ◆ 第 20.4 节“请求角色指派证明流程”（第 244 页）
- ◆ 第 20.5 节“请求用户指派证明流程”（第 245 页）
- ◆ 第 20.6 节“检查证明请求的状态”（第 247 页）

## 20.1 关于证明请求操作

Identity Manager User Application 中的 *合规性* 选项卡包含一组称为 *证明请求* 的操作。*证明请求* 操作使用户能够发出证明流程请求和检查所作请求的状态。

## 20.2 请求用户简介证明流程

*请求用户简介证明流程* 操作使您可以启动证明流程以校验一个或多个用户简介。它还使您可以选择将与证明请求相关联的细节（如参数和表单值）保存为预填充表单以备将来请求之用。

启动用户简介证明流程：

- 1 单击 *证明请求* 操作列表中的 *请求用户简介证明流程*。

User Application 将显示一个页面，使用该页面，您可指定有关证明流程的细节。

- 2 如果希望使用先前已保存请求中的细节作为此请求的基础，请单击 *使用已保存的请求*。有关详细信息，请参见第 19.6.7 节“使用已保存的请求”（第 239 页）。
- 3 指定请求的显示标签和说明。有关详细信息，请参见第 19.6.1 节“指定请求的标签和说明”（第 235 页）。

4 在用户框中，选中将校验简介的用户：

4a 要显式地包含一个或多个用户，请在下拉列表中选择用户。



使用对象选择器选择用户。在对象选择器中，您可通过单击各项的复选框然后单击选择来包含多个用户。

有关使用对象选择器的细节，请参见第 1.4.4 节“常用用户操作”（第 24 页）。

4b 要包含一个或多个组中的用户，请在下拉列表中选择组。

使用对象选择器选择组。在对象选择器中，您可通过单击各项的复选框然后单击选择来包含多个组。

4c 要包含一个或多个角色中的用户，请单击下拉列表中的角色。

使用对象选择器选择角色。在对象选择器中，您可通过单击各项的复选框然后单击选择来包含多个角色。

4d 要包含容器中的用户，请单击下拉列表中的容器。

使用对象选择器可向下钻取所需容器，然后单击该容器以将其选中。

如果希望用户指派报告包含选定子容器中的所有用户，则需要选中选定项列表底部的包含子容器的所有用户复选框。

您必须至少选择一个用户、组、角色或容器才能启动证明流程。但是，不要求您必须选择用户、组、角色或容器才能保存请求。

5 在证明者字段中，注明该字段为只读。在用户简介证明流程中，证明者是用户字段中选定的用户，以及用户字段中添加的任何组、角色和容器中的所有成员。这是因为每个用户必须是自身简介的证明者，任何其他用户都不能是证明者。

6 指定证明流程的最后期限。有关详细信息，请参见第 19.6.3 节“指定最后期限”（第 236 页）。

7 定义证明表单的细节。有关详细信息，请参见第 19.6.4 节“定义证明表单”（第 236 页）。

8 提交请求。有关详细信息，请参见第 19.6.5 节“提交证明请求”（第 238 页）。

9 也可单击保存请求细节来保存与证明流程请求相关联的细节（如参数和表单值）以备将来之用。有关详细信息，请参见第 19.6.6 节“保存请求细节”（第 238 页）。

## 20.3 请求 SoD 违反证明进程

请求 SoD 违反证明进程操作使您可以启动证明流程以校验一个或多个 SoD 限制的违反和例外。它还使您可以选择将与证明请求相关联的细节（如参数和表单值）保存为预填充表单以备将来请求之用。

启动 SoD 证明流程时，User Application 将为证明者生成一组本地化的报告以供审阅。

证明者不需要具有选定限制的权限就可审阅报告。如果 SoD 证明流程的选定请求者不具有查看 SoD 限制的权限，则 User Application 仍允许该证明者查看显示该限制的违反和例外的报告。

启动 SoD 违反证明流程：

- 1 单击 *证明请求* 操作列表中的 *请求 SoD 违反证明进程*。

User Application 将显示一个页面，使用该页面，您可指定有关证明流程的细节。

请求 SoD 违反证明进程

为新的 SoD 违反证明提交请求，重新启动现有 SoD 违反证明或保存请求细节。（\* - 表示必需。）

使用已保存的请求

**选定进程请求：Default**

输入证明请求的标签和说明。“显示标签”将在“我的任务”列表、已保存请求列表以及其他显示列表中显示为证明进程的名称。“请求说明”出现在“查看证明请求状态”页面上的细节中。

显示标签：\*

请求说明：\*

选择证明进程中将其违反和异常的 SoD 限制。

SoD 限制：\*  所有 SoD 限制  选择 SoD 限制

选择将在证明进程中校验数据的用户。选择组和角色时，请选择是所有成员都必须校验数据，还是仅每个组和角色中的单个成员需要校验该数据以完成此进程。

证明者：\*

- 2 如果希望使用先前已保存请求中的细节作为此请求的基础，请单击 *使用已保存的请求*。有关详细信息，请参见第 19.6.7 节“*使用已保存的请求*”（第 239 页）。
- 3 指定请求的显示标签和说明。有关详细信息，请参见第 19.6.1 节“*指定请求的标签和说明*”（第 235 页）。
- 4 选择将校验违反和例外的 SoD 限制，如下所示：

**4a** 要包含所有现有限制，请选择 *所有 SoD 限制* 按钮。

选择证明进程中将其违反和异常的 SoD 限制。

SoD 限制：\*  所有 SoD 限制  选择 SoD 限制

**4b** 要单独选择限制，请选择 *选择 SoD 限制* 按钮。

使用 *对象选择器* 选择每个限制。在 *对象选择器* 中，您可通过单击各项的复选框然后单击 *选择* 来包含多个限制。

有关使用 *对象选择器* 和 *显示历史* 工具的细节，请参见第 1.4.4 节“*常用用户操作*”（第 24 页）。

您必须至少选择一个 SoD 限制才能启动证明流程。但是，不要求您必须选择 SoD 限制才能保存请求。

- 5 在 *证明者* 字段中，指定将作为证明流程的证明者的用户、组和角色。有关细节，请参见第 19.6.2 节“*定义证明者*”（第 235 页）。

您必须至少选择一个用户、组或角色作为证明者才能启动证明流程。但是，不要求您必须选择证明者才能保存请求。

- 6 指定证明流程的最后期限。有关详细信息，请参见第 19.6.3 节“*指定最后期限*”（第 236 页）。

- 7 在 *报告语言* 字段中，单击 *添加语言* 按钮以指定要将何种语言区域设置用于为证明流程生成的报告。在 *默认区域设置* 下拉列表中选择默认区域设置。然后，选取需要包含的语言并单击 *确定*。

启动 SoD 证明流程时，User Application 将为证明者生成一组本地化的报告以供审阅。这些报告以一种或多种语言提供了相同的数据。这些报告是在提交请求时生成的，用于确保所有证明者都在审阅相同的数据组。可为证明流程指定一组即将生成和储存的报告语言。证明者选择要进行审阅的证明任务后，系统将显示与证明者的首选区域设置（如果用户没有首选区域设置，则为浏览器区域设置）相匹配的本地化报告。如果不存在使用该区域设置的报告，则 User Application 将显示使用默认区域设置的报告。

- 8 定义证明表单的细节。有关详细信息，请参见第 19.6.4 节“定义证明表单”（第 236 页）。
- 9 提交请求。有关详细信息，请参见第 19.6.5 节“提交证明请求”（第 238 页）。
- 10 也可单击 *保存请求细节* 来保存与证明流程请求相关联的细节（如参数和表单值）以备将来之用。有关详细信息，请参见第 19.6.6 节“保存请求细节”（第 238 页）。

## 20.4 请求角色指派证明流程

*请求角色指派证明流程* 操作允许您启动证明流程以校验选定角色的指派的准确性。它还使您可以选择将与证明请求相关联的细节（如参数和表单值）保存为预填充表单以备将来请求之用。

启动角色指派证明流程时，User Application 将为证明者生成一组本地化的报告以供审阅。

证明者不需要具有选定角色的权限就可审阅报告。如果角色指派证明流程的选定证明者没有查看特定角色的权限，则 User Application 仍允许该证明者查看显示角色指派的报告。

为角色指派证明流程生成的报告显示指派给选定角色的用户。报告中仅包含具有指派的角色。

启动角色指派证明流程：

- 1 单击 *证明请求* 操作列表中的 *请求角色指派证明流程*。

User Application 将显示一个页面，使用该页面，您可指定有关证明流程的细节。

请求角色指派证明流程

为新的角色指派证明提交请求，重新启动现有角色指派证明或保存请求细节。（\* - 表示必需。）

使用已保存的请求

**选定进程请求：Default**

输入证明请求的标签和说明。“显示标签”将在“我的任务”列表、已保存请求列表以及其他显示列表中显示为证明进程的名称。“请求说明”出现在“查看证明请求状态”页面上的细节中。

显示标签：\*

请求说明：\*

选择在证明进程中将要校验其指派的角色。

校验以下对象的指派：\*

全部角色

选择角色

选择将在证明进程中校验数据的用户。选择组和角色时，请选择是所有成员都必须校验数据，还是仅每个组和角色中的单个成员需要校验该数据以完成此进程。

证明者：\*

选定组和角色的每一位成员都必须证明数据。

选定各组和角色的单个成员必须证明数据。

- 2 如果希望使用先前已保存请求中的细节作为此请求的基础，请单击 *使用已保存的请求*。有关详细信息，请参见第 19.6.7 节“使用已保存的请求”（第 239 页）。

- 3 指定请求的显示标签和说明。有关详细信息，请参见第 19.6.1 节“指定请求的标签和说明”（第 235 页）。
- 4 在为以下角色校验指派框中，选择要校验其指派的角色，如下所示：
  - 4a 要包含所有现有角色，请选择全部角色按钮。



- 4b 要单独选择角色，请选择选择角色按钮。

使用对象选择器或显示历史工具选择各个角色。在对象选择器中，您可通过单击各项的复选框然后单击选择来包含多个角色。

有关使用对象选择器和显示历史工具的细节，请参见第 1.4.4 节“常用用户操作”（第 24 页）。

您必须至少选择一个角色才能启动证明流程。但是，不要求您必须选择角色才能保存请求。
- 5 在证明者字段中，指定将作为证明流程的证明者的用户、组和角色。有关细节，请参见第 19.6.2 节“定义证明者”（第 235 页）。

您必须至少选择一个用户、组或角色作为证明者才能启动证明流程。但是，不要求您必须选择证明者才能保存请求。
- 6 指定证明流程的最后期限。有关详细信息，请参见第 19.6.3 节“指定最后期限”（第 236 页）。
- 7 在报告语言字段中，单击添加语言按钮以指定要将何种语言用于为证明流程生成的报告。在默认区域设置下拉列表中选择默认区域设置。然后，选取需要包含的语言并单击确定。

启动角色指派证明流程时，User Application 将为证明者生成一组本地化的报告以供审阅。这些报告以一种或多种语言提供了相同的数据。这些报告是在提交请求时生成的，用于确保所有证明者都在审阅相同的数据组。可为证明流程指定一组即将生成和储存的报告语言。证明者选择要进行审阅的证明任务后，系统将显示与证明者的首选区域设置（如果用户没有首选区域设置，则为浏览器区域设置）相匹配的本地化报告。如果不存在使用该区域设置的报告，则 User Application 将显示使用默认区域设置的报告。
- 8 定义证明表单的细节。有关详细信息，请参见第 19.6.4 节“定义证明表单”（第 236 页）。
- 9 提交请求。有关详细信息，请参见第 19.6.5 节“提交证明请求”（第 238 页）。
- 10 也可单击保存请求细节来保存与证明流程请求相关联的细节（如参数和表单值）以备将来之用。有关详细信息，请参见第 19.6.6 节“保存请求细节”（第 238 页）。

## 20.5 请求用户指派证明流程

请求用户指派证明流程操作允许您启动证明流程以校验选定用户的角色指派的准确性。它还使您可以选择将与证明请求相关联的细节（如参数和表单值）保存为预填充表单以备将来请求之用。

启动用户指派证明流程时，User Application 将为证明者生成一组本地化的报告以供审阅。

证明者不需要具有与选定用户相关联的角色的权限就可审阅报告。如果用户指派证明流程的选定证明者没有查看特定角色的权限，则 User Application 仍允许该证明者查看显示用户指派的报告。

报告将显示选定用户的角色指派。如果您选择容器、组或角色，该报告将显示选定容器、组或角色中用户的角色指派。

启动角色指派证明流程：

- 1 单击 *证明请求* 操作列表中的 *请求用户指派证明流程*。

User Application 将显示一个页面，使用该页面，您可指定有关证明流程的细节。



- 2 如果希望使用先前已保存请求中的细节作为此请求的基础，请单击 *使用已保存的请求*。有关详细信息，请参见第 19.6.7 节“*使用已保存的请求*”（第 239 页）。
- 3 指定请求的显示标签和说明。有关详细信息，请参见第 19.6.1 节“*指定请求的标签和说明*”（第 235 页）。
- 4 在 *校验指派给以下用户的角色* 框中，选择要校验其指派的用户：
  - 4a 要显式地包含一个或多个用户，请在下拉列表中选择 *用户*。

选择证明进程中要校验其角色指派的用户。将生成一份包含每个用户以及所选组、容器和角色的每个成员的关联角色指派的报告。  
校验指派到以下对象的角色: \*



使用 *对象选择器* 选择用户。在 *对象选择器* 中，您可通过单击各项的复选框然后单击 *选择* 来包含多个用户。

有关使用 *对象选择器* 的细节，请参见第 1.4.4 节“*常用用户操作*”（第 24 页）。

- 4b 要包含一个或多个组中的用户，请在下拉列表中选择 *组*。

使用 *对象选择器* 选择组。在 *对象选择器* 中，您可通过单击各项的复选框然后单击 *选择* 来包含多个用户。

- 4c 要包含一个或多个角色中的用户，请单击下拉列表中的 *角色*。

使用 *对象选择器* 选择角色。在 *对象选择器* 中，您可通过单击各项的复选框然后单击 *选择* 来包含多个角色。

**4d** 要包含容器中的用户，请单击下拉列表中的 *容器*。

使用 *对象选择器* 可向下钻取所需容器，然后单击该容器以将其选中。

如果希望用户指派报告包含选定子容器中的所有用户，则需要选中选定项列表底部的 *包含子容器的所有用户* 复选框。

您必须至少选择一个用户、组、角色或容器才能起动证明流程。但是，不要求您必须选择用户、组、角色或容器才能保存请求。

**5** 在 *证明者* 字段中，指定将作为证明流程的证明者的用户、组和角色。有关细节，请参见 [第 19.6.2 节“定义证明者”](#)（第 235 页）。

您必须至少选择一个用户、组或角色作为证明者才能起动证明流程。但是，不要求您必须选择证明者才能保存请求。

**6** 指定证明流程的最后期限。有关详细信息，请参见 [第 19.6.3 节“指定最后期限”](#)（第 236 页）。

**7** 在 *报告语言* 字段中，单击 *添加语言* 按钮以指定要将何种语言用于为证明流程生成的报告。在 *默认区域设置* 下拉列表中选择默认区域设置。然后，选取需要包含的语言并单击 *确定*。

启动用户指派证明流程时，*User Application* 将为证明者生成一组本地化的报告以供审阅。这些报告以一种或多种语言提供了相同的数据。这些报告是在提交请求时生成的，用于确保所有证明者都在审阅相同的数据组。可为证明流程指定一组即将生成和储存的报告语言。证明者选择要进行审阅的证明任务后，系统将显示与证明者的首选区域设置（如果用户没有首选区域设置，则为浏览器区域设置）相匹配的本地化报告。如果不存在使用该区域设置的报告，则 *User Application* 将显示使用默认区域设置的报告。

**8** 定义证明表单的细节。有关详细信息，请参见 [第 19.6.4 节“定义证明表单”](#)（第 236 页）。

**9** 提交请求。有关详细信息，请参见 [第 19.6.5 节“提交证明请求”](#)（第 238 页）。

**10** 也可单击 *保存请求细节* 来保存与证明流程请求相关联的细节（如参数和表单值）以备将来之用。有关详细信息，请参见 [第 19.6.6 节“保存请求细节”](#)（第 238 页）。

## 20.6 检查证明请求的状态

*查看证明请求状态* 操作使您可以查看证明请求的状态。此外，还使您可以查看为某个请求启动的各个工作流程的状态并可选择收回一个或多个正在运行的流程。

*查看证明请求状态* 操作显示所有证明请求，包含正在初始化、正在运行、已完成或出错的证明请求。

*User Application* 对于合规性模块管理员和证明管理者可在“查看证明请求状态”页上查看的内容不设任何限制。这两个角色都允许访问有关所有证明请求的状态信息。

查看证明请求：

**1** 单击 *证明请求* 操作列表中的 *查看证明请求状态*。

*User Application* 将显示所有证明请求的当前状态。



证明请求列表中的列如下所示：

- ◆ **显示标签**列提供为请求指定的证明流程的名称。可通过单击流程显示名称来查看请求的详细状态信息。
- ◆ **请求者**列标识发出请求的用户。
- ◆ **证明类型**列指示该证明流程的类型。类型确定流程要认证的信息类型，如下所示：

证明类型	说明
用户简介	指示此流程用于确保用户简介信息的准确性。要启动此类型的流程，合规性模块管理员或证明管理者需要使用 <i>请求用户简介证明流程</i> 操作。
SoD 违反	指示此流程用于确保责任分离违反和例外的准确性。要启动此类型的流程，合规性模块管理员或证明管理者需要使用 <i>请求 SoD 违反证明进程</i> 操作。
角色指派	指示此流程用于确保用户具有对资源、信息或系统的正确访问权，方法是校验每个选定角色是否具有正确的用户指派。要启动此类型的流程，合规性模块管理员或证明管理者需要使用 <i>请求角色指派证明流程</i> 操作。
用户指派	指示此流程用于确保用户具有对资源、信息或系统的正确访问权，方法是校验每个选定用户是否具有正确的角色指派。要启动此类型的流程，合规性模块管理员或证明管理者需要使用 <i>请求用户指派证明流程</i> 操作。

- ◆ **状态**列显示请求的状态以及一个提供该状态的可视指示符的图标。搜索具有特定状态的请求时，可从 **状态** 下拉列表中选择状态然后单击 **过滤器** 以缩小结果的范围：

状态	说明
正在初始化	表示这是一个新请求，且刚刚启动。
正在运行	表示该请求仍在处理中。

状态	说明
已完成	表示所有证明者均已应答（或者个别流程已由合规性模块管理员或证明管理者收回）且该请求已完成处理。
错误	表示在处理期间发生了错误。  错误的准确消息将写入跟踪日志或审计日志（如果任一日志处于活动状态）。如果出现错误，请检查跟踪或审计日志以查看该错误消息是否指示必须修复的严重问题。

- ◆ *请求日期*列显示发出请求的日期。
- ◆ *最后期限*列显示与此请求关联的所有流程必须完成的截止日期。如果该列为空白，则该请求没有最后期限。

2 您可以对请求列表进行过滤，如下所示：

**2a** 要仅查看以特定字符串开始的请求，请参见[过滤数据（第 27 页）](#)，以获取有关在*显示标签框*中输入的内容的信息。

**2b** 要仅查看具有特定类型的请求，请在*证明类型*下拉列表中选择类型。

**2c** 要查看带有特定状态的角色请求，请在*状态*下拉列表中选择状态。

状态	说明
所有	包含所有请求。
正在初始化	包含刚刚启动的请求。
正在运行	包含已经开始且当前正在处理的请求。
已完成	包含所有证明者均已应答（或者个别流程已由合规性模块管理员或证明管理者收回）且处理已完成的请求。
错误	包含已导致错误的请求。

**2d** 要对显示应用指定的过滤准则，请单击[过滤器](#)。

**2e** 要清除当前指定的过滤准则，请单击[重设置](#)。

**3** 要按照首次提交请求时生成的确认编号进行搜索，请在*确认编号*字段中键入编号，然后单击[搜索](#)。

**4** 要设置每个页面上显示的指派的最大数量，请在*每页最大行数*下拉列表选择一个数字。

**5** 要对请求列表排序，请单击包含想要排序的数据的列标题。

**6** 要查看特定请求的细节，请单击*显示标签列*中的名称并向下滚动，直至看到*请求细节组框*。

**注释：**如果状态为“正在初始化”，则*显示标签*是不可单击的，因为您不能查看正在初始化的请求的细节。

请求细节

**选定进程请求：角色指派 - 默认值**  
 进程请求说明：角色指派 - 默认值  
 确认编号：8e2538ce2f534728b530b7a03ec8a97

状态：✔ 已完成      完成日期：2008-06-13 02:27:45 下午  
 请求日期：2008-06-13 02:27:06 下午      请求者：main administrator

相关进程数量：1  
 正在运行的进程：0      已完成进程：1      已终止进程：0

**证明结果**  
✔ 为“是”的响应：1      ✘ 为“否”的响应：0      未采取任何操作：0

[查看证明表单细节](#)

过滤方式： 证明结果：  进程状态：     
 每页最大行数

选择：所有或无

证明者	完成日期	进程状态	证明结果
<input type="checkbox"/> main administrator		<span style="color: blue;">▶</span> 正在运行	未采取任何操作

选择：所有或无

除了显示摘要中已有的信息外，*请求细节*组框还显示与请求相关的所有流程的状态信息。

- ◆ *相关流程的数量*部分给出了流程的总数量，以及正在运行、已完成和已终止流程的数量。
- ◆ *证明结果*部分提供有关证明者如何进行应答的数据：

数据	说明
应答为“是”	提供对证明问题给出了肯定回答的证明者的总数。  <b>注释：</b> 确认回答的默认文本为是。但是，可修改此文本。如果修改了文本，字段标签将相应更改。
应答为“否”	提供对证明问题给出了否定回答的证明者的总数。  <b>注释：</b> 否定回答的默认文本为否。但是，可修改此文本。如果修改了文本，字段标签将相应更改。
未采取任何操作	提供尚未响应证明流程的证明者的总数。“未采取任何操作”总数还包含从未应答的各个证明者，以及由于超时而完成或者由合规性模块管理员或证明管理者收回的流程。

**6a** 要查看某个特定证明表单的细节，请单击 *查看证明表单细节*。

请求细节

**选定进程请求：角色指派 - 默认值**  
 进程请求说明：角色指派 - 默认值  
 确认编号：0e2f538ce2f534728b530b7a03ec8a97

状态：✔ 已完成      完成日期：2008-06-13 02:27:45 下午  
 请求日期：2008-06-13 02:27:06 下午      请求者：main administrator

相关进程数量：1  
 正在运行的进程：0      已完成进程：1      已终止进程：0

**证明结果**  
✔ 为“是”的响应：1      ✘ 为“否”的响应：0      未采取任何操作：0

[查看证明表单细节](#)

过滤方式： 证明结果：所有 进程状态：所有 过滤器 重设置  
每页最大行数 25

选择：所有 或 无  
收回选定进程

证明者	完成日期	进程状态	证明结果
<input type="checkbox"/> main administrator		<span style="color: blue;">▶</span> 正在运行	未采取任何操作

收回选定进程  
 选择：所有 或 无

证明流程的表单细节显示证明者应审阅的信息类型。表单细节根据证明类型是用户简介、SoD 违反还是角色指派而异。

要隐藏表单细节，请单击表单细节组框顶部的 *证明表单细节*。

[证明表单细节](#)  
 报告：

有关证明者在声明工作流程任务时必须审阅的表单细节的信息，请参见第 10.2.3 节“声明任务”（第 112 页）。

**6b** 您可以过滤流程列表，如下所示：

**6b1** 要仅查看具有特定结果的流程，请在 *证明结果* 下拉列表中选择结果。

结果	说明
所有	包含所有流程。
是	仅包含证明者做出肯定应答的流程。
否	仅包含证明者做出否定应答的流程。
未知	仅包含未采取任何操作的流程。“未知”过滤器还包含证明者从未应答的各个流程，以及由于超时而完成或者由合规性模块管理员或证明管理者收回的流程。

**6b2** 要查看带有特定状态的流程，请在 *流程状态* 下拉列表中选择状态。

状态	说明
所有	包含所有流程。
正在运行	包含已经启动且当前正在处理的流程。
已终止	包含已收回或已终止的流程。

状态	说明
已完成	包含证明者已应答或由于超时而完成的流程。

**6b3** 要对显示应用指定的过滤准则，请单击 *过滤器*。

**6b4** 要清除当前指定的过滤准则，请单击 *重设置*。

**6c** 要设置每个页面上显示的流程最大数量，请在 *每页最大行数* 下拉列表选择一个数字。

**6d** 要检查特定证明者的状态，请查看该证明者的 *流程状态列*。

*流程状态* 字段显示流程的状态以及状态图标。该图标提供了快速查看状态的简便方法。下表说明了状态代码：

状态	说明
正在运行	流程已经启动且当前正在处理。
已终止	该流程已在“查看证明请求状态”页上收回，或已在 iManager 中终止。
已完成	对于指派给某证明者的每个工作流程，所有证明者均已应答且处理已完成。  “已完成”状态包含证明者已应答的流程，以及由于超时而完成的流程。

**6e** 要收回一个或多个流程，请选择证明者然后单击 *收回所选流程*。如果希望收回所有流程，请单击 *全部*。要清除选择，单击 *无*。

如果已完成或终止流程，则将禁用 *收回所选流程* 复选框。如果高级别请求状态为“已完成”或“错误”，则将不显示 *收回所选流程* 按钮。