NetIQ® Identity Manager

Identity Applications 用户指南

2017 年 2 月

法律声明

有关 NetIQ 法律声明、免责声明、保证条款、出口和其他使用限制、美国政府限制权限、专利政策以及 FIPS 合规性的信息，请访问 http://www.netiq.com/company/legal/。

Copyright (C) 2017 NetIQ Corporation. 保留所有权利。

目录

关于本书和库 **11**
关于 NetIQ Corporation **13**

I 欢迎使用 Identity Manager **15**

1 入门 **17**

了解角色和资源 . . . 17
了解 Identity Applications . . . 17
Identity Manager 仪表板 . . . 17
Catalog Administrator . . . 18
User Application . . . 18
浏览仪表板 . . . 19
浏览 Catalog Administrator . . . 20
浏览 User Application . . . 21
获得帮助 . . . 22
常用用户操作 . . . 22
使用 Identity Applications 的典型方式 . . . 25
使用身份自助服务 . . . 25
使用角色和资源 . . . 26
使用处理请求 . . . 26
使用合规性 . . . 27

2 访问 Identity Applications **29**

访问 Identity Applications 的注意事项 . . . 29
首次登录 . . . 29
应对首选区域设置检查 . . . 31
登录问题查错 . . . 31
如果您忘记了口令 . . . 31
登录时出现问题 . . . 31
提示提供更多信息 . . . 31
绕过仪表板 . . . 32
注销 . . . 32

II 管理您的许可权限和身份配置文件 **33**

3 管理您的许可权限请求 **35**

查看您的许可权限 . . . 35
请求许可权限 . . . 35
查看您已发出的请求 . . . 36
跟踪请求 . . . 36
取消请求 . . . 36
去除许可权限 . . . 36

4 批准和拒绝请求 37

5 代表他人行事 39

查看您的代理指派 . . . 39
担当代理 . . . 39
管理代理指派 . . . 39

6 管理您的配置文件 41

在仪表板中更新您的配置文件 . . . 41
在 User Application 中管理您的配置文件 . . . 41
编辑信息 . . . 41
用电子邮件发送您的信息 . . . 42
链接至其他用户或组 . . . 43
选择首选语言 . . . 43

7 查看组织中的其他用户 45

了解组织结构图 . . . 45
在仪表板中浏览结构图 . . . 46
在 User Application 中浏览结构图 . . . 47
浏览至下个较高级别 . . . 47
重设置关系的根 . . . 48
切换默认关系 . . . 49
展开或折叠默认图 . . . 49
选择要展开或折叠的关系 . . . 50
在组织结构图中查找某个用户 . . . 52
显示有关用户的详细信息 . . . 53
从仪表板中向用户发送电子邮件 . . . 53
从 User Application 中向用户发送电子邮件 . . . 53
向图中的用户发送新电子邮件 . . . 53
用电子邮件发送图中用户的相关信息 . . . 54
向经理的小组发送电子邮件 . . . 54

8 管理您的口令 55

使用 Identity Manager 中的自助式口令管理 . . . 55
了解口令询问应答 . . . 56
更改口令 . . . 56
口令策略状态 . . . 56
使用旧式口令管理 . . . 57
口令询问应答 . . . 58
口令提示更改 . . . 58
更改口令 . . . 58
口令策略状态 . . . 59
口令同步状态 . . . 59

III 管理用户和组 61

9 创建用户或组 63

了解用户和组 . . . 63
创建用户 . . . 63
在仪表板中创建用户 . . . 63
在 User Application 中创建用户 . . . 63

创建组 64
使用 User Application 中的编辑按钮 65
查找容器 65
查找用户 66
使用历史列表 67

IV 使用工作仪表板选项卡 69

10 工作仪表板选项卡简介 71

关于工作仪表板选项卡 71
访问工作仪表板选项卡 71
浏览选项卡的功能 72
您可以执行的工作仪表板操作 73
了解工作仪表板上的图标 74
工作仪表板的安全许可权限 75
用户自助服务 75
处于管理模式时的域管理员 77
处于管理模式时的域管理者 79
处于管理模式时的小组管理者 81

11 管理您的工作 85

使用任务 85
查看任务列表 86
查看任务的摘要 87
选择任务 87
声明任务 88
重指派任务 90
释放任务 90
过滤任务列表 90
自定义任务列 91
控制任务列表默认情况下是否展开 92
控制任务细节的显示 92
设置打开任务的声明操作 92
对任务列表排序 93
刷新任务列表 93
控制页面中显示的项数 93
查看任务的注释 93
处理资源 93
查看资源指派 94
请求资源指派 95
刷新资源指派列表 95
去除资源指派 95
自定义资源指派列表显示 95
打印资源指派列表 96
处理角色 97
查看角色指派 98
请求角色 99
刷新角色指派列表 99
去除角色指派 99
自定义角色指派列表显示 99
打印角色指派列表 100
查看请求状态 101
查看请求列表 102
查看请求的摘要 105
过滤请求列表 105

自定义请求状态列 . . . 106
控制页面中显示的项数 . . . 106
控制请求状态细节的显示 . . . 106
对请求列表排序 . . . 107
刷新请求列表 . . . 107
查看请求的注释 . . . 107
查看请求的细节 . . . 107
收回请求 . . . 107

12 管理用户、组、容器、角色和小组的工作 109

选择用户、组、容器、角色或小组 . . . 109
更改为不同的受管实体 . . . 110
最大程度减小用户配置文件部分使用的屏幕空间 . . . 110
退出管理模式 . . . 111

13 控制您的设置 113

关于设置菜单 . . . 113
关于代理和委托 . . . 113
使用场景示例 . . . 114
设置菜单的用户访问权限 . . . 114
担当代理 . . . 116
指定您的可用性 . . . 116
设置可用性状态 . . . 117
创建或编辑可用性设置 . . . 117
删除可用性设置 . . . 118
查看和编辑代理指派 . . . 119
显示代理设置 . . . 119
创建或编辑代理指派 . . . 119
删除代理指派 . . . 120
查看和编辑委托指派 . . . 120
显示委托设置 . . . 120
创建或编辑委托指派 . . . 120
删除委托指派 . . . 121
查看和编辑小组代理指派 . . . 121
查看和编辑小组委托指派 . . . 124
指定小组的可用性 . . . 127
执行小组处理请求 . . . 129

14 发出处理请求 131

关于处理请求 . . . 131
发出处理请求 . . . 131
深度链接请求 . . . 134

V 管理角色和资源 137

15 角色和资源简介 139

关于角色和资源 . . . 139
关于角色 . . . 139
关于资源 . . . 144
访问角色和资源选项卡 . . . 145
浏览选项卡的功能 . . . 145
您可以执行的角色和资源操作 . . . 146

了解角色和资源选项卡上使用的图标 147

16 在 User Application 中管理角色 149

浏览角色编目 149
查看角色 149
创建新角色 150
编辑现有角色 154
删除角色 154
指派角色 155
刷新角色列表 156
自定义角色列表显示 156

17 在 User Application 中管理资源 157

浏览资源编目 157
查看资源 157
创建新资源 158
编辑现有资源 163
删除资源 163
指派资源 163
刷新资源列表 164
自定义资源列表显示 164

18 在 User Application 中管理责任分离 165

浏览 SoD 编目. 165
查看责任分离限制 165
创建新的责任分离限制 166
编辑现有的责任分离限制 167
删除责任分离限制 167
刷新责任分离限制列表 167

19 创建和查看报告 169

关于角色报告操作 169
角色报告 169
角色列表报告 169
角色指派报告 170
SoD 报告 171
SoD 限制报告 171
SoD 违例和异常报告 172
用户报告 172
用户角色报告 172
用户权利报告 173

20 配置角色和资源设置 175

关于配置角色和资源设置操作 175
配置角色设置 175
配置资源设置 176
配置权利查询设置 176
配置责任分离设置 176
配置报告设置 177

VI 使用合规性选项卡 179

21 合规性选项卡简介 181

关于合规性选项卡 . . . 181
关于合规性和证明 . . . 181
访问该选项卡 . . . 183
浏览选项卡的功能 . . . 184
可执行的合规性操作 . . . 184
了解证明请求图例 . . . 184
常用合规性操作 . . . 185
指定请求的标签和说明 . . . 186
定义证明者 . . . 186
指定最后期限 . . . 187
定义证明表单 . . . 187
提交证明请求 . . . 188
保存请求细节 . . . 188
使用已保存的请求 . . . 189

22 发出证明请求 191

关于证明请求操作 . . . 191
请求用户简介证明流程 . . . 191
请求 SoD 违反证明进程. . . 192
请求角色指派证明流程 . . . 193
请求用户指派证明流程 . . . 194
检查证明请求的状态 . . . 195

VII 附录 199

A 使用 Identity Manager Approvals 应用程序 201

产品要求 . . . 201
安装 Approvals 应用程序 . . . 202
配置 Approvals 应用程序 . . . 202
通过 User Application 请求移动访问权 . . . 202
使用配置链接或 QR 码 . . . 203
手动配置 Approvals 应用程序 . . . 203
Approvals 应用程序概述 . . . 205
任务视图 . . . 205
细节视图 . . . 206
批量模式 . . . 206
已完成任务视图 . . . 206
登录设置视图 . . . 206
高级设置视图 . . . 207
更改 Approvals 应用程序的显示语言 . . . 207

B 使用 User Application 中的目录搜索 209

了解目录搜索 . . . 209
执行基本搜索 . . . 210
执行高级搜索 . . . 210
选择表达式 . . . 212
为比较运算指定值 . . . 214
处理搜索结果 . . . 216
关于搜索结果 . . . 216

使用搜索列表 217
可以执行的其他操作 218
使用保存的搜索 219
要列出保存的搜索，请执行下列操作： 220
要运行保存的搜索，请执行下列操作： 220
要编辑保存的搜索，请执行下列操作： 220
要删除保存的搜索，请执行下列操作： 220

关于本书和库

本指南将介绍最终用户和部分管理员可以如何使用 NetIQ Identity Manager Identity Applications，尤其是仪表板和 User Application。

适用对象

本书提供的信息适用于负责了解管理概念及实施安全的分布式管理模型的人员。

库中的其他信息

此库提供了以下信息资源：

《Identity Manager 安装指南》

提供 Identity Manager 及其组件的概述。本书还提供 Identity Manager 的详细规划和安装信息。

《Designer Administration Guide》（Designer 管理指南）

提供有关在高生产力的环境中设计、测试、记录和部署 Identity Manager 解决方案的信息。

《Identity Applications: Design Guide》（Identity Applications：设计指南）

介绍如何使用 Designer 创建身份应用程序组件，包括如何使用 " 供应 " 视图、目录提取层编辑器、供应请求定义编辑器、供应小组编辑器和角色编目。

《Identity Reporting Module Guide》（Identity Reporting Module 指南）

介绍 Identity Reporting for Identity Manager，以及可如何使用它提供的功能，包括报告用户界面和自定义报告定义，此外还提供了安装指导。

《Analyzer Administration Guide》（Analyzer 管理指南）

介绍如何管理 Analyzer for Identity Manager。

《Identity Manager Common Driver Administration Guide》（Identity Manager 通用驱动程序管理指南）

提供对所有 Identity Manager 驱动程序都通用的管理任务的相关信息。

《Identity Manager Driver Guides》（Identity Manager 驱动程序指南）

提供有关 Identity Manager 驱动程序的实施信息。

关于 NetIQ Corporation

我们是一家全球性的企业软件公司，专注于您的环境中三大永恒挑战：变化、复杂性和风险，设法帮助您应对这些挑战。

我们的观点

适应变化及管理复杂性和风险实乃老生常谈

实际上在您面临的所有挑战中，这些也许是容易让您失控的最突出变数，从而无法安全地衡量、监视和管理您的物理环境、虚拟环境和云计算环境所需。

提供更好、更快的关键业务服务

我们相信，尽可能多地为 IT 组织提供控制，是更及时、经济有效地交付服务的唯一方法。只有在组织不断做出改变，并且管理这些变化所需的技术本身日益复杂时，持续存在的压力 （如变化和复杂性）才会继续增大。

我们的理念

销售智能解决方案，而不只是软件

为了提供可靠的控制，我们首先务必了解 IT 组织 （如贵组织）的实际日常运作情况。这才是我们可以开发出实用的智能型 IT 解决方案以成功取得公认的重大成果的唯一途径。并且，这比单纯销售软件要有价值得多。

推动您走向成功是我们的追求

我们将您的成功视为我们业务活动的核心。从产品启动到部署，我们深知：您需要与您当前购买的解决方案配合使用和完美集成的解决方案；您需要在部署后获得持续的支持并接受后续的培训；您还需要真正易于合作的伙伴一起应对变化。总之，只有您成功，才是我们都成功。

我们的解决方案

- 身份和访问管理
- 访问管理
- 安全管理
- 系统和应用程序管理
- 工作负载管理
- 服务管理

与销售支持联系

若对产品、定价和功能有疑问，请与本地合作伙伴联系。如果无法与合作伙伴联系，请与我们的销售支持团队联系。

全球：	www.netiq.com/about_netiq/officelocations.asp
美国和加拿大：	1-888-323-6768
电子邮件：	info@netiq.com
网站：	www.netiq.com

联系技术支持

有关具体的产品问题，请与我们的技术支持团队联系。

全球：	www.netiq.com/support/contactinfo.asp
北美和南美：	1-713-418-5555
欧洲、中东和非洲：	+353 (0) 91-782 677
电子邮件：	support@netiq.com
网站：	www.netiq.com/support

联系文档支持

我们的目标是提供满足您的需要的文档。 NetIQ 网站上提供了本产品 HTML 和 PDF 格式的文档，您无需登录即可访问该文档网页。如果您有改进这些文档的建议，请单击 www.netiq.com/documentation 上发布的 HTML 版文档任一页底部的**添加注释**。您还可以发送电子邮件至 Documentation-Feedback@netiq.com。我们会重视您的意见，欢迎您提供建议。

联系在线用户社区

NetIQ 在线社区 NetIQ Communities 是让您可与同行及 NetIQ 专家沟通的协作网络。 NetIQ Communities 上提供了更多即时信息、实用资源的有用链接，以及联系 NetIQ 专家的途径，有助于确保您掌握必要的知识，以充分发挥所依赖的 IT 投资的潜力。有关详细信息，请访问 http://community.netiq.com。

欢迎使用 Identity Manager

NetIQ Identity Manager 是一款系统软件产品，您的组织可使用它来安全地管理用户团体的访问需求。如果您是该用户团体的成员，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 （例如组组织结构图、部门白页或雇员查找），以及角色和资源 （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

请首先阅读此部分，了解 Identity Manager Identity Applications 以及如何开始使用它们。本指南旨在协助您完成组织中以下类型的联机活动：

- 管理与组织资源关联的联机身份
- 查看或修改您对组织角色和资源的访问权限
- 批准对资源和角色的访问权限的请求
- 管理与软件应用程序及您的组织提供给组织成员的其他资源关联的许可权限

1 入门

本章说明如何开始使用 Identity Applications。包括以下主题：

- 了解角色和资源 （第 17 页）
- 了解 Identity Applications （第 17 页）
- 浏览仪表板 （第 19 页）
- 浏览 Catalog Administrator （第 20 页）
- 浏览 User Application （第 21 页）
- 使用 Identity Applications 的典型方式 （第 25 页）

了解角色和资源

在 Identity Applications 中，**许可权限**表示为某用户或某组用户提供的针对某个角色或资源的访问权限。**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。例如，用户管理员角色可能会被授予重设置某个用户的口令的权限，而系统管理员角色则可以将用户指派给特定服务器。**资源**是业务用户进行访问需要具有的任意数字实体，例如用户帐户、计算机或数据库。

了解 Identity Applications

Identity Manager Identity Applications 指一组互联的基于浏览器的 Web 应用程序。它们可让您的组织管理用户帐户及与提供给用户的各种角色和资源关联的许可权限。您可以配置 Identity Applications，以便为您的用户提供自助服务支持，例如请求角色或更改他们的口令。您还可以设置工作流程，以提高管理和指派角色与资源的效率。

以下组件包含 Identity Applications：

- Identity Manager 仪表板 （第 17 页）
- Catalog Administrator （第 18 页）
- User Application （第 18 页）

Identity Manager 仪表板

Identity Manager 仪表板充当 Identity Applications 的主要进入门户。作为**用户**，您可从此处进行下列活动：

- 管理您的配置文件设置和口令
- 审阅并完成您的任务，例如批准用户的访问权限请求
- 请求针对角色、资源或流程的许可权限
- 查看您的许可权限请求的状态和历史记录
- 查找您组织中的其他用户

作为具有相应**管理员**角色的用户，您可以执行以下任务：

- 创建及修改用户配置文件
- 创建及修改代表若干组用户和组的小组，该小组可执行供应请求及与该小组关联的批准任务

Catalog Administrator

Catalog Administrator 用作与 Identity Manager 所管理组织中各种已连接系统关联的角色和资源的主要管理方法。尽管编目不是独特的数据库或一组文件，但它包含有关角色、资源及它们之间的关系的所有信息。

角色管理

如果您具有*角色管理员*权利，则可以执行以下任务：

- 创建、去除和修改角色。
- 建立批准和撤消角色的流程。
- 创建角色以及角色层次结构内的角色关系 .
- 创建、去除及修改责任分离 (SoD) 限制，以管理角色之间的潜在冲突。
- 浏览创建的角色的列表。
- 确定哪个角色与哪个容器关联。

资源管理

如果您具有*资源管理员*权利，则可以执行以下任务：

- 基于权利创建新资源，或创建不含权利的资源。
- 去除和修改资源。
- 建立批准和撤消资源的流程。
- 将资源与某些角色或与属于您组织中的其他角色、组或容器的某个角色关联。
- 浏览资源列表。
- 确定哪个资源与哪个容器关联。

相比 User Application 的角色和资源功能， Catalog Administrator 提供了一种更新的方法来管理角色和资源，但它不支持为角色和资源指派许可权限或所有权。

User Application

User Application 原先是 Roles Based Provisioning Module (RBPM) 的一部分。 RBPM 的部分功能已移到仪表板和 Catalog Administrator 中。 User Application 会继续提供这两个组件中都不具有的以下功能：

- 创建用户组，通常与其在您组织中的职务相关，例如财务部。
- 将角色和资源指派映射到组织内的资源，例如用户帐户、计算机和数据库。
- 指派角色和资源的所有权，并配置批准它们的方法。
- 配置口令管理设置，以使用户可以重设置自己的口令。
- 确保您的组织有校验相关人员完全了解组织策略并采取了相应步骤来遵循这些策略的方法。
- 确保对公司资源的访问权限符合组织策略，并且在符合公司安全策略的情况下进行供应。您可以以公司安全策略为准则授予用户对身份数据的访问权限。

- 创建工作流程，以减轻输入、更新和删除企业内所有系统中的用户信息的管理负担。这些工作流程为用户提供了一个基于 Web 的界面，用来操作根据需要触发工作流程的分布式身份数据。
- 支持复杂工作流程，以及管理身份、服务、资源和资产的手动和自动供应。

  您可以创建将供应请求发送到一个或多个机构的工作流程，以建立手动供应流程。要进行自动供应，您可以配置 User Application，让其自动启动工作流程来应对身份库中发生的事件。仪表板可以在用户请求许可权限时触发工作流程。

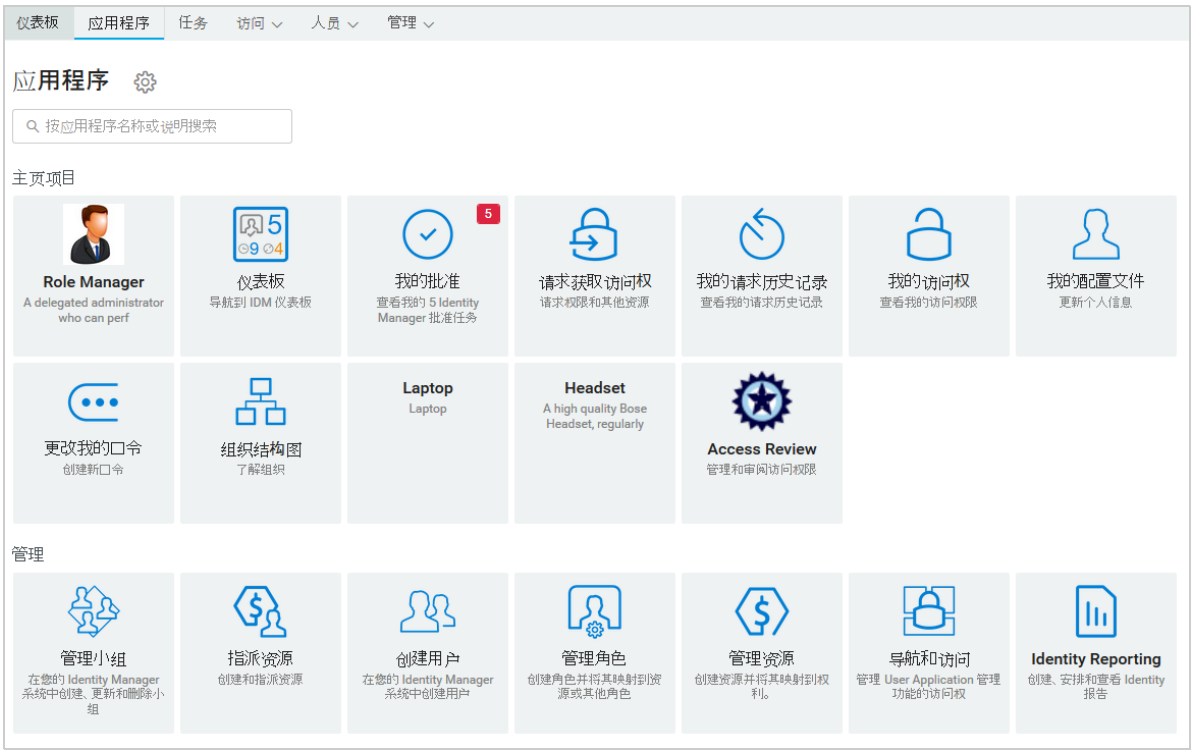
浏览仪表板

当您登录系统后，仪表板会显示有关您的任务、许可权限和请求的信息 （图 1-1）。

图 1-1 *个人仪表板示例*

仪表板中第二重要的视图为**应用程序**页面 （图 1-2），此页面提供若干个区域的默认链接，简化了最终用户和管理员在 Identity Manager 中所需执行的基本任务。

图 1-2　仪表板中的“应用程序”页面示例



您的身份管理员可自定义**应用程序**页面，以包含链接到日常请求的资源或用户经常访问的应用程序的磁贴。

此页面上的部分磁贴可能只对在 Identity Applications 中具有管理角色的用户显示。例如，可以创建或修改角色的人员应该能看到类似**创建用户**和**管理角色**的磁贴。

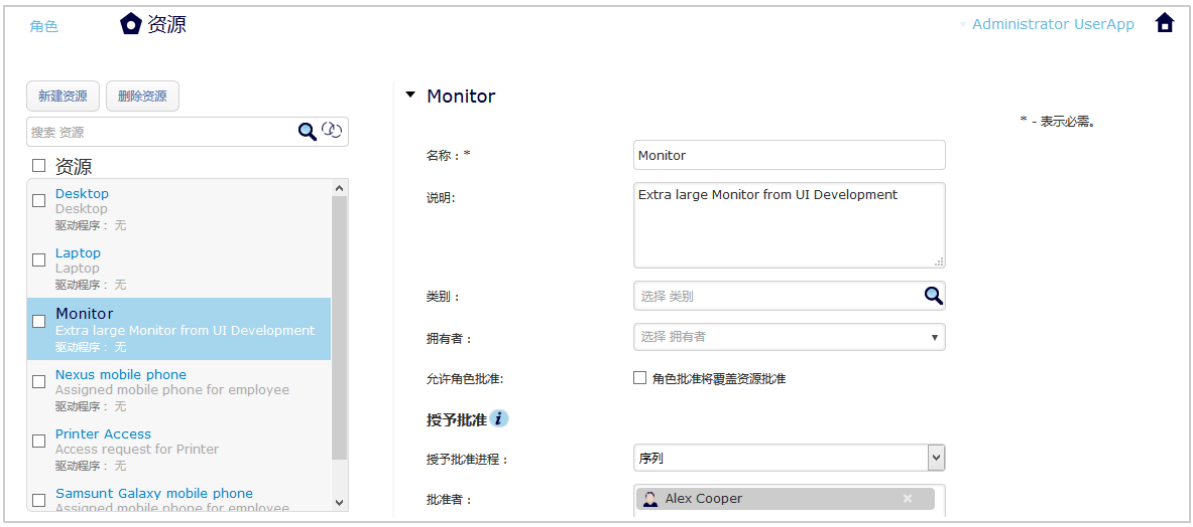
有关使用仪表板的详细信息，请参见第 III 章“管理用户和组”（第 61 页）和仪表板中的帮助。

浏览 Catalog Administrator

根据您要访问的 Catalog Administrator 功能，单击仪表板**应用程序**页面中的相应链接。例如，您可能想要更改某个资源的批准流程。

图 1-3 提供了可在 Catalog Administrator 中管理的某个现有资源的示例。有关管理角色和资源的详细信息，请参见第 V 部分“管理角色和资源”（第 137 页）和《*NetIQ Identity Manager - Administrator's Guide to the Identity Applications*》（NetIQ Identity Manager - Identity Applications 管理员指南）。

图 1-3 Catalog Administrator 中的 " 资源 " 页面示例



浏览 User Application

根据您要访问的 User Application 功能，单击仪表板应用程序页面中的相应链接。图 1-4 显示了 User Application 的默认界面。

图 1-4 User Application 的默认页面

User Application 提供了以下几个主要选项卡：

- *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，请参见第 II 部分 " 管理您的许可权限和身份配置文件 "（第 33 页）。

- *工作仪表板*

  要了解该选项卡及其操作方式，请参见第 IV 部分 " 使用工作仪表板选项卡 "（第 69 页）。

- *角色和资源*

  要了解该选项卡及其操作方式，请参见第 V 部分 " 管理角色和资源 "（第 137 页）。

- *合规性*

  要了解该选项卡及其操作方式，请参见第 VI 部分 " 使用合规性选项卡 "（第 179 页）。

注释：您看到的内容可能会因您拥有的安全许可权限而有所不同。

要从 User Application 中的任何位置返回到仪表板，请单击页面右上角的**主页**图标。

获得帮助

在 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**角色和资源**或**合规性**）。

2 单击**帮助**链接 （位于页面右上角）。

   此时会显示对应于当前选项卡的帮助页面。帮助页面中包含一个链接，通过此链接可查看 NetIQ 网站上的文档中包含的更多详细信息。

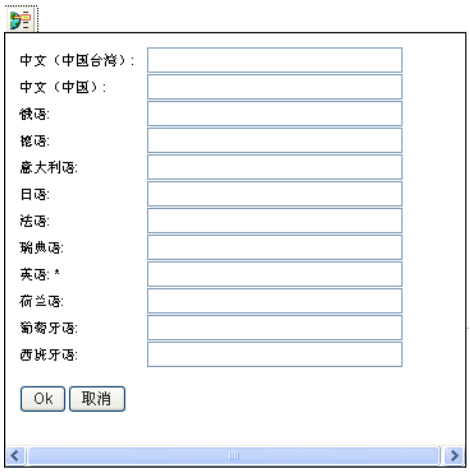
常用用户操作

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。本节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 23 页）
- 过滤数据 （第 24 页）
- 使用先行提示功能 （第 25 页）

表 1-1 *常用按钮*

按钮	说明
	对象选择器 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。 请参见使用 " 对象选择器 " 按钮进行搜索 （第 23 页）。

按钮	说明
	显示历史 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。
	重设置 清除当前选择。
	本地化 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。 
	添加 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。
	删除 删除当前所选项目。
	“ 向上 ” 或 “ 向下 ” 箭头 在列表中将当前所选对象上下移动
	图例 为用户界面中显示的符号提供说明。

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*

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。

   如果结果列表中包含所需的结果，请转至步骤 4。否则，请返回到步骤 2b。

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**工作仪表板**和**角色和资源**选项卡提供了一些过滤器，用于选择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：

- 按角色或资源指派和来源过滤 （“ 角色指派 ” 和 “ 资源指派 ” 操作中可用）
- 按角色或资源名称、用户和状态过滤 （“ 请求状态 ” 操作中可用）
- 按角色级别和类别过滤 （“ 角色编目 ” 操作中可用）

使用过滤功能：

1 在**过滤器**对话框中的文本字段 （例如，**角色名称**或**说明**字段）中指定一个值，方式如下：

   1a 要限制为以特定字符串开始的项目，请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。所应用的过滤将基于显示名称中的第一个字符。

   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*

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，请单击清除。

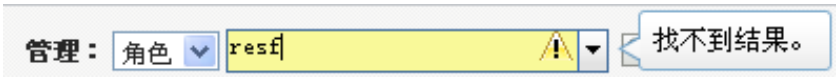
2 要设置过滤准则匹配项在每页上显示的最大数量，请在行下拉列表中选择一个数字。

使用先行提示功能

User Application 中的许多 AJAX 控件都支持智能先行提示 （或输入提示）处理。这种支持可以减少查找感兴趣项目所需的击键数量。要利用该功能，只需在控件中输入 4 个或更多字符，然后从自动生成的下拉列表中选择一个匹配项。

以下是一个示例，说明可以如何使用先行提示功能来搜索以字符串 Reso 开始的所有角色：

如果输入不存在任何匹配项的字符串，则会看到一条错误讯息，如下所示：



User Application 中用于输入单个值的所有用户查找、组查找或角色查找控件都支持该功能。

使用 Identity Applications 的典型方式

下面是一些介绍用户通常如何在组织中使用 Identity Applications 的示例。

- 使用身份自助服务 （第 25 页）
- 使用角色和资源 （第 26 页）
- 使用处理请求 （第 26 页）
- 使用合规性 （第 27 页）

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。

默认情况下， Identity Manager 使用 Self Service Password Reset (SSPR) 来允许用户修改其口令。不过， Identity Applications 可以使用其他方法来管理忘记的口令。有关详细信息，请参见《*NetIQ Identity Manager 安装指南*》中的 " 配置忘记的口令管理 "。

- 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 （一个最终用户）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。

使用角色和资源

- 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 创建这些角色需要的一些资源，并将资源与角色关联。
- 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）定义责任分离限制，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。要定义责任分离异常，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。他提供有关作出责任分离限制异常的调整。
- Edward （一个责任分离批准者）通过电子邮件收到有关责任分离冲突的通知。他批准 Arnold 关于覆盖该责任分离限制的请求。
- 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 （一个角色审核员）查看 SoD 违反和异常报告并了解到将 Ernest 同时指派给了 Doctor 和 Nurse 角色。此外，他还了解到已为 Ernest 指派了与这些角色关联的资源。

使用处理请求

- 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）定义责任分离限制，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。要定义责任分离异常，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。他提供有关作出责任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。

2 访问 Identity Applications

您需要在 Web 浏览器中访问 Identity Applications （例如仪表板）。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。您的组织应该会将访问应用程序所需的 URL 和身份凭证提供给您。

- 访问 Identity Applications 的注意事项 （第 29 页）
- 首次登录 （第 29 页）
- 应对首选区域设置检查 （第 31 页）
- 登录问题查错 （第 31 页）
- 绕过仪表板 （第 32 页）
- 注销 （第 32 页）

访问 Identity Applications 的注意事项

访问仪表板或任何其他 Identity Applications 之前，请先查看以下注意事项：

- 必须在 Web 浏览器中启用 Cookie 和 JavaScript*。
- 如果使用 Internet Explorer，应该至少设置中隐私级别。还应在**工具 > Internet 选项 > 常规 > 浏览历史记录 > 设置 > 检查所存网页的较新版本**下选择**每次访问网页时**选项。如果未选择该选项，则部分按钮可能无法正确显示。
- 如果您以前访问过 Identity Manager User Application，有可能此时可以使用相同的用户名和口令来访问仪表板。
- 您不能使用名称中包含任何下列字符的帐户来访问 Identity Applciations：

  \ /, * ? . $ # +

- 如果无法登录，可以单击**忘记了口令？** 。有关详细信息，请参见如果您忘记了口令 （第 31 页）。
- 访问 Identity Manager 用户界面时，如果所看到的第一页不相同，则原因通常是已针对您的组织自定义了应用程序。您可能会在使用时发现， Identity Applciations 的其他功能也已被自定义。

  在这种情况下，您应该咨询系统管理员，了解您的自定义 Identity Applications 与本指南所述的默认配置有哪些差别。

首次登录

您必须是授权用户才能登录 Identity Applciations （例如仪表板）。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。

当您第一次登录 Identity Applciations 时， Identity Manager 会要求您为自己的帐户建立安全参数，以便将来帮助重设置您的口令。如果您下次登录时忘记了口令并尝试重设置口令， Identity Manager 会提示这些配置的问题，要求您指定正确的答案。如果答案与您在此页面中保存的应答一致，您便可重设置口令。

要在第一次登录时设置安全问题，请执行以下操作：

1 输入用户名和口令，然后单击 “ 登录 ”。

2 登录页面会自动将您重定向到询问应答页面。

3 为 “ 安全问题 ” 指定问题和答案。

4 单击保存答案，系统会将您重定向到仪表板。

应对首选区域设置检查

如果您在登录时收到要求您选择自己的首选区域设置的提示，则表明您的管理员已将 Identity Applications 配置为在用户的浏览器上执行语言检查。为了确保您看到的内容以支持的语言显示，可能有必要如此设置。

收到添加区域设置的提示时，请打开**可用区域设置**列表，选择某个区域设置，然后单击**添加**。有关详细信息，请参见选择首选语言 （第 43 页）。

登录问题查错

本节将提供以下几种常见登录问题的解决方案：

- 如果您忘记了口令 （第 31 页）
- 登录时出现问题 （第 31 页）
- 提示提供更多信息 （第 31 页）

如果您忘记了口令

如果忘记了口令，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。

1. 出现登录提示时，单击**忘记了口令？**链接。
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. 回答所显示的询问问题。 Identity Manager 会提示您回答配置的问题。如果答案与您以前保存的应答一致，您便可重设置口令。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的口令策略，您可能会：
   - 收到包含有关该帐户的口令的电子邮件
   - 收到重设置口令的提示

登录时出现问题

如果您无法登录，请确保使用了正确的用户名，并且键入了正确口令 （拼写、大小写字母等）。如果仍有问题，请咨询系统管理员。如果您能够提供与所遇问题有关的细节 （如错误讯息），将会有助于解决问题。

提示提供更多信息

登录后，系统可能即会提示您提供其他类型的信息。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：

- 如果这是您第一次登录，系统会提示您定义您的询问问题和应答
- 如果口令已失效，系统会提示您重设置口令

绕过仪表板

如果您具有允许您管理角色和资源或运行报告的角色，则可直接登录 Catalog Administrator、 Identity Reporting 和 User Application，而无需先起动仪表板。输入系统管理员提供的特定身份应用程序 （例如 User Application）的地址 (URL)。

例如：http://myappserver:8180/IDMProv。

您会进入 User Application 的默认界面。或者，仪表板的**应用程序**页面中应该会提供这些 Identity Applications 的链接。

图 2-1 *User Application 的默认页面*

注销

当您在仪表板和其他 Identity Applications 中完成工作时，应该从中注销。在仪表板的右上角单击您的用户名，然后选择**注销**。

II 管理您的许可权限和身份配置文件

NetIQ Identity Manager 仪表板 （简称 " 仪表板 "）可帮助您请求完成日常任务所需资源和角色的访问权限。您还可以处理 Identity Manager 环境中指派给您的任何任务，例如批准访问权限请求。资源和角色的拥有者可以管理该流程。

当您请求许可权限后， Identity Manager 会启动一个流程来有效率地审阅您的请求，以便让您可以拥有所需的角色或资源。您的主管会收到审阅您的请求的通知，通知可能是电子邮件，也可能显示在仪表板中。在某些情况下，您的请求可能也会被组织中的其他人员批准。

有些用户还可以代表他人或作为另一个用户的代理来发出请求。

- 第 3 章 " 管理您的许可权限请求 "（第 35 页）
- 第 4 章 " 批准和拒绝请求 "（第 37 页）
- 第 5 章 " 代表他人行事 "（第 39 页）
- 第 6 章 " 管理您的配置文件 "（第 41 页）
- 第 7 章 " 查看组织中的其他用户 "（第 45 页）
- 第 8 章 " 管理您的口令 "（第 55 页）

3 管理您的许可权限请求

本章提供了以下活动的准则：

- 查看您的许可权限 （第 35 页）
- 请求许可权限 （第 35 页）
- 查看您已发出的请求 （第 36 页）
- 去除许可权限 （第 36 页）

您还可以在仪表板中查看这些活动的相关帮助。

查看您的许可权限

要查看您具有访问权限的角色和资源，请在仪表板中选择：

访问权限 > 许可权限

然后可以选择特定许可权限以了解有关该角色或资源的更多细节。许可权限可能还会列出针对该许可权限指派提供的任何原因。要在较大的列表中找到特定的许可权限，可以按名称或说明搜索，也可以过滤列表。

有关详细信息，请参见仪表板帮助。

请求许可权限

要请求角色和资源，请在仪表板中选择：

访问权限 > 请求

在请求许可权限之前，请先查看以下注意事项：

- 您可能可以代表另一个用户请求访问权限。例如，如果您是小组主管，通常可以代表小组成员行事。流程是一样的，只不过您必须指定该请求是为**他人**而非**自己**发出的。
- 指定要请求的许可权限时，请勿使用标点符号。如果要请求的许可权限名称包含标点符号，请在搜索时省略标点符号。
- 不同的许可权限需要不同的信息，具体取决于管理员是如何配置许可权限表单的。如果许可权限需要详细的信息，当您选择许可权限后，仪表板会将您重定向到另一个窗口。
- 一次可请求多个许可权限。

  但是，如果其中某个请求的许可权限表单需要特殊类型的信息，您可能便无法在一个多许可权限请求中包含该许可权限。要一次请求多个许可权限，各个请求的请求表单就不能需要详细的信息。

有关详细信息，请参见仪表板帮助。

查看您已发出的请求

要查看正在处理的请求的状态和已完成的请求，请在仪表板中选择：

访问权限 > 请求历史记录

发出请求后，直到 Identity Manager 完成处理之前，您都无法在**请求历史记录**中选择请求。如果您用来访问仪表板的连接速度较慢，则可能需要等待片刻，仪表板才会允许您单击列表中的请求名称。

- 跟踪请求 （第 36 页）
- 取消请求 （第 36 页）

有关详细信息，请参见仪表板帮助。

跟踪请求

对于每个请求，您不仅可以查看您的操作，而且可以查看批准或拒绝您的请求过程中涉及的工作流程。流程中的每个步骤都有相应的时戳。

要跟踪等待中的请求，请选择该请求，然后将右上方的菜单更改为**用户和系统**。仪表板即会显示该请求当前在批准流程中的状态。

取消请求

您可以从 " 历史记录 " 列表中取消*等待中*的请求。在列表中选择该请求，然后在随后显示的窗口中选择**取消此请求**。

去除许可权限

如果您不再需要对某个角色或资源的访问权限，可以去除相应的许可权限。在**访问权限 > 许可权限**中选择该许可权限，然后指定撤消它的原因。

去除许可权限时，应注意以下事项：

- 如果您使用仪表板添加、去除或修改许可权限，您的许可权限列表可能不会立即反映该更改。请按 **F5** 刷新列表。
- 您无法去除因为是 Identity Manager 环境中某个特定组的成员而被赋予的许可权限。要去除因为是某个组的成员而被指派的对某个角色或资源的访问权限，必须从该组中去除您的帐户。

有关详细信息，请参见仪表板帮助。

4 批准和拒绝请求

如果您负责批准或拒绝 Identity Manager 中请求的许可权限，可以使用仪表板以您之前可能在 User Application 中采用的方式来管理您的任务。您可以一次只批准或拒绝一个请求，也可以批量批准或拒绝多个不需要详细信息的简单请求。

要查看等待中的请求，请在仪表板中选择：

任务

或者，您可能会收到一封电子邮件通知，其中包含可让您在回复电子邮件中批准或拒绝请求的链接。

在处理用户请求之前，请先查看以下注意事项：

- 您可以选择多个任务来批量批准 / 拒绝。
- 对于需要详细信息的较复杂请求，仪表板不会显示复选框。您必须通过选择各请求并完成表单来批准或拒绝这些请求。
- 当您选择较复杂的请求来批准或拒绝时，仪表板可能需要在另一个浏览器标签页中打开请求表单。
- 一般而言，您必须提供一条注释以解释为何批准或拒绝所选任务。

有关详细信息，请参见仪表板帮助。

5 代表他人行事

某些组织中可能允许您作为代理或代表为他人完成任务。例如，个人助理可以为上司执行代理操作。此外，当同事休产假时，您可能会被临时指派来代表她处理事务。

- 查看您的代理指派 （第 39 页）
- 担当代理 （第 39 页）
- 管理代理指派 （第 39 页）

有关详细信息，请参见仪表板帮助。

查看您的代理指派

要查看您的代理指派，请在仪表板中选择：

访问权限 > 代理指派

担当代理

管理员可能会指派您充当另一个用户的代理。发生此情况时，应用程序会在位于右上角的您的帐户菜单中添加一个代理选项。

***您的 ID* > 代理身份**

例如，Sarah Smith 负责管理客户关系。Identity Applications 中包含一个客户关系小组，Sarah Smith 是小组主管。她可以代表小组成员 Maria Belafonte 行事。她在仪表板中选择 **ssmith > 代理身份**，然后指定 **mbelafonte**。

管理代理指派

作为管理员或小组主管，您可以创建、修改和删除指派。要让小组主管管理小组的代理指派，您必须适当配置小组。小组主管只能为小组成员创建指派。

6 管理您的配置文件

Identity Applications 提供了一种便捷的方式供您显示和处理您的身份信息。它们还能让您的组织随时为您提供访问其他用户相关信息所需的权限，从而提高组织的响应能力。例如，您可能想要：

- 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您组织中的其他人设置 Identity Applications 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。

在仪表板中更新您的配置文件

要查看并更新您的身份配置文件，请在仪表板中选择：

[您的 ID] > **我的配置文件**

您的配置文件包含您的姓名、电子邮件地址和电话号码等设置。您的组织会决定您可以修改哪些设置。例如，您可能可以更改您的电话号码，但不能更改您的姓氏。

该页面还会列出指派给您的角色和资源。

在 User Application 中管理您的配置文件

User Application 提供了用于管理您身份配置文件的附加功能：

- 通过电子邮件 （以链接的形式）将细节发送给某个用户
- 为您使用的 User Application 实例指定区域设置 （语言）。

本节说明如何使用 Identity Manager User Application 的**身份自助服务**选项卡上的**我的配置文件**页面。

注释：本章说明 " 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。

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。

3 完成编辑后，请单击保存更改，然后单击*返回*。

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。

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 替换或去除它。

3 单击该按钮显示 " 文件上载 " 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，将所选图像文件上载到服务器。

5 单击关闭窗口可返回到编辑页面。

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` *`your-user-id`*
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。

2 指定邮件的收件人 （以及所需的其他内容）。
3 发送邮件。

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滑线。
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 （市场营销副总裁）登录 Identity Manager User Application，然后进入 " 我的配置文件 " 页面并单击**编辑您的信息**。

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）。他单击**营销**，看到一个新窗口，其中显示了 " 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**，看到了用户 Allison Blake （他的员工之一）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。单击该链接后，他的电子邮件客户端创建了一封发送给 Allison 的新邮件。

他现在可以键入讯息内容，然后发送该讯息。

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**去除**，来更改自选设置顺序。
4 单击**保存更改**。

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。

在浏览器中定义首选语言

在 Firefox* 中，通过**工具 > 常规 > 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。

7 查看组织中的其他用户

仪表板和 User Application 都提供了显示组织中的用户层次结构的组织结构图。

注释：本章介绍 “ 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。

了解组织结构图

“ 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。

以下插图提供了仪表板和 User Application 中的组织结构图示例。

图 7-1　仪表板中的组织结构图示例

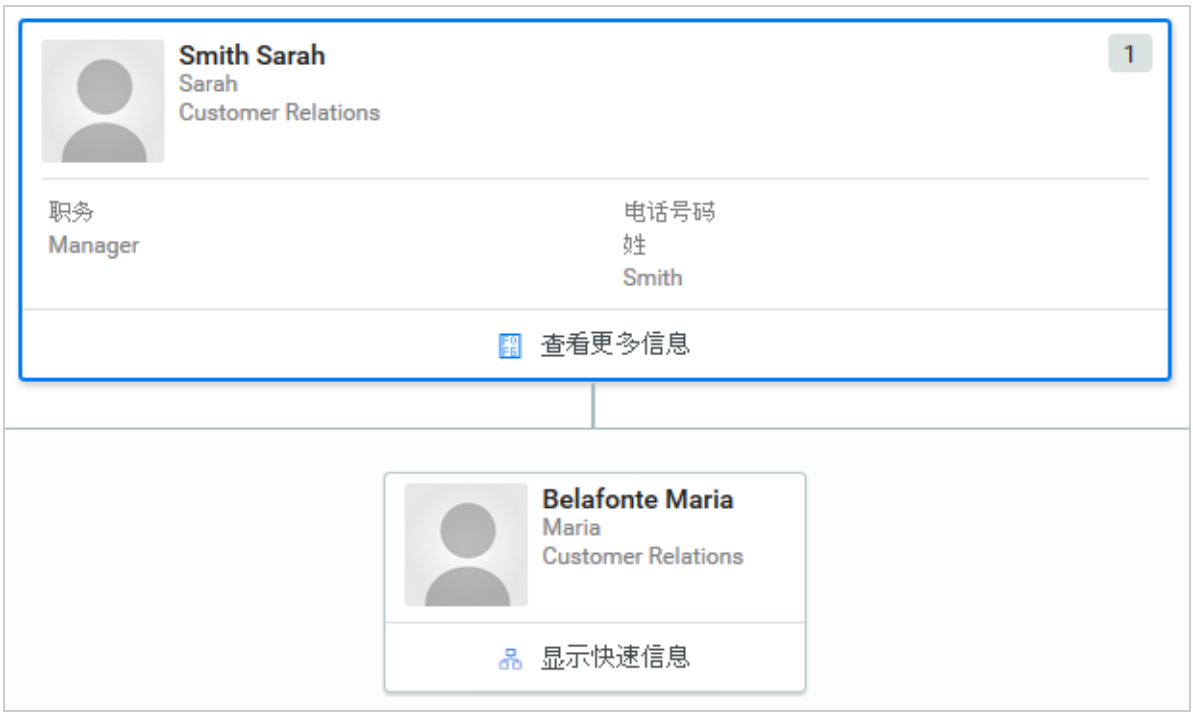
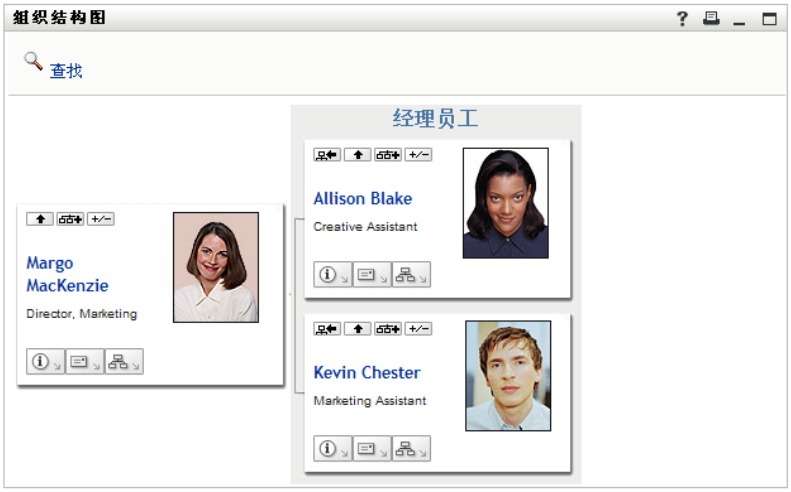


图 7-2　User Application 中的组织结构图示例



在仪表板中浏览结构图

仪表板提供了通过组织结构图查明组织中用户间关系的简化方法。在仪表板中选择：

人员 > 用户

选择任一用户，然后选择该用户姓名旁边的组织结构图图标。仪表板即会显示该用户的所有下属及上司。

在 User Application 中浏览结构图

本节说明如何通过以下方式在关系图中移动：

- 浏览至下个较高级别 （第 47 页）
- 重设置关系的根 （第 48 页）
- 切换默认关系 （第 49 页）
- 展开或折叠默认图 （第 49 页）
- 选择要展开或折叠的关系 （第 50 页）
- 在组织结构图中查找某个用户 （第 52 页）

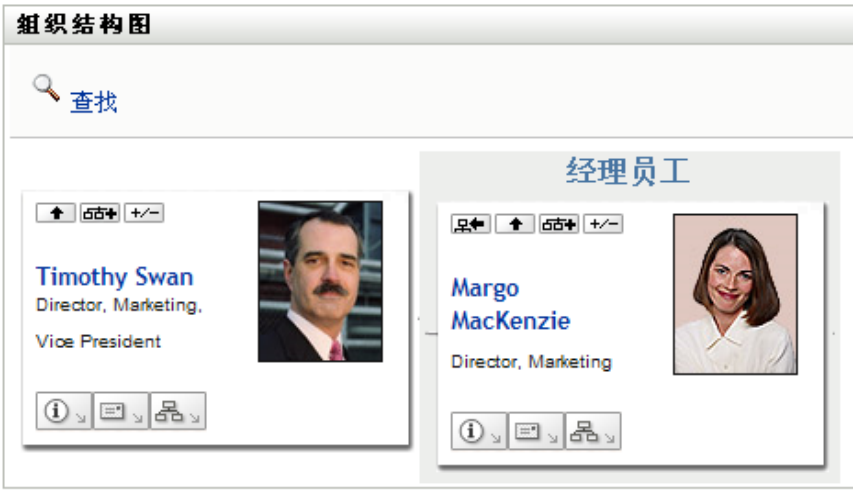
浏览至下个较高级别

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。

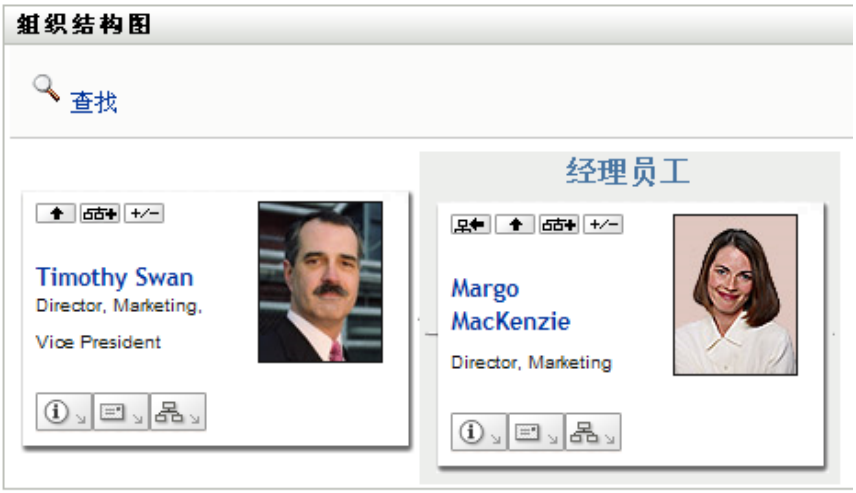
重设置关系的根

要重设置您的关系图视图的根：

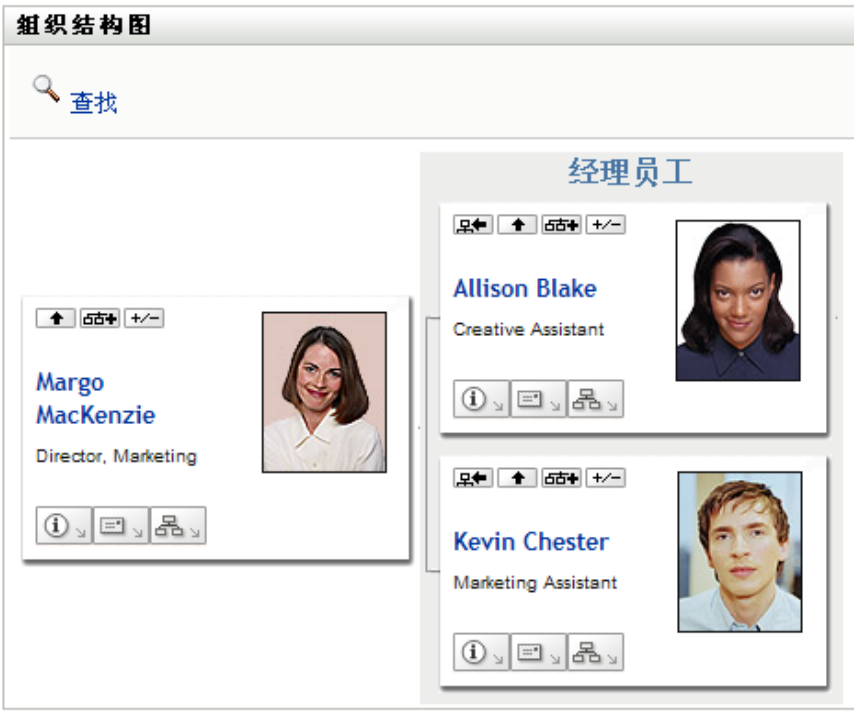
1 找到要用作新根的用户的名片。

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：



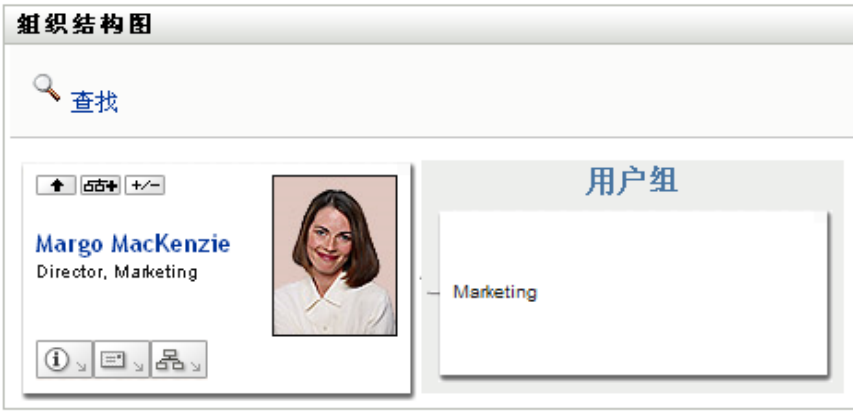
切换默认关系

1 单击切换到组织结构图 更改您的默认关系。
2 选择要显示的关系类型。您的管理员可以使用 NetIQ 提供的关系 （请参见表 7-1），也可以定义自定义关系。

表 7-1 NetIQ 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：



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。

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。

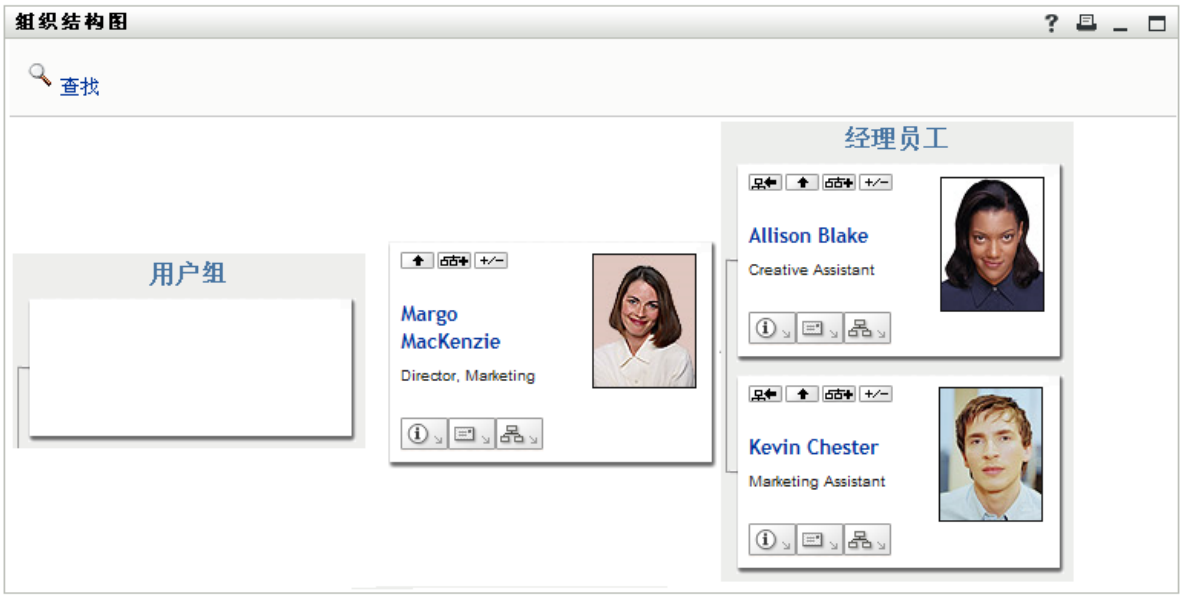
3 从下拉列表中选择关系和操作：

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。

然后她单击至左边并看到：



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*
```

不支持包含短划线的实体名称 显示的实体类型名称中有短划线 (-) 时，组织图中的搜索功能不起作用。本产品不支持名称中包含短划线的实体。

3 单击搜索。

“ 查找 ” 页将显示搜索结果。

如果看到了包含所需用户的用户列表，请继续下一步。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。

显示有关用户的详细信息

您可以显示在组织结构图中选择的用户的细节 （即 “ 配置文件 ” 页）。在**仪表板**中，针对该用户选择查看更多信息或显示快速信息。在 **User Application** 中完成以下步骤：

1 找到要显示其细节的用户的卡片。

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。

“ 配置文件 ” 页面即会显示，列出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。

4 使用完 “ 配置文件 ” 页面后，可以关闭该页面的窗口。

从仪表板中向用户发送电子邮件

您可以从仪表板中快速向用户发送电子邮件。在用户的配置文件中，或在组织结构图中查看用户时，选择用户的电子邮件地址。您的系统应该会在默认电子邮件程序中开启一封将发送给该用户的电子邮件。

从 User Application 中向用户发送电子邮件

本节将说明：

- 向图中的用户发送新电子邮件 （第 53 页）
- 用电子邮件发送图中用户的相关信息 （第 54 页）
- 向经理的小组发送电子邮件 （第 54 页）

向图中的用户发送新电子邮件

1 找到要向其发送电子邮件的用户的名片。

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**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，其他部分均是空白的。

4 填写邮件的内容。

5 发送邮件。

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

4 指定邮件的收件人 （以及所需的其他内容）。

5 发送邮件。

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*列表外其他部分均是空白的，“ 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 填写邮件的内容。

5 发送邮件。

8 管理您的口令

Identity Manager 包含 Self Service Password Reset (SSPR)，以帮助您管理更改口令和重设置忘记的口令的过程。在口令重设置期间， SSPR 使用询问应答鉴定方法来对您进行鉴定。

- 使用 Identity Manager 中的自助式口令管理 （第 55 页）
- 使用旧式口令管理 （第 57 页）

注释：本章将介绍管理您口令的默认功能。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。

使用 Identity Manager 中的自助式口令管理

SSPR 自动与 Identity Applications 和 Identity Reporting 的单点登录过程集成。它是 Identity Manager 的默认口令管理程序。当用户请求重设置口令时， SSPR 要求用户回答询问应答问题。如果答案正确， SSPR 会以下列其中一种方式响应：

- 允许用户创建新口令
- 创建新口令并将它发送给用户
- 创建新口令并将它发送给用户，同时将旧口令标记为已失效。

您可在 SSPR 配置编辑器中配置此响应。升级到 Identity Manager 的新版本之后，您可以将 SSPR 配置为使用 Identity Manager 一贯用来进行口令管理的 NMAS 方法。不过， SSPR 不能识别您用于管理忘记的口令的现有口令策略。要继续使用您的策略，请参见《*NetIQ Identity Manager 安装指南*》中的 " 了解旧式口令管理提供程序 "。您也可以将 SSPR 配置为使用其专用协议而不是 NMAS。进行此更改后，要恢复为使用 NMAS，将只能通过重设置口令策略来实现。

您可以使用 SSPR 来执行表 8-2 中列出的任何功能：

表 8-1 *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： ◆ 对管理员定义的询问问题的有效应答 ◆ 用户定义的询问问题和应答
更改口令	根据系统管理员设置的规则更改 （重设置）口令
口令策略状态	检查您的口令策略要求。

了解口令询问应答

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）

在 Identity Manager 4.5 中，登录过程中登录页面会自动将您重定向到 “ 询问应答 ” 页面。您可在此页面上设置询问问题的应答。有关详细信息，请参见如果您忘记了口令 （第 31 页）。当您再次登录并尝试重设置忘记的口令时， SSPR 会提示配置的问题，并要求您指定正确的答案。如果答案与您以前保存的应答一致， SSPR 便会允许您重设置口令。

更改口令

您可以更改您的口令，前提是系统管理员已授予您相应的权限。

1 在仪表板中单击**应用程序 > 更改我的口令**。

2 键入当前口令。将显示 “ 更改口令 ” 页面。

3 在**新口令**文本框中键入新口令。

4 在**确认口令**文本框中再次键入新口令。

5 单击**更改密码**。

   如果新口令违反管理员在口令策略中定义的任何口令规则，您将会在 “ 更改口令 ” 页面看到一条错误讯息。

   此页面一般提供有关如何指定符合管理员所定义策略要求的口令的信息。查看口令规则，然后重试。

6 单击**继续**。将显示您的请求的状态。成功后，您将回到 OSP 登录页面。

口令策略状态

注释：只有管理员用户才能使用此功能。

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。除非 User Application 管理员已授予您相应的权限，否则您无法查看您的口令策略要求。 User Application 管理员可在 Identity Manager 主页上查看口令策略的状态。此链接默认并不存在。要包含该连接，您需要自定义主页。有关自定义 Identity Manager Home 默认项目的信息，请参见《*NetIQ Identity Manager Home*

and Provisioning Dashboard User Guide》（NetIQ Identity Manager Home and Provisioning Dashboard 用户指南）中的 “Configuring Identity Manager Home” （配置 Identity Manager Home 项目）。

在登录页中，单击**口令状态和策略**链接。**口令策略状态和策略**页面随即显示。要更改 Identity Manager 口令，请转至 Identity Manager Home 并选择更改我的口令。Identity Manager Home 上的该链接会将您重定向到 SSPR 的 “ 更改口令 ” 区域。

使用旧式口令管理

本节说明如何使用 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：

- 口令询问应答 （第 58 页）
- 口令提示更改 （第 58 页）
- 更改口令 （第 58 页）
- 口令策略状态 （第 59 页）
- 口令同步状态 （第 59 页）

注释：本节说明 “ 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 6 章 “ 管理您的配置文件 ” （第 41 页）。

可以视需要使用 “ 口令管理 ” 页执行表 8-2 中列出的任一功能：

表 8-2 *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： ◆ 对管理员定义的询问问题的有效应答 ◆ 用户定义的询问问题和应答
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 （重设置）口令
口令策略状态	检查您的口令策略要求。
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。

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。

2 在每个应答文本框 （它们都是必填的）中键入适当应答，或者使用您以前储存的应答。如果选择使用储存的应答，则不会显示询问应答 （包括标签）。此外，用户定义的询问问题会被禁用。

   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。

   保存询问应答之后， User Application 会显示一条指示询问应答已成功保存的讯息，并再次显示询问应答屏幕，其中的 " 使用储存的应答？ " 处于选中状态。

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）。

   " 口令提示定义 " 页面随即显示。

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。

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：

   如果未应用任何口令策略，则会看到基本的 " 更改口令 " 页面，其中仅提供用于更改口令的字段。

   从版本 4.0.2 起， User Application 支持以下口令语法类型：

   - Microsoft 复杂性策略

     此口令语法类型用于与 Active Directory 2003 保持向后兼容。

   - Microsoft Server 2008 口令策略

     它是新添加到 8.8.7 eDirectory 中的口令语法类型，用于支持 Active Directory 2008。

Microsoft Server 2008 口令策略支持以下设置：

- 使用 Microsoft Server 2008 口令策略
- 口令中复杂性策略违例的最大次数 (0-5)

- Novell 语法

  Novell 语法支持以下新设置：

  - 非字母字符的最低数量 (1-512)
  - 非字母字符的最高数量 (1-512)

对于所有三种口令语法类型， User Application 支持下列功能：

- 与当前口令和历史口令的不同字符数量 (0-6)
- 字符排除时考虑的历史口令数量 (0-10)

如果您的管理员已启用 Microsoft Server 2008 策略语法，请在 " 更改口令 " 页面中的下列字段中填入相应数据：

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**重键入口令**文本框中再次键入新口令。

5 单击**提交**。

如果新口令违反管理员定义的任何口令规则，将会在 " 更改口令 " 页面看到一条错误讯息。如果使用 Microsoft Server 2008 策略，并且口令发生违例，用户界面将在页面顶部显示以下讯息：

```
Password AD2008 complexity policy violation.
```

如果新口令发生违例，请查看由管理员定义的口令规则，然后重试。

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，请参见口令提示更改 （第 58 页）。

7 将显示您的请求的状态。

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。

您不能更改标为无效的项目。

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。

注释：只有管理员可以看到**选择用户**框。

III 管理用户和组

如果您在 Identity Applications 中具有相应的角色，则可创建并管理用户和组。您可以在仪表板和 User Application 中创建用户，还可以在 User Application 中创建和管理组。

9 创建用户或组

本章说明如何在仪表板和 User Application 中创建用户和组。包括以下主题：

- 了解用户和组 （第 63 页）
- 创建用户 （第 63 页）
- 创建组 （第 64 页）
- 使用 User Application 中的编辑按钮 （第 65 页）

了解用户和组

系统管理员可以创建用户和组。系统管理员可允许其他人 （通常是选定的行政或管理职位的人员）访问此功能。

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，您可能会发现与本章中描述的功能有些差异。请咨询系统管理员以了解细节。

要查看哪些用户或组已存在，可使用 " 目录搜索 " 页面。请参见附录 B" 使用 User Application 中的目录搜索 " （第 209 页）。

创建用户

当您创建用户时， Identity Applications 只会显示目录提取层 (DAL) 中已配置为可搜索且可读取的属性。有关详细信息，请参见 《*NetIQ Identity Manager - Administrator's Guide to Designing the Identity Applications*》（NetIQ Identity Manager - 设计 Identity Applications 的管理员指南）中的 "Attribute Properties" （属性）。在 DAL 中添加的 isSearchable 和 isReadable 为 **true** 的用户属性会显示在仪表板的创建用户表单中。 isSearchable 和 isReadable 为 **false** 的任何其他属性均无法在创建用户表单页面中添加或显示。

在仪表板中创建用户

要创建用户，请在仪表板中选择：

人员 > 用户 > +

身份管理员会定义您可以为用户指定的值。此外，当您创建用户时，可以选择用户**容器**，但不能修改其值。此限制可确保所有用户都储存在同一个容器中。

有关详细信息，请参见仪表板帮助。

在 User Application 中创建用户

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**。

用户 - 设置属性面板随即显示。

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	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： `ou=users,ou=MyUnit,o=MyOrg` 要了解如何使用为指定容器而提供的按钮，请参见使用 User Application 中的编辑按钮 （第 65 页）。 如果系统管理员已经为此类型的对象建立了默认的创建容器，则系统不会提示您提供容器。
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，请参见创建用户 （第 63 页）。

5 单击继续。

创建口令面板随即显示。

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。

6 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。

至此便创建了用户和口令，随后，审阅面板将会显示以汇总结果。

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

创建组

如果您在 Identity Applications 中具有管理角色，则可创建组。

1 登录 User Application。

2 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。

3 使用对象类型下拉列表选择组，然后单击继续。

设置此组的属性面板随即显示。

4 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	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： `ou=groups,ou=MyUnit,o=MyOrg` 要了解如何使用为指定容器而提供的按钮，请参见创建用户 （第 63 页）。 **注释：**如果系统管理员已经为此类型的对象建立了默认的创建容器，则系统不会提示您提供容器。
说明	该新组的说明。

5 单击继续。

至此便创建了组，随后，审阅面板将会显示以汇总结果。

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

使用 User Application 中的编辑按钮

表 9-1 列出了您可以用于指定属性值的编辑按钮。

表 9-1 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历史列表。
	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。

查找容器

1 单击要查找容器的某个项右侧的查找：

“ 查找 ” 页面即会显示容器树。

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。

查找用户

1 在要查找其用户的项右侧，单击**查找**：

“ 查找 ” 页面随即显示。

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*
```

经理查找只会搜索身份为经理的用户。

3 单击**搜索**。

“ 查找 ” 页将显示搜索结果。

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。

使用历史列表

1 单击某个项 （要查看该项以前的值）右侧的历史：

历史列表随即显示，其中的值按字母顺序排列。

2 执行以下步骤之一：

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

IV 使用工作仪表板选项卡

以下几章说明如何使用 Identity Manager User Application 的**工作仪表板**选项卡。

- 第 10 章 " 工作仪表板选项卡简介 "（第 71 页）
- 第 11 章 " 管理您的工作 "（第 85 页）
- 第 12 章 " 管理用户、组、容器、角色和小组的工作 "（第 109 页）
- 第 13 章 " 控制您的设置 "（第 113 页）
- 第 14 章 " 发出处理请求 "（第 131 页）

注释：此功能绝大部分已被 Identity Manager 4.6 中引入的仪表板所替代。有关详细信息，请参见第 II 部分 " 管理您的许可权限和身份配置文件 "（第 33 页）和第 III 部分 " 管理用户和组 "（第 61 页）。

---

10 工作仪表板选项卡简介

本章概述工作仪表板选项卡。包括以下主题：

- 关于工作仪表板选项卡 （第 71 页）
- 访问工作仪表板选项卡 （第 71 页）
- 浏览选项卡的功能 （第 72 页）
- 您可以执行的工作仪表板操作 （第 73 页）
- 了解工作仪表板上的图标 （第 74 页）
- 工作仪表板的安全许可权限 （第 75 页）

关于工作仪表板选项卡

通过工作仪表板选项卡可以方便地管理任务、资源和角色。此外，通过它还可以查看请求的状态，以及更改 User Application 中的设置。工作仪表板选项卡仅显示应用程序最重要的功能，让您可以专注于工作。

如果某个请求需要组织中一个或多个人的许可，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。

发出请求时，User Application 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工作仪表板选项卡的内容。工作流程的控制流程以及表单的外观会因设计者和管理员如何配置应用程序而异。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。

访问工作仪表板选项卡

默认情况下，登录到 Identity Manager 用户界面之后，工作仪表板选项卡会打开：

图 10-1 工作仪表板

如果要在转至 Identity Manager 用户界面中的另一选项卡后返回，则只需单击工作仪表板选项卡再次将其打开。

浏览选项卡的功能

本节介绍工作仪表板选项卡的默认功能。（选项卡的外观可能由于针对您组织所做的自定义而不同；请咨询系统管理员或工作流程设计者。）

工作仪表板选项卡右侧会显示几个组成部分，通过它们可以访问典型的 " 工作仪表板 " 操作。以下对这些部分进行了说明：

表 10-1 " 工作仪表板 " 的各个部分

部分	说明
任务通知	通过它您可以检查工作流程队列，确定其中是否有指派给您或其他用户 （您有权管理该用户的任务）的任务。
资源指派	通过它您可以查看您具有哪些资源指派，以及发出申请更多资源指派的请求。
角色指派	通过它您可以查看您具有哪些角色，以及发出申请更多角色指派的请求。
请求状态	通过它您可以查看您发出的请求的状态。可通过该操作查看每个请求的当前状态。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。 请求状态会在单个统一列表中显示包括供应请求、角色请求和资源请求在内的请求。

" 工作仪表板 " 的屏幕左上角还包含一个 " 用户配置文件 " 部分。通过页面的该部分，您可以管理其他用户、组、容器和角色的工作。此外，通过它您可以管理您的设置和小组设置，以及发出处理请求（也称为供应请求）。

以下介绍了 " 用户配置文件 " 部分中的可用操作：

表 10-2 “ 用户配置文件 ” 部分中的可用操作

操作	说明
管理	通过它当前用户可以选择特定用户、组、容器、角色或小组，并使用 “ 工作仪表板 ” 界面来管理选定实体类型的工作。在用户选择某个实体之后，“ 工作仪表板 ” 上的数据和访问权限属于选定的实体，而不是属于当前登录的用户。但是，在用户处于 “ 管理 ” 模式时，设置和发出处理请求菜单仍然应用于已登录用户，而不是管理控件中选定的实体。
设置	通过它您可以充当另一个用户的代理。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。
发出处理请求	通过它您可以发出处理请求 （也称为供应请求）。默认情况下，“ 工作仪表板 ” 的 “ 用户配置文件 ” 部分不包含该操作。 发出处理请求菜单不能用于发出证明、资源或角色请求。提交这些请求的界面取决于您要发出的请求的类型，如下所述： ◆ 要发出证明请求，您需要使用合规性选项卡上的证明请求操作。 ◆ 要发出资源请求，您需要使用工作仪表板选项卡的资源指派部分，或者使用角色和资源选项卡上的资源编目。 ◆ 要发出角色请求，您需要使用工作仪表板选项卡的角色指派部分，或者使用角色和资源选项卡上的角色编目。

您可以执行的工作仪表板操作

“ 工作仪表板 ” 各个部分支持以下操作：

表 10-3 通用的 “ 工作仪表板 ” 操作

操作	说明
指派	指派角色或资源。 仅可用于角色指派和资源指派操作。
去除	去除角色或资源指派。 仅可用于角色指派和资源指派操作。
刷新	刷新显示内容。
自定义	通过它您可以指定要在显示内容中出现哪些列，以及它们的出现顺序。
过滤器	通过它您可以基于选择准则来过滤数据。
行	通过它您可以控制在显示内容的每页显示的行数。

您还可以通过在显示内容中单击标题来对列表中的数据排序。

保存用户自选设置 使用 “ 自定义 ”、“ 过滤器 ” 和 “ 行 ” 操作来自定义 “ 工作仪表板 ” 任意部分的显示内容时，或者更改所显示数据的排序顺序时，您的自定义设置会与您的其他用户自选设置一起保存到身份库中。要允许保存用户自选设置，管理员必须确保设置对于 srvprvUserPrefs 和 srvprvQueryList 属性的许可权限，使用户能够对这些属性进行写操作。

了解工作仪表板上的图标

使用 " 工作仪表板 " 时，您会在许多位置看到传达重要信息的图标。

下表详细说明了 " 工作仪表板 " 中使用的图标：

表 10-4　工作仪表板图标

图标	说明
已声明	表示特定的工作流程任务是否已由某个用户声明。 在 " 工作仪表板 " 的任务通知部分显示。
正在运行：正在处理	表示特定的请求仍在处理中。 在 " 工作仪表板 " 的请求状态部分显示。
已完成：已批准	表示已完成处理且已批准特定的请求。 在 " 工作仪表板 " 的请求状态部分显示。
已完成：已拒绝	表示已完成处理且已拒绝特定的请求。 在 " 工作仪表板 " 的请求状态部分显示。
已终止：已收回	表示某个用户 （提交请求的用户、小组管理者或域管理员 / 域管理者）已收回特定的请求。 在 " 工作仪表板 " 的请求状态部分显示。
已终止：错误	表示特定的请求由于出错而终止。 在 " 工作仪表板 " 的请求状态部分显示。
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。
删除	用于删除代理指派或委托指派。要删除指派，请选择它并单击删除图标。 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。
允许多个收件人	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，则可以使用执行小组处理请求操作将多个用户选择为收件人。 在执行小组处理请求页面显示。
指派给委托	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。 在 " 工作仪表板 " 的任务通知部分显示。
指派给用户	表示已将特定的工作流程任务指派给了某个用户。 在 " 工作仪表板 " 的任务通知部分显示。
指派给组	表示已将特定的工作流程任务指派给了某个组。 在 " 工作仪表板 " 的任务通知部分显示。

图标	说明
已指派给角色	表示已将特定的工作流程任务指派给某个角色。 在 " 工作仪表板 " 的任务通知部分显示。
指派给多个批准者	表示已将特定的工作流程任务指派给了多个用户。 在以下情况下会应用该图标： ◆ 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。 在 " 工作仪表板 " 的任务通知部分显示。
可用于所有请求	表示特定用户可用于所有类型的处理请求。该设置适用于委托。 在编辑可用性和小组可用性页面显示。
不可用于指定的请求	表示在特定的时段内，特定用户对某些类型的处理请求不可用。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。 在编辑可用性和小组可用性页面显示。
不可用于任何请求	表示特定用户对当前系统中的所有处理请求都不可用。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。 在编辑可用性和小组可用性页面显示。

工作仪表板的安全许可权限

本部分说明每个用户在 " 工作仪表板 " 上执行各种操作所需的许可权限。包括以下主题：

- 用户自助服务 （第 75 页）
- 处于管理模式时的域管理员 （第 77 页）
- 处于管理模式时的域管理者 （第 79 页）
- 处于管理模式时的小组管理者 （第 81 页）

用户自助服务

已鉴定用户无需任何安全许可权限即可对 " 工作仪表板 " 上的任务执行自助服务操作，如下表所示。

表 10-5　用户自助服务的任务通知

若要执行以下操作 ...	已鉴定用户必须为 ...	并且用户必须具有以下许可权限 ...
查看列表中的任务	任务的接收人。 或者，接收人已将任务委托给该用户，或该用户为某个组声明了该任务。 **注释：**在自助服务模式下，如果域管理员或域管理者是某个任务的收件人，则他 / 她还可以查看该任务。	无。
查看和处理任务细节	任务的接收人。 或者，接收人已将任务委托给该用户，或该用户为某个组声明了该任务。	无。
查看工作流程注释	任务的接收人。 或者，接收人已将任务委托给该用户，或该用户为某个组声明了该任务。	无。

已鉴定用户需要具有项浏览权限才能指派或去除角色和资源指派，如下表所示。

表 10-6　用户自助服务的角色和资源指派

若要执行以下操作 ...	已鉴定用户必须为 ...	并且用户必须具有以下许可权限 ...
查看列表中的角色或资源	收件人。 指派列表包含用户所属的组和容器的指派。	无。
指派或去除角色或资源的指派	收件人。 授予和撤消操作仅应用于已鉴定用户	受托者 （项浏览）

对于一些请求状态操作，已鉴定用户需要具有项浏览权限，如下表所示。

表 10-7　用户自助服务的请求状态

若要执行以下操作 ...	已鉴定用户必须为 ...	并且用户必须具有以下许可权限 ...
查看列表中的处理请求	发起人或收件人。	无。
处理和查看处理请求细节	发起人或收件人 （如果**限制查看**选项在 Designer 中设置为 false）。 如果**限制查看**选项设置为 true，则即使用户具有浏览权限，也只显示由该用户发起的任务。	受托者 （项浏览）

若要执行以下操作 ...	已鉴定用户必须为 ...	并且用户必须具有以下许可权限 ...
收回处理请求	发起人和收件人。 请求必须处于可收回的状态，即表示它尚未被批准、拒绝、取消或供应。	受托者 （项浏览）
查看处理请求的工作流程注释	发起人或收件人 （如果**限制查看**选项在 Designer 中设置为 false）。 如果**限制查看**选项设置为 true，则即使用户具有浏览权限，也只显示由该用户发起的任务。	受托者 （项浏览）
查看列表中的角色或资源请求	发起人或收件人。	无。
查看和处理角色或资源请求细节	发起人或收件人。	受托者 （项浏览）
收回角色或资源请求	发起人和收件人。 请求必须处于可收回的状态，即表示它尚未被批准、拒绝、取消或供应。	受托者 （项浏览）
查看角色或资源请求的工作流程注释	发起人或收件人。	角色 / 资源受托者 （项浏览）

处于管理模式时的域管理员

在管理模式下，域管理员无需任何安全许可权限即可对 “ 工作仪表板 ” 上的任务执行操作，如下表所示。

表 10-8 *处于管理模式时域管理员的任务通知*

若要执行以下操作 ...	受管用户、组、容器或角色必须为 ...	并且域管理员必须具有以下许可权限 ...
查看列表中的任务	任务的接收人或收件人。 **注释：**角色不能作为任务的收件人。它只能作为任务的接收人。 或者，接收人已将任务委托给该用户，或该用户为某个组声明了该任务。	无。
查看和处理任务细节	任务的接收人或收件人。 或者，接收人已将任务委托给该用户，或该用户为某个组声明了该任务。	无。
查看工作流程注释	任务的接收人或收件人。 或者，接收人已将任务委托给该用户，或该用户为某个组声明了该任务。	无。

在管理模式下，域管理员无需任何安全许可权限即可对 “ 工作仪表板 ” 上的角色和资源指派执行所有操作，如下表所示。

表 10-9　处于管理模式时域管理员的角色和资源指派

若要执行以下操作 ...	受管用户、组或容器必须为 ...	并且域管理员必须具有以下许可权限 ...
查看列表中的角色或资源	收件人。 指派列表包含用户所属的组和容器的指派。	无。
指派或去除角色或资源的指派	收件人。 指派列表包含用户所属的组和容器的指派。	无。 在工作仪表板中，域管理员可以编辑、指派或去除所有角色指派，不在授权其管理的域中的系统角色指派除外。这意味着角色域管理员可以去除角色管理员和角色管理者指派，但无法去除资源管理员或资源管理者指派。 域管理员可以查看和编辑所有资源。

在管理模式下，域管理员无需任何安全许可权限即可对 “ 工作仪表板 ” 上的请求状态执行自助服务操作，如下表所示。

表 10-10　处于管理模式时域管理员的请求状态

若要执行以下操作 ...	受管用户、组或容器必须为 ...	并且域管理员必须具有以下许可权限 ...
查看列表中的处理请求	发起人或收件人。	无。
处理和查看处理请求细节	发起人或收件人。	无。
收回处理请求	发起人或收件人。	无。
查看处理请求的工作流程注释	发起人或收件人。	无。
查看列表中的角色或资源请求	发起人或收件人。	无。
查看和处理角色或资源请求细节	发起人或收件人。 域管理员无法查看系统角色的请求。	无。 域管理员可以查看除系统角色请求之外的所有角色请求。 域管理员可以查看和编辑所有资源。
收回角色或资源请求	发起人或收件人。 请求必须处于可收回的状态。 域管理员无法收回系统角色的请求。	无。 域管理员可以收回除系统角色请求之外的所有角色请求。 域管理员可以查看和编辑所有资源。

若要执行以下操作 ...	受管用户、组或容器必须为 ...	并且域管理员必须具有以下许可权限 ...
查看角色或资源请求的工作流程注释	发起人或收件人。 域管理员无法查看系统角色的工作流程注释。	无。 域管理员可以查看和编辑除系统角色之外的所有角色。 域管理员可以查看和编辑所有资源。

处于管理模式时的域管理者

在管理模式下，域管理者无需任何安全许可权限 （但必须具有查看任务细节和工作流程注释的许可权限）即可查看任务，如下表所示。

表 10-11 *处于管理模式时域管理者的任务通知*

若要执行以下操作 ...	受管用户、组、容器或角色必须为 ...	并且域管理者必须具有以下许可权限 ...
查看列表中的任务	任务的接收人或收件人。 **注释：**角色不能作为任务的收件人。它只能作为任务的接收人。 或者，接收人已将任务委托给该用户，或该用户为某个组声明了该任务。	无。
查看任务细节	任务的接收人或收件人。 或者，接收人已将任务委托给该用户，或该用户为某个组声明了该任务。	管理接收人任务。
查看工作流程注释	任务的接收人或收件人。 或者，接收人已将任务委托给该用户，或该用户为某个组声明了该任务。	管理接收人任务。

在管理模式下，域管理者无需任何安全许可权限 （但必须具有指派角色和资源或去除现有指派的许可权限）即可查看角色和资源指派，如下表所示。

表 10-12　处于管理模式时域管理者的角色和资源指派

若要执行以下操作 ...	受管用户、组或容器必须为 ...	并且域管理者必须具有以下许可权限 ...
查看列表中的角色或资源	收件人。 指派列表包含用户所属的组和容器的指派。	无。
指派或去除角色或资源的指派	收件人。 指派列表包含用户所属的组和容器的指派。	角色的以下一种或多种受托者许可权限： ◆ 将角色指派给用户 ◆ 从用户撤消角色 ◆ 将角色指派给组和容器 ◆ 从组和容器撤消角色 资源的以下一种或多种受托者许可权限： ◆ 指派资源 ◆ 撤消资源

在管理模式下，域管理者无需任何安全许可权限 （但必须具有查看请求细节和工作流程注释的许可权限，以及收回请求的许可权限）即可查看处理、角色和资源请求，如下表所示。

表 10-13　处于管理模式时域管理者的请求状态

若要执行以下操作 ...	受管用户、组或容器必须为 ...	并且域管理者必须具有以下许可权限 ...
查看列表中的处理请求	发起人或收件人。	无。
处理和查看处理请求细节	发起人或收件人。	查看运行的 PRD
收回处理请求	发起人或收件人。	收回 PRD
查看处理请求的工作流程注释	发起人或收件人。	查看运行的 PRD
查看列表中的角色或资源请求	发起人或收件人。	无。
查看和处理角色或资源请求细节	发起人或收件人。	查看角色或查看资源 “ 查看角色 ” 许可权限控制您是否可以在 “ 工作仪表板 ” 的 “ 请求状态 ” 部分中看到角色请求的细节。 “ 查看资源 ” 许可权限控制您是否可以看到资源请求的细节。

若要执行以下操作 ...	受管用户、组或容器必须为 ...	并且域管理者必须具有以下许可权限 ...
收回角色或资源请求	发起人或收件人。 请求必须处于可收回的状态	角色的以下一种或多种受托者许可权限： ◆ 将角色指派给用户 ◆ 将角色指派给组和容器 ◆ 更新角色 ◆ 从用户撤消角色 ◆ 从组和容器撤消角色 资源的以下受托者许可权限： ◆ 撤消资源
查看角色或资源请求的工作流程注释	发起人或收件人。	查看角色或查看资源

处于管理模式时的小组管理者

在管理模式下，小组管理者无需任何安全许可权限 （但必须具有查看任务细节和工作流程注释的许可权限）即可查看任务，如下表所示。

表 10-14 处于管理模式时小组管理者的任务通知

若要执行以下操作 ...	受管用户必须为 ...	并且小组管理者必须具有以下许可权限 ...
查看列表中的任务	小组的成员，并且也是任务的接收人。 或者，接收人已将任务委托给该用户，或该用户为某个组声明了该任务。	无。
查看任务细节	小组的成员，并且也是任务的接收人。 或者，接收人已将任务委托给该用户，或该用户为某个组声明了该任务。	管理接收人任务。
查看工作流程注释	小组的成员，并且也是任务的接收人。 或者，接收人已将任务委托给该用户，或该用户为某个组声明了该任务。	管理接收人任务

在管理模式下，小组管理者无需任何安全许可权限 （但必须具有指派角色和资源的许可权限，或去除现有指派的许可权限）即可查看角色和资源指派，如下表所示。

表 10-15　处于管理模式时小组管理者的角色和资源指派

若要执行以下操作 ...	受管用户必须为 ...	并且小组管理者必须具有以下许可权限 ...
查看列表中的角色或资源	选定小组的成员。 用户必须同时也是收件人。 角色指派列表包含用户所属的组和容器的指派。 资源指派列表中只会包含受管用户的指派。	无。
指派或去除角色或资源的指派	选定小组的成员。 用户必须同时也是收件人。 指派列表包含用户所属的组和容器的指派。	角色的以下一种或多种受托者许可权限： ◆ 将角色指派给用户 ◆ 从用户撤消角色 ◆ 将角色指派给组和容器 ◆ 从组和容器撤消角色 资源的以下一种或多种受托者许可权限： ◆ 指派资源 ◆ 撤消资源

在管理模式下，小组管理者无需任何安全许可权限 （但必须具有查看请求细节和工作流程注释的许可权限，以及收回请求的许可权限）即可查看处理、角色和资源请求，如下表所示。

表 10-16　处于管理模式时小组管理者的请求状态

若要执行以下操作 ...	受管用户必须为 ...	并且小组管理者必须具有以下许可权限 ...
查看列表中的处理请求	发起人或收件人。	无。
处理和查看处理请求细节	发起人或收件人。	查看运行的 PRD
收回处理请求	发起人或收件人。	收回 PRD
查看处理请求的工作流程注释	发起人或收件人。	查看运行的 PRD
查看列表中的角色或资源请求	发起人或收件人。	无。
查看和处理角色或资源请求细节	发起人或收件人。	查看角色或查看资源 “ 查看角色 ” 许可权限控制您是否可以在 “ 工作仪表板 ” 的 “ 请求状态 ” 部分中看到角色请求的细节。 “ 查看资源 ” 许可权限控制您是否可以看到资源请求的细节。

若要执行以下操作 ...	受管用户必须为 ...	并且小组管理者必须具有以下许可权限 ...
收回角色或资源请求	发起人或收件人。 请求必须处于可收回的状态。	角色的以下一种或多种受托者许可权限： ◆ 将角色指派给用户 ◆ 将角色指派给用户和组 ◆ 更新角色 ◆ 从用户撤消角色 ◆ 从组和容器撤消角色 资源的以下受托者许可权限： ◆ 撤消资源
查看角色或资源请求的工作流程注释	发起人或收件人。	查看角色或查看资源

11 管理您的工作

本章介绍 " 工作仪表板 " 页面支持的操作。包括以下主题：

- 使用任务 （第 85 页）
- 处理资源 （第 93 页）
- 处理角色 （第 97 页）
- 查看请求状态 （第 101 页）

使用任务

通过**任务通知**操作您可以检查工作流程队列，确定其中是否有已指派给您或者某个用户、组、容器或角色 （您有权管理它的任务）的任务。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个用户、组或角色

注释：要重指派任务，您必须是具有**管理接收人任务**许可权限的供应管理员或供应管理者 （或小组管理者）。如果不具有该许可权限，则**重指派**按钮将不可用。

对于不具有任何管理特权的业务用户，只有他是某个任务的接收人时，才能看到该任务。如果他是某个任务的收件人，则他看不到该任务。向业务用户显示的任务列表中包含未声明的任务。

或者，接收人已将任务委托给该业务用户，或该用户为某个组声明了该任务。

注释：业务用户不需要具有对于启动工作流程的供应请求定义的目录浏览权限，就可以看到自己作为接收人的任务。

供应管理员和供应管理者可以管理其他用户的任务，如下所述：

- 如果在**管理**控件中未做任何选择，则任务列表会显示当前用户的任务。这些任务包括：用户作为收件人或接收人的任务，以及收件人或接收人是当前用户所属的组、容器或角色的任务。供应管理员或供应管理者可以对自己的任务执行任何操作，因为处理自己的任务不需要任何权限。
- 如果在**管理**控件中选择了某个用户，则列表会显示使用选定用户作为接收人的任务，以及该用户是收件人的那些任务。供应管理员或供应管理者可以对任务列表进行过滤，使之仅显示受管用户是接收人的那些任务。或者，用户可以对任务列表进行过滤，使之仅显示受管用户作为收件人的那些任务。
- 如果选择了某个组，则列表会显示使用选定组作为接收人的任务，以及该组是收件人的那些任务。供应管理员、供应管理者或小组管理者可以对任务列表进行过滤，使之仅显示受管组是接收人的那些任务。或者，用户可以对列表进行过滤，使之仅显示受管组是收件人的那些任务。
- 如果选择某个角色，则列表会显示使用选定角色作为接收人的任务。不能将角色指定为任务的收件人。
- 如果选择某个容器，则列表会显示使用选定容器作为收件人的任务。不能将容器指定为任务的接收人。

供应域的小组管理者可以管理小组成员的任务。在选择小组成员之前，小组管理者必须先选择小组。

通过任务通知操作，您可处理与资源请求、角色请求、处理请求和证明请求相关联的任务。在有些情况下，用户界面可能会因您选择处理的任务类型而异。对于证明请求，任务通知操作只显示将当前用户指定为证明者的那些任务。

声明与某个资源、角色或处理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 11-1 *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。
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个活动。 “ 拒绝 ” 操作适用于单个任务。用户界面不允许您对一组任务执行该操作。

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。

查看任务列表

要查看向您指派的任务，请执行下列操作：

1 在 “ 工作仪表板 ” 的操作组中单击任务通知。

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。

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会显示任务名称证明批准。

查看任务的摘要

要查看任务的摘要信息，请将鼠标指针停在任务列表中的任务名称上。

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。

此时会显示 " 任务细节 " 表单，它显示在一个讯息窗口中或内嵌在任务列表中。该行为由自定义对话框中的一个设置控制。下图显示了内嵌的 " 任务细节 " 表单：

下图显示了处于讯息窗口中的 " 任务细节 " 表单：

当一项任务指派给多个批准者时，" 任务细节 " 表单将显示多个批准者图标 （在指派给字段旁），并在该图标下显示文本以表示需要多个批准。

2 要显示关于指派给多个批准者的任务的详细信息，请单击多个批准者图标下的文本。

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，请遵循声明任务 （第 88 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 单击**注释和流程历史**。

4b 要显示用户注释，请单击**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）将是用户名。工作流程系统生成的注释将被自动本地化。
- 注释文本，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。有关详细信息，请参见 《*NetIQ Identity Manager - Administrator's Guide to Designing the Identity Applications*》（NetIQ Identity Manager - 设计 Identity Applications 的管理员指南）。

4c 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。活动列表包括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）将是用户名。工作流程系统生成的注释将被自动本地化。
- 注释文本，指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。

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

4e 单击**关闭**可关闭此窗口。

5 要返回到任务列表，请单击**后退**。

声明任务

要声明一个待处理的任务，请执行下列操作：

1 单击**声明**。

对于资源、角色和处理请求，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所有其他操作按钮，并且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，该表单显示需要您审阅的用户简介数据。

对于角色指派、用户指派和 SoD 证明流程，该表单包含显示需要您审阅的数据的报告。

对于所有证明类型，该表单显示一些控件，以便您回答必要的证明问题以及证明流程中包含的其他调查问题。

如果管理员为系统配置了数字签名，并且任务需要数字签名，页面右上角会显示**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 选择您要用的证书并单击**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。

注释：如果通过 " 工作仪表板 " 上的任务列表访问任务，任务完成窗口会在右上角提供关闭按钮 (**X**)。但是，如果通过电子邮件链接或通过深度链接访问并完成任务，任务完成窗口上的关闭按钮将不可用。

重指派任务

要重指派任务，请执行下列任务：

1 在 " 任务细节 " 窗口中单击**重指派**。

注释：要重指派任务，您必须是具有**管理接收人任务**许可权限的供应管理员或供应管理者 （或小组管理者）。如果不具有该许可权限，则**重指派**按钮将不可用。

---

2 单击所选输入框旁的**对象选择器**图标 。

3 在**新指派给**下拉列表中选择要向其重指派该任务的用户。

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。

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。在 " 任务细节 " 窗口中单击**释放**。

过滤任务列表

您可以通过对任务列表应用过滤器来限制返回的行数。通过过滤任务列表，可以更简便地找到要查找的任务，并提高性能。

要为任务列表定义过滤器，请执行下列操作：

1 单击**定义过滤器**按钮。

此时会显示 " 过滤器 " 对话框，其中显示了几个可用于指定数据过滤方式的字段。

2 要将搜索范围缩小为查找当前实体配置文件 （当前登录用户或在**管理**控件中选择的用户、组、容器或角色）是接收人的任务，可以在**任务执行人**字段中选择**指派给**。

注释：**任务执行人**字段对于最终用户不可用，因为最终用户只能看到他们自己是接收人的任务。只有域管理员、域管理者和小组管理者可以看到**任务执行人**字段。

---

3 要将搜索范围缩小为查找当前实体配置文件是收件人的任务，可以在任务执行人字段中选择收件人。

4 要包含当前实体配置文件是接收人或收件人的所有任务，请确保不要在任务执行人字段中选择任何选项。

5 要将搜索范围缩小为查找在特定时间点之前超时的任务，可以选择超时单位 （周、天或小时）并在超时字段中输入一个值。

6 单击过滤器，使用在 " 过滤器 " 对话框中指定的选择准则执行新的任务查询。

为任务列表定义过滤器时，过滤器定义会与您的其他用户自选设置一起保存到身份库中。

注释：无论是否在管理控件中选择了其他用户，所保存的自选设置始终应用于当前登录到 User Application 的用户。

要查看以前定义了哪些过滤器点，请执行下列操作：

1 查看定义过滤器图标左侧的框。

如果未定义任何过滤器，定义过滤器图标会显示两个空环。

如果已经定义了一个或多个过滤器点，则每个过滤器点会显示在单独的框中，如下所示：

要去除以前在 " 过滤器 " 对话框中指定的过滤器点，请执行下列操作：

1 单击要去除的过滤器点旁边的清除此过滤器图标 （看起来像一个 X）。

要去除所有以前定义的过滤器并将搜索结果更新为包含所有任务，请执行下列操作。

1 单击定义过滤器按钮来打开 " 过滤器 " 对话框。

2 单击清除过滤器按钮。

此时 " 过滤器 " 对话框会关闭，并且任务列表更新为包含所有任务。

自定义任务列

通过 " 工作仪表板 " 页面的 " 任务通知 " 部分，您可以选择和取消选择列，以及对任务列表显示内容中的列重新排序。该行为由 " 自定义任务通知显示 " 对话框中的一个设置控制。

在修改列的列表或对列重新排序时，您的自定义设置会与您的其他用户自选设置一起保存到身份库中。

要自定义任务列表中的列的显示方式，请执行下列操作：

1 在 " 工作仪表板 " 页面的任务通知部分中，单击自定义任务通知显示按钮。

User Application 会显示当前为显示内容选择的列的列表，以及可供选择的其他列的列表。

2 要在显示内容中包含其他列，可以选择可用列列表框中的列，并将它拖到选定列列表框中。

要在列表中选择多列，可以按住 Ctrl 键并选择这些列。要在列表中选择一起显示的某个列范围，可以按住 Shift 键并选择这些列。

您可以通过在选定列列表框中上移或下移某些列，对显示内容中的列重新排序。

3 要从显示内容中去除某个列，可以选择选定列列表框中的列，并将它拖到可用列列表框中。

任务和优先级列是必选列，不能从任务列表显示中去除。

4 要保存更改，请单击保存。

控制任务列表默认情况下是否展开

通过 “ 工作仪表板 ” 页面可以指定默认情况下，任务列表在页面的 “ 任务通知 ” 部分中是否展开。该行为由 “ 自定义任务通知显示 ” 对话框中的一个设置控制。

在修改该设置时，您的自选设置会与您的其他用户自选设置一起保存到身份库中。

要指定默认情况下是否展开任务列表，请执行下列操作：

1 在 “ 工作仪表板 ” 页面的**任务通知**部分中，单击**自定义任务通知显示**按钮。

   User Application 会显示 “ 自定义任务通知显示 ” 对话框，通过该对话框可以自定义任务列表的显示方式。所显示的控件组合会因管理员将哪些设置指定为可供用户覆盖而异。

2 要在默认情况下展开任务列表显示，请选择**默认情况下展开任务通知**复选框。要在默认情况下隐藏任务列表显示，请取消选择**默认情况下展开任务通知**复选框。

   默认情况下展开任务通知复选框控制 “ 工作仪表板 ” 的 “ 任务通知 ” 部分的初始外观。请注意，无论是选择还是取消选择该复选框，您都可以在页面的 “ 任务通知 ” 部分展开或折叠任务列表。

3 要保存更改，请单击**保存更改**。

控制任务细节的显示

通过 “ 工作仪表板 ” 页面可以指定，在页面的 “ 任务通知 ” 部分中单击任务时，如何显示任务的细节。您可以在列表中或单独的模态对话框中显示任务细节。该行为由 “ 自定义任务通知显示 ” 对话框中的一个设置控制。

在修改该设置时，您的自选设置会与您的其他用户自选设置一起保存到身份库中。

要控制任务细节的显示，请执行下列操作：

1 在 “ 工作仪表板 ” 页面的**任务通知**部分中，单击**自定义任务通知显示**按钮。

   User Application 会显示 “ 自定义任务通知显示 ” 对话框，通过该对话框可以自定义任务列表的显示方式。所显示的控件组合会因管理员将哪些设置指定为可供用户覆盖而异。

2 要在任务列表显示内容中显示细节，请在**打开任务细节**下拉列表中选择**在列表行中**。要在单独的模态对话框中显示细节，请选择**在讯息窗口中**。

3 要保存更改，请单击**保存更改**。

设置打开任务的声明操作

通过 “ 工作仪表板 ” 页面，您可以控制声明一个任务需要何种操作。您可以指定必须明确声明任务，也可以指定打开任务这一操作自动声明任务供您使用。该行为由 “ 自定义任务通知显示 ” 对话框中的一个设置控制。

在修改该设置时，您的自选设置会与您的其他用户自选设置一起保存到身份库中。

要指定声明一个任务需要何种操作，请执行下列操作：

1 在 “ 工作仪表板 ” 页面的**任务通知**部分中，单击**自定义任务通知显示**按钮。

   User Application 会显示 “ 自定义任务通知显示 ” 对话框，通过该对话框可以自定义声明操作。所显示的控件组合会因管理员将哪些设置指定为可供用户覆盖而异。

2 要指定打开任务这一操作自动声明任务供您使用，请选择查看任务细节时自动声明任务复选框。要指定必须明确声明任务，请取消选中该复选框。

3 要保存更改，请单击保存更改。

对任务列表排序

要对任务列表排序，请执行下列操作：

1 单击要作为排序依据的列的标题。

金字塔形状的排序指示符会指示哪一个列是新的主排序列。升序排序时，排序指示符以正常的直立方式显示。

降序排序时，排序指示符以倒立方式显示。

初始排序列由 RBPM 配置管理员设置。如果使用 “ 请求 ” 列之外的任何其他列作为列表排序依据，“ 请求 ” 列会用作二级排序列。

如果覆盖了初始排序列，则会将您的排序列添加到自定义任务通知显示对话框的必选列的列表中。必选列使用星号 (*) 指示。

在修改任务列表的排序顺序时，您的自选设置会与您的其他用户自选设置一起保存到身份库中。

刷新任务列表

要刷新任务列表，请单击刷新按钮。

控制页面中显示的项数

要指定在每页中显示的项数，请执行下列操作：

1 在行下拉列表中选择一个数字。

在修改行设置时，您的自选设置会与您的其他用户自选设置一起保存到身份库中。

查看任务的注释

要显示任务的注释文本，请单击任务列表中的 “ 注释 ” 图标。

注释：要查看任务的注释，您必须在选定列的列表中包含 “ 注释 ” 列。有关向任务列表中添加列的细节，请参见自定义任务列 （第 91 页）。

处理资源

通过资源指派操作，您可以查看您具有哪些资源指派，以及发出申请更多资源指派的请求。

资源管理员和资源管理者可以查看其他用户的资源指派，如下所述：

- 如果在管理控件中未做任何选择，则资源指派列表会显示当前用户的资源指派。这些资源指派包括：用户作为收件人或接收人的资源，以及收件人或接收人是当前用户所属的组、容器或角色的资源。用户可以对自己的资源指派执行任意操作，因为处理自己的资源无需任何权限。
- 如果在管理控件中选择了某个用户，则列表会显示使用选定用户作为收件人的资源指派。

- 如果选择了某个组，则列表会显示通过角色指派间接指派给选定组的资源指派。
- 如果选择了某个角色，则资源指派部分会显示一条讯息，指示通过角色指派授予的资源未显示。要查看角色的资源指派，您需要查看角色选项卡。
- 如果选择了某个容器，则列表会显示通过角色指派间接指派给选定容器的资源指派。

资源域的小组管理者可以管理小组成员的资源。在选择小组成员之前，小组管理者必须先选择小组。

在小组管理者处于管理模式时，资源指派列表只包含与为选定小组配置指定的域相关联的资源指派。

代理模式 资源指派操作在代理模式下不可用。

查看资源指派

要查看您自己的或在管理控件中选择的用户、组或容器的资源指派，请执行下列操作：

1 在 " 工作仪表板 " 的操作组中单击资源指派。

   此时会显示资源的列表。如果您不处于受管模式，则所显示的资源指派是您作为收件人的那些资源指派。如果您处于受管模式，则所显示的资源指派是选定用户、组或容器作为收件人的资源指派。对于组和容器，所列出的资源是通过角色指派间接指派给选定组或容器的那些资源。组或容器的资源指派列表不包含直接指派给选定组或容器中的用户的资源。

   注释：资源只能直接指派给用户。但是，包含某个资源的角色可以指派给组或容器，这种情况下，该资源将间接指派给组或容器中的所有用户。仪表板上的资源指派列表会显示用户的直接指派，以及组和容器的间接指派。

过滤资源指派列表

1 在资源指派显示内容的右上角单击 " 显示过滤器 " 按钮。
2 指定与资源指派关联的初始请求说明、资源名称、说明或参数的过滤字符串。
3 单击过滤器来应用您的选择准则。
4 要去除当前过滤器，请单击清除。

设置页面的最大行数

1 单击行下拉列表，然后选择要在每页显示的行数。

在资源指派列表中滚动

要在资源指派列表中滚动到另一页，请单击列表底部的 " 下一页 "、" 上一页 "、" 第一页 " 或 " 最后一页 " 按钮。

对资源指派列表排序

要对资源指派列表排序，请单击要作为排序依据的列的标题。

金字塔形状的排序指示符会指示哪一个列是新的主排序列。升序排序时，排序指示符以正常的直立方式显示。

降序排序时，排序指示符以倒立方式显示。

初始排序列由 RBPM 配置管理员决定。

如果覆盖了初始排序列，则会将您的排序列添加到必选列的列表中。必选列使用星号 (*) 指示。

在修改资源指派列表的排序顺序时，您的自选设置会与您的其他用户自选设置一起保存到身份库中。

请求资源指派

要发出资源指派请求，请执行下列操作：

1 在页面的 " 资源指派 " 部分顶部单击**指派**按钮。

注释：您需要具有**资源指派**导航许可权限才能看到 " 指派 " 按钮。

" 工作仪表板 " 随即会显示**指派资源**对话框，通过该对话框可以指定要请求的资源。

2 在**初始请求说明**字段中输入关于指派的说明文本。

3 单击 " 对象选择器 " 来搜索要指派的资源。

4 在 " 对象选择器 " 中，输入搜索字符串并单击 " 搜索 "。

5 选择所需的资源。

" 添加资源 " 对话框现在会显示选定的资源，以及在资源请求表单中定义的所有其他字段。

6 如果资源需要权利参数值，您需要使用对象选择器选择要用于该资源指派的值。

选择您要用的参数并单击**添加**。

7 如果表单中还有其他自定义字段，则一并填写这些字段。

8 单击**提交**发出资源请求。

刷新资源指派列表

要刷新资源指派列表，请单击**刷新**。

去除资源指派

要去除资源指派，请选择以前定义的资源指派，然后单击**去除**。

注释：您需要具有**资源去除**导航许可权限才能看到**去除**按钮。

自定义资源指派列表显示

通过仪表板的**资源指派**部分，您可以选择和取消选择列，以及对任务列表显示内容中的列重新排序。列的选择和顺序由 " 自定义资源指派显示 " 对话框中的设置控制。在修改列的列表或对列重新排序时，您的自定义设置会与您的其他用户自选设置一起保存到身份库中。

要自定义列的显示方式，请执行下列操作：

1 在仪表板的 " 资源指派 " 部分单击**自定义**。

User Application 会显示当前为显示内容选择的列的列表，以及可供选择的其他列的列表。

2 要在显示内容中包含其他列，可以选择**可用列**列表框中的列，并将它拖到**选定列**列表框中。

要在列表中选择多列，可以按住 Ctrl 键并选择这些列。要在列表中选择一起显示的某个列范围，可以按住 Shift 键并选择这些列。

您可以通过在选定列列表框中上移或下移某些列，对显示内容中的列重新排序。

3 要从显示内容中去除某个列，可以选择选定列列表框中的列，并将它拖到可用列列表框中。

资源名称列是必选列，不能从任务列表显示中去除。

4 要保存更改，请单击保存更改。

打印资源指派列表

仪表板的资源指派部分允许您打印页面上显示的资源指派列表。屏幕上的内容与打印资源指派列表时的内容实际上是相同的，但打印输出仅包括屏幕上的文本。指派给列或状态列中显示的任何图像都不会显示在打印输出中。

要打印资源指派，您需要在工作仪表板导航区域内具有资源指派打印导航许可权限。

打印资源指派列表：

1 在仪表板的资源指派部分单击打印视图。

User Application 会在单独的窗口中显示资源指派列表的可打印版本：

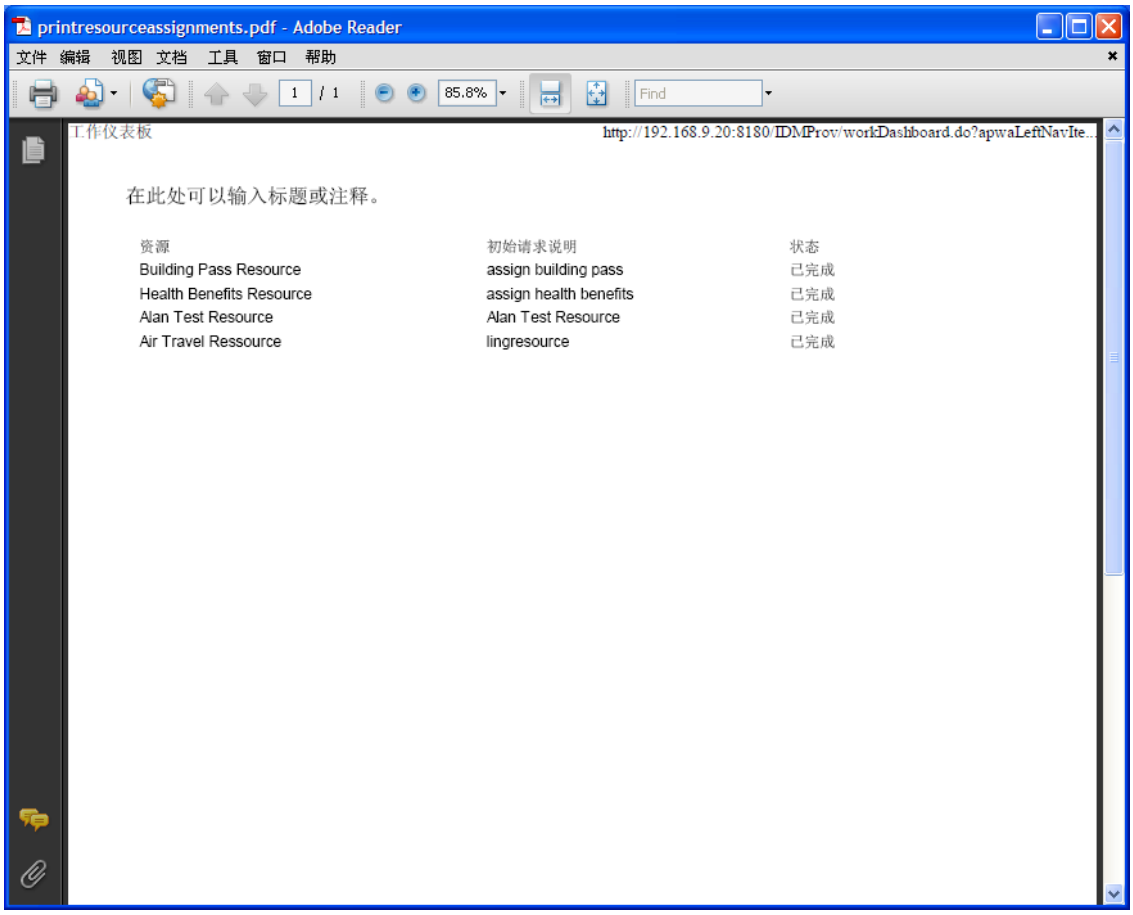
2 选择打印视图顶部的文本框中的文本。

在文本框中键入标题或添加注释。

3 单击打印。

可以直接打印到打印机，或打印到 PDF 文件。

下面是 PDF 示例，显示了打印输出的结果：



屏幕上显示的所有行都会打印出来，除非显示的行数达到了查询返回的最大结果数设置中定义的限制，它是由配置管理员在管理选项卡中指定的。如果达到了该限制，您会看到一个确认对话框，允许您指定是否要继续。如果想要在打印输出中包括屏幕上显示的所有行，请单击确定。对于每次用户会话，该讯息仅显示一次。

处理角色

通过角色指派操作，您可以查看您具有哪些角色指派，以及发出申请更多角色指派的请求。

角色管理员和角色管理者可以查看其他用户的角色指派，如下所述：

- 如果在管理控件中未作任何选择，则角色指派列表会显示当前用户的指派。这些角色指派包括：用户作为接收人或收件人的角色指派，以及接收人或收件人是当前用户所属的组、容器或角色的角色指派。用户可以对自己的角色指派执行任意操作，因为处理自己的角色无需任何权限。
- 如果在管理控件中选择了某个用户，则列表会显示使用选定用户作为接收人的直接和间接角色指派。在选择用户之前，小组管理者必须先选择小组。
- 如果选择了某个组，则列表会显示直接指派给选定组的角色。角色指派列表不包含指派给选定组或容器中的用户的角色。此外，其中不包括与直接指派给该组的角色相关的那些角色。
- 如果选择了某个角色，则角色指派部分会显示一条讯息，指示角色指派未显示。要查看特定角色的角色关系，您需要查看角色选项卡。
- 如果选择了某个容器，则列表会显示直接指派给选定容器的角色。角色指派列表不包含指派给选定容器中的用户的角色。此外，其中不包括与直接指派给该容器的角色相关的那些角色。

角色域的小组管理者可以管理小组成员的角色指派。在选择小组成员之前，小组管理者必须先选择小组。

“ 角色指派 ” 部分不会显示角色关系。要查看特定角色的角色关系，您需要查看 “ 角色关系 ” 选项卡，它可通过 “ 角色 ” 选项卡上的 “ 角色编目 ” 操作访问。

代理模式 角色指派操作在代理模式下不可用。

查看角色指派

要查看您自己的或在管理控件中选择的用户、组或容器的角色指派，请执行下列操作：

1 在 “ 工作仪表板 ” 的操作组中单击角色指派。

   此时会显示角色的列表。如果您不处于受管模式，则所显示的角色指派是您作为收件人的那些角色指派。

   如果您处于受管模式，则所显示的角色指派是选定用户、组或容器作为收件人的角色指派。

   角色可以指派给组或容器，这种情况下，该角色将间接指派给组或容器中的所有用户。仪表板上的角色指派列表会显示用户的直接指派，以及组和容器的间接指派。此外，如果某个用户被直接指派给某个父角色，则列表中会包含该指派，以及与该父角色相关的所有子角色的指派。例如，如果某个级别 30 角色 （父角色）向级别 20 角色 （子角色）添加了角色关系，而某个用户被直接指派给该父角色，则角色指派会同时显示这两种指派 （父角色和子角色）。如果在角色编目中查看子角色，将会在角色关系选项卡上看到角色之间的关系，但不会在角色指派选项卡上看到。

过滤角色指派列表

1 在角色指派显示内容的右上角单击 “ 定义过滤器 ” 按钮。

2 指定初始请求说明或角色名称的过滤字符串，或者通过选择指派类型 （用户、组、容器或角色）和一组属于选定指派类型的身份来缩小搜索范围。或者，您也可以通过选择角色指派的来源类型（指派给角色的用户、指派给角色的组、指派给角色的容器或与角色关联的角色）来缩小搜索范围。

   注释：选择组作为用于过滤的指派类型时，过滤器标题中将会显示 CN，而结果会显示另一个相关字段。

3 单击过滤器来应用您的选择准则。

4 要去除当前过滤器，请单击清除。

设置页面的最大行数

单击行下拉列表，然后选择要在每页显示的行数。

在角色指派列表中滚动

要在角色指派列表中滚动到另一个页面，请单击列表底部的下一页、上一页、第一页或最后一页按钮。

对角色指派列表排序

要对角色指派列表排序，请执行下列操作：

1 单击要作为排序依据的列的标题。

金字塔形状的排序指示符会指示哪一个列是新的主排序列。升序排序时，排序指示符以正常的直立方式显示。

降序排序时，排序指示符以倒立方式显示。

初始排序列由 RBPM 配置管理员决定。

如果覆盖了初始排序列，则会将您的排序列添加到必选列的列表中。必选列使用星号 (*) 指示。

在修改角色指派列表的排序顺序时，您的自选设置会与您的其他用户自选设置一起保存到身份库中。

请求角色

要发出角色指派请求，请执行下列操作：

1 在页面的**角色指派**部分顶部单击**指派**按钮。

注释：您需要具有**角色指派**导航许可权限才能看到**指派**按钮。

“ 工作仪表板 ” 会显示**指派角色**对话框，通过该对话框可以指定要请求的角色。

2 填写**添加角色指派**对话框中的字段：

   2a 在**初始请求说明**字段中输入关于请求原因的说明文本。

   2b 在 “ 对象选择器 ” 中，输入搜索字符串并单击 “ 搜索 ”。选择要指派的角色。

   单击 “ 对象选择器 ” 来搜索要指派的角色。

   2c 在**生效日期**字段中指定角色指派的开始日期。

   2d 在**失效日期**字段中指定角色指派的失效日期。

3 单击**指派**提交请求。

刷新角色指派列表

要刷新角色指派列表，请单击**刷新**。

去除角色指派

要去除角色指派，请选择以前定义的角色指派，然后单击**去除**。

注释：您需要具有**角色去除**导航许可权限才能看到**去除**按钮。

自定义角色指派列表显示

通过仪表板的**角色指派**部分，您可以选择和取消选择列，以及对任务列表显示内容中的列重新排序。列的选择和顺序由 “ 自定义角色指派显示 ” 对话框中的设置控制。在修改列的列表或对列重新排序时，您的自定义设置会与您的其他用户自选设置一起保存到身份库中。

要自定义列的显示方式，请执行下列操作：

1 在仪表板的 “ 角色指派 ” 部分单击**自定义**。

   User Application 会显示当前为显示内容选择的列的列表，以及可供选择的其他列的列表。

2 要在显示内容中包含其他列，可以选择**可用列**列表框中的列，并将它拖到**选定列**列表框中。

要在列表中选择多列，可以按住 Ctrl 键并选择这些列。要在列表中选择一起显示的某个列范围，可以按住 Shift 键并选择这些列。

您可以通过在**选定列**列表框中上移或下移某些列，对显示内容中的列重新排序。

3 要从显示内容中去除某个列，可以选择**选定列**列表框中的列，并将它拖到**可用列**列表框中。

角色列是必选列，不能从任务列表显示中去除。

4 要保存更改，请单击**保存更改**。

打印角色指派列表

仪表板的**角色指派**部分允许您打印页面上显示的角色指派列表。屏幕上的内容与打印角色指派列表时的内容实际上是相同的，但打印输出仅包括屏幕上的文本。**指派给**列或**状态**列中显示的任何图像都不会显示在打印输出中。

要打印角色指派，您需要在**工作仪表板**导航区域内具有**角色指派打印**导航许可权限。

打印角色指派列表：

1 在仪表板的**角色指派**部分单击**打印视图**。

User Application 会在单独的窗口中显示角色指派列表的可打印版本：

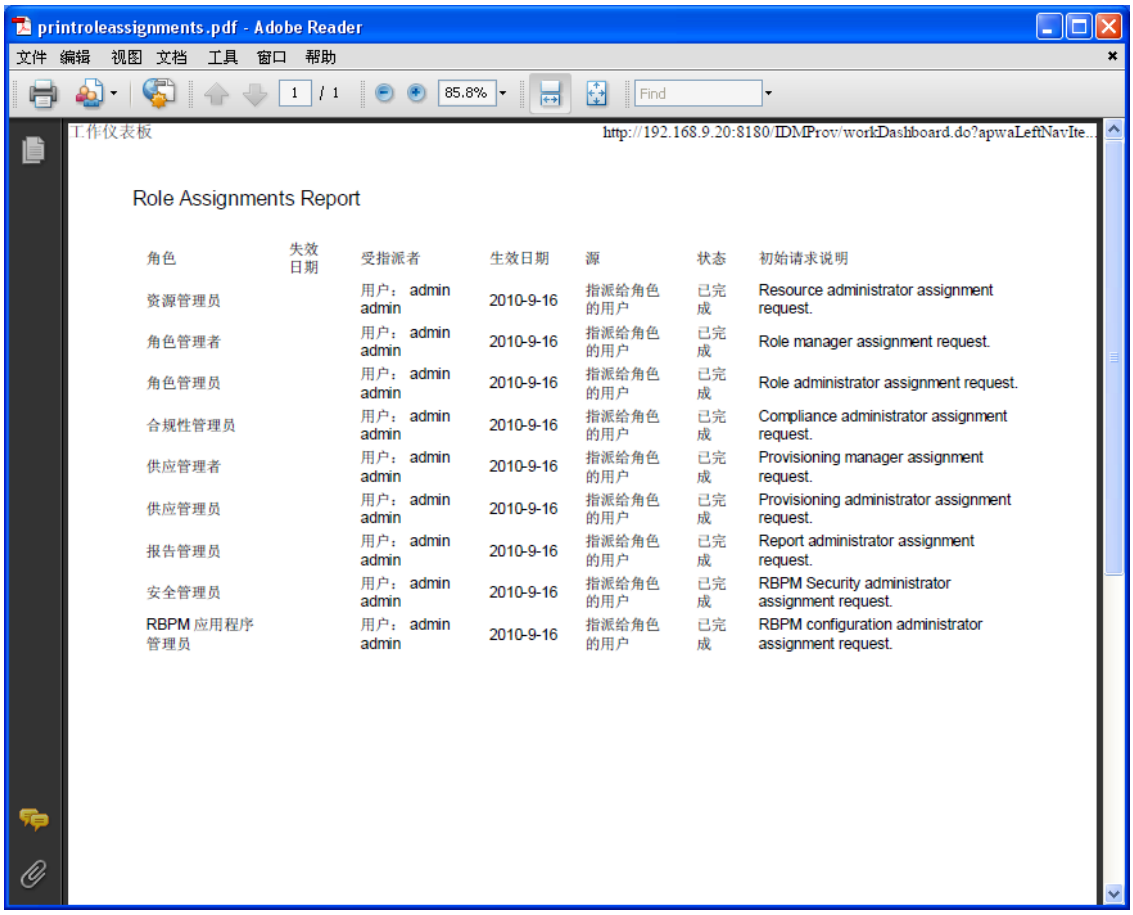
2 选择打印视图顶部的文本框中的文本。

在文本框中键入标题或添加注释：

3 单击**打印**。

可以直接打印到打印机，或打印到 PDF 文件。

下面是 PDF 示例，显示了打印输出的结果：



屏幕上显示的所有行都会打印出来，除非显示的行数达到了查询返回的最大结果数设置中定义的限制，它是由配置管理员在管理选项卡中指定的。如果达到了该限制，您会看到一个确认对话框，允许您指定是否要继续。如果想要在打印输出中包括屏幕上显示的所有行，请单击确定。对于每次用户会话，该讯息仅显示一次。

查看请求状态

通过请求状态操作，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。

请求状态操作会在单个统一列表中显示包括处理 （供应）请求、角色请求和资源请求在内的请求。列表会提供一个类型列，通过该列可以查看每个请求的类型。请求会显示在单个列表中，但列表可以按照请求类型进行排序或过滤。您可以从请求状态列表中收回仍然处于可收回状态的请求。

域管理员和域管理者可以查看其他用户的请求，如下所述：

- 如果在管理控件中未做任何选择，则请求列表会显示当前用户的请求。这些请求包括：用户作为收件人或接收人的请求，以及收件人或接收人是当前用户所属的组、容器或角色的请求。
- 如果在管理控件中选择了某个用户，则列表会显示使用选定用户作为收件人的请求。
- 如果选择某个组，则列表会显示使用选定组作为接收人的请求。
- 如果选择某个角色，则列表会显示使用选定角色作为收件人的请求。
- 如果选择某个容器，则列表会显示使用选定容器作为收件人的请求。

在域管理员或域管理者处于管理模式时，请求状态列表只包含与为管理员或管理者指派指定的域相关联的请求。

小组管理者可以查看小组成员的请求。在选择小组成员之前，小组管理者必须先选择小组。

在小组管理者处于管理模式时，请求状态列表只包含与为选定小组配置指定的域相关联的请求。

代理模式 请求状态操作在代理模式下不可用。

查看请求列表

要查看已发出的请求，请执行下列操作：

1 在 " 工作仪表板 " 的操作组中单击请求状态。

此时会显示请求的列表。如果您不处于受管模式，则所显示的请求是您作为收件人或请求者的那些请求。如果您处于受管模式，则所显示的请求是选定用户、组或容器作为收件人或请求者的那些请求。

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。

注释：如果向用户指派一个具有多个权利值的资源，则在请求状态选项卡上将仅列出一个条目。显示的那个条目是选定的第一个值。在指派选项卡上，将列出多个条目，并且用户的显示次数为选定值个数。

要查看请求的类型，您需要在显示内容的列的列表中包含类型列。包含类型列之后， User Application 会显示一个图标，指示请求是处理 （供应）请求、角色请求还是资源请求。

请求状态列表中的列如下所示：

- 请求的项目列提供为请求指定的角色、资源或处理的名称。
- 请求者列标识发出请求的用户。
- 收件人列标识批准请求时，将接收所请求项目的用户、组或容器。在角色关系中，收件人列会显示与在请求的项目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
正在运行，正在处理	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。
正在运行，正在处理	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 " 条件尝试重启动责任分离请求批准进程。 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	表明角色服务驱动程序无法启动责任分离批准进程且该进程已暂时停止。 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。 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。 此状态下的请求可以收回。
正在运行，正在处理	批准开始 - 待发	表明角色服务驱动程序正在随 “ 批准开始 - 暂停 ” 条件尝试重启动请求批准进程。 此状态下的请求可以收回。
正在运行，正在处理	批准开始 - 暂停	表明已为请求启动批准进程，但该进程已暂停。 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。 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。 此状态下的请求可以收回。
待发批准	SoD 异常 - 批准待发	表明责任分离批准进程已开始，正在等待一个或多个批准。 此状态下的请求可以收回。
待发批准	批准待发	表明请求的批准进程已开始，正在等待一个或多个批准。 此状态下的请求可以收回。

状态摘要图标	详细状态	说明
已批准	SoD 异常 - 已批准	表明此请求的责任分离异常已批准。 此状态下的请求可以收回。
已批准	已批准	表明请求已批准。 此状态下的请求可以收回。
已批准	供应	表明请求已批准 （如果要求批准），且已达到指派的激活时间。角色服务驱动程序正在进行授予指派的处理。 您不能收回此状态下的请求。
待发激活	待发激活	表明请求已批准，但尚未达到该指派的激活时间。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。 此状态下的请求可以收回。
已拒绝	SoD 异常 - 已拒绝	表明此请求的责任分离异常已被拒绝。 您不能收回此状态下的请求。
已拒绝	拒绝	表明此请求已被拒绝。 您不能收回此状态下的请求。
已完成，已供应	已供应	表明请求已批准 （如果要求批准），且已授予指派。 您不能收回此状态下的请求。
已完成，已供应	清理	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。 您不能收回此状态下的请求。
已终止	正在取消	表明角色服务驱动程序由于用户操作正在取消请求。 您不能收回此状态下的请求。
已终止	已取消	表明请求已由用户操作取消。 您不能收回此状态下的请求。
已终止	供应错误	表明在供应 （授予）或取回 （撤消）指派过程中出现了错误。 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。 您不能收回此状态下的请求。

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，“请求状态”和“角色指派”列表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“请求状态”部分的状态显示为“已供应”，但“角色指派”部分的状态显示为“待发激活”。如果等待一分钟左右，可能将看到“角色指派”部分的状态更改为“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。

查看请求的摘要

要查看请求的摘要信息，请将鼠标指针停在请求的项目列中的请求名称上。

过滤请求列表

您可以通过对请求列表应用过滤器来限制返回的行数。通过过滤请求列表，可以更简便地找到要查找的请求，并提高性能。

要为请求列表定义过滤器，请执行下列操作：

1. 单击定义过滤器按钮。

   此时会显示“过滤器”对话框，其中显示了几个可用于指定数据过滤方式的字段。

2. 要将搜索范围缩小为查找请求名称与特定字符串匹配的请求，请在请求的项目字段中输入字符串的第一个字符。
3. 要将搜索范围缩小为查找特定类型的请求，请在类型下拉列表中选择类型。
4. 要将搜索范围缩小为查找具有特定状态的请求，请在状态下拉列表中选择状态。

   可供选择的状态类别会因您在类型下拉列表中选择的类型而异。

5. 要将搜索范围缩小为查找具有特定确认编号的请求，请在确认编号字段中输入 ID。

   确认编号是一个内部标识符，它将一组同时请求的角色指派相关联。以下是一组角色指派共用一个确认编号的部分情形：

   - 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。

   在一组角色指派共用一个确认编号时，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。

6. 单击过滤器，使用在“过滤器”对话框中指定的选择准则执行新的请求查询。

   在定义请求列表的过滤器时，过滤器定义会与您的其他用户自选设置一起保存到身份库中。

   注释：无论是否在管理控件中选择了其他用户，所保存的自选设置始终应用于当前登录到 User Application 的用户。

要查看以前定义了哪些过滤器点，请执行下列操作：

1. 查看“定义过滤器”图标左侧的框。

   如果未定义任何过滤器，“定义过滤器”图标会显示两个空环，如下所示。

   如果已经定义了一个或多个过滤器点，则每个过滤器点会显示在单独的框中。

要去除以前在 “ 过滤器 ” 对话框中指定的过滤器点，请单击要去除的过滤器点旁边的清除此过滤器图标（看起来像一个 X）。

要去除所有以前定义的过滤器并将搜索结果更新为包含所有请求，请执行下列操作。

1 单击定义过滤器按钮来打开 “ 过滤器 ” 对话框。

2 单击重设置按钮。

   此时 “ 过滤器 ” 对话框会关闭，并且请求列表更新为包含所有请求。

自定义请求状态列

通过 “ 工作仪表板 ” 页面的 “ 请求状态 ” 部分，您可以选择和取消选择列，以及对请求列表显示内容中的列重新排序。对显示方式所做的所有自定义设置都会被保存，供以后使用。

要自定义请求状态列表中的列的显示方式，请执行下列操作：

1 在 “ 工作仪表板 ” 页面的请求状态部分中单击自定义按钮。

   User Application 会显示当前为显示内容选择的列的列表，以及可供选择的其他列的列表。

2 要在显示内容中包含其他列，可以选择可用列列表框中的列，并将它拖到选定列列表框中。

   要在列表中选择多列，可以按住 Ctrl 键并选择这些列。要在列表中选择一起显示的某个列范围，可以按住 Shift 键并选择这些列。

   您可以通过在选定列列表框中上移或下移某些列，对显示内容中的列重新排序。

3 要从显示内容中去除某个列，可以选择选定列列表框中的列，并将它拖到可用列列表框中。

   请求的项目和请求日期列是必选列，不能从请求列表显示中去除。

4 要保存更改，请单击确定。

控制页面中显示的项数

要指定您希望每页显示的项目数，请在行下拉列表中选择一个数字。

在修改行设置时，您的自选设置会与您的其他用户自选设置一起保存到身份库中。

控制请求状态细节的显示

通过 “ 工作仪表板 ” 页面可以指定，在页面的 “ 请求状态 ” 部分中单击请求时，如何显示请求的细节。您可以在列表中或单独的模态对话框中显示任务细节。该行为由 “ 自定义请求状态显示 ” 对话框中的一个设置控制。

在修改该设置时，您的自选设置会与您的其他用户自选设置一起保存到身份库中。

要控制任务细节的显示，请执行下列操作：

1 在 “ 工作仪表板 ” 页面的请求状态部分中单击自定义按钮。

   User Application 会显示自定义请求状态显示对话框，通过该对话框可以自定义请求列表的显示方式。所显示的控件组合会因管理员将哪些设置指定为可供用户覆盖而异。

2 要在任务列表显示内容中显示细节，请在打开请求状态细节下拉列表中选择在列表行中。要在单独的模态对话框中显示细节，请选择在讯息窗口中。

3 要保存更改，请单击保存更改。

对请求列表排序

要对请求列表排序，请执行下列操作：

1 单击要作为排序依据的列的标题。

   金字塔形状的排序指示符会指示哪一个列是新的主排序列。升序排序时，排序指示符以正常的直立方式显示。降序排序时，排序指示符以倒立方式显示。

   您可以依据多个列对列表排序，方法是单击每个排序列的标题。默认的排序方式是依据 “ 请求日期 ” 降序排序，这会使最近的请求先显示。如果使用 “ 请求日期 ” 列之外的任何其他列作为列表排序依据，“ 请求日期 ” 列会用作二级排序列。

在修改请求列表的排序顺序时，您的自选设置会与您的其他用户自选设置一起保存到身份库中。

刷新请求列表

要刷新请求列表，请执行下列操作：

1 单击**刷新**按钮。

   请求列表会更新为反映当前用户的请求列表的当前状态。**刷新**按钮不会去除任何已应用于请求列表的过滤器。刷新请求列表时，将会使用所有已定义的过滤器来更新列表，并且过滤器在您重设置它们之前一直保持有效。

查看请求的注释

1 要显示请求的注释文本，请单击请求列表中的 “ 注释 ” 图标。

注释：要查看请求的注释，您必须在选定列的列表中包含 “ 注释 ” 列。有关向任务列表中添加列的细节，请参见自定义请求状态列 （第 106 页）。

查看请求的细节

要查看请求的细节，请在**请求的项目**列中单击请求名称。

User Application 会显示请求的细节。

收回请求

如果您改变主意且不需要完成请求，则可通过 “ 工作仪表板 ” 页面的 “ 请求状态 ” 部分选择收回正在处理的请求。

最终用户可以收回自己是发起人的任何请求，前提是请求仍然处于可收回状态。域管理员可以收回自己管理的域中的任何请求。域管理者必须具有适当的安全许可权限才能收回请求。特别是，您必须具有撤消指派的许可权限，这会以隐含形式赋予您收回请求的能力。

要收回请求，请在 “ 请求细节 ” 窗口中单击**收回**。

只有与请求相关联的处理仍然在运行时，**收回**按钮才会启用。

12 管理用户、组、容器、角色和小组的工作

本章说明如何使用 " 管理 " 控件来管理其他用户、组、容器、角色和小组的工作。包括以下主题：

- 选择用户、组、容器、角色或小组 （第 109 页）
- 更改为不同的受管实体 （第 110 页）
- 最大程度减小用户配置文件部分使用的屏幕空间 （第 110 页）
- 退出管理模式 （第 111 页）

选择用户、组、容器、角色或小组

在域管理员或域管理者登录到 User Application 中时，" 工作仪表板 " 会显示管理控件，它是一个全局查找控件。通过管理控件，当前用户可以选择特定用户、组、容器、角色或小组成员，并使用 " 工作仪表板 " 界面来管理选定实体类型的工作。在用户选择某个实体之后，" 工作仪表板 " 上的数据和访问权限属于选定的实体，而不是属于当前登录的用户。但是，在用户处于 " 管理 " 模式时，设置和发出处理请求菜单仍然应用于已登录用户，而不是在管理控件中选定的实体。

要选择用户、组、容器、角色或小组成员，请执行下列操作：

1 在 " 工作仪表板 " 左上角单击管理。

" 工作仪表板 " 随即会显示 " 管理 " 弹出窗口。

2 在管理控件中，选择实体类型。

3 使用对象选择器选择某个特定的用户、组、容器、角色或小组。

选择用户、组、容器、角色或小组时，" 工作仪表板 " 会将您置于管理模式，并更新屏幕左侧的 " 用户配置文件 " 部分。" 用户配置文件 " 会更新它的显示内容，如下所示：

- 选择某个用户时，它会显示选定用户的照片、姓名、职务、电子邮件和电话号码。

  选择某个用户时，页面的 " 用户配置文件 " 部分以及 " 任务通知 "、" 资源指派 "、" 角色指派 " 和 " 请求状态 " 部分会显示以下图标：

该图标表明 “ 工作仪表板 ” 这些部分的数据和访问权限属于选定用户，而不是属于当前登录的用户。

- 选择某个组、容器或角色时，它会显示该组、容器或角色的 DN、显示名称和说明 （如果可用）。

  选择某个容器时，页面的 “ 用户配置文件 ” 部分以及 “ 任务通知 ”、 “ 资源指派 ”、 “ 角色指派 ” 和 “ 请求状态 ” 部分会显示以下图标：

  选择某个组时，页面的 “ 用户配置文件 ” 部分以及 “ 任务通知 ”、 “ 资源指派 ”、 “ 角色指派 ” 和 “ 请求状态 ” 部分会显示以下图标：

  选择某个角色时，页面的 “ 用户配置文件 ” 部分以及 “ 任务通知 ”、 “ 资源指派 ”、 “ 角色指派 ” 和 “ 请求状态 ” 部分会显示以下图标：

  这些图标表明 “ 工作仪表板 ” 这些部分的数据和访问权限属于选定实体，而不是属于当前登录的用户。

- 选择某个小组时，它会显示小组下拉列表让您选择小组。此外，它还会显示用于选择小组成员的下拉列表。

  选择某个小组成员时，页面的 “ 用户配置文件 ” 部分以及 “ 任务通知 ”、 “ 资源指派 ”、 “ 角色指派 ” 和 “ 请求状态 ” 部分会显示以下图标：

更改为不同的受管实体

要切换至另一个受管实体，请单击 “ 用户配置文件 ” 部分的**管理用户、组、角色或容器**按钮。

最大程度减小用户配置文件部分使用的屏幕空间

要最小化 “ 用户配置文件 ” 部分使用的屏幕空间，请单击 “ 用户配置文件 ” 部分的**宽布局**按钮。

“ 用户配置文件 ” 部分会隐藏关于当前选定实体的细节，为您留出更多空间来处理页面的 “ 任务通知 ”、 “ 资源指派 ”、 “ 角色指派 ” 和 “ 请求状态 ” 部分。

要将 “ 用户配置文件 ” 部分恢复为它的正常显示大小，以便可以看到实体细节，请单击**默认布局**按钮。

退出管理模式

要退出管理模式，并将 “ 工作仪表板 ” 重设置为显示当前登录用户的数据和访问许可权限，请使用下列任一种方法：

- 单击 “ 用户配置文件 ” 部分中的 X：
- 在 “ 管理 ” 对话框中，单击退出管理模式按钮。

代理模式 管理控件在代理模式下不可用，即使用户代理的是域管理员或域管理者用户。当用户处于代理模式时，“ 工作仪表板 ” 上的菜单项的导航访问权限会显示所代理用户的许可权限，而不是登录用户的许可权限。

13 控制您的设置

本章说明如何使用 " 工作仪表板 " 上的设置菜单。包括以下主题：

- 关于设置菜单 （第 113 页）
- 担当代理 （第 116 页）
- 指定您的可用性 （第 116 页）
- 查看和编辑代理指派 （第 119 页）
- 查看和编辑委托指派 （第 120 页）
- 查看和编辑小组代理指派 （第 121 页）
- 查看和编辑小组委托指派 （第 124 页）
- 指定小组的可用性 （第 127 页）
- 执行小组处理请求 （第 129 页）

关于设置菜单

您可以通过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。如果您是供应域的供应管理员、供应管理者或小组管理者，则您还可能有权定义代理和委托指派，以及小组可用性设置。

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，代理指派与处理请求无关，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 不会对用户已具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。也可能他们与将充当代理的人的角色存在冲突。

使用场景示例

本节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 114 页）
- 委托使用场景 （第 114 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，可以为这六种处理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。

设置菜单的用户访问权限

对于登录到 User Application 中的所有用户，“ 工作仪表板 ” 中的设置菜单会显示以下选项：

表 13-1 *所有已鉴定用户可用的“ 设置 ” 菜单选项*

“ 设置 ” 菜单选项	说明
退出代理模式	使您担当另一用户的代理。 有关细节，请参见担当代理 （第 116 页）。
编辑可用性	允许您查看或编辑您可以处理的请求，以及您的指派委托可以处理的那些请求。要编辑可用性，必须具有 “ 配置可用性 ” 许可权限。 有关细节，请参见指定您的可用性 （第 116 页）。
我的代理指派	用于查看或编辑代理指派。要编辑代理指派，必须具有 “ 配置代理 ” 许可权限。 有关细节，请参见查看和编辑代理指派 （第 119 页）。
我的委托指派	用于查看或编辑委托指派。要编辑委托指派，必须具有 “ 配置委托 ” 许可权限。 有关细节，请参见查看和编辑委托指派 （第 120 页）。

当供应管理员、供应管理者或小组管理者登录到 User Application 中时，设置菜单还会另外显示以下菜单选项：

表 13-2 管理员和小组管理者可用的“ 设置 ” 菜单选项

“ 设置 ” 菜单选项	说明
小组设置 > 小组可用性	允许您指定小组成员及其委托可以处理哪些请求。 必须在小组配置中启用 “ 配置可用性 ” 许可权限。禁用该许可权限时，将不允许该操作。 有关细节，请参见指定小组的可用性 （第 127 页）。
小组设置 > 小组代理指派	用于为小组成员指定代理指派。 必须在小组配置中启用 “ 配置代理 ” 许可权限。该功能禁用时，不允许该操作。 有关细节，请参见查看和编辑小组代理指派 （第 121 页）。
小组设置 > 小组委托指派	用于为小组成员指定委托指派。 必须在小组配置中启用 “ 配置委托 ” 许可权限。如果小组权限允许管理者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。在小组配置中禁用该许可权限时，将不允许该操作。 有关细节，请参见查看和编辑小组委托指派 （第 124 页）。
小组设置 > 执行小组处理请求	允许您为所在小组的成员发出处理请求。 必须在小组配置中启用 “ 启动 PRD” 许可权限。在小组配置中禁用该许可权限时，将不允许该操作。 有关细节，请参见执行小组处理请求 （第 129 页）。

“ 小组设置 ” 菜单选项的行为会因当前用户是管理员还是小组管理者，以及已授予哪些许可权限而异，如下所述：

表 13-3 “ 小组设置 ” 菜单选项的用户访问权限

用户	功能
供应管理员 （或安全域管理员）	无需选择小组就可以选择用户。 具有与供应域相关联的所有许可权限，因而可以看到 “ 小组代理指派 ”、 “ 小组委托指派 ” 和 “ 小组可用性 ” 菜单选项。 可以访问 “ 小组代理指派 ”、 “ 小组委托指派 ” 和 “ 小组可用性 ” 页面中的新建按钮。

用户	功能
供应管理者	无需选择小组就可以选择用户。 需要被授予安全权限才能看到 “ 小组代理指派 ”、“ 小组委托指派 ” 和 “ 小组可用性 ” 菜单选项。 如果已经授予了适当的安全权限，则可以访问 “ 小组代理指派 ”、“ 小组委托指派 ” 和 “ 小组可用性 ” 页面中的新建按钮。 在 “ 小组委托指派 ” 用户界面中，供应管理者只能选择他们有权指派的供应请求。在供应管理者提交委托指派请求时，只有允许他们做出的指派才会成功完成。
小组管理者	选择用户之前必须先选择小组。 需要被授予安全权限才能看到 “ 小组代理指派 ”、“ 小组委托指派 ” 和 “ 小组可用性 ” 菜单选项。 如果已经授予了适当的安全许可权限，则可以访问 “ 小组代理指派 ”、“ 小组委托指派 ” 和 “ 小组可用性 ” 页面中的新建按钮。

担当代理

您可以通过进入代理模式操作担当另一用户的代理。

1 在 “ 工作仪表板 ” 的 “ 用户配置文件 ” 部分中的设置操作组中，单击进入代理模式。
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。

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，您在特定时间段内没空处理的那些处理请求。在您无法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处理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。您需要请供应管理员 （或者供应管理者或小组管理者）为您创建委托指派。

- 设置可用性状态 （第 117 页）
- 创建或编辑可用性设置 （第 117 页）
- 删除可用性设置 （第 118 页）

设置可用性状态

1 在设置操作组中单击编辑可用性。

User Application 将显示 " 编辑可用性 " 页。如果没有任何现有的可用性设置，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 要查看与可用性指派关联的特定处理的细节，请单击该处理的名称。

该页面随即显示一个弹出窗口，提供关于委托指派的信息。

在同一处理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	这是默认状态。它表示您全局可用。如果该状态有效，则向您指派的请求不会被委托，即使已为您指派了委托，也是如此。 使用可用于所有请求状态将覆盖其他设置。如果将状态更改为其他设置之一，然后又重新更改为可用于所有请求，则会去除以前定义的任何选择性可用设置。
不可用于任何请求	指定您对当前系统中的任何请求定义全局地不可用。 选择不可用于任何请求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不可用于指定的请求。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。
不可用于指定的请求	指定您不可用于特定的处理请求定义。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。 选择不可用于指定的请求后，您将进入 " 编辑可用性 " 页面。该操作相当于单击新建按钮。

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于的请求。

显示的处理请求列表中只包含那些具有委托指派的请求。

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 2009 年 10 月 31 日失效，则不能对可用性设置指定失效日期 2009 年 11 月 15 日。如果您指定失效日期为 2009 年 11 月 15 日，则将该日期提交为在 2009 年 10 月 31 日失效时，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： **选定的：** 允许您向选择的任何用户发送电子邮件通知。

5 在请求类型列表中选择一个或多个处理请求，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。

添加的每个处理请求将包含在在指定期间谢绝列表中。

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 要从列表中去除一个请求，请单击去除。

8 单击提交可提交更改。

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：

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。如果您是供应管理员、供应管理者或小组管理者，则还可以使用该操作来编辑代理指派。

只有供应管理员、供应管理者和小组管理者可以指派代理，如下所示：

- 供应管理员和供应管理者可以为组织中的所有用户定义代理指派。
- 根据团队定义，团队经理也许可以定义该团队中用户的代理设置。代理必须也在团队内。要定义代理，团队经理必须使用团队代理指派操作。

如果小组管理者需要选择小组外的代理，他必须请求供应管理员或供应管理者定义代理关系。

显示代理设置

1 在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。

   如果您不是供应管理员、供应管理者或小组管理员，将会看到您的代理指派的只读视图。

   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。

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。

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：

注释：在您更改某个代理指派的许可权限之后，User Application 不会立即将您从代理模式注销。这让您可以更改错误的值。因此，如果您在处于代理模式时删除了某个代理指派，则即使在去除该代理指派之后，您仍然能够编辑该代理指派，并且还可以处理代理用户的任务。

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。如果您是供应管理员、供应管理者或小组管理者，则还可以使用该操作来编辑委托指派。

只有供应管理员、供应管理者和小组管理者可以指派委托，如下所示：

- 供应管理员和供应管理者可以为组织中的所有用户定义委托指派。
- 根据团队权限的定义，团队经理可能可以定义其团队中用户的委托设置。委托必须也在团队内。要定义委托，团队经理必须使用团队委托指派操作。

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。

显示委托设置

1 在设置操作组中单击我的委托指派。

User Application 将显示当前设置。

如果您不是供应管理员、供应管理者或小组管理员，将会看到您的委托指派的只读视图。

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。

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， User Application 将显示以下供您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处理请求的类别。选择全部以包含来自所有可用类别的请求。

6 从所选类别中的可用请求列表中选择一个或多个要委托的请求，然后单击添加。

添加的每个处理请求将包含在选定的请求列表中。

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 要从列表中去除一个请求，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，指出是否已成功提交委托指派。

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：

查看和编辑小组代理指派

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，则可能有权为您所在小组的成员定义代理。要定义代理，小组管理者在小组定义中必须具有 “ 配置代理 ” 许可权限。
- 供应管理员可以为组织中的任何用户、组或容器设置代理。
- 供应管理者可能可以为组织中的任何用户、组或容器设置代理。要定义代理，供应管理者必须具有 “ 配置代理 ” 许可权限。

要为小组成员指派代理，请执行下列操作：

1 在设置 > 小组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管理者的小组。

如果您是供应管理员或供应管理者，则不会看到选择小组框。

小组列表包含允许小组管理者为其设置代理的小组，以及已禁用代理设置功能的小组。如果特定小组定义不允许小组管理者设置代理，他仍可以查看由管理员或这些用户所属的另一个小组的管理者为小组成员定义的代理设置。但是，小组管理者不能编辑这些设置，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 在小组成员选择框中，输入用户名字的至少 4 个字符来选择用户。

或者，使用小组成员选择框旁的“对象选择器”图标 来选择小组成员。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
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：
	所有：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。
	指派自：指定只有要指派代理的小组成员会收到电子邮件通知。
	指派至：指定只有担当代理的小组成员会收到电子邮件通知。
	选定的：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	**不失效：**如果希望代理指派在被去除或修改之前保持有效，请选择不失效。
	指定失效：选择指定失效定义结束日期。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 在设置 > 小组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管理者的小组。

如果您是供应管理员或供应管理者，则不会看到选择小组框。

小组列表包含允许小组管理者为其设置代理的小组，以及已禁用代理设置功能的小组。如果特定小组定义不允许小组管理者设置代理，他仍可以查看由管理员或这些用户所属的另一个小组的管理者为小组成员定义的代理设置。但是，小组管理者不能编辑这些设置，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 在小组成员选择框中，输入用户名字的至少 4 个字符来选择用户。

或者，使用小组成员选择框旁的“对象选择器”图标来选择小组成员。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： **所有：**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。 **指派自：**指定只有要指派代理的小组成员会收到电子邮件通知。 **指派至：**指定只有担当代理的小组成员会收到电子邮件通知。 **选定的：** 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	**不失效：**如果希望代理指派在被去除或修改之前保持有效，请选择不失效。 **指定失效：**选择指定失效定义结束日期。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 在设置 > 小组设置操作组中单击小组代理指派。

2 要去除代理设置，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。

查看和编辑小组委托指派

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管理者的小组的成员定义委托，只要小组定义赋予您该许可权限。要配置小组委托指派，小组管理者必须具有 " 配置委托 " 许可权限。
- 供应管理员可以为组织中的任何用户、组或容器定义委托指派。
- 供应管理者可能可以为组织中的任何用户、组或容器设置委托。要定义委托，供应管理者必须具有 " 配置委托 " 许可权限。

要定义委托指派，请执行下列操作：

1. 在设置 > 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管理者的小组。

   如果您是供应管理员或供应管理者，则不会看到选择小组框。

   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. 在小组成员选择框中，输入用户名字的至少 4 个字符来选择用户。

   或者，使用小组成员选择框旁的 " 对象选择器 " 图标 来选择小组成员。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： ◆ **指派委托：**在表中选择用户。 ◆ **按关系指派：**从下拉列表中选择委托关系。
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。

字段	说明
接收人	指定哪些用户应收到电子邮件通知： **所有：** 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。 **指派自：** 指定只有要指派委托的小组成员会收到电子邮件通知。 **指派至：** 指定只有担当委托的小组成员会收到电子邮件通知。 **选定的：** 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	**不失效：** 如果希望委托在被去除或修改之前保持有效，请选择不失效。如果此选项有效，则委托永久有效。 **指定失效：** 选择指定失效定义结束日期。单击 " 日历 "，然后选择委托指派的失效日期和时间。
请求类型	从列表中选择一个类别。 这会填充所选类别中的可用请求列表。
所选类别中的可用请求	从该列表中选择一个或多个处理请求，然后单击添加。
选定的请求	该列表会显示已被委托的处理请求类型。要去除一个请求类型，请从列表中选择它，然后单击去除。

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 在小组成员选择框中，输入用户名字的至少 4 个字符来选择用户。

或者，使用小组成员选择框旁的 " 对象选择器 " 图标 来选择小组成员。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	通过选择下列选项之一，指派可以执行受委托工作的用户： ◆ **指派委托：**在表中选择用户。 ◆ **按关系指派：**从下拉列表中选择委托关系。
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： **所有：**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。 **指派自：**指定只有要指派委托的小组成员会收到电子邮件通知。 **指派至：**指定只有担当委托的小组成员会收到电子邮件通知。 **选定的：** 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	**不失效：**如果希望委托在被去除或修改之前保持有效，请选择不失效。如果此选项有效，则委托永久有效。 **指定失效：**选择指定失效定义结束日期。单击 “ 日历 ”，然后选择委托指派的失效日期和时间。
请求类型	从列表中选择一个类别。 这会填充所选类别中的可用请求列表。 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全部。 **注释：**“ 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。
所选类别中的可用请求	从该列表中选择一个或多个处理请求，然后单击添加。 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。
选定的请求	该列表会显示已被委托的处理请求类型。要去除请求类型，请从列表中选择该请求类型，然后单击去除。

8 单击提交保存选择。

要删除委托指派，请执行下列操作：

1 在设置 > 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，请在要删除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。

指定小组的可用性

使用小组可用性操作可以指定您的小组成员没空处理的处理请求。在您或者您的小组成员没空的时间段内，该类型的任何处理请求都将被转发到委托的队列。

可以单独地或全局地指定对每个处理请求的可用性。只能为已指派委托的用户指定可用性。

1 在设置 > 小组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管理者的小组。

如果您是供应管理员或供应管理者，则不会看到选择小组框。

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。

3 单击继续。

4 在小组成员选择框中，输入用户名字的至少 4 个字符来选择用户。

或者，使用小组成员选择框旁的 “ 对象选择器 ” 图标 来选择小组成员。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 要查看与可用性指派关联的某个特定资源，请单击该资源的名称。

该页面随即显示一个弹出窗口，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	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的请求不会被委托，即使已为其指派了委托，也是如此。 **注释：**如果更改了状态，然后又重新更改为可用于所有请求，则会去除以前定义的任何选择性可用设置。

状态	说明
不可用于任何请求	指定小组成员对当前系统中的所有处理请求都不可用。（这又称为 “ 全局不可用 ”。） 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不可用于指定的请求。 这些指派可立即生效，并且在委托指派失效前保持有效。 **注释：**此设置不影响在此时间点后新建的指派的可用性。
不可用于指定的请求	如果选择该选项，系统将提示您指定小组成员的可用性。（该操作相当于单击新建按钮。）系统将提示您指定： ◆ 小组成员没空处理的请求类型。 ◆ 小组成员没空的时间段。 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。

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	指定应收到电子邮件通知的用户： **选定的：** 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。

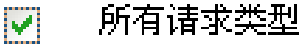
10 在请求类型列表框中选择一个或多个请求，然后单击添加。

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。结果是将这些请求委托给其他用户。

添加的每个请求将包含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。



所有请求类型复选框仅当委托指派的请求类型设置为全部时才可用。

12 要从列表中去除一个请求，请单击去除。

13 单击*提交*可保存更改。

执行小组处理请求

通过执行小组处理请求操作，您可以为小组成员发出处理请求。

1 在设置 > 小组设置操作组中单击执行小组处理请求。

   此时会显示 " 执行小组处理请求 " 页面。

2 单击选择小组选择指定您作为小组管理者的小组。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。

4 单击继续。

   " 执行小组处理请求 " 页面会显示您可以请求的处理列表。该列表只包含小组管理者可发起请求的那些处理。

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，您可能会在收件人选择框旁看到图标 " 对象选择器 " 图标，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。

   如果您是供应管理者或供应管理员，则还会显示历史记录图标。否则，此图标不可用。

   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 " 执行小组处理请求 " 页面会显示请求表单。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。

   表单中的字段会因所请求的处理而异。

   如果管理员为系统配置了数字签名，并且您请求的过程需要数字签名，页面右上角会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。

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。

9i 单击**预览**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。

“ 执行小组处理请求 ” 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。

14 发出处理请求

本章提供关于发出处理请求的信息。包括以下主题：

- 关于处理请求 （第 131 页）
- 发出处理请求 （第 131 页）
- 深度链接请求 （第 134 页）

关于处理请求

通过**发出处理请求**菜单，您可以发出处理请求 （也称为供应请求）。**发出处理请求**菜单不能用于发出证明、资源或角色请求。提交这些请求的界面取决于您要发出的请求的类型，如下所述：

- 要发出证明请求，您需要使用**合规性**选项卡上的**证明请求**操作。
- 要发出资源请求，您需要使用**工作仪表板**选项卡的**资源指派**部分，或者使用**角色和资源**选项卡上的**资源编目**。
- 要发出角色请求，您需要使用**工作仪表板**选项卡的**角色指派**部分，或者使用**角色和资源**选项卡上的**角色编目**。

发出处理请求菜单上显示的处理请求列表取决于当前登录到 User Application 中的是哪种用户：

- 如果您是供应管理员 （供应域的域管理员），则可以选择所有处理请求。
- 如果您是供应管理者 （供应域的域管理者），则只能看到已经授予您相应许可权限的那些请求。
- 如果您是小组管理者，则只能看到已经授予您相应许可权限的那些请求。

在选择处理请求之前，需要先选择类别。类别列表中会包含所有类别。

注释：默认情况下，列表中会包含 “ 证明 ” 和 “ 角色 ” 类别。您并不能通过这两个类别发出标准的、立即可用的证明或角色指派请求。包含这两个类别只是为了让您的管理员可以定义自定义处理请求来执行特殊的证明或基于角色的功能。

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。

提交某个处理请求时，该请求会启动一个工作流程。工作流程可协调完成请求所需的批准。有些处理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。

发出处理请求

要发出处理请求，请执行下列操作：

1. 在工作仪表板的 “ 用户配置文件 ” 部分中单击**发出处理请求**。

   此时会显示 “ 发出处理请求 ” 页面。

2. 在**处理请求类别**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**。

“ 发出处理请求 ” 页面会显示当前用户可用的处理请求的列表。

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 通过单击处理名称选择所需的处理。

“ 发出处理请求 ” 页面会显示初始请求表单。

如果管理员为系统配置了数字签名，并且您请求的过程需要数字签名，页面右上角会显示**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。

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。

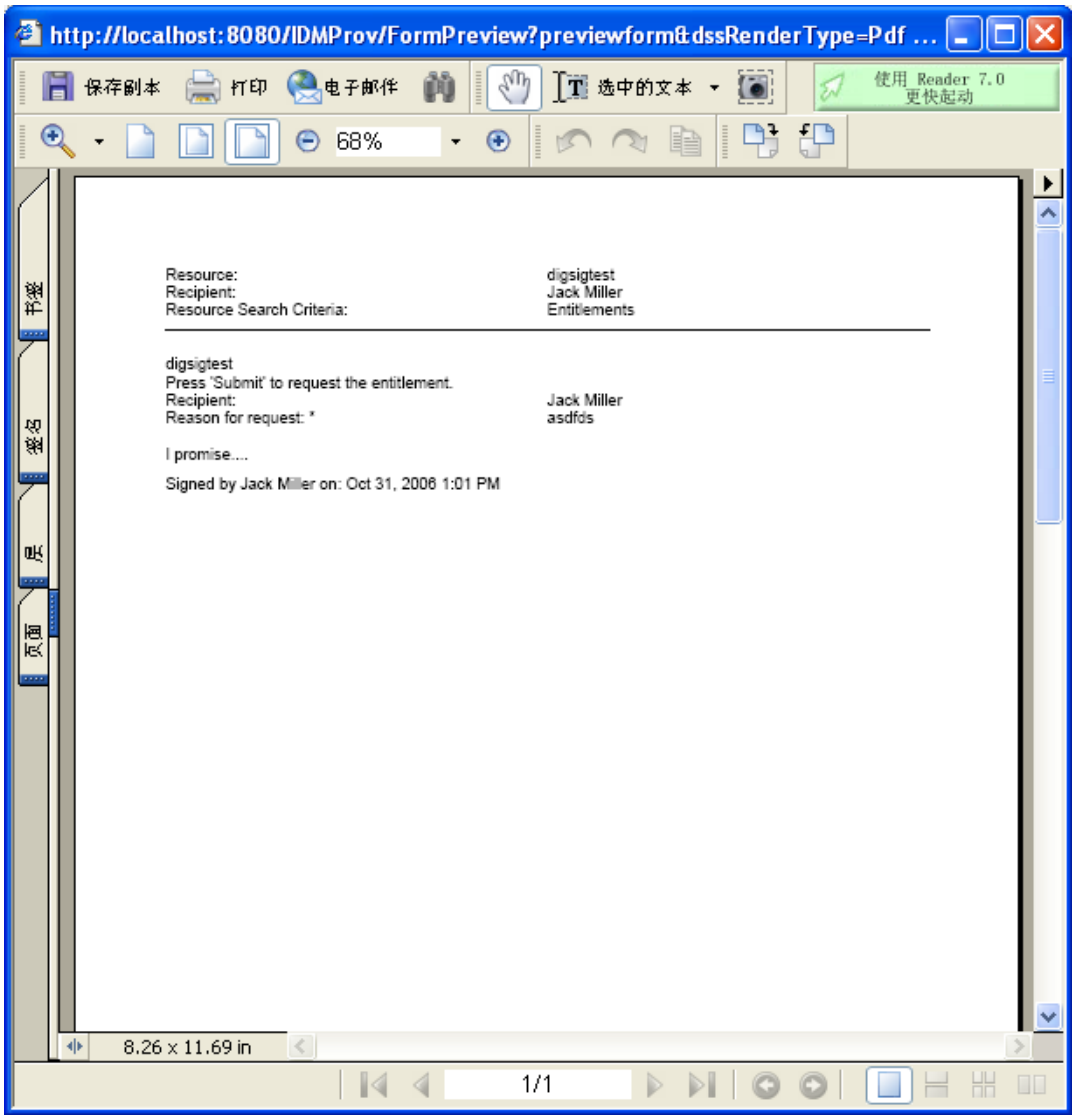
5h 如果选择已导入智能卡的证书，请键入智能卡的 PIN，并单击**确定**。

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。

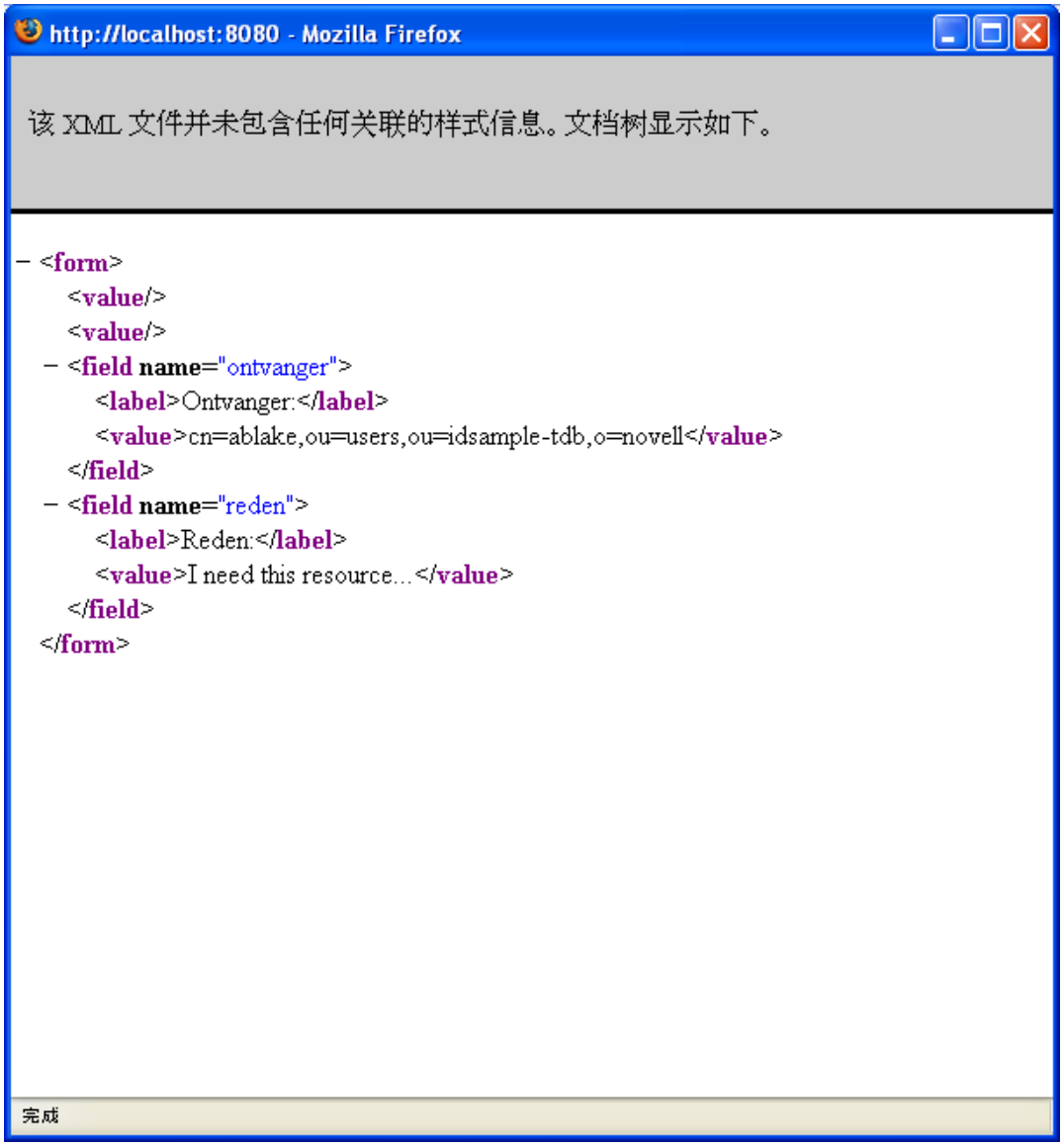
如果您的管理员启用了预览用户协议功能，则将启用**预览**按钮。

5i 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。


http://localhost:8080/IDMProv/FormPreview?previewform&dssRenderType=Pdf ...
保存副本
打印
电子邮件
选中的文本
使用 Reader 7.0 更快起动
68%
书签
签名
层
页面
Resource: digsigtest
Recipient: Jack Miller
Resource Search Criteria: Entitlements
digsigtest
Press 'Submit' to request the entitlement.
Recipient: Jack Miller
Reason for request: * asdfds
I promise....
Signed by Jack Miller on: Oct 31, 2006 1:01 PM
8.26 x 11.69 in
1/1

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**。

“ 发出处理请求 ” 页面将显示状态讯息，指明是否已成功提交请求。

深度链接请求

User Application 提供了深度链接当前用户的特定处理请求 （也称为供应请求）的功能。通过该功能，经理可以向某个雇员发送特定处理请求的 URL，从而该雇员无需通过 User Application 界面就可以快速请求处理。深度链接处理请求时，请求表单会与 User Application 的标题一起显示在页面主体中：

发出某个请求之后，该请求会显示在请求者在 “ 工作仪表板 ” 的**请求状态**下看到的请求列表中。此外，批准者会在 “ 工作仪表板 ” 的**任务通知**下看到该任务。

用于深度链接处理请求的 URL 采用以下格式：

```
http://<server:port>/IDMProv/makeRequestDetail.do?requestId=<PRD
ID>&requestType=<requesttype>
```

<PRD ID> 必须指定供应请求定义的 DN 或者角色或资源的唯一 ID。 *< 请求类型 >* 必须为 PROV。

以下是可以用来深度链接供应请求定义的 URL 示例：

```
http://testserver:8080/IDMProv/
makeRequestDetail.do?requestId=cn=EmailChange,cn=RequestDefs,cn=AppConfig,cn=Picas
soDriver,cn=TestDrivers,o=novell&requestType=PROV
```

V 管理角色和资源

以下几章说明如何使用 Identity Manager User Application 的**角色和资源**选项卡。

- 第 15 章 " 角色和资源简介 "（第 139 页）
- 第 16 章 " 在 User Application 中管理角色 "（第 149 页）
- 第 17 章 " 在 User Application 中管理资源 "（第 157 页）
- 第 18 章 " 在 User Application 中管理责任分离 "（第 165 页）
- 第 19 章 " 创建和查看报告 "（第 169 页）
- 第 20 章 " 配置角色和资源设置 "（第 175 页）

15 角色和资源简介

本章概述角色和资源选项卡。包括以下主题：

- 关于角色和资源 （第 139 页）
- 访问角色和资源选项卡 （第 145 页）
- 浏览选项卡的功能 （第 145 页）
- 您可以执行的角色和资源操作 （第 146 页）
- 了解角色和资源选项卡上使用的图标 （第 147 页）

关于角色和资源

角色和资源选项卡的作用是让您可以方便地执行基于角色的供应操作。通过这些操作，您可以管理组织内的角色定义和角色指派，以及资源定义和资源指派。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。或者，也可以将资源直接指派给用户。例如，可以使用角色和资源选项卡执行以下操作：

- 为自己或组织中的其他用户发出角色和资源请求
- 创建角色以及角色层次结构内的角色关系
- 创建责任分离 (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

如果角色或资源指派请求需要组织中一个或多个人的许可，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。有些指派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。

注释：只有显式地将角色指派给用户时，才会触发角色批准。

如果角色指派请求可能产生责任分离冲突，发起人可以覆盖责任分离限制，并且对产生限制异常提供调整。在某些情况下，责任分离冲突可能导致工作流程启动。工作流程协调允许责任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和资源选项卡的内容。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。

关于角色

本节概述角色和资源选项卡中所用的术语和概念：

- 角色与角色指派 （第 140 页）
- 角色编目与角色层次结构 （第 140 页）
- 责任分离 （第 142 页）

- 角色报告与审计 （第 142 页）
- 角色安全性 （第 142 页）
- Role and Resource Service 驱动程序 （第 144 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。通过**角色和资源**选项卡，用户可以请求*角色指派*，角色指派是角色与用户、组或容器之间的关联。通过**角色和资源**选项卡，用户还可以定义*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。

注释：只有显式地将角色指派给用户时，才会触发角色批准。

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，角色和资源子系统将管理角色请求的生命周期。要了解用户或子系统本身对请求执行了哪些操作，可以在**角色编目**的**请求状态**选项卡中检查请求的状态。

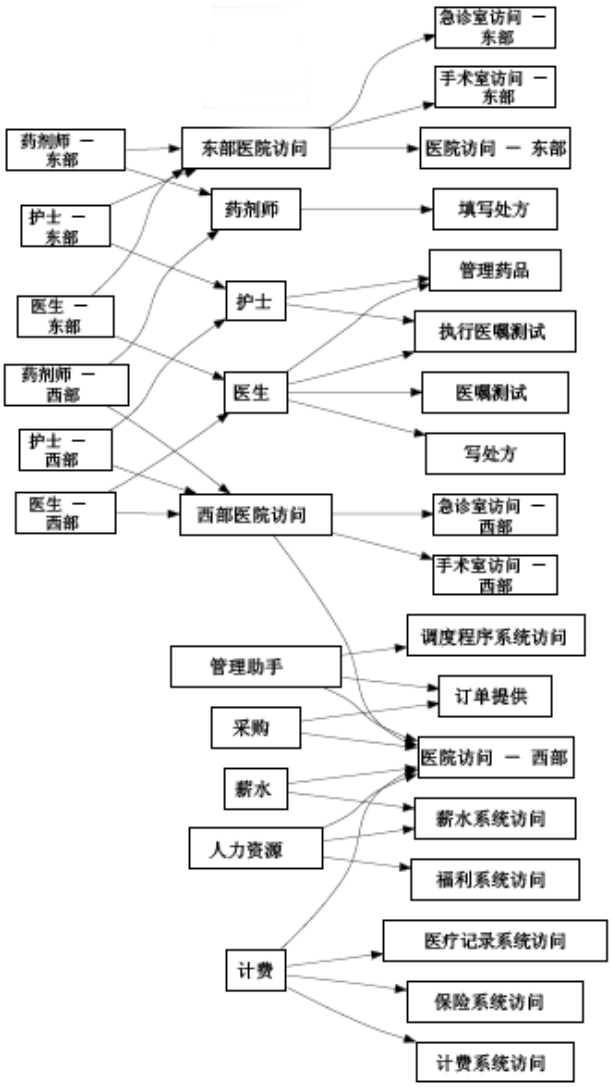
角色编目与角色层次结构

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**是所有角色定义以及角色和资源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角色层次结构示例，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 15-1　角色层次结构示例



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。

责任分离

角色和资源子系统的一个关键功能是定义*责任分离 (SoD) 限制*。责任分离 (SoD) 限制是定义认为存在冲突的两个角色的规则。角色管理员 / 角色管理者可为组织创建责任分离限制。通过定义 SoD 限制，他们可以防止将用户指派给冲突的角色，或是维护审计追踪，以便跟踪允许违规的情况。在责任分离限制中，冲突的角色在角色层次结构中的级别必须相同。

某些责任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*责任分离违例*。已经批准的冲突称为*已批准的责任分离异常*。角色和资源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者角色关系）的 SoD 违反。

如果责任分离冲突需要批准，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，充当角色和资源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

角色和资源子系统提供了一套丰富的报告工具，帮助审核员分析 " 角色编目 "，以及角色指派与 SoD 限制、违反和异常的当前状态。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

除了通过报告工具提供信息之外，角色和资源子系统还可以配置为向 Novell 或 OpenXDAS 审核客户端记录事件。

角色安全性

角色和资源子系统使用一组系统角色来保护对**角色和资源**选项卡内的功能的访问。**角色和资源**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某一角色的成员，则**角色和资源**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：

- 角色管理员
- 角色管理者

下文将详细说明这些系统角色。

表 15-1 系统角色

角色	说明
角色管理员	这是一个系统角色，它允许成员创建、去除或修改所有角色，以及授予或撤消对任何用户、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： ◆ 创建、去除和修改角色。 ◆ 修改角色的角色关系。 ◆ 请求将用户、组或容器指派给角色。 ◆ 创建、去除和修改 SoD 限制。 ◆ 浏览 “ 角色编目 ”。 ◆ 配置角色和资源子系统。 ◆ 查看所有请求的状态。 ◆ 收回角色指派请求。 ◆ 运行任何或全部报告。
角色管理者	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消角色指派。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： ◆ 创建新的角色和修改用户具有浏览权限的现有角色。 ◆ 修改用户具有浏览权限的角色的角色关系。 ◆ 请求将用户、组或容器指派给用户具有浏览权限的角色。 ◆ 浏览 “ 角色编目 ”（范围受浏览权限的限制）。 ◆ 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）。 ◆ 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）。

已鉴定用户

除支持这些系统角色之外，角色和资源子系统还允许已鉴定用户进行访问。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。

Role and Resource Service 驱动程序

角色和资源子系统使用 Role and Resource Service 驱动程序来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消权利，并且执行已完成请求的清理过程。

更改资源权利的结果 如果更改现有资源的权利，则驱动程序不会为当前被指派了该资源的用户授予新权利。要授予新权利，您需要去除该资源，然后将该资源重指派给需要权利的用户。

有关 Role and Resource Service 驱动程序的细节，请参见 《*NetIQ Identity Manager - Administrator's Guide to the Identity Applications*》（NetIQ Identity Manager - Identity Applications 管理员指南）。

关于资源

本节概述在 User Application 中使用的资源管理术语和概念。

关于基于资源的供应

User Application 中的资源功能的作用是让您可以方便地执行基于资源的供应操作。通过这些操作，用户可以管理组织内的资源定义和资源指派。资源指派可以映射到公司内的用户或角色。例如，可以使用资源执行下列操作：

- 为自己或组织中的其他用户发出资源请求
- 创建资源并将它们映射到权利

如果资源指派请求需要组织中一个或多个人的许可，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。有些资源指派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。

以下业务规则控制 User Application 中资源的行为：

- 资源只能指派给用户。这并不会排除资源基于隐式角色指派授予容器或组中的用户。但是，该资源指派将只与一个用户关联。
- 可以通过以下任意方式指派资源：
  - 用户通过 UI 机制直接指派
  - 通过供应请求
  - 通过角色请求指派
  - 通过 Rest 或 SOAP 接口
- 可以多次将同一资源授予用户 （如果在资源定义中启用了该功能）。
- 资源定义只能绑定一项权利。
- 资源定义可绑定一个或多个相同权利参照。该功能用于支持此类权利：权利参数代表已连接系统上的可供应帐户或许可权限。
- 权利和决策支持参数可以在设计时 （静态）或请求时 （动态）指定。

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 User Application。基于资源的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。

资源

资源是业务用户进行访问需要具有的任意数字实体，例如用户帐户、计算机或数据库。通过 User Application，最终用户可以方便地请求自己所需的资源。此外，它还提供了管理员可用于定义资源的工具。

每个资源都映射到一项权利。资源定义只能绑定一项权利。资源定义可以多次绑定到同一权利，每个资源使用不同的权利参数。

资源请求

资源只能指派给用户。不能将它们指派给组或容器。但是，如果将某个角色指派给某个组或容器，则可能会自动授予该组或容器中的用户对于与该角色关联的资源的访问权限。

资源请求可能会需要批准。资源的批准进程可以通过供应请求定义处理，也可以通过外部系统处理（通过设置资源请求中的状态代码）。

如果某个资源授予请求是通过角色指派发出的，那么有可能即使供应了角色，也不会授予该资源。出现这种情况最有可能的原因是未提供必需的批准。

资源请求可以用于向用户授予资源，也可以用于撤消用户的资源。

Role and Resource Service 驱动程序

User Application 使用 Role and Resource Service 驱动程序来管理资源的后端处理。例如，它管理所有资源请求、启动资源请求的工作流程，以及启动资源请求的供应处理。

访问角色和资源选项卡

要访问角色和资源选项卡，请执行下列操作：

1. 在 User Application 中单击角色和资源。

   默认情况下，角色和资源选项卡会显示角色编目页面。

   如果转至用户界面中的另一个选项卡，但随后又希望返回前一个选项卡，则仅需单击角色和资源选项卡，即可将其再次打开。

浏览选项卡的功能

本节介绍角色和资源选项卡的默认功能。（选项卡的外观可能由于针对您组织所做的自定义而不同；请咨询系统管理员或工作流程设计者。）

角色和资源选项卡的左侧显示可以执行的操作的菜单。这些操作按照类别 （角色和资源、报告和配置）列出：

如果您未被授予导航访问权限，则**角色和资源**选项卡上的一些菜单可能不可用。

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，它可能会显示一个可供您在其中输入数据或进行选择的列表或表单。

您可以执行的角色和资源操作

下面是默认情况下可以在**角色和资源**选项卡中使用的操作的摘要：

表 15-2 *角色和资源操作*

类别	操作	说明
角色和资源	角色编目	通过它可以创建、修改和删除角色。通过它还可以定义角色关系、将资源与角色关联，以及将角色指派给用户、组和容器。 有关细节，请参见第 16 章 " 在 User Application 中管理角色 " （第 149 页）。
	资源编目	通过它可以创建、修改和删除资源。通过它还可以将资源指派给用户。 有关细节，请参见第 17 章 " 在 User Application 中管理资源 " （第 157 页）。
	SoD 编目	通过它可以定义责任分离 (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，请参见在 User Application 中管理责任分离 （第 165 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，请参见角色报告 （第 169 页）。
	SoD 报告	使用户可创建和查看说明责任分离限制、冲突与已批准异常的当前状态的报告。 有关细节，请参见 SoD 报告 （第 171 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，请参见用户报告 （第 172 页）。
配置	配置角色和资源设置	通过它可以指定角色和资源子系统的管理设置。 有关细节，请参见配置角色和资源设置 （第 175 页）。

了解角色和资源选项卡上使用的图标

使用角色和资源选项卡时，您会在许多位置看到传达重要信息的图标。

下表详细说明了角色和资源选项卡上使用的图标：

表 15-3 “ 角色和资源 ” 选项卡上使用的图标

图标	描述
正在运行：处理中	表示一个角色请求仍在处理中。 显示在 “ 请求状态 ” 页面。
待发批准	表示一个 （责任分离异常或角色指派本身的）角色请求正在等待批准。 显示在 “ 请求状态 ” 页面。
已批准	表示一个角色请求已批准。如果检测到责任分离异常，也可将该状态用于表示已批准该异常。 显示在 “ 请求状态 ” 页面。
已完成：已供应	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）。 显示在 “ 请求状态 ” 页面。
拒绝	表示一个角色请求已拒绝。如果检测到责任分离异常，也可将该状态用于表示已拒绝该异常。 显示在 “ 请求状态 ” 页面。
已终止	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。 显示在 “ 请求状态 ” 页面。

图标	描述
角色	表示对象为角色。 显示在 “ 请求状态 ” 页面。
较高级别关系	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。 显示在 “ 角色关系 ” 页面。
较低级别关系	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。 显示在 “ 角色关系 ” 页面。
用户	表示对象为用户。 显示在 “ 角色指派 ” 页面。
组	表示对象为组。 显示在 “ 角色指派 ” 页面。
容器	表示对象为容器。 显示在 “ 角色指派 ” 页面。
直接指派	表示角色是直接指派给当前所选用户、组或容器的。 显示在 “ 角色指派 ” 页面。
待发激活	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。 显示在 “ 请求状态 ” 页面。

16 在 User Application 中管理角色

本章介绍 User Application 的角色管理功能。包括以下主题：

- 浏览角色编目 （第 149 页）

浏览角色编目

通过 Identity Manager 用户界面的**角色和资源**选项卡上的**角色编目**操作，您可以查看以前在编目中定义的角色。通过它还可以创建新角色，以及修改、删除和指派现有角色。

- 查看角色 （第 149 页）
- 创建新角色 （第 150 页）
- 编辑现有角色 （第 154 页）
- 删除角色 （第 154 页）
- 指派角色 （第 155 页）
- 刷新角色列表 （第 156 页）
- 自定义角色列表显示 （第 156 页）

查看角色

在**角色和资源**操作列表中单击**角色编目**。

User Application 会显示当前在编目中定义的角色的列表。

过滤角色列表

1. 在**角色编目**显示内容的右上角单击**显示过滤器**按钮。
2. 指定角色名称或说明的过滤字符串，或者在**过滤器**对话框中选择一个或多个角色级别或类别。
3. 单击**过滤器**来应用您的选择准则。
4. 要去除当前过滤器，请单击**重设置**。

设置页面的最大角色数量

单击**行**下拉列表，然后选择要在每页显示的行数。

在角色列表中滚动

要在角色列表中滚动到另一个页面，请单击列表底部的 “ 下一页 ”、 “ 上一页 ”、 “ 第一页 ” 或 “ 最后一页 ” 按钮。

对角色列表排序

要对角色列表排序，请单击要作为排序依据的列的标题。

金字塔形状的排序指示符会指示哪一个列是新的排序列。升序排序时，排序指示符以正常的直立方式显示。

降序排序时，排序指示符以倒立方式显示。

初始排序列由管理员决定。

如果覆盖了初始排序列，则会将您的排序列添加到必选列的列表中。必选列使用星号 (*) 指示。

在修改任务列表的排序顺序时，您的自选设置会与您的其他用户自选设置一起保存到身份库中。

创建新角色

1 在角色编目显示屏幕的顶部单击新建按钮。

User Application 会显示 " 新建角色 " 对话框：

2 提供角色定义的细节，如表 16-1 中所述。

表 16-1 角色细节

字段	说明
显示名称	当角色名称显示在 User Application 中时使用的文本。创建角色时，不能在显示名称中包含以下字符： < > , ; \ " + # = / | & * 可以将此名称翻译为 User Application 所支持的任意一种语言。有关更多信息，请参见表 1-1" 常用按钮 " （第 22 页）。
说明	当角色说明显示在 User Application 中时使用的文本。与 " 显示名称 " 一样，可以将其翻译为 User Application 所支持的任意一种语言。有关更多信息，请参见表 1-1" 常用按钮 " （第 22 页）。
角色级别	（修改角色时为只读。）从下拉列表中选择一个角色级别。 角色级别使用 Designer for Identity Manager 角色配置编辑器定义。
角色子容器	（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。
类别	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。
拥有者	指定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。

3 单击保存保存角色定义。

User Application 会在窗口底部另外显示几个选项卡，通过这些选项卡可以完成角色定义。

定义角色关系

通过**角色关系**选项卡，可以定义角色在较高和较低角色包容层次结构中的关系。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。如果选择了顶层级别角色，则只能在 " 角色关系 " 页面上添加较低级别角色 （子角色）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。通过 " 角色关系 " 页面，可以添加较低级别角色 （子角色）或较高级别角色 （父角色）。
- 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。通过 " 角色关系 " 页面只能添加较高级别角色。

要定义角色关系，请执行下列操作：

1. 单击**角色关系**选项卡。
2. 单击**添加**。

   此时会显示**添加角色关系**对话框。
3. 在**初始请求说明**字段中输入关于关系的说明文本。
4. 通过在**角色关系**下拉列表中选择类型来指定要定义的关系的类型。

   如果新角色是 IT 角色，则通过**角色关系**下拉列表可以定义**子**或**父**关系。如果新角色是业务角色，则**角色关系**下拉列表会显示只读文本，表明它是**子**关系，因为只有较低级别角色可以与业务角色关联。如果新角色是许可权限角色，则**角色关系**下拉列表会显示只读文本，表明它是**父**关系，因为只有较高级别角色可以与许可权限角色关联。

   供选择的角色的列表会根据您选择的类型进行过滤。
5. 使用**选定的角色**字段右侧的 " 对象选择器 " 来选择要与新角色关联的角色。
6. 单击**添加**。

将资源与角色关联

要将资源与角色关联，请执行下列操作：

1 单击资源选项卡。

2 单击添加。

User Application 会显示添加资源关联对话框。

3 使用 " 对象选择器 " 选择所需的资源，并输入关于关联原因的说明文本。

向导会显示一个页面，其中提供关于选定资源的信息，例如资源类别的名称、拥有者、权利和权利值。

对于接收静态参数值 （为权利提供附加的属性或详细信息）的权利，向导会在权利值标签旁显示这些静态值。对于接收动态参数的权利，向导会显示资源请求表单，表单中会包含对应于动态参数的字段，以及为表单定义的所有决策支持字段。

4 在关联说明字段中，输入说明将资源与角色关联的原因的文本。

5 单击添加将资源与角色关联。

资源关联列表会显示您添加到角色定义中的资源。

现有角色指派会发生何种情况 当向已指派有用户身份的角色添加新的资源关联时，系统会启动新的请求，以将资源授予每个用户身份。

要删除角色的资源关联，请执行下列操作：

1 在资源关联列表中选择资源关联。

2 单击去除。

现有角色指派会发生何种情况 当从已指派有用户身份的角色去除资源关联时，系统会启动新的请求，以从每个用户身份撤消资源。

定义角色的批准进程

要定义角色的批准进程，请执行下列操作：

1 单击批准选项卡。

2 提供批准进程的细节，如下所述：

表 16-2 批准细节

字段	说明
必需批准	如果角色在请求时需要批准，且您希望批准进程执行标准角色指派批准定义，请选择该复选框。 如果角色在请求时不需要批准，则取消选择该复选框。 **注释：**只有显式地将角色指派给用户时，才会触发角色批准。
自定义批准	如果希望使用自定义批准定义 （供应请求定义），则选择该单选按钮。使用对象选择器选择批准定义。
标准批准	如果该角色使用在角色和资源子系统配置中指定的标准角色指派批准定义，则选择该单选按钮。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。 必须选择批准类型 （序列或仲裁人数）以及有效批准者。

字段	说明
批准类型	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。 如果希望批准者列表中一定百分比的用户批准该角色，请选择仲裁人数。当达到指定的用户百分比时，该批准完成。 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。 **提示：**“ 序列 ” 和 “ 规定数 ” 字段中的悬浮文本对其行为进行了介绍。
批准者	如果应将角色批准任务指派给一个或多个用户，请选择用户。如果应将角色批准任务指派给一个组，请选择组。如果应将角色批准任务指派给一个容器，请选择容器。如果应将角色批准任务指派给一个角色，请选择角色。 要查找特定用户、组、容器或角色，请使用对象选择器。要更改列表中的批准者顺序或去除某个批准者，请参见常用用户操作 （第 22 页）。
需要撤消批准 （与授予配置相同）	如果角色在撤消时需要批准，请选中此复选框。 用于角色撤销请求核准过程，以及核准者的列表与角色授予请求相同。如果您指示希望核准过程来执行标准角色分配核准定义，将使用此过程。或者，您可以为角色授予请求和角色撤消请求指定一个自定义批准过程。在自定义供应请求定义中，可以指定操作是授予还是撤消，并相应地自定义批准过程。 如果角色在撤消时不需要批准，则取消选择该复选框。

作出角色指派

有关作出角色指派的细节，请参见指派角色 （第 155 页）。

检查请求的状态

通过请求状态操作，可以查看角色指派请求的状态，包括已直接发出的请求和您所属组或容器的角色指派请求。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。

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、已完成、已拒绝或已终止的请求。

要查看角色指派请求的状态，请执行下列操作：

1 单击请求状态选项卡。

   请求操作会显示操作是授予还是撤消。如果需要批准，并且批准过程尚未完成，其状态将显示待批准。

2 要查看请求的详细状态信息，请单击状态。

   “ 指派细节 ” 窗口随即会显示。

   有关状态值含义的细节，请参见查看请求状态 （第 101 页）

3 要收回某个请求，请选择该请求并单击收回。

您需要具有收回请求的许可权限。

如果请求已完成或终止，则尝试收回请求时会看到错误讯息。

编辑现有角色

1 选择以前定义的角色并单击**编辑**。

2 对角色设置进行更改，然后单击**保存**。

与现有角色关联的权利 在先前版本的 Roles Based Provisioning Module 中定义的角色可能有一些关联的权利。如果某个角色具有关联的权利，用户界面中会显示**权利**选项卡，通过该选项卡可以查看权利映射，并可有选择地去除它。在该版本中，角色的权利映射仍可正常工作，但 NetIQ 现在建议您将权利与资源关联，不要与角色关联。

删除角色

1 选择以前定义的角色并单击**删除**。

当指示 User Application 删除某个角色时，它会先将角色状态设置为**待删除**。然后， Role and Resource Service 驱动程序会检测到状态变化，并执行以下步骤：

- 删除角色的资源指派
- 删除角色本身

Role and Resource Service 驱动程序会优化此过程。但是，此过程可能需要一定时间，具体取决于指派了角色的用户数量；因为 Role and Resource 驱动程序必须确保：如果用户是通过其他方式获得某个资源的，则不删除用户的此资源。如果角色保持**待删除**状态很长时间，请仔细检查驱动程序，以确保它当前正在运行。

当角色的状态为**待删除**时，将无法编辑、删除或指派角色。

现有角色指派会发生何种情况 对于具有关联资源和指派有一个或多个用户身份的角色，如果删除该角色，系统会从具有关联资源的每个用户身份中去除资源指派。

注释：如果您删除为其指派了资源的角色 （或从角色中去除用户），则即使这些资源是首次直接指派，系统也会去除该角色的用户的资源指派。出现这种情况的原因在于，系统假定资源指派的最后权威来源是该资源的控制器，如以下情境中所说明：

1. 创建资源并将其映射到权利。
2. 向上面创建的资源指派用户。
3. 创建与前面第一步中创建的资源绑定的角色。
4. 然后向上面创建的角色指派相同用户
5. 从角色中去除用户。

在此情况下，即使为用户直接指派了资源，也会从资源中去除这些用户。最初，视资源指派为权威来源。但是，当向与同一资源关联的角色指派用户时，该角色就成为权威来源。

删除 SoD 限制中的角色 删除 SoD 限制的冲突角色时，在 SoD 编目列表中， SoD 限制将在名称后的括号中显示 **Invalid**，例如 **Doctor Pharmacists SoD [Invalid]**。

警告：已经被授予系统角色 （或包含这些角色的容器）的 “ 删除角色 ” 许可权限的角色管理者可以删除系统角色。系统角色不应删除。如果删除了任意系统角色， User Application 将无法正常工作。

指派角色

您可以通过两种方式指派角色：

- 通过角色编目
- 通过编辑角色对话框

下面介绍了这两种方法。

通过编目指派角色

1 在角色编目中选择以前定义的角色，然后单击指派。

User Application 会显示指派角色对话框。

2 填写添加角色指派对话框中的字段：

2a 在初始请求说明字段中输入关于请求原因的说明文本。

2b 在 " 指派类型 " 字段中，选择用户、组或容器，指明将角色指派给哪种用户身份类型。

2c 在 " 对象选择器 " 中，输入搜索字符串并单击 " 搜索 "。选择要指派的用户、组或容器。

将角色指派给多个用户身份 您可以为角色指派选择一个或多个用户 （或者组或容器）。如果选择多个用户身份，则所有选定用户身份会接收到相同的角色指派值。

2d 在生效日期字段中指定角色指派的开始日期。

您可以使用格式 mm/dd/yyyy hh:mm:ss a （其中， a 指定 AM 或 PM）输入日期。或者，您也可以单击 " 日历 " 图标，然后从 " 日历 " 弹出窗口中选择日期。

2e 在失效日期字段中指定角色指派的失效日期。

注释：失效日期仅适用于用户指派。对于组和容器，失效日期字段不可用。

要指定失效日期，请单击指定失效日期。您可以使用格式 mm/dd/yyyy hh:mm:ss a （其中， a 指定 AM 或 PM）输入日期。或者，您也可以单击 " 日历 " 图标，然后从 " 日历 " 弹出窗口中选择日期。

默认情况下，失效日期设置为不失效，它表示该角色指派将无限期保持有效。

3 单击提交。

通过 " 编辑角色 " 对话框指派角色

1 在角色编目中选择角色，然后单击编辑打开编辑角色对话框。

2 单击指派选项卡。

指派选项卡会显示已被授予选定角色的指派的列表。

3 要添加新的指派，请单击指派。

User Application 会显示指派角色对话框。

有关使用角色指派请求表单的细节，请参见通过编目指派角色 （第 155 页）。

解决责任分离冲突

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。有关责任分离限制的详细信息，请参见浏览 SoD 编目 （第 165 页）。

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。

如果一个用户间接添加到一个角色中，接着系统检测到存在潜在的责任分离冲突，User Application 会允许添加这个新指派，同时会记录该违例以供报告和审计之用。如果需要，角色管理员可通过重新定义角色来更正违例。

刷新角色列表

要刷新角色列表，请单击**刷新**。

注释：如果创建一个角色指派，然后去除它，您会看见一条讯息，表示已去除该指派，但可能仍会列出该指派。如果刷新页面，您会看到该指派已去除。

自定义角色列表显示

通过**角色编目**，您可以选择和取消选择列，以及对任务列表显示内容中的列重新排序。该行为由**自定义角色编目显示**对话框中的一个设置控制。在修改列的列表或对列重新排序时，您的自定义设置会与您的其他用户自选设置一起保存到身份库中。

要自定义列的显示方式，请执行下列操作：

1. 在**角色编目**中单击**自定义**：

   User Application 会显示当前为显示内容选择的列的列表，以及可供选择的其他列的列表。

2. 要在显示内容中包含其他列，可以选择**可用列**列表框中的列，并将它拖到**选定列**列表框中。

   要在列表中选择多列，可以按住 Ctrl 键并选择这些列。要在列表中选择一起显示的某个列范围，可以按住 Shift 键并选择这些列。

   您可以通过在**选定列**列表框中上移或下移某些列，对显示内容中的列重新排序。

3. 要从显示内容中去除某个列，可以选择**选定列**列表框中的列，并将它拖到**可用列**列表框中。

   角色名称列是必选列，不能从角色列表显示中去除。

4. 要保存更改，请单击**保存**。

17 在 User Application 中管理资源

本章介绍 User Application 的资源管理功能。包括以下主题：

- 浏览资源编目 （第 157 页）

浏览资源编目

通过 Identity Manager 用户界面的角色和资源选项卡上的资源编目操作，您可以查看以前在编目中定义的资源。通过它还可以创建新资源，以及修改、删除和指派现有资源。

- 查看资源 （第 157 页）
- 创建新资源 （第 158 页）
- 编辑现有资源 （第 163 页）
- 删除资源 （第 163 页）
- 指派资源 （第 163 页）
- 刷新资源列表 （第 164 页）
- 自定义资源列表显示 （第 164 页）

查看资源

要查看资源，请在角色和资源操作列表中单击资源编目。

User Application 会显示当前在编目中定义的资源的列表。

过滤资源列表

1. 在资源编目显示内容的右上角单击显示过滤器按钮。
2. 在过滤器对话框中，指定资源名称或说明的过滤字符串，或者选择一个或多个要查看资源的类别。单击过滤器。
3. 要去除当前过滤器，请单击清除。

设置页面的最大资源数量

单击行下拉列表，然后选择要在每页显示的行数。

在资源列表中滚动

要在资源列表中滚动到另一个页面，请单击列表底部的 “ 下一页 ”、 “ 上一页 ”、 “ 第一页 ” 或 “ 最后一页 ” 按钮。

对资源列表排序

要对资源列表排序，请执行下列操作：

1 单击要作为排序依据的列的标题。

金字塔形状的排序指示符会指示哪一个列是新的排序列。升序排序时，排序指示符以正常的直立方式显示。

降序排序时，排序指示符以倒立方式显示。

初始排序列由管理员决定。

如果覆盖了初始排序列，则会将您的排序列添加到必选列的列表中。必选列使用星号 (*) 指示。

在修改任务列表的排序顺序时，您的自选设置会与您的其他用户自选设置一起保存到身份库中。

创建新资源

1 在资源编目显示屏幕的顶部单击新建按钮。

User Application 会显示 “ 新建资源 ” 对话框。

2 提供资源定义的细节，如下所述：

字段	说明
显示名称	当资源名称显示在 User Application 中时使用的文本。创建资源时，不能在显示名称中包含以下字符： < > , ; \ " + # = / | & * 可以将此名称翻译为 User Application 所支持的任意一种语言。有关更多信息，请参见表 1-1“ 常用按钮 ” （第 22 页）。
说明	当角色说明显示在 User Application 中时使用的文本。与 “ 显示名称 ” 一样，可以将其翻译为 User Application 所支持的任意一种语言。有关更多信息，请参见表 1-1“ 常用按钮 ” （第 22 页）。
类别	通过它可以为资源组织对资源进行分类。类别用于对资源列表进行过滤。类别是多选的。
拥有者	指定为资源定义拥有者的用户。资源拥有者不会自动具备管理资源定义更改的授权。

3 单击保存保存角色定义。

User Application 会在窗口底部另外显示几个选项卡，通过这些选项卡可以完成资源定义。

定义资源指派的权利

1 单击权利选项卡。

2 单击浏览权利以选择权利。

User Application 会显示可用权利的树视图列表。

列表显示在 User Application 驱动程序集中找到的所有驱动程序和权利。

注释：如果未正确配置资源，您在访问浏览权利页面以选择权利时，将会看到一条讯息，指出您尚未为资源映射配置权利。

有关配置资源映射的驱动程序和权利的信息，请参见《*NetIQ Identity Manager - Administrator's Guide to the Identity Applications*》（NetIQ Identity Manager - Identity Applications 管理员指南）中的 "Enabling Drivers for Resource Mappings" （启用资源映射的驱动程序）。

3 选择您要用的权利并单击**确定**。

权利选项卡会显示关于权利可能需要的任何值的信息：

4 指定权利绑定的细节。细节会因要与资源关联的权利的类型而异。

权利类型	说明
无值权利	权利不接收任何参数值。例如，资源可能与名为 " 保健津贴 " 的权利绑定，该权利使收件人有资格获得保健津贴。该类型的权利具有固定的行为，因而不需要请求者提供进一步的信息。 绑定到无值权利时，无需进一步的配置。
带自由格式值的权利	在请求时需要将参数值指定为自由格式字符串的权利。例如，资源可能与称为 " 服装 " 的权利绑定，该权利允许请求者指定代表他们喜好颜色的值。 在定义资源时，您可以在设计时赋值，也可以允许用户在请求时赋值。 有关更多信息，请参见绑定到带自由格式值的权利 （第 159 页）。
单值权利	需要单个参数值的权利。例如，资源可能与称为 " 停车许可 " 的权利绑定，该权利允许请求者选择停车位。所允许的值通过权利列表提供，列表中可包含由管理员定义的静态值列表，也可以包含通过 LDAP 查询生成的动态值列表。 在定义资源时，您可以在设计时赋值，也可以允许用户在请求时赋值。 有关更多信息，请参见绑定到单值权利 （第 159 页）。
多值权利	接受一个或多个参数值的权利。例如，资源可能与称为 " 建筑物通行证 " 的权利绑定，该权利允许请求者选择一个或多个建筑物。所允许的值通过权利列表提供，列表中可包含由管理员定义的静态值列表，也可以包含通过 LDAP 查询生成的动态值列表。 在定义资源时，您可以在设计时赋值，也可以允许用户在请求时赋值。 有关更多信息，请参见绑定到多值权利 （第 160 页）。

绑定到带自由格式值的权利

1 要在设计时赋予静态值，请选择**立即赋予权利值**。

为资源键入一个自由格式的值。

2 要在请求时赋予动态值，请选择**允许用户在请求资源时赋予权利值**。

2a 指定用户将在请求资源时看到的标签。

2b 要本地化该标签，请单击**添加语言显示值**按钮，然后指定该标签的外语文本。

绑定到单值权利

1 要在设计时赋予静态值，请选择**立即赋予权利值**。

从默认权利列表中选择单个值。

2 要在请求时赋予动态值，请选择允许用户在请求资源时赋予权利值。

   2a 指定用户将在请求资源时看到的标签。

   2b 要本地化该标签，请单击添加语言显示值按钮，然后指定该标签的外语文本。

   2c 在显示权利列表的值下拉列表中，选择要用于显示允许值的列表。

对于管理员定义的权利或查询权利，允许的值通过在权利中定义的列表提供。这些值会先装载到代码映射数据库表中，以允许您提供用户友好的标签和本地化字符串。装载之后，这些表可以用作创建其他权利列表的来源。

默认情况下，User Application 会创建包含该列表中所有行的权利列表。如果希望仅显示选定行，您可以创建更多权利列表。

绑定到多值权利

1 要在设计时赋予静态值，请选择立即赋予权利值。

   使用对象选择器选择权利值。

2 从默认权利列表中选择一个或多个值。

3 要在请求时赋予动态值，请选择允许用户在请求资源时赋予权利值。

   3a 指定用户将在请求资源时看到的标签：

   3b 要本地化该标签，请单击添加语言显示值按钮，然后指定该标签的外语文本：

   3c 在显示权利列表的值下拉列表中，选择要用于显示允许值的列表。

   3d 通过选择允许用户通过选择多个值来请求多个赋值复选框来指定用户是否可以选择多个值。

      由于权利定义允许多个赋值，所以您可以指定是否希望资源也允许多个赋值。

定义请求表单

资源的请求表单会显示一种类型的字段：

- 决策支持字段，请求者可以通过这些字段提供可能有助于批准者决定是批准还是拒绝请求的附加信息。

请求表单选项卡会显示此字段，并提供用于创建和编辑决策支持字段的用户界面。

除了请求表单选项卡中显示的字段之外，请求表单总是会包含以下必填字段：

- 用户
- 原因

请求表单上的所有字段会在批准表单上显示为只读值。

要定义请求表单，请执行下列操作：

1 单击请求表单选项卡。

   请求表单选项卡会显示对应于权利参数的字段的列表，这些字段的值将在请求时指定。权利参数字段的属性在 “ 操作 ” 选项卡中配置。您无法更改映射到权利参数的字段的行为。

2 要添加决策支持数据字段，请执行下列操作：

   2a 单击加号 (+) 以添加新字段。

   2b 请求表单选项卡会向字段列表中添加一个新字段 （默认标签为字段标签 1），并显示 “ 属性 ” 面板供您定义字段的特征。

   2c 要立即赋予决策支持值，请单击立即。

提供字段的显示标签，以及数据类型和值。支持以下数据类型：

数据类型	说明
布尔	具有两个可能值的逻辑数据类型：true 或 false。
整数	自然数序列。
列表	用于从中选择一个值的一组预定值。
字符串	代表文本的值序列。

要在请求表单上隐藏该值，请单击隐藏。在请求表单上隐藏的字段在批准表单上仍然是可见的。

2d 要允许用户在请求时赋值，请单击请求资源时。

提供字段的显示标签，并指定值是必须为特定数据类型还是来自列表。

定义批准流程设置

要定义批准进程，请执行下列操作：

1. 单击批准选项卡。
2. 通过选择或取消选择允许角色批准进程覆盖资源批准进程复选框来指定角色的批准进程是否可以覆盖资源的批准进程。

   如果选择了允许角色批准进程覆盖资源批准进程复选框，则每次将资源与角色关联时，角色批准进程总是会覆盖资源批准进程。在关联的角色被批准之后，无需任何批准，就会自动供应资源。
3. 定义授予操作的批准进程，方式如下：

   3a 打开批准选项卡的授予批准部分。

   3b 指定批准细节，如下所述：

字段	说明
必需	如果资源在请求时需要批准，则选择该框。 如果资源在请求时不需要批准，则取消选择该框。
自定义批准	选择自定义批准时，您需要选择一个自定义的资源指派批准定义。它是在请求资源时执行的供应请求定义的名称。
标准批准	选择标准批准时，资源会使用在资源子系统配置设置中指定的标准资源指派批准定义。
批准类型	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。 如果希望批准者列表中一定百分比的用户批准该角色，请选择仲裁人数。当达到指定的用户百分比时，该批准完成。 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。 **提示：**“ 信息 ” 按钮会显示关于批准类型的说明文本。

字段	说明
批准者	如果应将角色批准任务指派给一个或多个用户，请选择用户。如果应将角色批准任务指派给一个组，请选择组。如果应将角色批准任务指派给一个角色，请选择角色。 要查找特定用户、组或角色，请使用对象选择器或历史按钮。要更改列表中的批准者顺序或去除某个批准者，请参见常用用户操作 （第 22 页）。

4 定义撤消操作的批准细节，如下：

4a 打开 " 批准 " 选项卡的撤消批准部分。

4b 指定批准细节，如下所述：

字段	说明
必需	如果资源在请求时需要批准，则选择该框。 如果资源在请求时不需要批准，则取消选择该框。
与授予配置相同	选择该框可以将用于授予操作的设置复制到用于撤消操作的设置中。

有关所有其他批准细节，请参见授予操作的字段说明，该内容位于步骤 3b （第 161 页）。

供应资源

该供应操作可让您定义在授予或撤消资源之后，应该通过工作流程完成的其他工作。

供应请求定义下拉列表显示已经为资源定义的供应请求定义。供应请求定义创建后，其处理类型为资源供应。

此工作流程会在资源被授予或撤消之后执行为其定义的任何其他工作。

指派资源

有关细节，请参见通过 " 编辑资源 " 对话框指派资源 （第 163 页）。

检查请求的状态

通过请求状态操作，您可以查看资源指派请求的状态，包括直接发出的请求和通过角色指派的资源。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。

请求状态操作将显示所有资源指派请求，包括正在运行、待发批准、已批准、已完成、已拒绝或已终止的请求。

1 单击请求状态选项卡。

对于请求表单上的每个字段，" 请求状态 " 会在列表中显示单独的列。例如，请求列表中添加了 " 车库 " 列，以便显示为资源指派指定的权利值。

2 要查看请求的详细状态信息，请单击状态。

" 指派细节 " 窗口随即会显示。

有关状态值含义的细节，请参见查看请求状态 （第 101 页）

3 要收回某个请求，请选择该请求并单击**收回**。

如果请求已被完成或终止，则尝试收回请求时会看到错误讯息。

编辑现有资源

1 选择以前定义的资源，然后单击**编辑**。

2 对资源设置进行更改，然后单击**保存**。

删除资源

1 选择以前定义的资源，然后单击**删除**。

现有资源指派会发生何种情况 当删除已经指派有一个或多个用户身份的资源时，系统会从那些用户身份中去除该资源。如果资源已经与某个角色关联，则系统还会去除与所删除资源有关的所有角色关联。

指派资源

您可以通过两种方式指派资源：

- 通过**资源编目**
- 通过**编辑资源**对话框

下面介绍了这两种方法。

通过编目指派资源

1 在**资源编目**中选择以前定义的资源，然后单击**指派**。

User Application 会显示资源请求表单。

初始请求说明和**用户**字段是必填字段，会显示在所有资源请求表单中。您可以使用 " 对象选择器 " 为资源指派选择用户。

将资源指派给多个用户 您可以为资源指派选择一个或多个用户。如果选择多个用户，所有用户会接收到相同的资源指派参数值。

请求表单中可能会包含一些附加字段，用于接受动态参数值或决策支持值。

在以上显示的示例中，**建筑物许可权限**字段用于接受权利参数值，而**公司名称**和**需要停车？**字段是决策支持字段。这些字段不是权利定义的一部分。相反地，这些字段已添加到资源定义中。

2 填写请求表单中的字段。

3 单击**提交**。

通过 " 编辑资源 " 对话框指派资源

1 在**资源编目**中选择资源，然后单击**编辑**打开**编辑资源**对话框。

2 单击**指派**选项卡。

指派选项卡会显示已被授予选定资源的指派的列表。

3 要添加新的指派，请单击**指派**。

User Application 会显示资源请求表单。

有关使用请求表单的细节，请参见通过编目指派资源 （第 163 页）。

刷新资源列表

要刷新资源列表，请单击**刷新**。

注释：如果创建一个资源指派，然后去除它，您会看见一条讯息，表示已去除该指派，但可能仍会列出该指派。如果刷新页面，您会看到该指派已去除。

自定义资源列表显示

通过**资源编目**，您可以选择和取消选择列，以及对任务列表显示内容中的列重新排序。列的选择和顺序由**自定义资源编目显示**对话框中的设置控制。在修改列的列表或对列重新排序时，您的自定义设置会与您的其他用户自选设置一起保存到身份库中。

要自定义列的显示方式，请执行下列操作：

1. 在**资源编目**中单击**自定义**。

   User Application 会显示当前为显示内容选择的列的列表，以及可供选择的其他列的列表。

2. 要在显示内容中包含其他列，可以选择**可用列**列表框中的列，并将它拖到**选定列**列表框中。

   要在列表中选择多列，可以按住 Ctrl 键并选择这些列。要在列表中选择一起显示的某个列范围，可以按住 Shift 键并选择这些列。

   您可以通过在**选定列**列表框中上移或下移某些列，对显示内容中的列重新排序。

3. 要从显示内容中去除某个列，可以选择**选定列**列表框中的列，并将它拖到**可用列**列表框中。

   资源名称列是必选列，不能从任务列表显示中去除。

4. 要保存更改，请单击**保存**。

18 在 User Application 中管理责任分离

本章介绍 User Application 的责任分离 (SoD) 管理功能。包括以下主题：

- 浏览 SoD 编目 （第 165 页）

浏览 SoD 编目

通过 Identity Manager 用户界面的**角色和资源**选项卡上的 **SoD 编目**操作，您可以执行以下操作：

- 定义责任分离 (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。

- 查看责任分离限制 （第 165 页）
- 创建新的责任分离限制 （第 166 页）
- 编辑现有的责任分离限制 （第 167 页）
- 删除责任分离限制 （第 167 页）
- 刷新责任分离限制列表 （第 167 页）

查看责任分离限制

1. 在**角色和资源**操作列表中单击 **Sod 编目**。

   User Application 会显示当前在编目中定义的责任分离限制的列表。

过滤责任分离列表

1. 在**责任分离限制**显示内容的右上角单击**显示过滤器**按钮。
2. 在**过滤器**对话框中指定限制名称或说明的过滤字符串。
3. 单击**过滤器**来应用您的选择准则。
4. 要去除当前过滤器，请单击**重设置**。

设置页面的最大行数

1 单击 “ 行 ” 下拉列表，然后选择希望每页显示的行数。

在责任分离列表中滚动

1 要在限制列表中滚动到另一个页面，请单击列表底部的 “ 下一页 ”、 “ 上一页 ”、 “ 第一页 ” 或 “ 最后一页 ” 按钮。

对责任分离列表排序

要对限制列表排序，请执行下列操作：

1 单击要作为排序依据的列的标题。

   金字塔形状的排序指示符会指示哪一个列是新的排序列。升序排序时，排序指示符以正常的直立方式显示。

   降序排序时，排序指示符以倒立方式显示。

   初始排序列由管理员决定。

如果覆盖了初始排序列，则会将您的排序列添加到必选列的列表中。必选列使用星号 (*) 指示。

在修改限制列表的排序顺序时，您的自选设置会与您的其他用户自选设置一起保存到身份库中。

创建新的责任分离限制

1 在**责任分离限制**显示屏幕的顶部单击**新建**按钮。

   User Application 会显示**新建责任分离限制**对话框。

2 在 **SoD 限制名称**字段中提供限制的名称，并在 **SoD 限制说明**字段中输入说明。

3 在两个冲突角色字段中分别选择每个冲突角色。角色的选择顺序并不重要。

4 定义批准细节，如定义批准流程设置 （第 167 页）下所述。

定义批准流程设置

1 打开页面的批准部分。

2 指定批准细节，如下所述：

字段	说明
必需	如果对于异常， SoD 限制需要批准，则选择该框。 如果对于异常， SoD 限制不需要批准，则取消选择该框。
使用默认批准者	如果希望使用在 SoD 批准定义中定义的默认批准者列表，则选择是。如果选择是，则页面会显示在批准定义中指定的批准者列表。您无法编辑该列表。 如果希望指定其他列表作为 SoD 限制定义的一部分，则选择否。如果选择否，则需要使用批准者控件来指定将负责批准 SoD 异常的用户。
默认批准者	显示在配置角色和资源设置页面中指定的批准者的只读列表。
批准者	通过它可以指定一个批准者列表，作为限制定义的一部分。 如果应将批准任务指派给一个或多个用户，请选择用户。如果应将批准任务指派给一个组，请选择组。如果应将批准任务指派给一个或多个容器，请选择 “ 容器 ”。如果应将批准任务指派给一个角色，请选择角色。 要查找特定用户、组或角色，请使用对象选择器按钮。要更改列表中的批准者顺序或去除某个批准者，请参见常用用户操作 （第 22 页）。

编辑现有的责任分离限制

1 选择以前定义的 SoD，然后单击编辑。

2 对 SoD 设置进行更改，然后单击保存。

删除责任分离限制

1 选择以前定义的 SoD，然后单击删除。

刷新责任分离限制列表

1 单击刷新。

19 创建和查看报告

本章介绍可以通过角色和资源选项卡创建和查看的报告。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。

重要：您可从角色和资源选项卡创建和查看的报告已被弃用，将来版本中将不支持这些报告。 NetIQ 现在建议您使用 Identity Reporting Module 来生成报告。

本章包括以下主题：

- 关于角色报告操作 （第 169 页）
- 角色报告 （第 169 页）
- SoD 报告 （第 171 页）
- 用户报告 （第 172 页）

关于角色报告操作

通过角色和资源选项卡，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、修改和删除角色或责任分离。

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。

角色报告

角色报告有两种：

- 角色列表报告
- 角色指派报告

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**报告 > 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。请使用此图标来进行选择。

   打开对象选择对话框。

   要选择一个用户，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。

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**以创建和查看 PDF 报告。

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。

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**报告 > 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 选择以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 170 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 170 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**以创建和查看 PDF 报告。

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。

SoD 报告

下面的两个报告说明责任分离的当前状态：

- SoD 限制报告
- SoD 违例和异常报告

SoD 限制报告

“SoD 限制报告 ” 显示：

- 当前按名称定义的责任分离限制
- 责任分离的说明
- 冲突角色列表
- 具有批准责任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**报告 > 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 170 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 170 页）的选择框图标说明。

5 单击**运行报告**以创建和查看 PDF 报告。

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。

SoD 违例和异常报告

“SoD 违例和异常报告 ” 显示：

- 每个责任分离限制的名称，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。这些是作为责任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**报告 > 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。

用户报告

用户报告有两种：

- 用户角色报告
- 用户权利报告

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**报告 > 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 170 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
仅显示直接指派的角色。	“ 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。
包括直接指派角色的批准信息。	“ 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。
仅显示指派了角色的用户。	“ 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 单击运行报告以创建和查看报告。
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。

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，然后选择报告 > 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 170 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 PDF 报告。
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。

20 配置角色和资源设置

本章介绍用于配置角色和资源设置的用户界面。它包含下列主题：

- 关于配置角色和资源设置操作 （第 175 页）
- 配置角色设置 （第 175 页）
- 配置资源设置 （第 176 页）
- 配置权利查询设置 （第 176 页）
- 配置责任分离设置 （第 176 页）
- 配置报告设置 （第 177 页）

关于配置角色和资源设置操作

通过**配置角色和资源设置**操作，您可以定义角色和资源系统的基本配置。页面具有以下部分：

- 角色设置
- 资源设置
- 权利查询设置
- 责任分离 (SoD) 设置
- 报告设置

要在编辑模式下修改**配置角色和资源设置**，必须*同时*具有以下两种指派：

- 角色管理员 （或具有**配置角色设置**许可权限的角色管理者）
- 资源管理员 （或具有**配置资源设置**许可权限的资源管理者）

要在只读模式下查看**配置角色和资源设置**页面上的设置，只需具有以上列出的*一种*许可权限。

处于编辑模式时，**配置角色和资源设置**页面中只有部分设置是可编辑的。一些设置会显示在安装时设置的只读值，不能修改。

配置角色设置

要配置角色设置，请执行下列操作：

1. 在**配置**操作组中单击**配置角色和资源设置**。
2. 滚动到页面的**角色设置**部分。

   以下设置是在安装时固定的只读设置：

   - 角色容器
   - 角色请求容器
   - 默认角色批准定义
3. 指定 （以秒为单位）**角色指派宽限期**。

该值以秒为单位指定从角色编目中去除角色指派之前的时间量 （默认情况下为 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。

注释：角色指派宽限期是一项仅影响角色到权利指派的旧设置；它并不会影响角色到资源到权利的映射。它对使用此版本中提供的新资源模型创建或指派的角色不会产生任何影响。

---

4 定义角色级别的显示名称。每个级别具有单独的显示名称，可以翻译为几种不同语言。要提供外语字符串，请单击添加语言显示值。

5 单击保存使设置永久保存。

配置资源设置

要查看资源设置，请执行下列操作：

1 在配置操作组中单击配置角色和资源设置。

2 滚动到页面的资源设置部分。

这些设置控制 User Application 的资源管理组件的行为。所有资源设置都是只读的。

配置权利查询设置

要配置权利查询设置，请执行下列操作：

1 在配置操作组中单击配置角色和资源设置。

2 滚动到页面的权利查询设置部分。

这些设置控制 User Application 执行的权利查询的行为。您可以定义权利查询的超时间隔和刷新频率。此外，您还可以查看权利值是否已刷新，并开始手动刷新 （如果需要）。

配置责任分离设置

要配置责任分离 (SoD) 设置，请执行下列操作：

1 在配置操作组中单击配置角色和资源设置。

2 滚动到页面的责任分离 (SoD) 设置部分。

“SoD 容器 ” 设置是在安装时固定的只读设置。

- SoD 容器
- 默认 SoD 批准定义

3 在 SoD 批准定义字段中，选择将用于处理 SoD 批准的供应请求定义。

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	如果希望批准者列表中一定百分比的用户批准该角色，请选择仲裁人数。当达到指定的用户百分比时，该批准完成。 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。

5 修改默认 SoD 批准者。

字段	说明
默认 SoD 批准者	如果应将角色批准任务指派给一个或多个用户，请选择用户。如果应将角色批准任务指派给一个组，请选择组。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，请选择角色。与组相同，仅角色中的一个成员需要批准。 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去除一个批准者，请参见常用用户操作 （第 22 页）

6 单击保存使设置永久保存。

配置报告设置

报告容器值是在安装时固定的只读设置。

VI 使用合规性选项卡

以下几章说明如何使用 Identity Manager User Application 的**合规性**选项卡。

- 第 21 章 " 合规性选项卡简介 "（第 181 页）
- 第 22 章 " 发出证明请求 "（第 191 页）

21 合规性选项卡简介

本章概述 " 合规性 " 选项卡。包括以下主题：

- 关于合规性选项卡 （第 181 页）
- 访问该选项卡 （第 183 页）
- 浏览选项卡的功能 （第 184 页）
- 可执行的合规性操作 （第 184 页）
- 了解证明请求图例 （第 184 页）
- 常用合规性操作 （第 185 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 17 页）。

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

代理模式仅在工作仪表板选项卡上起作用，在合规性选项卡上不受支持。如果在工作仪表板选项卡上进入代理模式，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模式。

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**工作仪表板**选项卡上的**任务通知**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。

Roles Based Provisioning Module 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， Roles Based Provisioning Module 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。表单通常由合规性管理员定义。

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 ” 选项卡识别称为 “ 合规性管理员 ” 的单个管理员角色。合规性管理员在安装时指定。安装之后，可以向合规性管理员角色中另外指派用户。要另外指派用户，需要使用 User Application 中的 **RBPM 供应和安全性 > 管理员指派**页面。

下面详细介绍了合规性管理员角色：

表 21-1 *合规性功能的系统角色*

角色	说明
合规性管理员	具有合规性域中的全部功能的管理员。合规性管理员可以执行合规性域中的所有对象的所有可能操作。 这些操作包含以下功能： ◆ 请求用户简介证明流程。 ◆ 请求 SoD 违反证明进程。 ◆ 请求角色指派证明流程。 ◆ 请求用户指派证明流程。 ◆ 查看已提交的所有证明请求的状态。 **注释：**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 “ 合规性管理员 ” 角色。

如果已鉴定用户不具有以上列出的合规性管理员角色的成员资格，则这些用户不能访问**合规性**选项卡。

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。

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。这些操作列在证明请求类别中。

仅当您是合规性管理员时，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，它可能会显示一个可供您在其中输入数据或进行选择的列表或表单。

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，请参见了解证明请求图例 （第 184 页）。

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 21-2　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，请参见请求用户简介证明流程 （第 191 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，请参见请求 SoD 违反证明进程 （第 192 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，请参见请求角色指派证明流程 （第 193 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，请参见请求用户指派证明流程 （第 194 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，请参见检查证明请求的状态 （第 195 页）。

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。该图例简要说明整个合规性选项卡中使用的图标。表 21-3 提供了图例中图标的详细说明。

表 21-3 “图例”图标

图标	描述
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。
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。
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。
用户	表示证明者是用户。 出现在“查看证明请求状态”页面中的“证明者”列中。
组	表示证明者是组。 出现在“查看证明请求状态”页面中的“证明者”列中。
角色	表示证明者是角色。 出现在“查看证明请求状态”页面中的“证明者”列中。

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：

- 指定请求的标签和说明 （第 186 页）
- 定义证明者 （第 186 页）
- 指定最后期限 （第 187 页）
- 定义证明表单 （第 187 页）
- 提交证明请求 （第 188 页）

- 保存请求细节 （第 188 页）
- 使用已保存的请求 （第 189 页）

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。

定义证明者

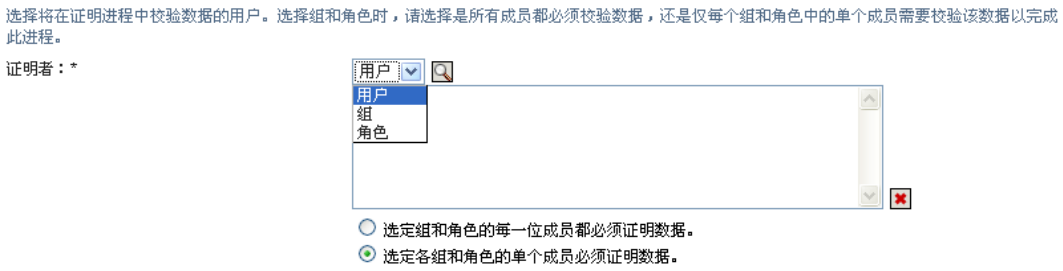
请求 SoD 违反证明进程、请求角色指派证明流程和请求用户指派证明流程操作提供了一个用于定义证明者的一致界面。

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。



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，请参见常用用户操作 （第 22 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用户。

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。

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。

最后期限对于起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。

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。

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。该数字也称为关联 ID，因为它将一组关联的工作流程与单个请求关联。

以下是起动请求所必需的字段：

表 21-4 *起动请求所需的字段*

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。

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 21-5 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。

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。

22 发出证明请求

本章提供发出证明请求的说明。包括以下主题：

- 关于证明请求操作 （第 191 页）
- 请求用户简介证明流程 （第 191 页）
- 请求 SoD 违反证明进程 （第 192 页）
- 请求角色指派证明流程 （第 193 页）
- 请求用户指派证明流程 （第 194 页）
- 检查证明请求的状态 （第 195 页）

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。

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，请参见使用已保存的请求 （第 189 页）。

3 指定请求的显示标签和说明。有关详细信息，请参见指定请求的标签和说明 （第 186 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，请参见常用用户操作 （第 22 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。只有在下拉列表中选择容器时，才会显示包含子容器的所有用户复选框。但是，您可以更改包含子容器的所有用户设置，而无需去除和添加以前选择的任何容器。

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，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，请参见指定最后期限 （第 187 页）。

7 定义证明表单的细节。有关详细信息，请参见定义证明表单 （第 187 页）。

8 提交请求。有关详细信息，请参见提交证明请求 （第 188 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，请参见保存请求细节 （第 188 页）。

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。

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，请参见使用已保存的请求 （第 189 页）。

3 指定请求的显示标签和说明。有关详细信息，请参见指定请求的标签和说明 （第 186 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。

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，请参见常用用户操作 （第 22 页）。

您必须至少选择一个 SoD 限制才能起动证明流程。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，请参见定义证明者 （第 186 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，请参见指定最后期限 （第 187 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，请参见定义证明表单 （第 187 页）。

9 提交请求。有关详细信息，请参见提交证明请求 （第 188 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，请参见保存请求细节 （第 188 页）。

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。

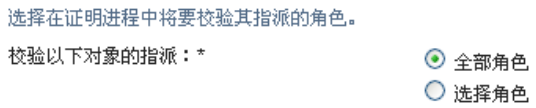
User Application 将显示一个页面，使用该页面，您可指定有关证明流程的细节。

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，请参见使用已保存的请求 （第 189 页）。

3 指定请求的显示标签和说明。有关详细信息，请参见指定请求的标签和说明 （第 186 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，请参见常用用户操作 （第 22 页）。

您必须至少选择一个角色才能起动证明流程。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，请参见定义证明者 （第 186 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，请参见指定最后期限 （第 187 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，请参见定义证明表单 （第 187 页）。

9 提交请求。有关详细信息，请参见提交证明请求 （第 188 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，请参见保存请求细节 （第 188 页）。

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，请参见使用已保存的请求 （第 189 页）。

3 指定请求的显示标签和说明。有关详细信息，请参见指定请求的标签和说明 （第 186 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。

      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，请参见常用用户操作 （第 22 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。只有在下拉列表中选择**容器**时，才会显示**包含子容器的所有用户**复选框。但是，您可以更改**包含子容器的所有用户**设置，而无需去除和添加以前选择的任何容器。

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，请参见定义证明者 （第 186 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，请参见指定最后期限 （第 187 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，请参见定义证明表单 （第 187 页）。

9 提交请求。有关详细信息，请参见提交证明请求 （第 188 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，请参见保存请求细节 （第 188 页）。

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 对于合规性管理员可在 “ 查看证明请求状态 ” 页面上查看的内容不设任何限制。该角色允许访问关于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。要启动此类型的进程，合规性管理员需要使用**请求用户配置文件证明进程**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。要启动此类型的进程，合规性管理员需要使用**请求 SoD 违反证明进程**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。要启动此类型的进程，合规性管理员需要使用**请求角色指派证明进程**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。要启动此类型的进程，合规性管理员需要使用**请求用户指派证明进程**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。
已完成	表示所有证明者均已应答 （或者个别进程已由合规性管理员收回）且该请求已完成处理。
错误	表示在处理期间发生了错误。 错误的准确讯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讯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，请参见常用用户操作 （第 22 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 （或者个别进程已由合规性管理员收回）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。

确认编号字段支持确认编号可能的最大长度，即 255 个字符。

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中选择一个数字。

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。

请求细节组框中的证明者列会在每个证明者旁边显示一个图标，指示证明者是用户、组还是角色。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。 **注释：**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。 **注释：**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每个证明者，以及由于超时而完成或者由合规性管理员收回的进程。

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。

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。

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，请参见声明任务 （第 88 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每个进程，以及由于超时而完成或者由合规性管理员收回的进程。

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。
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中选择一个数字。

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。

VII 附录

接下来的附录提供了 Identity Manager User Application 的其他参考信息和高级主题。

- 附录 A“ 使用 Identity Manager Approvals 应用程序 ”（第 201 页）
- 附录 B“ 使用 User Application 中的目录搜索 ”（第 209 页）

A 使用 Identity Manager Approvals 应用程序

除了 Identity Manager 客户使用的 User Application 用户界面之外，您现在还可以使用一款新的 iOS 应用程序，它可让 Identity Manager 用户通过 Roles Based Provisioning Module for Identity Manager 远程批准或拒绝请求。

安装并配置 Approvals 应用程序之后，您就可以在该应用程序中看到通常在 User Application 界面中所看到的相同批准任务。所有更改都会在 Approvals 应用程序和 User Application 之间同步。

您还可以在与 Identity Manager Roles Based Provisioning Module 服务器断开连接后，在脱机模式下工作，一旦连接恢复， Approvals 应用程序将会自动同步任何更改。

此附录提供了有关安装和使用新的 Approvals 应用程序的信息。有关 Identity Manager 管理员可如何配置其环境以允许用户使用该应用程序的信息，请参见《*NetIQ Identity Manager - Administrator's Guide to the Identity Applications*》（NetIQ Identity Manager - Identity Applications 管理员指南）中的 "Configuring the Identity Manager Approvals App" （配置 Identity Manager Approvals 应用程序）。

有关 Approvals 应用程序的更多详细信息，请参见下列各节：

- 产品要求 （第 201 页）
- 安装 Approvals 应用程序 （第 202 页）
- 配置 Approvals 应用程序 （第 202 页）
- Approvals 应用程序概述 （第 205 页）
- 更改 Approvals 应用程序的显示语言 （第 207 页）

产品要求

Approvals 应用程序需要使用安装了 Apple iOS 5、 iOS 6 或 iOS 7 的 Apple iPhone 或 iPad。

注释：如果您的管理员尚未授予 Approvals 应用程序的使用权限，安装应用程序之后，您可能无法对其进行配置。有关管理员可如何配置 Identity Manager 环境以授予 Approvals 应用程序的使用权限的信息，请参见《*NetIQ Identity Manager - Administrator's Guide to the Identity Applications*》（NetIQ Identity Manager - Identity Applications 管理员指南）中的 "Configuring the Identity Manager Approvals App" （配置 Identity Manager Approvals 应用程序）。

安装 Approvals 应用程序

您可以从 Apple App Store 中的 Approvals 应用程序页面 (http://appstore.com/NetIQIdentityManagerApprovals) 上，将 NetIQ Identity Manager Approvals 应用程序安装到您的设备上。

安装 Approvals 应用程序之后，您必须配置该应用程序，以便能够与 Roles Based Provisioning Module 服务器连接。

注释：如果您的 User Application 口令已失效，则建议您在安装和配置 Approvals 应用程序之前先更改口令。如果您环境中的口令策略在口令失效后仅允许限定的宽限登录次数， Approvals 应用程序在尝试将您的 Identity Manager 任务同步到您的设备时，有可能会用完所有这些登录次数。

配置 Approvals 应用程序

您可以用多种方法配置 NetIQ Identity Manager Approvals 应用程序，具体取决于环境的需要以及管理员是如何配置 Identity Manager 的：

- 在 User Application 界面中提出访问 Approvals 应用程序的请求，然后在您的设备上，通过 Identity Manager 管理员提供的电子邮件链接启动该应用程序。该链接包括所有必需的配置信息。
- 单击配置链接或使用您的设备扫描配置 QR 码，其中，链接或 QR 码可提供所有必需的配置信息或您公司通用的配置信息。
- 直接在该应用程序中手动输入您的环境的配置信息。

重要：要让用户能够使用链接或 QR 码自动配置 Approvals 应用程序， Identity Manager 环境的管理员必须先启用链接或 QR 码。

通过 User Application 请求移动访问权

如果管理员已进行相应配置，则您可以使用 User Application 请求访问 Approvals 应用程序的权限。Identity Manager 随后会发送一封含有自定义链接的电子邮件，您可以在您的设备上打开该链接来自动使用您的信息配置该应用程序。

要通过 User Application 请求移动访问权：

1. 在 Web 浏览器中，使用 HTTPS (https://) 协议登录 Identity Manager User Application。

   注释：要请求访问 Approvals 应用程序的权限，您必须使用 HTTPS 协议登录 User Application。

   ---

2. 单击**提出处理请求**。
3. 单击 “ 处理请求类别 ” 下拉菜单并选择**帐户**。
4. 单击**继续**。
5. 单击**请求移动批准应用程序**。

   注释：处理请求类别和名称可能会因管理员配置 Approvals 应用程序请求处理的方式而异。

   ---

6 在处理请求表单中提供必需的信息，然后单击**提交**。

7 当您收到 Identity Manager 管理员发送的电子邮件时，在您的设备上打开电子邮件，然后单击其中提供的链接，以将您的设备连接到 Roles Based Provisioning Module 服务器。

注释：如果您以前已安装该应用程序，该应用程序可能显示一条警告讯息，指出将会重写现有设置。请确保警告讯息中显示的主机名就是您请求访问应用程序时访问的相同主机。如果不确定，请不要单击链接，应与您的管理员联系。

如果主机名正确，请单击**接受**以重写现有设置。

---

8 当应用程序启动后，输入您的口令，然后单击 " 测试连接 " 图标 以验证您的设置。

使用配置链接或 QR 码

Identity Manager 管理员可能会提供一个用于配置 Approvals 应用程序的配置链接。在设备上的浏览器中打开该链接，以自动配置该应用程序。

不过，此链接只能提供部分必需的设置。一般而言，链接或代码只能提供 Approvals 应用程序正常工作所需的 Roles Based Provisioning Module 服务器细节。单击该链接之后，您必须手动配置您的用户名和口令设置，以及无法自动配置的任何其他设置。

在有些环境中，您可能无法从您的设备上访问电子邮件。如果您不能在您的设备上接收电子邮件，可以使用设备扫描 Identity Manager 管理员提供的个性化 QR 码。

在您的计算机上显示提供的 QR 码或将其打印在纸上 （如有必要），然后在您的设备上使用 QR 码读取器扫描该代码。在 QR 码自动根据您的环境配置 Approvals 应用程序之后，手动配置您的用户名和口令设置。

手动配置 Approvals 应用程序

如果 Identity Manager 环境的管理员未提供用于配置 Approvals 应用程序的链接或 QR 码，您也可以手动配置所需的设置。

警告：由于在您的设备上手动配置应用程序需要具有 Identity Manager 组件的深层知识，因此只建议企业中了解 Roles Based Provisioning Module 和 User Application 环境的高级用户手动配置应用程序设置。其他用户应该联系其 Identity Manager 管理员，以了解有关配置该应用程序的信息。

在应用程序中，单击设置图标 ，指定必需的设置，然后单击 " 测试连接 " 图标 以验证您的设置。

Approvals 应用程序需要您进行下列设置：

登录设置名称	登录设置说明
用户名	指定您用来访问 Roles Based Provisioning Module 服务器的用户名。
口令	指定您用来访问 Roles Based Provisioning Module 服务器的口令。

登录设置名称	登录设置说明
数据同步	指定是否要让该应用程序主动将数据同步到 Roles Based Provisioning Module 服务器。
高级 > 服务器细节 > 服务器	指定 Roles Based Provisioning Module 服务器的完全限定域名或 IP 地址。
高级 > 服务器细节 > 安全端口	指定应用程序用来连接服务器的 HTTPS 端口。
高级 > 服务器细节 > 环境	指定安装 User Application WAR 文件时使用的环境。默认值为 IDMProv。
高级 > 服务器细节 > 用户容器	指定存储用户信息的身份库容器的完整 DN。
高级 > 服务器细节 > 超时	指定在尝试连接服务器时，应用程序在取消连接之前等待的秒数。默认值为 5 秒。
高级 > 数据定义设置 > 用户实体	指定在身份库中表示用户的 LDAP 实体。默认值为 user。
高级 > 数据定义设置 > 名称格式	指定应用程序用来设置用户全名格式的 DAL 属性表示法。默认值为 FirstName LastName。
高级 > 数据定义设置 > 名属性	指定表示用户名字的 DAL 属性的名称。默认值为 FirstName。
高级 > 数据定义设置 > 姓属性	指定表示用户姓氏的 DAL 属性的名称。默认值为 LastName。
高级 > 数据定义设置 > 用户照片属性	指定包含用户照片的 DAL 属性的名称。默认值为 UserPhoto。 **注释：**如果您未在 Identity Manager 中配置图片，或将 Identity Manager 配置为不显示图片，则应用程序会显示通用图像。
高级 > 数据定义设置 > 办公室电话属性	指定表示用户办公室电话号码的 DAL 属性的名称。默认值为 TelephoneNumber。
高级 > 数据定义设置 > 移动电话属性	指定表示用户移动电话号码的 DAL 属性的名称。默认值为 mobile。
高级 > 数据定义设置 > 电子邮件属性	指定表示用户电子邮件地址的 DAL 属性的名称。默认值为 Email。
高级 > 数据定义设置 > 照片 LDAP 属性	指定包含用户照片的 LDAP 属性的名称。默认值为 photo。
高级 > 数据定义设置 > 命名属性	指定在身份库中用来描述名称的命名 DAL 属性。默认值为 cn。
高级 > 数据定义设置 > 供应管理员	指定您是否为 Roles Based Provisioning Module 服务器上的供应管理员。

登录设置名称	登录设置说明
高级 > 接受的证书	指定您允许 Approvals 应用程序接受的来自 Roles Based Provisioning Module 服务器的任何无效或自我签名证书。 当 Approvals 应用程序检测到自我签名或无效的证书时，会询问您要接受还是拒绝该证书。如果您接受证书，应用程序会将该证书添加至 “ 接受的证书 ” 列表。您可以通过单击某个证书的名称并重新启动应用程序，将该证书从 “ 接受的证书 ” 列表中去除。 **注释：**如果 Roles Based Provisioning Module 服务器证书有效，应用程序不会将该证书添加至 “ 接受的证书 ” 列表。应用程序默认会接受有效的证书。
高级 > 拒绝的证书	指定您不想让 Approvals 应用程序接受的来自 Roles Based Provisioning Module 服务器的任何无效或自我签名证书。 当 Approvals 应用程序检测到自我签名或无效的证书时，会询问您要接受还是拒绝该证书。如果您拒绝证书，应用程序会将该证书添加至 “ 拒绝的证书 ” 列表。此后，当服务器出示拒绝的证书时，应用程序将无法与服务器建立连接。 您可以通过单击某个证书的名称将其从 “ 拒绝的证书 ” 列表中去除。

Approvals 应用程序概述

本节提供 NetIQ Identity Manager Approvals 应用程序用户界面的概述。包括以下主题：

- 任务视图 （第 205 页）
- 细节视图 （第 206 页）
- 批量模式 （第 206 页）
- 已完成任务视图 （第 206 页）
- 登录设置视图 （第 206 页）
- 高级设置视图 （第 207 页）

任务视图

Approvals 应用程序的默认视图是 “ 任务 ” 视图。此视图显示当前指派给您或由您认领的所有任务，以及任务的标题和任务接收人的姓名和图片。视图按失效日期列出任务，失效日期最近的任务显示在最上面，没有失效日期的任务显示在下面。

注释：如果用户未在 Identity Manager 中配置图片或将 Identity Manager 配置为不显示图片，则应用程序会显示通用图像。

如果要批准或拒绝请求，或者查看特定任务的细节，请单击该任务或任务接收人姓名。如果要联系任务接收人，请单击接收人的图片。

细节视图

“ 细节 ” 视图显示指派给您的某个特定任务的细节。显示的字段会因请求而异。

要批准或拒绝任务，请提供所有必需的信息，然后单击**批准**或**拒绝**。

批量模式

如果您需要批准或拒绝大量类似的任务，可以在 “ 任务 ” 视图中从默认的单任务模式切换到批量模式。

注释：您不能在批量模式下批准所有任务。对于较复杂的任务 （如证明任务），必须在单任务模式下分别批准每个证明任务。当您单击 “ 批量模式 ” 图标后，应用程序只会在列表中显示您可以在批量模式下批准的任务。

要批准或拒绝多个任务：

1. 在 “ 任务 ” 视图中，单击批量模式图标 。
2. 选择要批准或拒绝的任务。您不能同时批准一些任务又拒绝另一些任务。
3. （可选）如果要批准或拒绝所有任务，请单击**全部**。
4. （可选）如果您改变主意，不想批准或拒绝任何任务，请单击单任务模式图标 。
5. 单击**批准**或**拒绝**。
6. （可选）提供有关批量操作的注释。
7. 单击**确认**。

已完成任务视图

要查看您已完成的任务，请单击 “ 已完成任务 ” 图标 。视图即会显示已完成的任务，以及批准或拒绝任务的时间。您可以单击某个已完成的任务，以查看该特定任务的细节。对于较复杂的请求，可以单击**表单值**以查看该请求的特定信息。

如果需要，您可以从 “ 已完成任务 ” 视图中删除一个或多个已完成的任务。要删除多个任务，请单击 “ 批量模式 ” 图标 ，选择要删除的任务，然后单击**删除**。

注释：“ 已完成任务 ” 视图只显示在您的设备上完成的任务。您不能查看在 User Application 中或在其他安装了 Approvals 应用程序的设备上完成的任务。

登录设置视图

“ 登录设置 ” 视图允许您查看或修改您的登录设置。

警告：如果 Identity Manager 管理员提供了用于自动配置您的应用程序设置的链接或 QR 码，建议您不要修改那些默认设置，除非管理员要求您这么做。

高级设置视图

“ 高级设置 ” 视图可让您查看或修改高级设置，这些设置决定您以何方式接收来自 Roles Based Provisioning Module 服务器的数据。

警告：如果 Identity Manager 管理员提供了用于自动配置您的应用程序设置的链接或 QR 码，建议您不要修改那些默认设置，除非管理员要求您这么做。

如果您不小心更改了 “ 高级设置 ” 视图中的 “ 数据定义设置 ”，请单击**恢复默认值**恢复 Identity Manager 提供的默认设置。**恢复默认值**不会更改您的用户名、口令或任何服务器细节设置。

更改 Approvals 应用程序的显示语言

Approvals 应用程序包含多种语言的本地化文本字符串。要更改 Approvals 应用程序使用的语言，请在您的 iOS 设备上更改 “ 语言 ” 和 “ 区域格式 ” 设置。 “ 区域格式 ” 设置用于配置设备上日期、时间和电话号码的显示方式。

要修改语言和区域设置：

1. 在您的 iOS 设备上，单击**设置**。
2. 单击**常规**。
3. 单击**国际**。
4. （可选）如果要更改设备使用的语言，请单击**语言**，选择要使用的语言，然后单击**完成**。
5. （可选）如果要更改设备用于日期和时间的区域格式，请单击**区域格式**，选择要使用的格式，然后单击**国际**。
6. 返回到设备的主页屏幕。

B 使用 User Application 中的目录搜索

本章说明如何使用 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：

- 了解目录搜索 （第 209 页）
- 执行基本搜索 （第 210 页）
- 执行高级搜索 （第 210 页）
- 处理搜索结果 （第 216 页）
- 使用保存的搜索 （第 219 页）

注释：本章说明 " 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。

了解目录搜索

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 B-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。他只需以此准则指定一个基本搜索。

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。

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。他想起要查找的人是 Kip Keller 的下属，于是将搜索范围缩小到 Cal Central。

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 添加了一些常用的已保存搜索。

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
```

更多信息请参见选择表达式 （第 212 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
```

更多信息请参见为比较运算指定值 （第 214 页）。

6 单击**搜索**。

将显示搜索结果。

要了解下一步操作，请参见处理搜索结果 （第 216 页）。

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）：

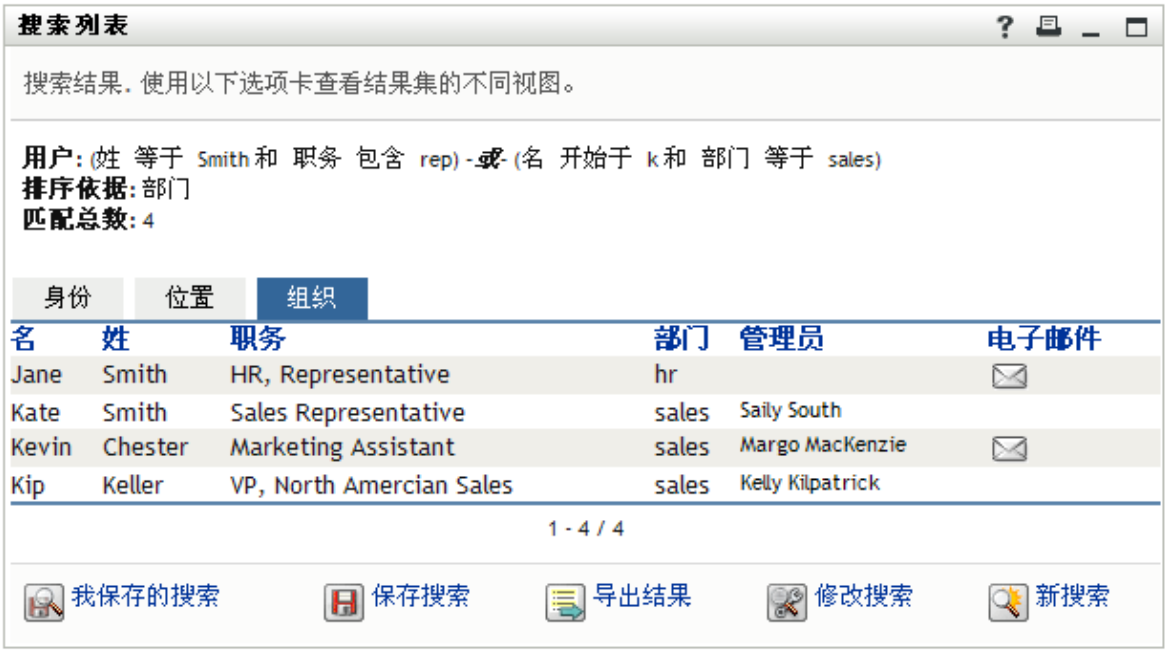
```
(Last Name equals Smith AND Title contains Rep) OR (First Name starts with k AND
Department equals Sales)
```

指定图 B-2 在第 211 页 中显示的以下选项：

图 B-2　在“搜索列表”页面上指定高级搜索

此搜索的结果在图 B-3 在第 211 页 中显示。

图 B-3　高级搜索结果



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**。“高级搜索”页面随即显示。

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
```

更多信息请参见选择表达式 （第 212 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
```

更多信息请参见为比较运算指定值 （第 214 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**添加条件分组**。

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。

要删除某个条件分组，请单击该条件分组正上方的**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，请参见处理搜索结果 （第 216 页）。

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 B-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）	◆ 起始字符 ◆ 包含 ◆ 等于 ◆ 结束字符 ◆ 存在 ◆ 起始字符不是 ◆ 不包含 ◆ 不等于 ◆ 结束字符不是 ◆ 不存在
具有预先确定的选项列表的字符串 （文本） 用户或组 （或 DN 标识的其他对象） 布尔值 （true 或 false）	◆ 等于 ◆ 存在 ◆ 不等于 ◆ 不存在
用户 （项目类别：管理员、组或直接报告）	◆ 等于 ◆ 存在 ◆ 不等于 ◆ 不存在
组 （项目类别：成员）	◆ 等于 ◆ 存在 ◆ 不等于 ◆ 不存在
时间 （格式为日期 - 时间或仅有日期） 数字 （整数）	◆ 等于 ◆ 大于 ◆ 大于等于 ◆ 小于 ◆ 小于等于 ◆ 存在 ◆ 不等于 ◆ 不大于 ◆ 不大于等于 ◆ 不小于 ◆ 不小于等于 ◆ 不存在

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 B-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 标识的其他对象）	使用右侧显示的**查找**、**历史**和**重设置**按钮。
时间 （格式为日期 - 时间或仅有日期）	使用右侧显示的**日历**和**重设置**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 “ 重设置 ” 按钮

有些搜索准则会显示 “ 查找 ”、“ 历史 ” 和 “ 重设置 ” 按钮。本节介绍如何使用这些按钮：

表 B-3 搜索准则中的“查找”、“历史”和“重设置”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历史列表
	重设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：

“查找”页面随即显示。

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 添加组作为搜索准则，然后单击搜索术语 查找“查找”按钮 。

“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说明 Marketing：

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

3 单击搜索。

“ 查找 ” 页将显示搜索结果。

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 在要查看其以前值的项右侧，单击历史 ：

历史列表按字母顺序显示以前使用该准则搜索到的值。

2 执行以下步骤之一：

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

处理搜索结果

本节说明如何处理成功搜索后显示的结果：

- 关于搜索结果 （第 216 页）
- 使用搜索列表 （第 217 页）
- 可以执行的其他操作 （第 218 页）

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 217 页）
- 对于组搜索 （第 217 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）

对于组搜索

组搜索的结果只提供信息的 “ 组织 ” 视图。

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：

- 要切换到其他视图，请执行下列操作：（第 217 页）
- 要对信息行排序，请执行下列操作：（第 217 页）
- 要显示用户或组的细节，请执行下列操作：（第 217 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 218 页）

要切换到其他视图，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）。

   “ 配置文件 ” 页面随即显示，列出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。
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，其他部分均是空白的。

3 填写邮件的内容。

4 发送邮件。

可以执行的其他操作

显示搜索结果时，还可以：

- 保存搜索 （第 218 页）
- 导出搜索结果 （第 218 页）
- 修改搜索准则 （第 219 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，请参见使用保存的搜索 （第 219 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）。

“ 导出 ” 页面随即显示。

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**。

“ 导出 ” 页面随即显示。

4 使用**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.*date*.*time*.csv 例如： `SearchListResult.27-Sep-05.11.21.47.csv`
制表符分隔	SearchListResult.*date*.*time*.txt 例如： `SearchListResult.27-Sep-05.11.20.51.txt`
XML （如果导出至磁盘则可用）	SearchListResult.*date*.*time*.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 根据下列几节中的指导修改搜索准则：
- 执行基本搜索 （第 210 页）
- 执行高级搜索 （第 210 页）

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。本节说明可对已保存搜索执行的操作：

- 要列出保存的搜索，请执行下列操作：（第 220 页）
- 要运行保存的搜索，请执行下列操作：（第 220 页）
- 要编辑保存的搜索，请执行下列操作：（第 220 页）
- 要删除保存的搜索，请执行下列操作：（第 220 页）

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。

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，请参见处理搜索结果 （第 216 页）。

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 根据下列几节中的指导修改搜索准则：
   - 执行基本搜索 （第 210 页）
   - 执行高级搜索 （第 210 页）
4 要保存对搜索所做的更改，请参见处理搜索结果 （第 216 页）。

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。