CA Identity Manager™

管理指南

12.6.4

ca technologies

CA Technologies 产品引用

本文档引用以下 CA Technologies 产品：

- CA CloudMinder™ 身份管理
- CA Directory
- CA Identity Manager ™
- CA Identity Governance（以前是 CA GovernanceMinder）
- CA SiteMinder®
- CA 用户活动报告
- CA AuthMinder ™

联系技术支持

要获取在线技术帮助以及办公地址、主要服务时间和电话号码的完整列表，请联系技术支持：http://www.ca.com/worldwide。

目录

第 1 章： 角色规划

在规划角色前，首先要确定您的企业或组织需要哪些类型的角色，以及您要如何指派用户的管理权限及其应用程序访问权限。 然后，基于这些决策确定每个角色的特征。

要有效地使用角色，请考虑下列有关用户需求和管理员职责的问题：

- 需要管理哪些部门和组织的用户？
- 在管理端点中，用户需要添加哪些附加帐户？
- 哪些用户应是其他用户的管理员？
- 管理员应由谁管理？
- 每个角色需要哪些管理和访问任务？
- 谁应创建角色和任务？
- 如何使用角色指派工作？

  最后一个问题是如何分配用户管理和应用程序访问授权工作。 有关指派模型的详细信息，请参阅“指派管理”。

根据对这些问题的回答，就可以确定需要多少角色以及需要哪些类型的角色。

此部分包含以下主题：

角色决策

以下内容提供的信息可以帮助您做出明智的角色决策。

角色用途

要有效地使用角色，请考虑下列有关用户需求和管理员职责的问题：

- 需要管理哪些部门和组织的用户？
- 在管理端点中，用户需要添加哪些附加帐户？
- 哪些用户应是其他用户的管理员？
- 管理员应由谁管理？

- 每个角色需要哪些管理和访问任务？
- 谁应创建角色和任务？
- 如何使用角色指派工作？

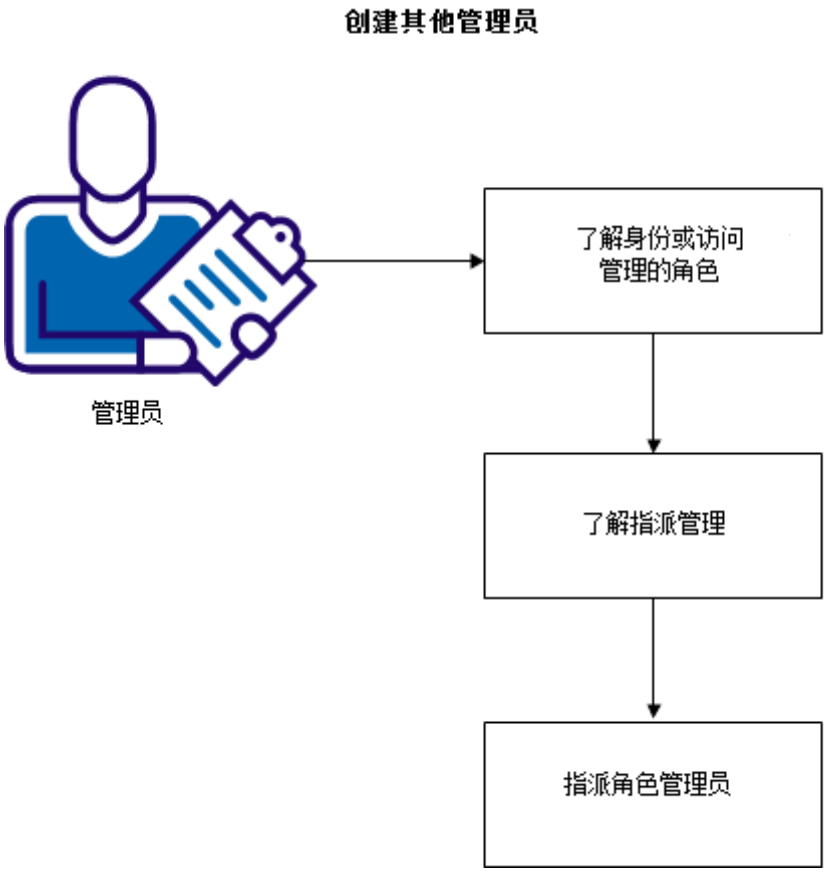
  最后一个问题是如何分配用户管理和应用程序访问授权工作。 有关指派模型的详细信息，请参阅“指派管理”。

根据对这些问题的回答，就可以确定需要多少角色以及需要哪些类型的角色。

创建其他管理员

您既可以全权负责将所有角色授予系统中的用户， 也可以指派其他管理员来负责授予用户角色的工作。 此方法称为*指派管理*。

下图说明了在创建其他管理员时要了解的信息以及要执行的步骤。



下列主题说明如何创建其他管理员：

- 用于身份或访问管理的角色 (p. 19)
- 指派管理 (p. 19)
- 指派角色管理员 (p. 20)

用于身份或访问管理的角色

CA CloudMinder 提供两种类型的角色，以启用对用户身份和用户对其他帐户的访问权的管理。 拥有管理角色的用户可以管理用户，如修改用户密码或组成员资格。 管理角色还可包括在用户控制台中显示的任何任务。 拥有配给角色的用户可以使用其他业务应用程序，如电子邮件系统。

下表列出了有关角色的详细信息：

角色类型	用途
管理角色	包含被授予此角色的用户可以在 CA CloudMinder 中执行的管理员任务（如管理用户的任务）。
配给角色	包含用于定义管理端点（如电子邮件系统）中存在的帐户的帐户模板。 帐户模板也用于定义如何将用户属性映射到这些帐户。
访问角色	访问角色提供另一种在 CA Identity Manager 或其他应用程序中提供权利的方式。 例如，您可使用访问角色来完成下列操作： ■ 提供对用户属性的间接访问。 ■ 创建复杂的表达式。 ■ 设置其他的应用可用于确定权限的配置文件属性。

指派管理

指派管理是使用角色来分担管理用户和授予应用程序访问权的工作。

对于在系统中的每个角色，用户可以提供以下一个或多个功能：

功能	定义
角色所有者	修改角色。
角色管理员	为用户和其他角色管理员指定角色。
角色成员	使用此角色来执行管理或访问任务，或者使用端点帐户。

通过将这些功能分配给用户，您可以让其他用户分担管理角色的工作。 例如，您可以让低级别管理员来管理角色成员资格，而让高级别管理员来修改角色。

您可以通过以下方法来实施指派管理：

- 直接将用户指定为给定角色的管理员。
- 为角色配置*管理规则*。 管理规则用于定义哪些用户可以是某个角色的管理员。 当用户符合规则中指定的条件时，系统将自动创建其他管理员。

  注意：具有修改角色权限的管理员才能配置该角色的管理规则。 典型的做法是，由系统管理员执行此活动。 若要为角色配置自动指派管理的管理规则，请参阅位于“联机帮助”的“参考信息”部分下的“为管理角色授权”部分。

指派角色管理员

您可以将某个用户指定为角色管理员。 然后管理员就可以将角色分配给其他用户。

遵循这些步骤:

1. 以具有角色管理任务的用户身份登录到“用户控制台”。
2. 依次选择“任务”、“角色和任务”。
3. 选择以下任务之一：
   - 管理角色、修改管理角色成员/管理员
   - 开通角色、修改开通角色成员/管理员
   - 访问角色、修改访问角色成员/管理员

   此时显示一个搜索屏幕。
4. 选择要分配给用户的角色。
5. 单击“管理员”选项卡。

   此时显示当前角色管理员列表。
6. 单击“添加用户”。

   此时显示一个搜索屏幕。
7. 搜索要添加为管理员的用户，然后单击“选择”。

   此时显示更新后的角色管理员列表。
8. 单击“提交”。

   该用户便成为角色的管理员。通过此步骤可完成指派开通角色管理的过程。管理员现在可以将角色分配给其他用户，将访问权限授予关联的端点帐户。

指派步骤

根据“角色用途”决定如何使用角色后，会出现下列指派管理情况：

1. 管理员使用适用于角色所有者、管理员或成员的规则创建角色。
2. 角色所有者在需要时对角色进行修改。

3. 角色管理员：
   - 分配更多角色管理员（可选）。
   - 分配更多角色成员（可选）。

   某些用户满足了在相应角色中定义的规则，因而已经是角色管理员或成员。
4. 角色成员使用相应角色：
   - 管理角色成员会管理用户和 Identity Manager 环境中的其他对象。
   - 访问角色成员会执行业务应用程序中的功能。
   - 配给角色成员会使用角色中策略定义的帐户。

指派示例

您可以使用确定成员或管理员的规则创建角色。 之后，您可以分配该角色，从而让其他用户（尚不符合规则）也可以成为角色成员或管理员。

让我们来看下下面这个负责管理最终用户业务应用程序权限的管理员示例：

- Jeff 是“会计”角色的角色所有者；因此在角色需要更改时，Jeff 便会修改该角色。
- David 和 Lisa 是该角色的角色管理员。 他们将区域用户分配为角色成员。
- 其他用户在未分配的情况下成为角色成员。他们符合成为角色成员的规则。

  角色成员可使用“会计”角色来生成订购单，并在财务应用程序中执行其他任务。

“角色特征”部分提供了有关规则及其他角色特征的详细信息。

角色特征

在创建角色时，定义在下表中显示的特征：

特征	定义
角色配置文件	角色的一般特征。
任务	管理角色的任务。
帐户模板	对于配给角色，用于定义管理端点中帐户的模板。

特征	定义
成员规则、 成员策略	成员规则用于定义用户成为访问角色或管理角色成员的条件。 成员策略用于将成员规则与作用域规则结合起来。 **注意：**配给角色没有成员规则和策略。 要让用户成为成员，请使用“修改配给角色成员/管理员”。
管理规则、 管理策略	■ 管理规则用于定义用户成为角色管理员的条件。 ■ 管理策略用于将管理规则与作用域规则以及用于分配角色的管理员权限结合起来。
所有者规则	用户成为角色所有者的条件。
作用域规则	有关角色可以管理哪些对象的限制。
添加操作、 删除操作	当添加或删除作为角色成员或管理员的用户时，对用户配置文件所做的更改。

角色配置文件

角色配置文件包含了角色的名称和说明以及角色是否启用的信息。 如果角色已启用，则您可在其创建后使用它。

角色的任务

对于管理角色，您可以从一个或多个类别中选择一个或多个管理任务，其中包括外部任务。

帐户模板

每个配给角色都包含帐户模板。 它们定义了位于管理端点中的帐户。 例如，Exchange 帐户的端点可能定义了邮箱的大小。 帐户模板还定义了用户属性如何映射到帐户。

您可以为每个端点类型选择一个或多个端点。 被分配角色的用户会获得端点中的帐户。

成员、管理员和所有者规则

每个角色均包括关于哪些人可以成为该角色的成员、管理员或所有者的规则。因此，用户可以是一个角色或多个角色的成员，也可以不属于任何角色。

成员、管理员和所有者规则将使用下表中的条件：

规则条件	示例	规则语法
用户必须与一个属性值相匹配。	Users where title starts with senior	where <用户筛选>
用户必须与多个属性值相匹配。	职位=经理且位置=东部的用户	where <用户筛选>
用户必须属于指定的组织。	销售部门及下级组织中的用户	in <组织规则>
用户必须属于符合组织属性指定条件的组织。	Users in organizations where Business Type=gold or platinum	in organizations where <组织筛选>
用户必须属于特定组织并与特定的用户属性相匹配。	职位=经理、位置=东部，且于销售或营销组织中的用户	where <用户筛选> and who are in <组织规则>
用户必须属于特定组。	属于 401K 组成员的用户	who are members of group <组>
用户必须是某个角色的成员。	属于“帮助中心”角色成员的用户	who are members of <角色规则>
用户必须是某个角色的管理员。	属于“销售经理”角色管理员的用户	who are administrators of <角色规则>
用户必须是某个角色的所有者。	属于“用户经理”角色所有者的用户	who are owners of <角色规则>
用户必须属于满足组属性指定条件的组。	属于所有者=CIO 的组成员的用户	who are members of group <组筛选>

规则条件	示例	规则语法
用户必须满足 LDAP 查询的条件。	（在 Identity Manager 用户控制台中创建的查询条件不充分时，使用 LDAP 目录）	ldap_query 查询返回的用户

某些规则可能会涉及将一个值与多值属性进行比较。 对于要应用的规则，多值属性中必须至少有一个值满足该规则。例如，如果该规则为“属性 A 等于 1”且用户 X 的属性 A 的值为 1、2、3，则用户 X 满足该标准。

创建角色的用户可能无法修改该角色。 为了能修改角色，该用户必须符合所有者规则中的条件。

注意：在大型实施中，可能需要花费大量的时间来评估成员、管理员和所有者规则。要缩短包括用户属性的规则的评估时间，您可以启用内存中的评估选项。有关详细信息，请参阅*《Configuration Guide》*。

作用域规则

将成员和管理规则与作用域规则合并。 *作用域规则*限制可使用角色的对象。

- 对于角色成员，作用域规则控制可与角色一同管理的对象。
- 对于角色管理员，作用域规则控制可成为角色成员和管理员的用户。

作用域适用于任务的主要对象。例如，用户是创建用户任务的主要对象。然而，作用域不适用于该用户的组，因为组是次要对象。

对于大多数对象类型，您可以在下表中指定作用域规则类型。

规则条件	示例	规则语法
全部	角色成员可管理所有对象	All
对象必须与一个或多个属性值相匹配。	Users where **title** starts with **senior**	where <筛选>

在您选择筛选选项时，CA Identity Manager 显示两种类型的筛选：

<属性> <比较运算符><值>

对象的配置文件中的属性必须匹配特定值。

<属性> <比较运算符> admin's <用户属性>

对象的配置文件中的属性必须匹配管理员配置文件中的属性。例如：Users where manager = admin's UserID。

在下表中说明的其他选项，可用于用户、组和组织对象。

注意：以下用户作用域规则为示例。您可以创建其他规则，以便处理管理员和管理员可以管理的用户之间的不同关系。

规则条件	示例	规则语法
用户必须与一个属性值相匹配。	Users where member of group sales or cell phone does not equal null	where <用户筛选>
用户必须与多个属性值相匹配。	Users where title=manager and locality=USA	where <用户筛选>
用户必须属于指定的组织。	Users in organization Australia or New Zealand **注意**：组织作用域规则应用于满足该规则的组织的子组织。例如，如果组织规则是"in Organization1"，那么作用域规则则适用于 Organization1.1 和 Organization1.2，但不适用于 Organization1。	in <组织规则>
用户必须属于符合组织属性指定条件的组织。	Users in organizations where Business Type=gold or platinum	in organizations where <组织筛选>
用户必须属于特定组织并与特定的用户属性相匹配。	Users where title=manager and locality=east and who are in organization sales or organization marketing	where <用户筛选> and who are in <组织规则>

规则条件	示例	规则语法
用户配置文件上的属性必须匹配管理员配置文件上的属性。	Users where manager = admin’s UserID	where <用户属性> <比较运算符> admin’s <用户属性> **注意：**请使用带有多值属性的“不等于”比较运算符。
用户与管理员位于同一组织。	Users in the organization where Jeff (the administrator) is a member	admin’s organization
用户位于列在管理员属性上的组织。	Users in sales or marketing	organization that is a value in admin’s <管理属性>

注意：以下组作用域规则仅为示例。 您可以创建其他规则，以便处理管理员和管理员可以管理的组之间的不同关系。

规则条件	示例	规则语法
组必须与一个属性值相匹配。	Group name where Group name = 401K	where <组筛选>
组必须属于指定的组织。	Groups in organization accounting and lower	in <组织规则>
组必须与一个属性值相匹配，且属于指定的组织。	Groups where BusinessType = finance and who are in organization sales and lower	where <组筛选> and who are in <组织规则>
组必须列在管理员的属性中。	Groups where Description = Engineering	where <组属性> <比较运算符> admin’s <用户属性> **注意：**请使用带有多值属性的“不等于”比较运算符。

注意：以下组织作用域规则仅为示例。 您可以创建其他规则，以便处理管理员和管理员可以管理的组织之间的不同关系。

规则条件	示例	规则语法
组织必须与一个属性值相匹配。	organizations where org Name=finance	where <组织筛选>
组织必须属于指定的组织。	organizations in finance and lower	in <组织规则>
组织必须与一个属性值相匹配，且属于指定的组织。	organizations where org Name=finance and are in finance and lower	where <组织筛选> and are in <组织筛选>

更多信息：

关于规则的通用指南 (p. 27)

关于规则的通用指南

无论您创建的是什么类型的规则，您都应当了解 Identity Manager 处理它们的方式。

运算符求值

在创建角色的规则时，可以使用 >=、<=、< 和 > 运算符。 但是，这些运算符在求值时会被 LDAP 目录或关系数据库当做字符串处理。大多数用户存储按照字母表顺序比较字符串。 因此，在比较 500 和 1100 时，用户存储可能会认为 500 更大，因为 5 大于 1。

您可以更改字符串在用户存储中的比较方式。请参阅 LDAP 目录服务或关系数据库软件相关文档。

规则中的大小写

创建管理或访问角色时，您创建的规则可能以不区分大小写或区分大小写的方式进行求值，具体取决于用户存储。

但是，在创建或修改操作结束时，系统会按不区分大小写的方式对规则进行内部求值，然后才会将更改应用于用户存储。 例如，如果规则包含了条件 title=manager，则无论用户存储对象使用了 manager 还是 Manager 的标题值，该规则都会与其匹配。

添加和删除操作

您必须为 Identity Manager 指定添加操作和删除操作，以在管理员授予或吊销角色时正确地管理该角色的成员资格。

- 添加操作必须使用户符合角色成员条件中的其中一条。 例如，如果用户管理者角色的成员规则声明角色成员使用"用户管理者"作为其管理角色属性的值，则添加操作必须将"用户管理者"添加到管理角色属性中。
- 删除操作应更改用户的配置文件，便于在撤销成员规则时此用户不再符合该规则。

每个角色可以有两个*添加操作*和两个*删除操作*。

如果管理员可以添加和删除角色的成员，您就要定义添加和删除操作。 否则，用户只能通过满足成员规则（例如属于 RoleAdmins 组）来获得角色。 例如：

- 角色 A 可以由管理员分配，因此要定义添加或删除操作。
- 角色 B 使用了以下规则：组“finance”的所有成员都具有该角色。 此角色不能分配，因此没有添加或删除操作。

在定义添加和删除操作时，请考虑使用“管理角色”属性，Identity Manager 可以使用该属性存储用户的角色列表。 例如，在将某个用户添加为“员工”角色的成员时，您可以配置添加操作，将“员工”添加到该用户的管理角色属性中。 在管理员将“员工”角色分配给已经具有“自行管理员”和“用户管理者”角色的经理时，该经理的管理角色属性将包含以下值：“Self Administrator”（自行管理员）、“User Manager”（用户管理者）、“Employee”（员工）。

要使用管理角色属性，必须将 %ADMIN_ROLE_CONSTRAINT% 这一常用属性映射到用户配置文件中的某一多值属性。有关详细信息，请参阅*《CA Identity Manager 配置指南》*。

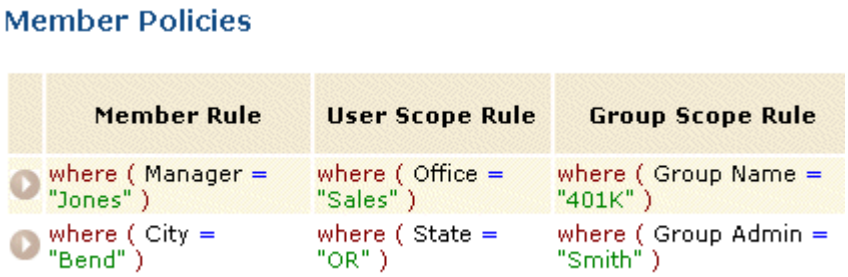
重要说明！ 在定义添加操作时，应避免设置引用您正在定义的角色的规则。 例如，不要定义通过成为角色 A 的成员来生成角色 A 的成员的添加操作。 这将形成递归错误，导致策略服务器重新启动。

成员策略

*成员策略*表示如果用户满足成员规则，则会具有相应策略中定义的作用域。 下图显示了具有两个成员策略的角色。

- 第一个策略表示，如果角色成员有 Manager Jones，则该成员可以针对销售部的用户使用这一角色，并将他们作为 401k 组的成员进行管理。

- 第二个策略表示，如果角色成员位于本德市，则该角色成员可以针对俄勒冈州的用户使用这一角色，并将他们作为具有 Group Admin of Smith 的组成员进行管理。

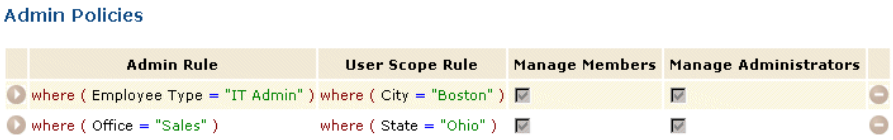


管理策略

*管理策略*表示如果用户满足管理规则，则会具有相应策略中定义的用户作用域和管理员权限。 用户作用域定义了角色的使用范围。 管理员权限确定了角色管理员可以管理成员还是管理角色的管理员。

下图显示了具有两个管理策略的角色，其定义如下：

- 对于第一个策略，IT 管理员可以添加或删除波士顿市用户的角色成员和管理员。
- 对于第二个策略，销售部门中的管理员可以添加和删除俄亥俄州的成员。



角色规划清单

在创建角色之前，请使用此角色特征清单。

角色特征	详细信息
角色配置文件	定义角色的名称和说明，并且设置“已启用”状态。
任务	包括管理或访问任务。
帐户模板	包括定义位于端点（仅配给角色）中的帐户的帐户模板。

角色特征	详细信息
成员策略	对于每个成员策略，定义： ■ 成员规则－谁可以使用角色 ■ 作用域规则－角色成员可以管理哪些对象 ■ 添加操作－用户成为成员后配置文件会发生什么 ■ 删除操作－用户作为成员被删除后配置文件会发生什么
管理策略	对于每个管理策略： ■ 管理规则－谁可以作为成员或管理员管理用户 ■ 作用域规则－哪些用户可以作为成员或管理员由该管理员进行管理 ■ 添加操作－用户成为管理员后配置文件会发生什么 ■ 删除操作－用户作为管理员被删除后配置文件会发生什么
所有者规则	定义可以修改角色的人。

第 2 章： 管理角色

此部分包含以下主题：

管理角色和管理任务

您可以根据您的特定业务需求，创建包含管理对象任务的角色。 例如，您可以创建若干个管理用户任务的角色，以及管理您所创建角色的任务的其他角色。

此外，您还可以创建承担以下任务的独立角色：

- 用于管理员管理用户的任务
- 管理管理员的任务
- 管理管理角色的任务
- 管理访问角色的任务

注意：您还可以使用 CA Identity Manager 附带的默认管理角色。 这些角色所承担的任务按照与前面列表类似的类别分组。

管理角色和 Identity Manager 环境

登录到 Identity Manager 环境后，您的用户帐户将具有一个或多个管理角色。每个管理角色都包含在该 Identity Manager 环境中使用的任务，例如创建用户。

例如，在*中心* Identity Manager 环境中，管理角色 *Help Desk* 承担重置密码的任务。 该角色具有一个成员规则，即用户必须是 IT 雇员。 IT 雇员登录到*中心* Identity Manager 环境后，他们便具有了 *Help Desk* 角色，并且可以在该 Identity Manager 环境中重置用户的密码。

管理角色和用户控制台

通过用户控制台可以查看 Identity Manager 环境。分配给您的管理角色确定您在该控制台中看到的内容，如下表所示：

分配的角色	用户控制台的格式
系统管理员角色	针对所有对象以及所有管理这些对象的默认管理任务的类别列表
管理多种对象类型的角色	对于您可以管理的每种对象类型，类别列表中均包含对应的项目
管理对象类型的角色，例如用户	*没有*类别列表的对象（如修改用户）的任务
批准角色	工作列表屏幕 如果管理员承担等待批准的任务（例如，自行注册的用户需要批准），则显示此屏幕

如果您可以管理多个对象，则显示类别列表，该列表将在屏幕顶部以选项卡的形式显示您可以修改的对象，例如用户和组。 选择选项卡可查看分配给您的角色中的任务。

注意：如果您的 Internet 浏览器不支持层叠样式表 (CSS)，则用户控制台将使用其他格式。 要控制该格式，请参阅*《配置指南》*。

创建管理角色

了解角色需求后，就可以创建管理角色。 这些要求涉及将使用此角色的人员、此角色要管理的对象以及要管理的对象所在的环境。

开始创建管理角色

可从用户控制台创建管理角色。

创建管理角色

1. 登录到具有创建管理角色任务的角色的 CA Identity Manager 帐户。

   例如，某环境的第一位用户具有系统管理员角色，该角色具有创建管理角色的任务。

2. 依次选择“角色和任务”、“管理角色”和“创建管理角色”。

3. 确定是创建角色还是复制角色。

   将显示“配置文件”选项卡，您可以在其中开始定义管理角色。

4. 定义管理角色配置文件。

定义管理角色配置文件

在“配置文件”选项卡上，可以定义角色的基本特征。

定义配置文件

1. 输入名称和说明，并完成为该角色定义的所有其他自定义属性。

   注意：可以在“配置文件”选项卡指定自定义属性，以便用于指定管理角色的有关附加信息。 可以使用这些附加信息帮助在含有很多角色的环境中进行角色搜索。

2. 如果想要在创建角色之后即使其可用，请选择“已启用”。
3. 为角色选择管理任务 (p. 33)。

为角色选择管理任务

在“任务”选项卡上，选择要包括在角色中的管理任务。 可以包括其他类别的任务或复制在其他角色中使用的任务。

选择管理任务

1. 在“按类别筛选”字段中选择类别。

   要查看可用任务类别列表，请单击向下箭头图标。

2. 选择该任务包括在“添加任务”字段中的角色。

   CA CA Identity Manager 将任务添加到角色中的任务列表。

3. 重复步骤 1 和 2 添加其他任务。
4. 通过单击该任务的减号 () 从角色中删除任务。
5. 为管理角色定义成员策略 (p. 34)。

为管理角色定义成员策略

在“成员”选项卡上，可以创建确定哪些人员可以成为角色成员的成员策略。

定义成员策略

1. 单击“添加”以定义成员策略。 成员策略包含以下规则：
   - 成员规则，用于定义用户要成为角色成员的必要条件。

     注意：在成员规则中，以下运算符将数字按字符处理：

     - 小于 (<)
     - 小于或等于 (<=)
     - 大于 (>)
     - 大于或等于 (=>)

     例如，“10”将出现在“1”的后面、“2”的前面。
   - 范围规则，用于限制角色中的任务所适用的主要对象和次要对象。

     例如，如果角色包含通过将用户分配到组从而修改用户的任务，则用户范围规则将限制可以查找到的用户（主要对象），组范围规则将限制可以分配的组（次要对象）。

   注意：请确保至少为一个范围问题输入答案。 范围规则用于限制角色中的任务所适用的主要对象和次要对象。 例如，如果角色包含通过将用户分配到组从而修改用户的任务，则用户范围规则将限制可以查找到的用户（主要对象），组范围规则将限制可以分配的组（次要对象）。
2. 验证“成员”选项卡上显示的成员策略。
   - 要编辑策略，请单击左侧的右箭头符号。
   - 要删除策略，请单击减号图标。
3. 在“成员”选项卡上，启用内容为“管理员可以添加和删除该角色的成员”的复选框，用户符合成员规则才成为成员的情况除外。

   启用此功能后，屏幕将展开。
4. 在展开的区域中，定义将用户作为角色成员进行添加或删除时的对应添加操作和删除操作。

   重要说明！定义添加操作时，避免设置涉及到您正在定义的角色的规则。例如，请勿定义以下添加操作：通过已经是角色 A 的成员产生角色 A 的成员。这可能会导致错误。
5. 为管理角色定义管理策略 (p. 35)。

为管理角色定义管理策略

在“管理员”选项卡上，定义可以将用户作为此角色的成员和管理员进行添加或删除的人员。

定义管理策略

1. 如果要使“管理管理员”选项可用，请启用内容为“管理员可以添加和删除此角色的管理员”的复选框。

   启用此功能后，屏幕将展开。

2. 在展开的区域中，将用户作为角色的管理员进行添加或删除，定义添加操作和删除操作。

3. 定义包含管理规则和范围规则以及至少一种管理员权限（管理成员或管理管理员）的管理策略。

   注意：可以为符合规则的管理员添加若干个具有不同规则和不同权限的管理策略。

4. 要编辑策略，请单击左侧的箭头符号。 要删除策略，请单击减号图标。

5. 为管理角色定义所有者规则 (p. 35)。

为管理角色定义所有者规则

在“所有者”选项卡上，可以定义以下规则：可以成为角色所有者的人员以及可以修改角色的用户。

定义所有者规则

1. 定义所有者规则，用于确定哪些用户可以修改角色。

2. 单击“提交”。

   将显示一条消息，指出该任务已经提交。 可能会出现短暂的延迟，之后用户才能够使用角色。

如果创建此角色时选择了“启用”，则可以使用此角色。 如果用户符合成员规则中的条件，则该用户此时即可以登录到 Identity Manager 环境并可以使用此角色中的任务。

验证管理角色

要检查角色是否已创建，请依次选择“管理角色”、“查看管理角色”，然后选择角色的名称。

或者，可以依次选择“系统”、“查看提交的任务”以查看角色创建任务是否已完成。

允许用户自行分配角色

用户可以将特定角色分配给自己。 例如，您可能希望允许用户申请为指派管理员角色，以便他们可以将某一用户的工作项指派给其他用户。

要控制用户可以分配给自己的角色，请在“角色自主管理器”任务中配置标准。

遵循这些步骤:

1. 按以下步骤修改“角色自主管理器”任务：
   a. 依次选择“角色和任务”、“修改管理任务”，然后搜索“角色自主管理器”任务。
   b. 选择“选项卡”选项卡。

      CA Identity Manager 将显示应用于此任务的选项卡列表。
   c. 选择“角色自主管理器”选项卡旁边的右箭头图标以对其进行编辑。
   d. 填写以下字段：

      仅显示符合以下规则的管理角色

      指定 CA Identity Manager 用于确定允许用户将哪些角色分配给自己的标准。

      要添加其他规则，请单击加号 (+) 图标。

      用作管理角色管理员的用户

      为用户可以分配给自己的角色指定管理员。

      用户可以分配给自己的角色必须将您在此字段中选择的用户用作管理员，*并*满足在“仅显示符合以下规则的管理角色”字段中指定的标准。

      列表屏幕

      为用户可以选择自行分配角色的角色列表指定列和格式。
   e. 单击“确定”，然后单击“提交”。
2. 将“角色自主管理器”任务添加到角色，并将该角色分配给应具有此功能的用户。

第 3 章： 管理任务

此部分包含以下主题：

管理任务规划

管理角色由管理任务组成，这些管理任务代表管理对象的各种细粒度功能。 例如，您可以使用以下管理任务管理用户对象：

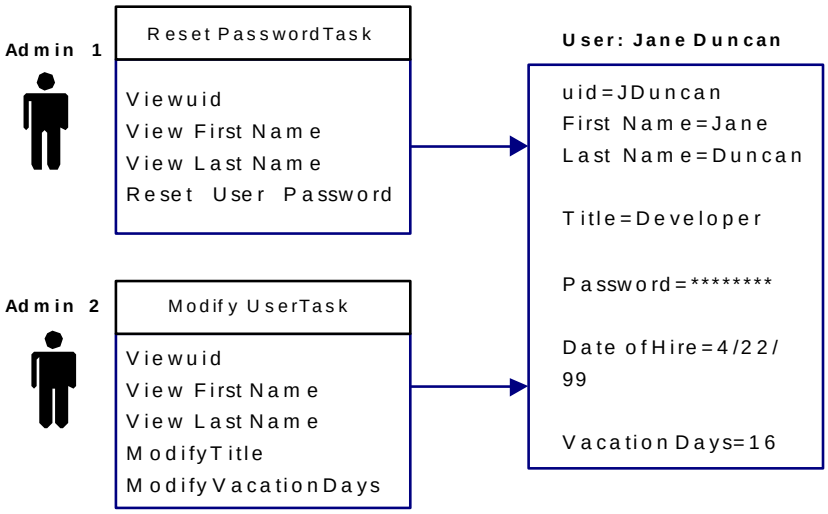
- 创建用户
- 查看用户
- 修改用户
- 重置用户密码

创建或修改每项任务以符合具体要求。 然后，将相应的管理任务合并到分配给管理员的管理角色中。通过这些角色，管理员拥有了管理对象所需的确切权限。

为规划管理任务的创建，需决定需要管理的对象（用户、组、组织、角色或任务）以及将要使用这些任务的管理员。 例如：

- 要管理用户，Help Desk 管理员需要具有管理用户属性（例如用户 ID 或职位）的任务。
- 要管理用户对应用程序的访问权限，其他管理员需要具有使用户成为访问角色成员的任务。
- 要管理 Help Desk 管理员所使用的角色，较高级别的管理员需要承担管理管理角色的任务。

对于一种类型的对象（例如用户），您可以创建多个任务，以便不同的管理员可以管理不同的属性。 例如，下图显示了受两个管理员管理的某个用户。



- 管理员 1 承担“重置用户密码”任务；该管理员可以查看雇员的用户 ID 和姓名或重置她的密码。
- 管理员 2 承担“修改用户”任务；该管理员可以查看雇员的用户 ID 和姓名或修改她的职位和休假天数。

管理任务示例

创建管理任务时，可以定义任务中屏幕的内容和布局，包括：

- 任务的名称
- 显示任务的类别
- 任务中要使用的选项卡和字段，以及字段显示属性
- 管理员可在搜索查询中使用的字段，以及搜索结果中显示的字段

要了解任务的元素，请参见“修改用户”任务。 在此情况下，“用户”是类别，“管理用户”是子类别，“修改用户”是任务。 创建任务时您会创建类别及任务名称。

选择“修改用户”后，将显示一个搜索屏幕。 *搜索屏幕*提供了用于查找要查看或修改的对象的选项。每个选项都称为一项*筛选*，是对搜索查找到的对象的限制。

填写搜索屏幕后，将显示带有多个选项卡的屏幕。例如，下图显示了“修改用户”任务的选项卡。 首先显示的是“配置文件”选项卡，该选项卡显示了用户属性；其他选项卡显示了该用户的角色和组权限。

对于您创建的任务，您可以确定要包括的选项卡及其顺序和内容。

例如，将“修改用户”任务用作模板，您可以创建“修改承包商”任务，该任务对以下方面进行了更改：

- “配置文件”选项卡上的字段
- 任务中要包括的选项卡及其内容
- 在其中显示任务的类别

  您可以在新类别“承包商”下创建此任务。

“修改承包商”任务包括“修改用户”任务中“配置文件”选项卡上的某些字段以及其他一些字段，例如合同的生效日期和承包商所在的公司。 管理员可以通过搜索承包商的姓名、公司及生效日期来搜索承包商。

新任务还包括一个“承包商角色”选项卡，可从中为承包商添加角色。

管理任务使用选项

Identity Manager 提供了两种使用管理任务的方法：

- **选择任务**

  选择类别和任务，然后搜索任务应用到的对象。

  例如，要修改用户配置文件，您应选择“用户”类别，然后选择“修改用户”任务。 然后搜索要修改的用户。

- **选择对象**

  使用“管理”任务（例如“管理用户”或“管理组”）搜索对象。 选择对象后，可以显示可用于管理此对象的任务列表。 此方法称为*对象-任务导航*。

  例如，要使用此方法修改用户，您应选择“用户”类别，然后选择“管理用户”任务。 搜索并选择要管理的用户。 在搜索结果中，单击图标以查看可用于管理所选用户的任务列表。 从该列表中，可以选择“修改用户”或任何其他相应的任务。

  还可以在任务中而不是在管理任务中配置任务列表。 例如，可以将任务列表添加到“成员资格”选项卡中。在此例中，“成员资格”选项卡上显示的每个成员均可以使用任务列表。

  注意：只有当前管理员可以使用的任务才会显示在对象的任务列表中。

默认管理任务

CA Identity Manager 包括一组默认管理任务和角色，通过在管理控制台中导入一个角色定义文件来将其添加到 CA Identity Manager 中。 当您在管理控制台中创建环境并选择创建默认角色时，CA Identity Manager 会自动导入一个角色定义文件。

注意：要支持某些功能（如特定端点类型的帐户管理），可能需要导入附加的角色定义文件才能创建所需的角色和任务。

大多数情况下，您可以使用已安装的默认任务。 但是，您可能需要修改某些默认用户任务中的“配置文件”选项卡，如“创建用户”、“修改用户”和“查看用户”。“配置文件”选项卡包括目录配置文件中为用户对象定义的所有字段。 您可能想限制选项卡上出现的字段数量，或更改字段显示属性。

注意：建议您创建默认任务的副本用来修改，而不是直接修改默认任务。

如何创建自定义管理任务

*管理任务*是用户可以在 Identity Manager 中执行的管理功能。 管理任务包括“创建用户”、“修改组”和“查看角色成员资格”等。

CA Identity Manager 包含可进行修改以适用于您业务需求的默认管理任务。

创建自定义管理任务时，需要完成以下步骤：

注意：“Active Directory 先决条件 (p. 59)”部分包括关于 CA Identity Manager 是否管理 Active Directory 用户存储的其他注意事项。

1. 在 CA Identity Manager 用户控制台中，依次选择“角色和任务”、“管理任务”、“创建管理任务”。

   CA Identity Manager 将询问您是要创建新任务还是基于现有任务创建任务。

   例如，选择“修改用户”任务作为新任务的基础。

2. 选择“创建现有任务的副本”，然后搜索要复制的任务。

   注意：建议修改默认任务的副本，而不是直接修改默认任务。

3. 选择“确定”之后，您将看到包含 6 个选项卡的屏幕：

选项卡	用途	参阅此主题
配置文件	定义所创建任务的配置文件	定义任务的配置文件 (p. 43)
搜索	限制由任务管理的对象的范围	定义任务范围 (p. 47)
选项卡	为任务选择并设计选项卡	为任务选择选项卡 (p. 55)
字段	显示所有选项卡上使用的字段	查看任务中的字段 (p. 59)
事件	如果 CA Identity Manager 环境和任务均使用工作流，则为每个事件选择工作流流程	为事件分配工作流流程 (p. 59)
角色使用	显示包括要修改或查看的任务的角色。	查看角色使用 (p. 59)

注意：有关创建自定义管理任务的详细信息，请参阅《*用户控制台设计指南*》。

定义任务的配置文件

“配置文件”选项卡包括任务的常规设置。

定义任务的配置文件

1. 为任务选择称为主要对象的对象类型，以及要对其执行的操作。
2. 填写必填字段，并根据任务的需要选择相应的复选框。

   注意：如果要创建与现有任务具有类似配置文件设置的任务，请单击“从其他任务复制配置文件”。此选项将使用您选择的任意现有任务的配置文件设置，填充要创建的任务的配置文件设置。 然后为新任务添加名称和说明。
3. （可选）将业务逻辑任务处理程序与任务相关联。
4. 完成此选项卡后，继续进行下一步定义任务范围 (p. 47)。

“管理任务配置文件”选项卡

“管理任务配置文件”选项卡用于为管理任务定义常规设置。

此选项卡包含以下字段：

- **名称**

  定义任务的名称。
- **标记**

  定义任务的唯一标识符。 它在 URL、Web 服务或属性文件中使用。 该标记可以包含 ASCII 字符（a-z，A-Z）、数字 (0-9) 或下划线字符，以字母或下划线开头。
- **说明**

  指定关于任务用途的可选说明。
- **任务顺序**

  指定任务的显示顺序。 如果未指定顺序，则任务将按字母顺序显示。
- **类别**

  指定任务的类别。 类别显示为屏幕顶部的选项卡。
- **类别顺序**

  指定类别选项卡显示的顺序。例如，如果将类别顺序设置为 3，则您指定的类别将显示为第三个选项卡。
- **类别 2**

  指定第二级类别，此类别显示为类别选项卡列表下面的链接。 第二级类别仅在选择了第一级类别的选项卡时才显示。 例如，如果创建了具有第一级类别“雇员”和第二级类别“雇员管理”的任务，则“雇员管理”类别将仅在选择了“雇员”选项卡时才会显示。

- **类别 2 顺序**

  如果主要类别中存在多个第二级类别，则指定第二级类别的显示顺序。

- **类别 3**

  指定第三级类别，显示在左侧导航窗格中。 任务在第三级类别下列出。 例如，在默认环境中，当具有系统管理员角色或用户管理员角色的用户选择“用户”选项卡后，他将看到第三级类别“管理用户”。

- **类别 3 顺序**

  指定第三级类别的显示顺序。

- **主要对象**

  指定对其执行任务的对象。

- **操作**

  指定要对对象执行的操作。

- **用户同步**

  指定任务是否将用户与身份策略同步。 可以选择以下选项之一：

  - **关闭**（默认值）

    指定此任务不触发用户同步。

  - **任务完成时**

    指定 CA CA Identity Manager 在任务中的所有事件完成后启动用户同步过程。 此设置是“创建用户”、“修改用户”和“删除用户”任务的默认同步选项。 所有其他任务的默认设置为“关闭”。

    注意：如果为包括多个事件的任务选择“任务完成时”选项，则直到任务中的所有事件都完成时，CA CA Identity Manager 才会同步用户。如果其中一个或多个事件需要工作流批准，则可能需要几天时间。如果不想让 CA CA Identity Manager 等到所有事件完成才应用身份策略，请选择“每个事件时”选项。

  - **每个事件时**

    指定 CA CA Identity Manager 在任务中的每个事件完成时启动用户同步过程 (p. 389)。

    对于同一用户具有主要事件和次要事件的任务，将用户同步设置为“每个事件时”可能会导致应用到一个用户的身份策略多于选择“任务完成时”选项时所应用的身份策略。

- **帐户同步**

  如果启用了配给，则将同步存在于配给服务器中的帐户。

  - **关闭**（默认值）

    指定此任务不触发帐户同步。

  - **任务完成时**

    指定 CA CA Identity Manager 在任务中的所有事件完成后启动帐户同步过程。

  - **每个事件时**

    指定 CA CA Identity Manager 在任务中的每个事件完成时启动帐户同步过程。

    注意：要获得最佳性能，请选择“任务完成时”。 但是，如果为包括多个事件的任务选择“任务完成时”选项，则直到任务中的所有事件都完成时，CA CA Identity Manager 才会同步帐户。如果其中一个或多个事件需要工作流批准，则可能需要几天时间。 如果不想让 CA CA Identity Manager 等到所有事件完成才同步帐户，请选择“每个事件时”选项。

- **隐藏于菜单**

  防止任务显示在菜单中。 如果任务仅由 URL 或另一任务调用，则启用此控件。

- **公共任务**

  使尚未登录到 CA CA Identity Manager 的用户可以使用该任务。 默认公共任务为忘记的密码和自行注册。

- **启用审核**

  在审核数据库中记录任务的信息。 审核信息可用于生成报告。 请参阅*《Configuration Guide》*（《配置指南》）。

- **启用工作流**

  如果安装了工作流引擎，则启用与任务关联的 CA CA Identity Manager 事件来触发工作流流程。 例如，与“删除组”任务关联的事件可能会触发包括批准步骤的工作流流程。

- **启用 Web 服务**

  将任务标记为可以为其从管理控制台生成 Web 服务描述语言 (WSDL) 输出的一个任务。 如果要使用远程任务提交，则启用此控件。 有关详细信息，请参阅*《Programming Guide for Java》*（《Java 编程指南》）。

- **工作流流程**

  启用任务 级的工作流配置。 单击铅笔图标配置 基于策略或不基于策略的工作流。

- **任务优先级**

  确定 CA CA Identity Manager 执行任务的顺序。先执行具有高优先级的任务，然后执行具有中等优先级或低优先级的任务。 任务的默认优先级为“中”。

  注意：可以使用“查看提交的任务”任务来搜索具有特定优先级的任务，然后显示其状态。

- **业务逻辑任务处理程序**

  将业务逻辑任务处理程序 (p. 63)与任务相关联。

- **工作流操作按钮**

  将自定义操作按钮添加到工作流批准任务。

- **从其他任务复制配置文件**

  从其他任务的“配置文件”选项卡中复制数据。

  例如，您可以复制“修改用户”任务中“配置文件”选项卡的设置，然后添加名称和说明。

任务配置属性

任务配置属性控制任务的显示属性和特定行为。

任务图标路径

指定要用作此任务在任务列表中的图标的图形的 URL。

任务图标预览

显示任务的图标，与其在任务列表中显示的一样。

禁止任务导航

选定后，一旦用户选择任务，就会隐藏顶层导航和任务列表。 这会防止用户远离当前任务，直到他们完成所需的操作或取消任务为止。

目标窗口

在此字段中提供值后，CA Identity Manager 会在新的浏览器窗口中打开此任务。 使用此字段可以为将用户重定向到其他网站的外部任务打开新的浏览器窗口。

您可以为窗口指定任何名称。

注意：不要使用此字段在单独的浏览器窗口中打开 CA Identity Manager 管理任务。 CA Identity Manager 不支持针对单个 CA Identity Manager 用户会话打开多个浏览器窗口。

定义任务范围

可以在“搜索”选项卡上定义任务范围，用于限制任务的对象。 例如，如果任务的对象是用户，您可以把范围定义为是承包商的用户。

注意：如果任务不具有主要对象，或者如果操作是自行修改、自行查看或批准，则不显示“搜索”选项卡。

可以在“搜索”选项卡上配置以下设置：

搜索屏幕

搜索屏幕基于筛选限制任务范围。 单击“浏览”可查看可用的搜索屏幕选项。

注意：您可能希望创建自己的搜索屏幕 (p. 48)。 要创建现有搜索屏幕的修改版本，请选择该搜索屏幕并单击“复制”。 然后您就可以修改该搜索屏幕，而无需更改初始搜索屏幕定义。 要创建搜索屏幕，请单击“新建”。

搜索选项

搜索选项仅在对象是角色或组时才显示。

- 第一个选项根据在搜索屏幕上定义的字段限制搜索。通过这些限制，搜索将在管理员的范围内查找所有组或角色。
- 其他选项基于指示限制搜索。

请注意下列事项：

- 默认情况下，组搜索屏幕支持筛选。这意味着管理员可以指定标准以限制组搜索范围。要删除筛选功能，请创建新的搜索屏幕，该屏幕不能包含任何要包括在搜索查询中的字段。
- 对象是角色时，“搜索”选项卡上将显示*不支持筛选*，这表示任务将显示符合所选选项中条件的所有角色。 将忽略在搜索屏幕上配置的搜索字段。

经过修改的对象必须保留在管理员作用域内

选中此复选框时，如果对任务所做的更改导致管理员的作用域不能涵盖主要对象，CA CA Identity Manager 将显示一个错误。 例如，管理员可能使用“修改用户”将用户的“雇员类型”属性更改为“经理”。 此更改可能会将该用户置于管理员作用域之外。

搜索屏幕配置

可以配置搜索屏幕以限制任务的范围，并控制用户执行搜索可依据的字段。 搜索屏幕适用于两种类型的对象：

- *主要对象* - 任务要修改或查看的对象。
- *次要对象* - 与主要对象相关的对象。

  例如，如果您在创建用户任务中包括组选项卡，则用户是主要对象，组是辅助对象。 组选项卡需要用于组的搜索屏幕。

  注意：配置搜索屏幕后，您可以将该屏幕用于任何任务，以搜索主要对象和辅助对象。

搜索筛选

搜索筛选会限制搜索返回的对象。 例如，如果对象是用户，您可以将搜索限制为仅查找承包商。 您可以将筛选配置为查找雇员类型为承包商的用户。

您可以为搜索配置以下字段：

仅显示符合以下规则的对象

定义要与用户定义的筛选共同使用的、用来限制搜索的其他标准。

使用该字段时，请注意以下事项：

- 由于配给角色搜索的限制，这些标准将覆盖用户输入的同名筛选字段。
- 配置此字段时使用的属性不应添加为搜索屏幕上的可用搜索字段。

  例如，如果将搜索屏幕配置为仅显示“已启用”属性设置为“是”的角色，请从用户可在搜索条件中指定的属性的列表中删除“已启用”属性。

  否则，将忽略用户输入的条件。

默认搜索筛选

定义管理员使用搜索屏幕时默认显示的筛选。 例如，如果您要为“修改承包商”任务配置搜索屏幕，并且您知道管理员通常根据合同企业名称来搜索承包商，则可以将默认筛选设置为合同企业 = *。 管理员可以通过指定不同的搜索标准来覆盖默认筛选。 如果管理员在开始搜索前未指定筛选，则设置默认筛选可通过限制返回的结果数来提高性能。

在用于多项选择任务中时自动选择所有搜索结果

指定在默认情况下选择所有搜索结果。 如果选中此复选框，搜索结果列表中的所有对象名称旁边均会显示一个选中的复选框。

自动执行搜索

指定与搜索结果一起显示一个搜索字段。

仅有一条搜索结果时自动设置任务主题

仅有一个对象与搜索筛选匹配时，自动设置任务的主要对象。

例如，假设为与“修改用户”任务相关联的用户搜索屏幕选择了此选项。管理员打开该“修改用户”任务后，如果输入的搜索筛选仅返回一个用户，则 CA CA Identity Manager 将针对该用户打开“修改用户”任务。 管理员无需选择该用户以打开“修改用户”任务。

注意：要使得该设置得以应用，必须同时选择“自动执行搜索”。

保存搜索筛选

指定将对于当前会话中的用户保存该任务的搜索筛选。 下次用户在任务中搜索时，将显示保存的搜索筛选。

注意：CA CA Identity Manager 在用户会话期间保存该搜索筛选。 在用户注销时，该搜索筛选将清除。

在组织中搜索

在搜索屏幕上显示组织筛选。 如果选中此复选框，管理员则可以指定一个筛选来限制 CA CA Identity Manager 在其中搜索对象的组织。您可以通过在“组织搜索”字段中指定搜索屏幕，为组织搜索筛选指定默认设置。

保存搜索组织

指定如果为搜索建立了组织，则保存该任务的这个组织。 下次用户在该任务中搜索时，将显示该组织。

组织搜索

指定 CA CA Identity Manager 使用的搜索屏幕，通过该搜索屏幕，管理员可以搜索组织。

默认组织搜索范围

指定管理员使用搜索屏幕时所显示的默认组织搜索范围。 搜索范围决定包括在搜索中的“组织”树级别。通过在搜索屏幕上指定不同搜索条件，管理员可以覆盖默认组织搜索范围。

例如，如果在一个组织树中各层级都存储有合同工信息的环境中为一个自定义“修改合同工”任务配置搜索屏幕，则可以将默认组织搜索范围设置为“及更低”。

单个表达式搜索

定义显示在搜索屏幕上的搜索筛选类型。 选择此复选框后，用户可以指定单个搜索筛选，例如 <属性><比较器><值>。清除此复选框后，用户可以指定多个搜索筛选。 例如，<属性 1><比较器><值 1> AND <属性 2><比较器> <值 2>。 符合所有筛选中条件的对象将返回搜索结果中。 在之前的示例中，包括 <值 1> 和 <值 2> 的对象将作为搜索结果返回。

仅等于搜索

禁止管理员使用等于之外的搜索操作符。

显示结果数

显示匹配的搜索结果数。 如果选中此复选框，则所有搜索都将返回消息“有 X 条结果”。

为 <任务名称> 添加任务按钮

将指向其他任务的链接添加到搜索屏幕。 该链接显示为一个按钮。通常，此字段用于将创建任务添加到配置为使用对象-任务导航的搜索屏幕。

可选标签

为在上一字段中选择的任务指定一个标签。此标签显示在表示该任务的按钮上。

为 <任务名称> 添加多项删除按钮

添加一个链接，该链接指向允许管理员选择多个对象进行删除的任务。 该链接显示为一个按钮。
此字段通常使用对象-任务导航。

搜索字段和搜索结果

在搜索屏幕的另一部分上，您可选择管理员可以在搜索查询中使用的字段，以及显示在搜索结果中的字段。

选择用户执行搜索可依据的字段

选择管理员可用于创建搜索查询的字段。

要添加其他字段，请选择搜索字段表下面列表框中的字段。

在选择字段后，您可以通过使用字段右侧的向上箭头和向下箭头图标更改这些字段的显示顺序。

注意：如果您未指定管理员执行搜索可依据的字段，CA CA Identity Manager 将自动开始搜索。

选择显示在搜索结果中的字段

选择 CA Identity Manager 显示在搜索结果中的字段。您可以选择不能用于搜索查询的字段。

要添加其他字段，请选择搜索字段表下面列表框中的字段。

样式

选择要显示在搜索结果中的字段时，您可以选择以下样式选项之一：

- **布尔值显示名称**

  显示所有结果为“true”的字段的名称。 例如，如果输入“启用”作为指示用户帐户状态的属性名称，则“启用”将显示在所有活动用户帐户的搜索结果中。

- **复选标记**

  根据属性的值，将值显示为一个选中的复选标记。 例如，如果选择复选标记样式来表示用户帐户的启用/禁用状态，则对于所有活动帐户，CA CA Identity Manager 都将显示选中复选标记。

- **多值字符串**

  在单独的行中显示多值属性中的值。 这些值按字母顺序列出。

- **只读复选框**

  将值显示为只读复选框。

- **字符串**

  将值显示为文本字符串。

- **任务**

  将任务列表添加到字段。 用户单击箭头图标将显示一个任务列表，列出了可针对与搜索字段相关联的对象执行的任务。 例如，如果您将任务列表添加到搜索结果中的“姓氏”字段，则用户单击该字段中的箭头图标后，即可查看可针对所选用户执行的任务列表。

  该设置也能用于使属性值显示为任务链接。

  如果选择“任务”样式，则“样式”列旁边将显示一个右箭头图标。 单击该箭头可打开“字段属性”对话框。 使用此对话框可配置任务列表。

- **任务列表**

  添加用户可以对搜索和列表屏幕中的对象执行的其他任务。 例如，您可以在“修改用户”任务中配置搜索屏幕，以便使用户可以执行某个任务，如禁用通过搜索返回的用户列表中的用户。

  在您选择此选项时，请确定用户是通过单击图标还是通过文本链接来访问任务。

- **任务菜单**

  将其他任务（类似于“任务列表”样式）作为弹出菜单项添加。

  在您选择此选项时，搜索或列表屏幕中的每个对象旁边都会显示一个“操作”按钮。 用户单击“操作”按钮即可查看可以为该对象执行的任务的列表。

注意：要查看“任务列表”和“任务菜单”样式选项，请在您将字段添加到搜索结果表时选择“(分隔符)”。 有关将其他任务添加到搜索和列表屏幕的详细信息，请参阅*《User Console Design Guide》*（《用户控制台设计指南》）。

可排序

选择此复选框后，管理员可以按字段对搜索结果进行排序。

设置搜索结果的默认排序顺序

指定搜索结果的显示顺序。 搜索结果按照其显示顺序，先按列表中第一个字段进行排序，然后按其他每个字段进行排序。 选择“降序”复选框可对结果降序排序。

选择字段*字段名称*有变化的对象

指定当用户单击“选择”按钮时，将选择其中的指定字段发生更改的对象。

返回 *N* 个结果

选择每页显示的结果数。 搜索结果超出指定数目时，CA Identity Manager 将显示指向每个结果页面的链接。

搜索屏幕上用户定义的帮助

如果要将自定义文本添加到您的搜索屏幕，可以在相应的 HTML 文本框中定义文本。 可以在以下区域添加文本：

- 页面开始处或结尾处
- 创建前或创建后
- 结果前或结果后

搜索屏幕的类型

Identity Manager 包括以下预配置的搜索屏幕。

访问角色搜索屏幕

通过访问角色搜索屏幕，您可以配置搜索筛选以查找与特定标准匹配的访问角色。

访问任务搜索屏幕

通过访问任务搜索屏幕，您可以配置搜索筛选以查找与特定标准匹配的访问任务。 此搜索屏幕用于查找要查看或修改的访问任务，或者将任务添加到访问角色。

管理角色搜索屏幕

通过管理角色搜索屏幕，您可以配置搜索筛选以查找与特定标准匹配的管理角色。

管理任务搜索屏幕

通过管理任务搜索屏幕，您可以配置搜索筛选以查找与特定标准匹配的管理任务。 此搜索屏幕用于查找要查看或修改的管理任务，或者将任务添加到管理角色。

批准搜索屏幕

通过批准搜索屏幕，您可以配置批准任务顶部的显示内容。

开始认证用户搜索屏幕

通过开始认证用户搜索屏幕，您可以配置搜索筛选以查找设置为要求认证的用户。 所选用户的认证状态将设置为*要求认证*。

认证用户搜索屏幕

通过认证用户搜索屏幕，您可以配置搜索筛选以查找要求认证的用户。

指派搜索屏幕

通过指派搜索屏幕，您可以配置搜索筛选以查找作为指派人添加的其他用户。 指派人是指可以被临时授予对工作流工作项的查看或解析权限的其他用户。

启用/禁用用户搜索屏幕

通过启用/禁用用户搜索屏幕，您可以配置搜索筛选以启用/禁用与特定标准相匹配的用户。

结束认证用户搜索屏幕

通过结束认证用户搜索屏幕，您可以配置搜索筛选以查找应完成认证期的用户。

最终用户许可协议搜索屏幕

通过最终用户许可协议搜索屏幕，您可以通过一个页面（特定于基于您身份的应用程序）配置“自行注册”任务。

浏览和关联搜索

通过浏览和关联搜索屏幕，您可以为与特定标准匹配的浏览和关联定义配置搜索筛选。

Feeder 文件上载搜索

通过 Feeder 文件上载搜索屏幕，您可以浏览要上载的 Feeder 文件。Feeder 文件用于自动执行针对大量受管理对象的重复操作。

忘记密码搜索屏幕/忘记用户 ID 搜索屏幕

通过忘记密码搜索屏幕，您可以将“忘记密码”任务配置为提示用户输入用于验证其身份的信息。

组搜索屏幕

通过组搜索屏幕，您可以为组配置搜索筛选，例如财务组织中的组。

身份策略集搜索屏幕

通过身份策略集搜索屏幕，您可以配置搜索筛选以查找与特定标准匹配的身份策略集。

逻辑属性处理程序搜索屏幕

通过逻辑属性处理程序搜索屏幕，您可以配置搜索筛选以查找逻辑属性处理程序。 此屏幕用于查找要查看或修改配置的逻辑属性处理程序。

管理报告搜索屏幕

通过管理报告搜索屏幕，您可以配置搜索筛选以查找要查看或删除的报告。

非认证用户搜索屏幕

通过非认证用户搜索屏幕，您可以配置搜索筛选以查找认证期结束时没有经过认证的用户。

组织搜索屏幕

通过组织搜索屏幕，您可以配置搜索筛选以将可选组织限制为特定的子组织。

配给角色搜索屏幕

通过配给角色搜索屏幕，您可以为检索配给角色配置搜索筛选。

帐户模板搜索屏幕

通过帐户模板搜索屏幕，您可以为检索帐户模板配置搜索筛选。

密码策略搜索屏幕

通过密码策略搜索屏幕，您可以配置搜索筛选以查找与特定标准匹配的密码策略。

快照定义搜索屏幕

通过快照定义搜索屏幕，您可以配置搜索筛选以查找要查看、修改或删除的快照定义。

标准搜索屏幕

通过标准搜索屏幕，您可以配置筛选以查找自定义的受管理对象。

用户搜索屏幕

通过用户搜索屏幕，您可以配置搜索筛选以查找与特定标准匹配的用户。 例如，您可以搜索是承包商的用户。

填写“搜索”选项卡后，为任务选择选项卡。

为任务选择选项卡

在“选项卡”选项卡上命名并配置选项卡；每个选项卡均包含一组您包括在任务中的字段。 可以使用默认选项卡或创建新选项卡。 例如，“修改用户”任务包括以下选项卡：

- 配置文件
- 访问角色
- 管理角色

- 组
- 指派工作项

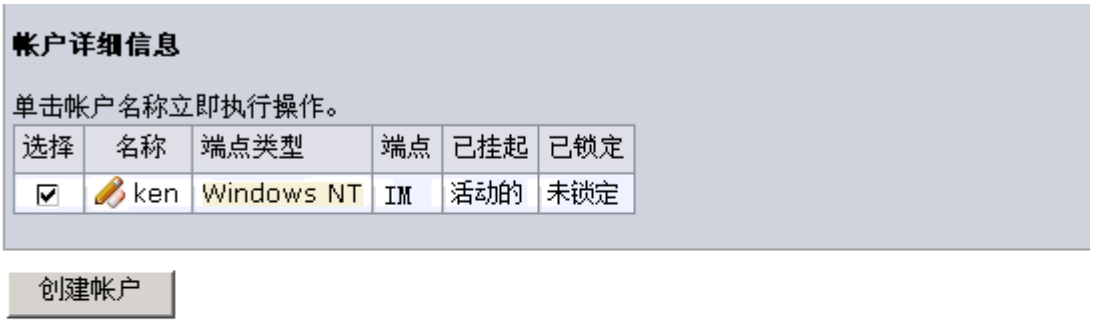
要编辑选项卡的定义，请单击选项卡名称旁的编辑图标 ()。

更多信息：

"帐户"选项卡 (p. 56)
"排定"选项卡 (p. 58)

"帐户"选项卡

"帐户"选项卡将为已分配配给角色的用户列出受管理端点中的帐户。 通常，该选项卡将添加到允许查看或修改用户的任务中。



将"帐户"选项卡添加到"修改用户"任务后，管理员可以针对用户帐户执行其他操作。 例如：

- 挂起或恢复帐户
- 对由于不正确或不适当访问而被自动锁定的帐户解除锁定。 例如，如果用户尝试登录帐户的失败次数超出 Identity Manager 密码策略中设置的可接受值，则可能会锁定该帐户。
- 更改一个或多个帐户中的用户密码。
- 分配或取消分配帐户给用户。

有关可在"帐户"选项卡上提供的其他选项的详细信息，请参阅用户控制台帮助中的配置"帐户"选项卡。

使用“帐户”选项卡的先决条件

要使用“帐户”选项卡，Identity Manager 必须通过配给支持进行配置，且 Identity Manager 环境必须包括配给目录。

注意：要为环境配置配给支持，请参阅 *《配给指南》*。

“帐户”选项卡上的字段

“帐户”选项卡显示了有关用户在端点系统上所拥有帐户的详细信息。

以下是一些较为重要的字段：

- 名称 - 帐户的登录名称、电子邮件名称或其他名称。
- 端点类型 - 与帐户相关联的端点类型，例如 LDAP 目录。
- 端点 - 与帐户关联的特定端点。
- 已挂起 - 三种状态之一。
  - 如果帐户为启用状态，则显示“活动”。
  - 如果帐户为禁用状态，则显示“已挂起”。
  - 如果帐户无法恢复或已挂起，则显示“激活挂起 (手工)”。 登录到端点系统恢复或挂起该帐户。
  - 如果由于端点无法通信而无法检索状态，则显示“不可用”。
- 已锁定 - 如果帐户已锁定则显示该状态。当用户多次尝试使用错误密码登录帐户时，将执行锁定。 如果由于端点无法通信而无法检索状态，则显示“不可用”。

“帐户”选项卡上的其他操作

如果修改用户的任务中包括“帐户”选项卡，则管理员可以使用该任务针对用户帐户执行功能。 选项卡配置确定可用操作。

您可以使用包含“帐户”选项卡的任务中的“修改管理任务”来选择可用操作。 可以编辑“帐户”选项卡，以确定“分配帐户”和“取消分配帐户”等功能在该选项卡中是否可用。

有关详细信息，请参联机帮助中的“配置‘帐户’选项卡”。

“排定”选项卡

通过排定，您可以在以后自动执行任务。 如果您排定了一项与工作流相关联的任务，CA Identity Manager 将按照定义执行该工作流中的所有任务。已排定任务的状态可以在“查看提交的任务”页面中查看。

可以通过“查看提交的任务”页面取消 CA Identity Manager 尚未执行的已排定任务。

注意： 如果取消了一个排定的任务，并且重新提交该任务，则该任务将立即执行，而不管是否到了排定的执行时间。

CA Identity Manager 以特殊选项卡的形式提供排定程序。要访问排定程序，您必须通过“排定”选项卡配置任务。

将“排定”选项卡添加到管理任务

通过 CA Identity Manager，您可以将任务排定为在特定日期和时间执行。要排定任务，您必须将“排定”选项卡添加到管理任务。

注意：在 CA Identity Manager 中，无法将“排定”选项卡添加到所有管理任务。如果任务无法排定，则“排定”选项卡在“修改管理任务”屏幕中不可用。

将“排定”选项卡添加到管理任务

1. 依次单击“角色和任务”、“管理任务”、“修改管理任务”。

   将显示“选择管理任务”页面。

2. 在“其中”字段中选择“名称”或“类别”，输入要搜索的字符串，然后单击“搜索”。

   CA Identity Manager 将显示符合搜索标准的管理任务。

3. 选择一项管理任务，然后单击“选择”。

   CA Identity Manager 将显示所选管理任务的任务详细信息。

4. 单击“选项卡”。

   将显示为所选管理任务配置的选项卡。

5. 从“哪些选项卡应出现在该任务中”下拉列表中选择“排定”，然后单击 。

   “排定”选项卡将添加到显示在所选管理任务中的选项卡的列表。

6. 单击“提交”。

   “排定”选项卡将添加到所选管理任务。

查看任务中的字段

在“字段”选项卡上，您可以查看适用于此任务的字段。 这些字段是在此任务的选项卡上创建的字段。 要更改使用的字段，请返回“选项卡”选项卡，然后选择需要进行更改的选项卡。

填写此选项卡后，继续执行下一步“为事件分配工作流流程” (p. 59)。

不过，如果此 Identity Manager 环境不使用工作流，则此时可单击“提交”。 将显示一条消息，指示任务是否成功。 如果任务成功，则可以将该任务添加到角色，以便角色成员可以开始使用该任务。

查看角色使用

在“角色使用”选项卡中，可以查看包括您正在查看或修改的任务的角色。

角色所有者可以添加任务和将其从角色中删除。

注意：默认管理角色在管理角色中提供了一个任务列表，这是默认情况下随 CA Identity Manager 一起安装的内容。

为事件分配工作流流程

如果对此 Identity Manager 环境启用了工作流，请使用“事件”选项卡为该任务启动的每个事件选择一个工作流流程。所选工作流流程将覆盖 Identity Manager 管理控制台中默认情况下选择的工作流流程。

有关默认工作流映射的详细信息，请参阅 *《配置指南》* 的“高级设置”一章。

要完成创建此任务，请单击“提交”。 将显示一条消息，指示任务是否成功。 如果任务成功，则可以将该任务添加到角色，以便角色成员可以开始使用该任务。

管理 Active Directory 用户存储

如果 Active Directory 是用户存储，在创建管理任务之前，您可能需要配置特定 Active Directory 功能。

sAMAccountName 属性

sAMAccountName 属性适用于用户和组。 此属性是必需的，且必须包括在用于创建用户和组的任务屏幕中。

注意：创建用户时，sAMAccountName 属性的值不能超过 20 个字符。 此限制不适用于组。

您可以编写一个自定义逻辑属性处理程序，用于在创建用户或组时自动生成唯一的 sAMAccountName。 在这种情况下，您可以将 sAMAccountName 属性作为隐藏字段包括在“创建用户”屏幕和“创建组”屏幕中。

有关详细信息，请参阅 *《Java 编程指南》*中的“逻辑属性”一章。

组类型和范围

在 Active Directory 中，有两种类型的组：

- 安全组 - 在访问控制列表 (ACL) 中列出，用于定义资源和对象的权限。
- 分发组 - 用于将对象进行分组，例如用户和组。在 Active Directory 中，分发组不能用于授予权限。

每种类型的组都具有可确定以下内容的范围：

- 成员位置 - 潜在成员可以驻留的位置
- 权限 - 组所对应的不同访问权限（如果组为安全组）。
- 其他组中的组员资格 - 该组所属的组的位置

每种类型的组都可以具有以下范围之一：

范围	成员位置	权限	其他组中的组员资格
通用	组成员可以是通用组、全局组和树系中任意域中的用户。	可以用于授予对树系中任意域的访问权限。	可以是树系中任意域中的域本地组和通用组的成员。
全局	组成员可以是全局组以及与全局组位于同一域中的用户。	可以用于授予对树系中任意域的访问权限。	可以是树系中任意域中的全局组、域本地组和通用组的成员。

范围	成员位置	权限	其他组中的组员资格
域本地	组成员可以是通用组、全局组和树系中任意域中的用户。成员还可以是位于同一域的域本地组。	只能是该域中其他域本地组的成员。	只能为该域中其他域本地组的成员。

组类型和范围不属于必需属性；但是，如果您未指定组类型和范围，Active Directory 将创建全局范围的安全组。

要创建不同类型的组，您可以创建一个自定义逻辑属性处理程序。请参阅《*Java 编程指南*》中的“逻辑属性”一章。

配置这些 Active Directory 特性后，请继续执行下一步：创建管理任务。

应用程序功能的外部任务

外部任务执行下列操作：

- 允许管理员从用户控制台执行除 CA Identity Manager 外的应用程序中的某项功能。
- 可任选地向应用程序传递信息以生成特定用户、组或组织的任务。

例如，外部任务可能将组织方面的信息传递给生成订单的应用程序。 执行该任务的管理员可以从用户控制台查看组织的未履行订购单。

通过在新的浏览器窗口中打开应用程序或者将外部任务视为 CA Identity Manager 管理任务中的选项卡，可以查看外部任务。

有两个适用于“外部”任务的选项卡。 这些选项卡以相同的方式配置；然而，他们以不同的方式运行。

- “外部”选项卡为可见选项卡，即任务将在选项卡内显示 URL 的内容。
- “外部 URL”是非可见选项卡，即任务重定向到输入的 URL。

外部选项卡

可以将外部选项卡添加到任何“创建”、“查看”或“修改”任务，从而使任务成为外部任务。 例如，如果您添加“创建用户”任务的“外部”选项卡，选项卡则出现在该任务中。

针对“外部”选项卡：

- 不会为外部任务生成任何事件。
- 您可以选择性地使用受管理对象。
- 在“外部 URL”字段中，您可以将应用程序的地址指定为：
  - 包括完全限定域名的完整地址 -- 例如：

    http://server1.mycompany.org/report/viewUserReport
  - 相对路径 -- 例如：

    /report/viewUserReport

    如果您指定了相对路径，CA Identity Manager 会自动附加安装 CA Identity Manager 的服务器的完全限定域名。
- 在“配置文件”选项卡上配置要传递到应用程序的属性。
- 您可以在 URL 中包括或排除管理员 DN 或任务名称。

外部 URL 选项卡

您可以将“外部 URL”选项卡添加到查看任务，例如“查看用户”。 使用“查看用户”任务时，将重定向到由 URL 标识的网站。 其他选项卡均不可见。

针对“外部”选项卡：

- “外部 URL”选项卡必须是任务中唯一的选项卡。如果存在与同一任务相关联的其他选项卡，外部选项卡将不会将用户重定向到指定的 URL。
- 该任务可以生成可以进行审核的事件。
- 在“外部 URL”字段中，您可以将应用程序的地址指定为：
  - 包括完全限定域名的完整地址 -- 例如：

    http://server1.mycompany.org/report/viewUserReport
  - 相对路径 -- 例如：

    /report/viewUserReport

    如果您指定了相对路径，CA Identity Manager 会自动附加安装 CA Identity Manager 的服务器的完全限定域名。

- 您可以选择性地使用受管理对象。
- 您可以配置要传递到 URL 的属性。

  向要启动并包括要传递到应用程序的属性的应用程序提供 URL。
- 您可以在 URL 中包括或排除管理员 DN 或任务名称。

高级任务组件

通过高级任务组件，您可以为任务指定自定义处理：

- 任务级别验证根据任务中的其他属性验证某个属性值。 例如，您可以验证用户提供的电话号码中的区号是否对应于用户所在的城市和省/自治区/直辖市。
- 在提交 CA Identity Manager 任务以进行处理之前，业务逻辑任务处理程序 (p. 63)执行自定义业务逻辑。 通常，自定义业务逻辑会验证数据。 例如，在 CA Identity Manager 将新成员添加到组之前，业务逻辑任务处理程序可以检查该组的成员资格限制。 如果达到了组成员资格限制，业务逻辑任务处理程序显示消息，通知组管理员无法添加新成员。

创建业务逻辑任务处理程序

您可以通过以下步骤定义业务逻辑任务处理程序的完全限定类名称：

1. 创建或修改管理任务。
2. 在“管理配置文件”选项卡上，单击“业务逻辑任务处理程序”。

   将显示“业务逻辑任务处理程序”屏幕。 此屏幕列出了分配给任务的所有现有业务逻辑任务处理程序。 Identity Manager 将按照处理程序在列表中显示的顺序来执行这些处理程序。
3. 单击“添加”。

   将显示“业务逻辑任务处理程序详细信息”屏幕。

对于要分配给任务的业务逻辑任务处理程序，可以使用“业务逻辑任务处理程序详细信息”屏幕为其定义以下信息：

名称

要分配给业务逻辑任务处理程序的名称。

说明

业务逻辑任务处理程序的说明（可选）。

Java 类

如果业务逻辑任务处理程序在 Java 中实施，则是指完全限定的业务逻辑任务处理程序类名称，例如：

com.mycompany.MyJavaBLTH

Identity Manager 预期类文件位于为自定义 Java 类文件指定的根目录中。 有关部署 Java 类文件的信息，请参阅 *《Java 编程指南》*。

JavaScript 文件名

如果业务逻辑任务处理程序在 JavaScript 中实施，且 JavaScript 代码包含在某个文件中，则可在此字段中指定该文件的名称。 例如，当业务逻辑任务处理程序要由多个任务屏幕使用时，您可能希望将 JavaScript 置于某个文件中。

Identity Manager 预期该文件位于为自定义 JavaScript 文件指定的根目录中。有关部署 JavaScript 文件的信息，请参阅 *《Java 编程指南》*。

如果要将该文件存储在根目录的子目录中，请在指定 JavaScript 文件名时包括子目录名称，例如：

JavaScriptSubDir\MyJavaScriptBLTH.js

必须根据部署 JavaScript 文件的平台，使用合适的斜线。

JavaScript

您可以通过在此字段（而非文件）中输入完整的 JavaScript 代码，实施 JavaScript 业务逻辑任务处理程序。 例如，如果脚本很短，或者不在任何其他任务屏幕中使用，您可能希望将此 JavaScript 置于此字段中。

属性和值

在 Java 实施过程中，这些字段为传递到 Java 业务逻辑任务处理程序的 init() 方法中的数据的可选名称/值对，并且将以处理程序业务逻辑所需的任何方式来使用。

要添加用户定义的属性，请指定属性名称和值，然后单击“添加”。

注意：如果添加了 Java 业务逻辑任务处理程序，请重新启动应用程序服务器，以加载该处理程序。

管理任务和事件

管理任务包括 CA Identity Manager 要完成任务所执行的*事件*和操作。 一项任务可能包括多个事件。 例如，“创建用户”任务可能包括创建用户的配置文件、将用户添加到组以及分配角色等事件。

CA Identity Manager 审核事件、强制执行与事件相关联的客户特定的业务规则，以及当事件映射到工作流流程时要求批准事件。

如果为某项任务生成了多个事件且这些事件已映射到工作流流程，则所有工作流流程都必须完成之后 CA Identity Manager 才能完成这项任务。

主要事件和次要事件

通常，事件之间是彼此独立的。 但是，某些任务与一个主要事件以及一个或多个次要事件相关联：

- 主要事件的失败会导致其所有的次要事件被自动拒绝。 例如，如果 CreateUserEvent 失败，则对于用户来说，就没有必要执行 AddToGroupEvent。这还会导致取消相关联的任务。
- 某个次要事件失败却不会对任务执行的任何其他事件成功与否以及任务本身的执行产生影响。 例如，在“创建用户”任务中，AddToGroupEvent 可能被拒绝，这意味着新用户无法添加到某个特定组中。 而该用户仍可被创建 (CreateUserEvent) 并分配给配给角色 (AssignProvisioningRoleEvent)，甚至添加到其他组中。

查看任务的事件

您可以在 CA Identity Manager 用户控制台查看与某项任务相关联的事件。

查看任务的事件

1. 在用户控制台中，依次选择“角色和任务”和“查看管理任务”。
2. 搜索并选择相应的任务。
3. 选择“事件”选项卡。

   CA Identity Manager 会显示与当前任务相关联的事件。

针对未修改的配置文件生成的事件

用户、组和组织对象每个都包含了一套存储在用户目录中的物理属性。 如果上述对象之一的某个物理属性在配置文件选项卡上进行了更改，Identity Manager 则会在用户提交提交任务之后生成一个 Modify... 事件。 例如，如果*标题*属性在“用户配置文件”选项卡上进行了更改，Identity Manager 则会生成 ModifyUserEvent 事件。

如果用户、组或组织对象显示在配置文件选项卡上，但是没有更改物理属性，则在用户单击“提交”时，Identity Manager 不生成 Modify... 事件。 而是会生成相应的 View... 事件，如下所示：

- 生成 ViewUserEvent，而不生成 ModifyUserEvent
- 生成 ViewGroupEvent，而不生成 ModifyGroupEvent
- 生成 ViewOrganizationEvent，而不生成 ModifyOrganizationEvent

管理任务处理

处理任务所花费的时间取决于所涉及的步骤。 提交任务以进行处理后，CA Identity Manager 将执行以下步骤：

1. CA Identity Manager 验证正在提交的数据。

   这就是*同步阶段*。

2. 如果任务需要批准，则 CA Identity Manager 会将任务发送到工作流引擎。

   a. 工作流引擎确定批准人，并将批准任务置于批准人的工作列表中。

   b. 或者，CA Identity Manager 发送电子邮件，向批准人通知等待批准的工作项。

   c. 批准人将保留工作项（此操作会从其他批准人的工作列表中删除该项目），然后批准或拒绝该工作项。

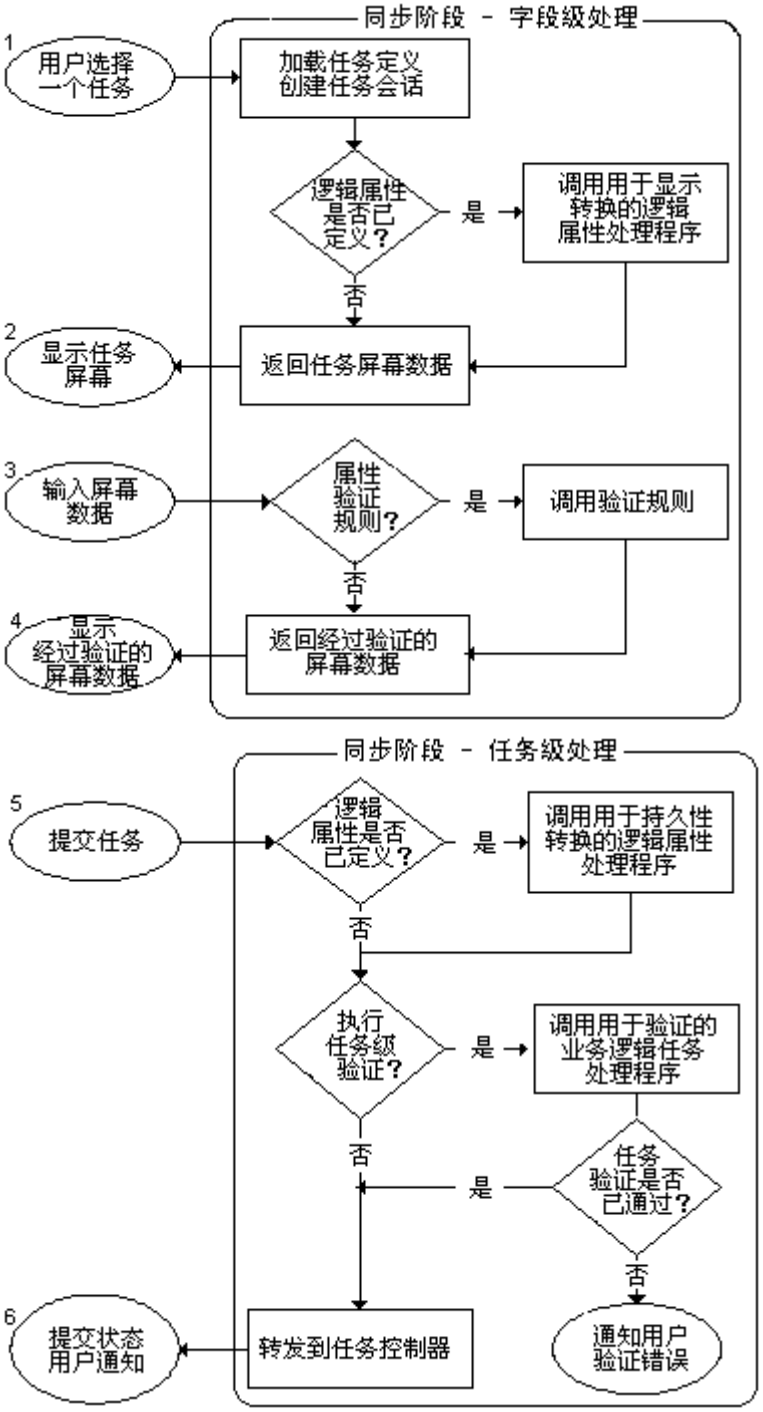
   d. 或者，CA Identity Manager 发送电子邮件，向有关用户通知任务的状态。

   这就是*异步阶段*。

3. 如果任务未被拒绝，CA Identity Manager 将执行该任务。

同步阶段处理

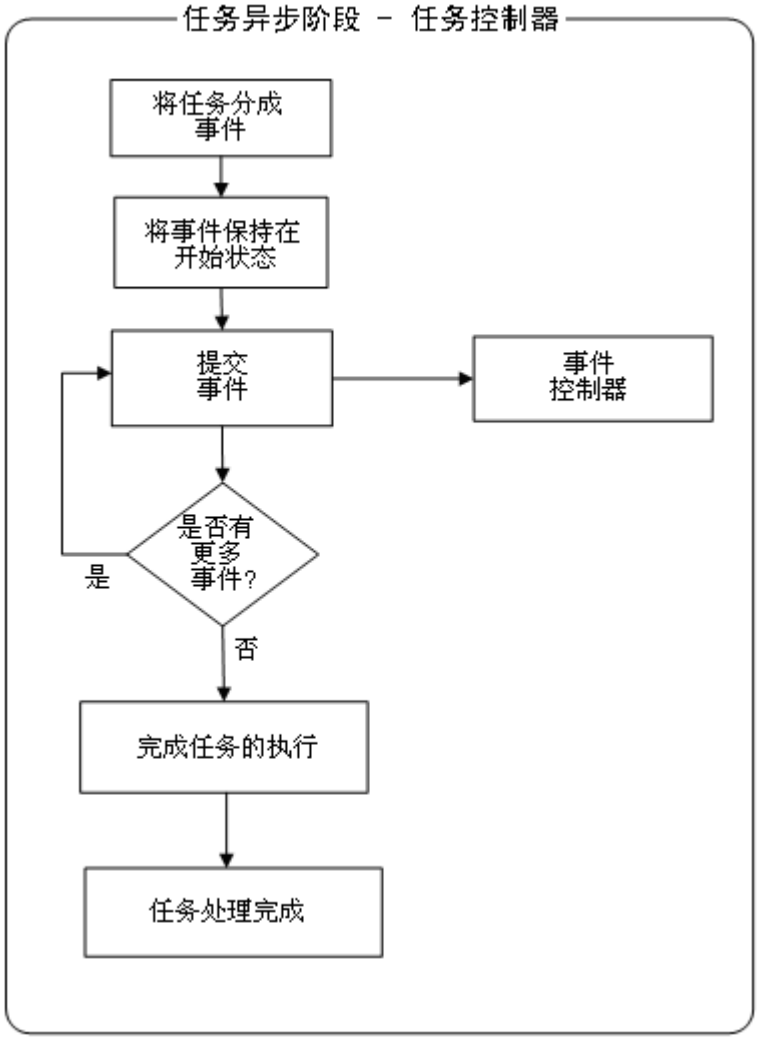
在同步阶段过程中，Identity Manager 可以转换并验证用户在任务屏幕中输入的数据，并可以在提交任务进行处理之前强制该数据的业务逻辑。 以下图表就此阶段中所发生的情况提供了概括说明。



异步阶段处理

同步阶段一经完成，该任务即进入执行的异步阶段。 在此阶段过程中，任务会生成一个或多个事件。 这些事件可能是用户定义的，如创建用户配置文件或将用户添加到组，也可能是系统生成的，如将信息写入审核日志。

任务控制器是 Identity Manager 服务器的一个组件，负责任务及其事件的整个周期，如下图所示：



对于多数事件，周期、执行和操作独立于任何其他事件。 （创建任务要求在次要事件之前执行主要对象的创建事件。）

通常，事件在以下状态之间转换：

- 开始
- 未决
- 已批准
- 执行
- 已完成
- 发布

注意：Identity Manager 提供名为 EventListeners 的 hook，“侦听”特定事件或事件组。 发生事件时，事件侦听程序将执行适合于事件和当前事件状态的自定义业务逻辑。 您可以使用 Event Listener API 编写自定义事件侦听程序。 有关详细信息，请参阅*《Programming Guide for Java》*。

管理任务的映像

您可以为置于主页的管理任务创建映像，以便使用。

第 4 章： 用户

此部分包含以下主题：

创建用户

用户配置文件可让管理员管理用户信息；管理权限、应用程序和服务访问；授予用户对其帐户和服务的自主管理权限。 创建用户配置文件是系统管理员的常见任务。

创建和配置用户时，需要考虑以下用户帐户元素：

自助服务任务：默认情况下，用户配置文件被配置为授予用户访问特定自助服务任务（例如更改密码和配置文件信息）的权限。 具有相应任务的系统管理员可以修改默认授予用户的自助服务任务。

组：组可简化角色管理。例如，具有相应任务的系统管理员可以配置多个角色，以便系统自动分配给被添加为组成员的用户。

管理角色：管理角色定义用户可在用户控制台中执行的任务。 例如，一个任务可让用户修改用户帐户信息，例如地址或职位。 其他任务可让用户管理任务，例如授予用户组成员资格。 将管理角色分配给用户后，用户可以执行与该角色关联的任务。

端点帐户和配给角色：存在于其他系统上的帐户称为端点帐户。 您可以通过配给角色将端点中的帐户分配给 CA CloudMinder 用户。 例如，用户需要 Exchange 帐户收发电子邮件，需要 Oracle 帐户访问数据库以及需要 Active Directory 帐户使用 Windows 系统。 将配给角色分配给用户后，用户将获得配给角色指定的端点帐户。

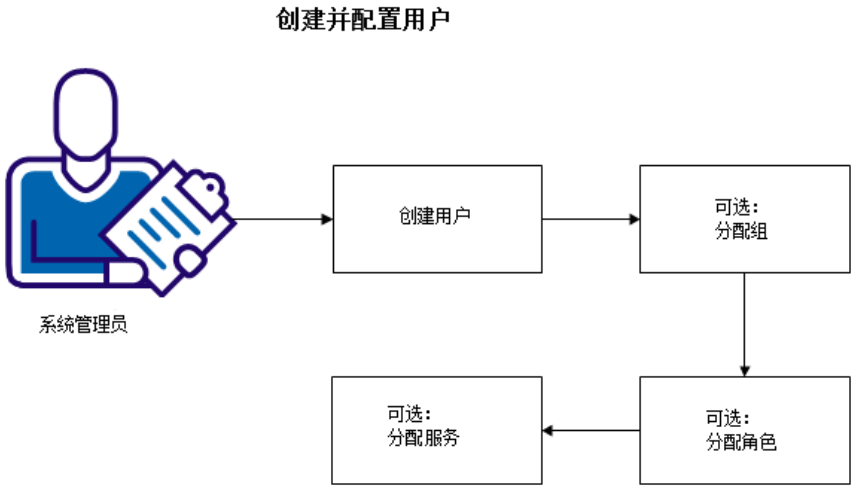
访问角色：访问角色提供了另一种在 CA Identity Manager 或其他应用程序中授予权利的方式。 例如，您可使用访问角色来完成下列任务：

- 提供对用户属性的间接访问
- 创建复杂的表达式
- 在用户配置文件中设置一个属性，另一个应用程序使用该属性来确定权利

服务：通过服务，您可以将所选的用户任务、角色、组以及属性整合到一个包里。 您可以将此权限包作为权限集进行管理。 例如，所有新销售员工都需要访问定义的一系列任务、特定端点系统上的帐户以及添加到其用户帐户配置文件中的信息。 将服务分配给用户后，用户将获得该服务指定的全部角色、任务、组和帐户属性。

密码策略：密码策略通过实施管理密码到期、组成及使用的规则和限制来管理用户密码。 如果系统管理员已为您的环境创建了密码策略，这些策略将自动应用于与一个或多个密码策略规则匹配的新用户。 具有相应任务的系统管理员可以修改密码策略。

下图说明了在创建和配置用户时要了解的信息以及执行的步骤。



以下主题将详细介绍如何创建用户以及如何配置用户。

1. 创建用户 (p. 72)。
2. 分配组 (p. 73)。（如果需要）
3. 将角色分配给用户 (p. 73)（如果需要）
4. 分配服务 (p. 74)。（如果需要）

创建用户配置文件

使用此步骤可创建用户配置文件。您也可以使用此任务定义其他配置文件元素，具体视“创建用户”任务的配置方式而定。 您可以将用户添加到组中，或者让用户成为管理或配给角色的成员。

遵循这些步骤:

1. 以具有用户管理任务的用户身份登录到用户控制台。

   默认“用户管理员”角色会授予相应的任务。

2. 依次选择“任务”、“用户”、“管理用户”、“创建用户”。

   将打开“创建用户”任务。

3. 根据需要填写用户配置文件信息的字段。
4. 单击“下一步”。
5. 填写该任务中其他选项卡的字段（如果适用）。

   例如，将用户添加到组中，或将管理角色、配给角色或服务分配给用户（如果这些选项可用）。

6. 单击“完成”。

   用户即已创建。

将组分配给用户

您可以让用户成为组成员。

遵循这些步骤:

1. 以具有用户管理任务的用户身份登录到用户控制台。
2. 依次选择“任务”、“组”、“修改组成员”。

   将显示您可以管理的组列表。

3. 选择一个组，然后单击“选择”。

   将显示分配给该组的用户列表。

4. 单击“添加用户”。
5. 搜索要为其分配该组的用户。

   要显示您有管理权限的所有用户的列表，请单击“搜索”而不修改搜索条件。

6. 选择一个用户，然后单击“选择”。

   将显示分配给该组的用户的更新列表。

7. 单击“提交”。

   指定用户即成为该组的成员。

将角色分配给用户

您可以将配给角色分配给各个用户。

遵循这些步骤:

1. 以具有“修改配给角色成员/管理员”任务的用户身份登录到用户控制台。
2. 选择“角色和任务”。
3. 选择以下任务之一：
   - 管理角色、修改管理角色成员/管理员
   - 配给角色、修改配给角色成员/管理员
   - 访问角色、修改访问角色成员/管理员

   此时显示一个搜索屏幕。
4. 选择要分配给用户的角色。

   将显示“成员资格”选项卡。
5. 单击“添加用户”。
6. 搜索要为其分配角色的用户。

   要显示您有管理任务的所有用户的列表，请单击“搜索”而不要修改搜索条件。
7. 选择一个用户，然后单击“选择”。
8. 单击“提交”。

   指定角色即被分配给用户。

将服务分配给用户

您可以将服务直接分配给个别用户。 该用户成为该服务的*成员*。

遵循这些步骤:

1. 依次导航到“服务”、“请求和查看访问”。

   此时显示一个您可以管理的服务的列表。
2. 选择要分配给用户的服务，然后单击“选择”。

   此时显示一个分配给服务的用户的列表。
3. 单击“请求访问”。
4. 搜索您要给其分配服务的用户。

   要显示您有管理权限的所有用户的列表，请单击“搜索”而不修改搜索条件。
5. 选择一个用户，然后单击“选择”。

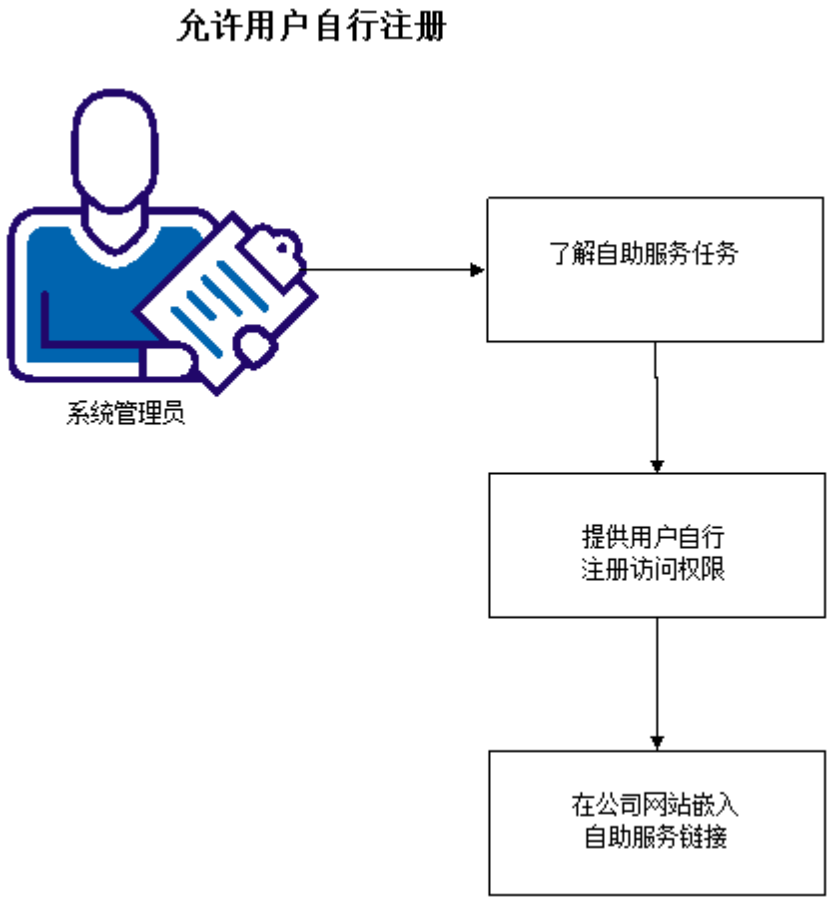
   此时显示一个分配给服务的用户的更新列表。
6. 单击“保存更改”。

   用户会收到指定的服务。 用户收到包括在该服务中的所有应用程序、角色、组和属性。

允许用户自行注册

自助服务任务可让用户管理自己的环境。 通过自行注册任务，用户可以利用公共用户控制台创建自己的用户帐户和配置文件。 例如，Bentley Cola 可让新员工和客户通过 Bentley Cola 企业网站嵌入的链接创建自己的用户帐户和配置文件。

下图说明了在允许用户自行注册时要了解的信息以及执行的步骤。



以下主题将详细介绍如何授予用户自行注册访问权限。

1. 了解自助服务任务 (p. 76)。
2. 授予用户自行注册访问权限 (p. 76)。
3. 在企业网站中嵌入自助服务链接 (p. 77)。

自助服务任务

自助服务任务是，用户通常可以通过用户控制台所采取的用于管理其配置文件的操作。在默认情况下，用户帐户已配置为授予用户访问特定自助服务任务（如更改密码和配置文件信息）的权限。 具有适当权限的系统管理员可以修改在默认情况下将哪些自助服务任务的权限授予用户。

自助服务任务分为以下两种类型：

- 公共任务－无需配给登录证书，用户即可访问的任务。 公共任务包括自行注册、忘记密码以及忘记用户 ID 等。
- 受保护的任务－用户需提供有效证书的任务。 包括更改密码或配置文件信息等。

下表列出默认自助服务任务。

任务类型	任务
公共任务	■ 自行注册－允许用户在公司网站注册 ■ 忘记密码重置－允许用户重置忘记的密码 ■ 忘记密码－显示用户可用于登录到 CA Identity Manager 的临时密码。用户登录后，将提示用户输入新密码 ■ 忘记用户 ID－找回或重置忘记的用户 ID
受保护的任务	■ 请求及查看访问－允许用户请求访问及删除服务。 ■ 更改我的密码－允许用户重置其密码 ■ 修改我的配置文件－维护配置文件信息，例如地址和电话号码 ■ 修改我的组－允许用户订阅组 ■ 查看我的角色－显示用户的角色 ■ 查看我提交的任务－显示用户启动的 CA Identity Manager 任务

访问自助服务任务

为您的环境配置自助服务任务后，可以将这些任务的 URL 添加到企业网站中。

自助服务任务的 URL 具有以下格式：

https://*domain*/iam/im/*public_alias*/ui7/index.jsp?task.tag=*task_tag*

其中：

- *domain* 是环境中运行 CA CloudMinder 的 Web 服务器的完全限定域名。
- *public_alias* 是环境的公共别名。 系统管理员在创建环境时定义公共别名。
- *"task_tag"*是任务的唯一标识符。

  对于默认的"忘记密码重置"任务，任务标签为 ForgottenPasswordReset。

  https://*domain*/iam/im/*public_alias*/ui7/index.jsp?task.tag=ForgottenPasswordReset

  对于默认的"忘记用户 ID"任务，任务标签为 ForgottenUserID：

  https://*domain*/iam/im/*public_alias*/ui7/index.jsp?task.tag=ForgottenUserID

在企业网站中嵌入自助服务链接

要允许通过企业网站访问公共自助服务任务，您可以添加指向任何网页的链接。用户单击链接时，将打开任务屏幕。 用户完成任务后，将默认重定向至用户控制台。

要更改用户重定向至的页面，您可以将 task.RedirectURL 标记附加到与链接关联的 URL，如下所示：

<A href="http://*domain*/iam/im/*public_alias*/ui7/index.jsp?task.tag=*tasktag*&task.RedirectURL=http://*domain*/*redirect_URL*">*链接文本*</A>

domain

CA Identity Manager 运行环境中的 Web 服务器的完全限定域名。

public_alias

添加到 URL 的唯一字符串，用于访问公共任务。

公共任务是自助服务任务，例如自行注册或忘记密码任务。 用户不需要登录即可访问公共任务。

注意：有关公共任务和别名的更多信息，请参阅*《配置指南》*。

tasktag

任务的唯一标识符。要确定任务标记，请使用"修改管理任务"查看任务的配置文件。

redirect_URL

用户提交任务后被定向至的 URL。

例如，您可以在用户自行注册后将用户重定向至"欢迎"页面。

链接文本

用户访问目标 URL 时要单击的文本。

例如，公司可以添加让用户能够重置忘记的密码，然后将他们定向至欢迎页面的链接。

下面的 HTML 为链接文本的示例：

<A href="http://myserver.mycompany.org/iam/im/Employees/ui7/index.jsp?task.tag=ForgottenPasswordReset&task.RedirectURL=http://myserver.mycompany.org/ welcome.html">重置我的密码</A>

要将用户返回到访问自助服务任务的页面，请将 RefererURL 指定为 task.RedirectURL 标记的值，如下所示：

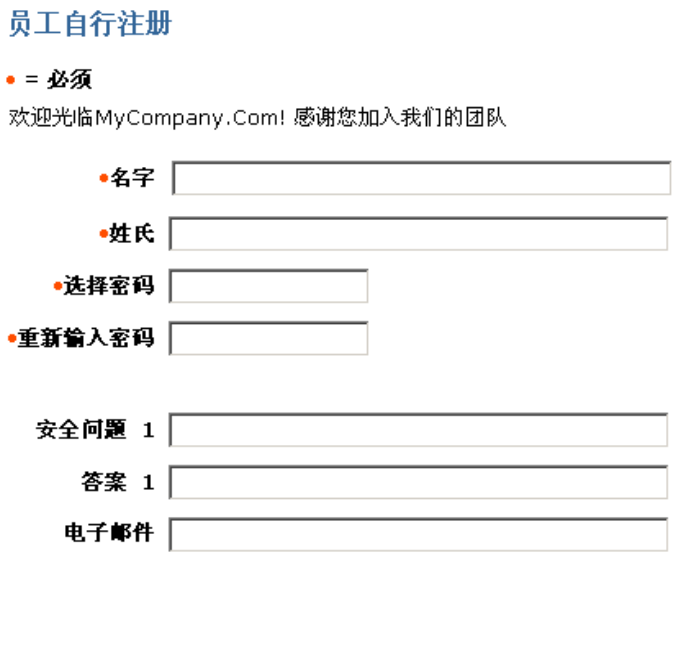
<A href="http://*domain*/iam/im/*public_alias*/ui7/index.jsp?task.tag=*taskta g*&task.RedirectURL=RefererURL</A>

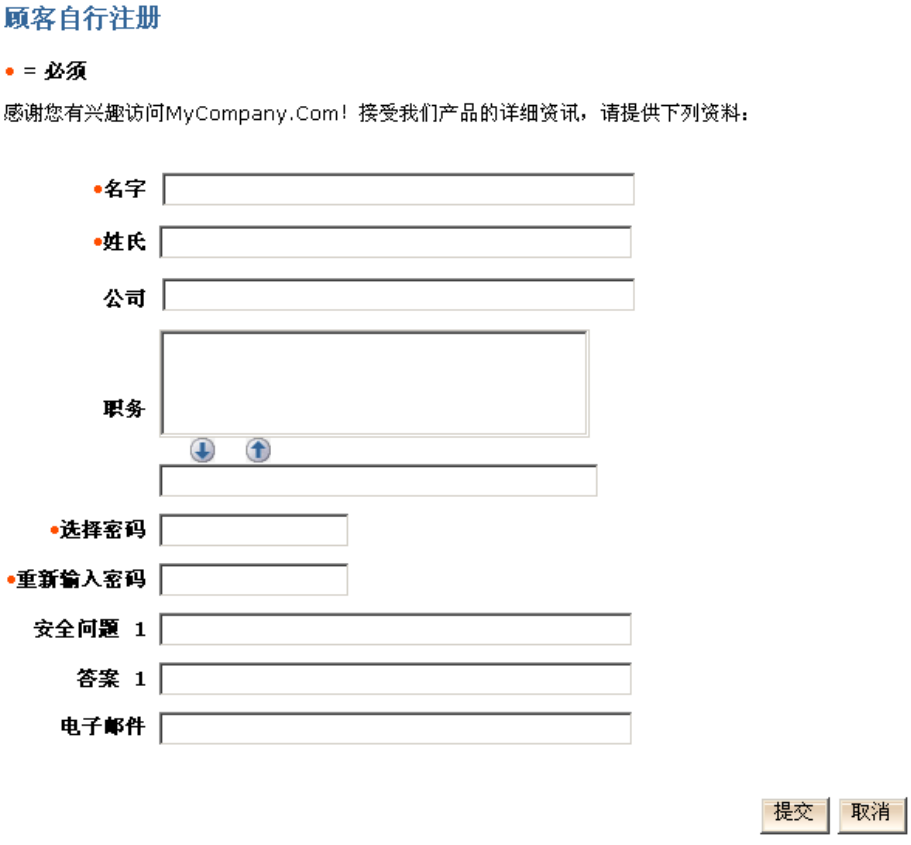
配置多个自助服务任务

可以为不同类型的用户创建多个自助服务任务。 例如，可以创建一个任务来注册新员工，创建另一个任务来注册客户。 通过使用不同的自行注册任务，您可以：

- 收集不同信息
- 注册不同组织的用户
- 用户注册后将其重定向至不同的注销页面
- 使用不同的商标

下图分别显示了新员工和客户的自行注册任务。





要配置同一类型的多个自助服务任务，请在创建任务时指定一个唯一的标签。“标签”字段位于任务的配置配置文件屏幕上。

将用于访问任务的链接添加到网站时，可以附加任务标签，同时创建唯一的 URL。

例如，您可以按如下所示创建两个任务：

任务	标记	URL
注册为新员工	selfregistration_employee	http://*domain*/iam/im/*alias*/index.jsp?task.tag=SelfRegistration_employee
注册为客户	selfregistration_customer	http://*domain*/iam/im/*alias*/index.jsp?task.tag=SelfRegistration_customer

限制对自行管理器角色的访问权限

默认情况下，将为所有用户分配“自行管理器”角色，该角色允许用户管理其配置文件信息及查看其角色和已提交的任务。

要为用户子集分配“自行管理器”角色，请删除现有成员策略并按照定义管理角色的成员策略中的说明创建新策略。

第 5 章： 密码管理

此部分包含以下主题：

Identity Manager 中的密码管理

Identity Manager 包括若干种用于管理用户密码的功能：

- 密码策略 - 这些策略通过执行管理密码到期、组成及用法的规则和限制来管理用户密码。
- 密码管理员 - 当用户致电 Help Desk 时，具有密码管理员角色的管理员可以重置密码。
- 自助式服务密码管理 - Identity Manager 包括若干个使用户可以管理其各自密码的自助式服务任务。 这些任务包括：
  - 自行注册 - 用户在公司网站注册时，指定密码。
  - 更改我的密码 - 用户无需 IT 或 Helpdesk 人员的帮助即可修改其密码
  - 忘记密码 - 在 Identity Manager 验证用户的身份后，用户即可重置或找回忘记的密码。
  - 重置密码或解除帐户锁定 - 用户可重置或找回忘记的密码，也可以在其用来访问 Identity Manager 的系统上，解除 Windows 帐户的锁定。
  - 忘记用户 ID - 在 Identity Manager 验证用户的身份后，用户即可找回忘记的用户 ID。
- 端点帐户中的密码同步 - 密码更改在 Identity Manager、配给服务器及其目标系统中同步。 根据 Identity Manager 密码策略验证新密码。

密码策略概述

密码策略是一系列的规则和限制。 这些规则规定了密码的创建和到期。 在 CA Identity Manager 环境中配置密码策略时，该策略适用于与此环境关联的用户存储。 如果用户目录与多个环境关联，则在一个环境中定义的密码策略可适用于其他环境。

在密码策略中，可以配置以下设置：

注意：部分这些设置需要为特定属性进行用户目录映射。 请参阅启用其他密码策略 (p. 83)。

- 将密码应用于一组特定用户
- 密码到期－定义导致密码到期的事件，例如过去的天数或失败登录尝试的次数。 密码到期后，将禁用用户帐户。
- 密码组成－指定新密码的内容要求。 例如，可以配置设置，要求用户创建的密码至少包含八个字符，并且是一个数字一个字母。
- 正则表达式－提供确定有效密码格式的表达式。 可以指定密码是否与该格式匹配。 也可以指定多个正则表达式。
- 密码限制－设置对密码重新使用的限制。 例如，用户必须等待 90 天，才能重新使用密码。
- 高级密码选项－指定在处理密码之前 CA Identity Manager 执行的操作，例如将密码改成小写。 如果应用了多个密码策略，还可以指定密码策略的优先级。

SiteMinder 用户还可以在 SiteMinder 管理用户界面中配置密码策略。 这些策略将显示在 CA Identity Manager 用户控制台中。

注意：在 CA Identity Manager 与 SiteMinder 集成时，SiteMinder 将实施*所有*密码策略。

创建密码策略

通过 CA Identity Manager 用户控制台创建密码策略。

注意：部分密码策略选项需要映射特定常用属性才可使用。 请参阅启用其他密码策略 (p. 83)。

遵循这些步骤：

1. 在用户控制台中，选择以下任一选项：
   - 策略、管理密码策略、创建密码策略。
   - 任务、策略、管理密码策略、创建密码策略。
2. 为密码策略输入一个唯一的名称和说明（可选）。
3. 配置这些密码策略设置，以最好地适应您的实施：
   - 将密码策略应用于用户组 (p. 84)
   - 配置密码到期 (p. 85)
   - 配置密码组成 (p. 88)
   - 指定正则表达式 (p. 89)
   - 设置密码限制 (p. 91)
   - 配置高级密码选项 (p. 93)

启用其他密码策略

CA Identity Manager 可让您创建通过实施密码到期、组成和使用来管理用户密码的基本密码策略。 您也可以定义以下其他密码规则和限制：

- 密码到期：
  - 跟踪失败或成功的登录。
  - 验证登录。
  - 未进行更改而造成的密码到期
  - 密码处于非活动状态
  - 密码不正确
  - 多个正则表达式
- 密码限制：
  - 重新使用前最少天数
  - 重新使用前密码的最少数量
  - 与上一个密码的差异百分比
  - 检查差异时忽略顺序。

遵循这些步骤:

1. 在管理控制台中转到“目录”、<目录名称>、“用户”。
2. 确认 %PASSWORD DATA% 和 %ENABLED STATES% -> 'STATE' 已映射到物理属性。
3. 默认情况下，示例 directory.xml 文件中映射了这些属性。 如果没有映射这些属性，请参阅 *《CA Identity Manager Configuration Guide》* 了解更多信息。

将密码策略应用于用户组

您可以指定确定密码策略适用的用户组的规则。 此功能可让您为一般员工设置一个密码策略，为高级经理设置一个更严格的策略。

遵循这些步骤:

1. 在用户控制台中创建或修改密码策略
2. 在“目录筛选”字段中选择要配置的筛选类型。

   有关每个筛选类型的说明，请参阅下表。

   注意: 密码策略适用的用户存储类型决定“目录筛选”列表框中的选项。在 CA Identity Manager 与 SiteMinder 集成时，部分筛选类型对关系数据库和 CA Directory 用户存储不可用。
3. 通过选择属性和运算符并输入值来指定条件。
4. 要添加其他条件，请单击加号。

下表说明了目录筛选类型选项，并提供了每种筛选类型的示例。 在下面的示例中，“=”左侧的属性是用户目录定义区域中规定的属性。 对于创建类型的用户任务，只有同时满足以下两个条件时，才会应用配置了目录筛选的密码策略：

- CA Identity Manager 未与 SiteMinder 集成。
- 目录筛选类型不是用户、组、组筛选或组搜索。

筛选类型	用途	示例
组织中	浏览并选择组织。	
组中	浏览并选择组。	
一个用户	浏览并选择一个用户。	
用户筛选（与 SiteMinder 集成时，对于关系数据库不可用）	指定用于用户的筛选。	雇员类型 = 承包商 部门 = 安全

筛选类型	用途	示例
用户搜索表达式	输入用于用户的搜索查询。	uid=jsmith（对于 LDAP） TBLUSERS.ID = jsmith（对于关系数据库）
组筛选 （与 SiteMinder 集成时，对于关系数据库不可用）	指定用于组的筛选。	自行订阅 = *
组搜索表达式	输入用于组的搜索查询。	cn=Sales（对于 LDAP） TBLGROUPS.NAME=GroupA（对于关系数据库）
组织筛选 （与 SiteMinder 集成时，对于关系数据库不可用）	指定用于组织的筛选。	组织名称 = *营销
组织搜索表达式	输入用于组织的搜索查询。	ou=Boston（对于 LDAP） TBLORGANIZATIONS.NAME=Boston（对于关系数据库）
搜索	指定未包含在筛选类型其他选项中的查询。	(&(uid=*smith)(ou=Boston))

配置密码到期

为帮助管理用户访问，您可以定义诸如多次登录失败尝试或帐户非活动等事件。发生这些事件时，CA Identity Manager 将禁用相应的用户帐户。 在 CA Identity Manager 与 SiteMinder 集成时，您可以指定重定向。

注意：这些设置需要其他配置。 请参阅启用其他密码策略 (p. 83)。

您可以配置以下密码到期设置：

- “跟踪失败登录”/“跟踪成功登录”复选框
- “登录跟踪失败时进行身份验证”复选框
- “如未更改，密码到期”设置
- “由于未活动密码到期”设置
- “密码不正确”设置

“跟踪失败登录”/“跟踪成功登录”复选框

此复选框可启用和禁用对用户登录尝试的跟踪，包括上次登录尝试的时间。 如果启用此复选框，CA Identity Manager 会将登录信息写入用户存储中的密码数据属性。

注意：此设置需要其他配置。 请参阅启用其他密码策略 (p. 83)。

启用“跟踪失败登录”复选框后，“密码不正确”部分以及“登录跟踪失败时进行身份验证”复选框处于活动状态。 启用“跟踪成功登录”复选框后，“由于未活动密码到期”部分和“登录跟踪失败时进行身份验证”复选框处于活动状态。

如果有多个密码策略，请确保所有适用的密码策略均禁用登录详细信息。否则，一个启用跟踪登录详细信息的策略即可导致密码策略无法正常运行。

“登录跟踪失败时进行身份验证”复选框

在用户跟踪失败时，选中此复选框可登录。 默认情况下，此复选框为禁用。 禁用登录跟踪时，用户无法登录。

选中此复选框后，请务必同时选中“跟踪失败登录”或“跟踪成功登录”复选框。

注意：此设置需要其他配置。 请参阅启用其他密码策略 (p. 83)。

“如未更改，密码到期”设置

在“如未更改，密码到期”字段中，可以配置已到期密码的行为。 或者，您可以指定提前多长时间警告用户密码即将到期。

注意：此设置需要其他配置。 请参阅启用其他密码策略 (p. 83)。

您可以配置以下字段：

***<number>* 天后**

确定密码到期后，在禁用用户或强制密码更改之前 CA Identity Manager 等待的天数。

注意：在经过规定天数之后用户尝试登录帐户前，CA Identity Manager 不会禁用用户帐户。

禁用用户

选中此单选按钮会在密码到期后禁用用户。 通过以下方式可启用已禁用的用户：

- 用户控制台中的“启用/禁用用户”任务。 （默认“系统管理员”、“组织管理员”以及“安全管理员”角色包含“启用/禁用用户”任务。）
- SiteMinder 管理用户界面。

  注意：有关详细信息，请参阅*《CA SiteMinder Policy Server Administration Guide》*。

强制密码更改

选中此单选按钮会在用户下一次尝试登录时强制更改密码。

提前 *<number>* 天发布到期警告

输入提前通知用户密码即将到期的天数。

“由于未活动密码到期”设置

“由于未活动密码到期”设置可让您指定用户登录尝试之间的时间间隔。 经过这段时间后，用户帐户将被视为非活动帐户。 您也可以使用此部分指定被视为非活动帐户的用户有权登录时的操作。

要配置“由于未活动密码到期”部分中的设置，请务必启用跟踪登录详细信息复选框。

注意：此设置需要其他配置。 请参阅启用其他密码策略 (p. 83)。

“由于未活动密码到期”部分包含以下设置：

- *<number>* 天后－决定密码到期前处于不活动状态的天数。
- 禁用用户－在密码由于未活动而到期后禁用用户，用户帐户被禁用。 之后，必须使用“启用/禁用用户”任务启用已禁用的用户。
- 强制密码更改－在密码由于未活动而到期后，强制更改密码。 用户下一次尝试登录时更改密码。

“密码不正确”设置

在“密码不正确”设置部分中，您可以指定在禁用用户帐户之前允许登录失败的次数。 您也可以指定用户可以尝试再次登录之前帐户被禁用的时间。 只有选中“跟踪失败登录”复选框后，本部分才适用。

注意：此设置需要其他配置。 请参阅启用其他密码策略 (p. 83)。

“密码不正确”部分包含以下字段：

连续 *<number>* 次密码错误后禁用帐户

此设置决定用户可以连续登录失败的次数。 限制不成功尝试的次数可以防御旨在通过重复尝试密码直至找到正确密码来访问资源的程序。 如果用户在进行了规定次数的尝试后无法正确登录，CA Identity Manager 将禁用该帐户。 需要管理员重新启用帐户。

***<number>* 分钟后**

此设置决定用户在再次尝试登录或帐户重新启用前需要等待的时间。 如果用户再次输入错误密码，CA Identity Manager 将再次禁用该帐户。 用户在重试之前需等待规定的一段时间。

允许一次登录尝试

此设置指定用户输入错误密码后需要等待多少分钟才能再次尝试登录。

重新启用帐户

此设置可以在指定的时间后重新启用帐户。

配置密码组成

您可以指定用于确定新创建密码的字符组成的规则。 在针对字符要求确定值时一定要考虑最大密码长度。 如果字母和数字的总数超过最大密码长度，则会拒绝所有密码。例如，如果“字母”或“数字”均设为六个，则所有密码包含至少 12 个字符（6 个字母和 6 个数字）。 在本例中，如果最大密码长度是八个字符，则会拒绝所有密码。

密码组成设置包括：

最小密码长度

指定用户密码的最小长度。

最大密码长度

指定用户密码的最大长度。

最大重复字符数

确定密码中可以连续出现的相同字符的最大数目。

例如，如果此值设为 3，则密码中任何地方均不能出现“aaaa”。 但密码内可接受“aaa”。设置此值，以确保用户无法输入单个字符的密码。

大写字母

指定是否允许使用大写字母字符，以及密码必须包含的最少数目（如果允许）。

小写字母

指定是否允许使用小写字母字符，以及密码必须包含的最少数目（如果允许）。

字母

指定是否允许使用字母，以及密码必须包含的最少数目（如果允许）。

注意：当允许使用大写或小写字母时，会自动选中“字母”复选框。

数字

指定是否允许使用数字，以及密码必须包含的最少数目（如果允许）。

字母和数字

指定是否允许使用字母和数字，以及密码必须包含的最少数目（如果允许）。如果与“数字”一起配合设置此设置，则字符需要同时满足两方面的要求。 例如，如果此设置和“数字”均设为 4，则密码“1234”是有效密码。

注意：当允许使用大写或小写字母或数字时，会自动选中“字母或数字”复选框。

标点符号

指定是否允许使用标点符号，以及密码可以包含的最少数目（如果允许）。 标点符号可以是句号、逗号、感叹号、斜杠、破折号以及连字符。

非打印

指定是否允许使用非打印字符，以及密码可以包含的最少数目（如果允许）。 这些字符在计算机屏幕上无法显示。

注意：某些浏览器不支持非打印字符。

非字母数字

指定是否允许使用非字母数字字符，如标点符号和其他符号（“@”、“$”和“*”），以及密码可以包含的最少数目（如果允许）。 也包括非打印字符。 非字母数字字符也要满足“标点符号”和“非打印”字符要求。

指定正则表达式

密码正则表达式可让您为每个密码匹配或不匹配的字符串匹配指定正则表达式文本模式，以便字符串有效。 例如，您要求第一个字符是数字，而最后一个字符不是数字时，此测试非常有用。

可以为一个密码策略配置多个表达式。 如果创建多个表达式，可接受的密码匹配*所有*指定表达式。

遵循这些步骤:

1. 在“名称”字段中，为表达式键入描述性标记（无空格）。
2. 使用在“必须匹配”字段的“正则表达式语法”中描述的语法，键入正则表达式。
3. 如果密码不匹配正则表达式，选中“不得匹配”列中的复选框。

注意：您可以通过单击加号 (+) 符号以添加表达式，来指定多个表达式。

示例：可使用下面的正则表达式定义要求所有密码必须以大写或小写字母开头：
Name: MustStartAlpha

表达式：[a-zA-Z].*

正则表达式语法

本节描述用来为密码匹配构建正则表达式的语法。 该语法与在指定领域时针对资源匹配所支持的正则表达式语法是一致的。

字符	结果
\	用来援引元字符（类似于“*”）
\\	匹配单一“\”字符
(A)	组子表达式（影响模式赋值的顺序）
[abc]	简单字符类（方括号中的任何字符匹配目标字符）
[a-zA-Z]	具有范围的字符类（方括号中的任何字符范围匹配目标字符）
[^abc]	求反字符类
.	匹配除换行符外的任何字符
^	仅匹配一行的开头
$	仅匹配一行的末尾
A*	匹配 A 0 次或更多次（贪婪）
A+	匹配 A 1 次或更多次（贪婪）
A?	匹配 A 1 次或 0 次（贪婪）
A*?	匹配 A 0 次或更多次（勉强）

字符	结果
A+?	匹配 A 1 次或更多次（勉强）
A??	匹配 A 0 次或 1 次（勉强）
AB	匹配 A，之后紧接着是 B
A|B	匹配 A 或 B
\1	后向引用第 1 个括号内的子表达式
n	后向引用第 *n* 个括号内的子表达式

默认情况下，所有闭包运算符（+、*、?）都是贪婪的，这意味着其在不会导致整体匹配失败的情况下，匹配尽可能多的字符串元素。 如果希望闭包是勉强的（非贪婪），只需紧随其后加个“?”即可。 勉强闭包将在查找匹配项时，匹配尽可能少的字符串元素。

设置密码限制

您可以对密码使用规定限制。 这些限制包括用户必须等待多长时间才能重新使用密码，以及密码必须与之前选择的密码有多大差异。 您也可以禁止用户指定您认为有安全风险或包含个人信息的词。

注意：此设置需要其他配置。 请参阅启用其他密码策略 (p. 83)。

“限制”部分包含以下字段：

重新使用前最少天数

决定用户必须等待多少天才能重新使用密码。

重新使用前密码的最少数量

决定必须使用多少个密码后才能重新使用密码。

注意：如果您指定了时间和密码的数目，两个条件都满足后才能重新使用密码。 例如，您可以将密码策略配置为要求用户在 365 天后并使用了 12 个其他密码后才能重新使用密码。 一年后，如果用户只使用了六个密码，则还需要再使用六个密码，才可以重新使用第一个密码。

与上一个密码的差异百分比

指定新密码需要包含的字符的百分比。您可以将该值设置为 100。在这种情况下，新密码无法包含之前密码中存在的字符。

检查差异时忽略顺序

确定百分比时忽略密码中字符的位置。

例如，如果初始密码是 BASEBALL12 并选中“检查差异时忽略顺序”复选框，则 12BASEBALL 不可接受。 取消选中该复选框时，12BASEBALL 是可以接受的密码，因为每个字母的位置不同。

为加强安全，请选中“检查差异时忽略顺序”复选框。

密码	差异百分比	忽略顺序	已接受
BASEBALL12（旧） 12BASEBALL	0	已选中 已取消选中	Y Y
BASEBALL12（旧） 12BASEBALL	100	已选中 已取消选中	N Y
BASEBALL12（旧） 12SOFTBALL	0	已选中 已取消选中	Y Y
BASEBALL12（旧） 12SOFTBALL	90	已选中 已取消选中	N Y
BASEBALL12（旧） 12SOFTBALL	100	已选中 已取消选中	N N

配置文件属性

配置“匹配长度”字段可避免用户在密码中使用个人信息。“匹配长度”字段确定与目录条目中的属性相比，密码策略的最小序列长度。 例如，如果此值设置为四，CA Identity Manager 验证密码不包括用户配置文件属性的最后四个字符，例如，姓氏或电话号码。

字典

指定不能在密码中使用的字符串列表。

注意：字典条目的最后一行后有回车。

字典设置包含以下字段：

- 路径－包含字典文件的完整路径和名称。
- 匹配长度－控制字符串与字典文件中的值相对比的长度。对比将忽略字符串的大小写。 您可以将“匹配长度”字段留空，或将其设置为零。 在这些情况下，CA Identity Manager 仅拒绝与字典中的字符串完全匹配的密码。 在匹配长度大于零时，CA Identity Manager 会在以下条件下拒绝条目：
  - 密码包含起始字符序列与字典条目相同的子字符串。
  - 连续匹配的字符数目大于或等于“匹配长度”字段中指定的数目。

  例如，考虑包含以下条目的字典文件：
  - lion
  - tiger
  - bear

  在“匹配长度”字段设置为四时，会产生以下操作：

  “TeddyBear”，由于 Bear 与字典文件中的 bear 条目匹配被拒绝。

  “prestige”，因为“tige”与字典文件中 tiger 条目的前四个字符匹配被拒绝。

  “Geiger Counter”，因为“iger”不包含字典文件中 tiger 条目的第一个字母被接受。

配置高级密码选项

通过高级密码策略选项，您可在验证和存储之前配置所提交密码的预处理。 您还可为策略分配优先级，以便对适用于相同用户目录或命名空间的多个密码策略进行可预测的评估。

不强制大小写 | 强制大写 | 强制小写

确定是否在处理和存储之前将密码强制为大写或小写。 通过单击“强制大写”或“强制小写”单选按钮，选择大小写强制选项。 否则，确保选中“不强制大小写”单选按钮（默认）。

重要说明！ 您指定的任何大小写强制选项一定要与您已定义的任何大小写相关组成要求一致。

删除前导空格

选中该项，可在处理前删除密码中的前导空格。

删除尾空格

选中该项，可在处理前删除密码中的尾空格。

删除中间空格

选中该项，可在处理前删除所有中间空格。

注意：一些用户目录实施会在存储之前自动删除属性值（用户密码存储在其中）中的前导或尾空格。 您在密码策略中指定的设置将会无效。

评估优先级

指定密码策略的评估优先级。 值的范围是 0（默认）到 999。 适用策略按降序评估（999 最先；0 最后）。

应用较低优先级密码策略

确定在此之后是否应用较低优先级密码策略。

管理密码策略

具有相应权限的管理员可以使用查看、修改、创建和删除密码策略任务来管理密码策略。 默认情况下，这些任务显示在“策略”类别中。

访问其中一个任务时，CA Identity Manager 将显示适用于与当前 CA Identity Manager 环境相关联的用户存储的密码策略列表。 如果 CA Identity Manager 与 SiteMinder 集成，则该列表可能包括使用密码服务在 SiteMinder 管理用户界面中创建的密码策略。 您可以管理在 CA Identity Manager 或 SiteMinder 中创建的密码策略。

密码策略和关系数据库

如果配置适用于关系数据库的密码策略，必须使用以下格式为 SiteMinder 用户目录配置密码数据属性：

tablename.columnname

为避免执行期间出现语法问题，建议该字段位于主表格中。

CA CA Identity Manager 和 Siteminder 集成密码条件

在 CA CA Identity Manager 与 SiteMinder 集成并使用 Siteminder 的密码处理功能时，密码策略是从 Siteminder 策略存储获取的。 在这种情况下，会构造满足 Siteminder 密码条件的密码。 只有以下标点符号字符满足 Siteminder 密码条件：

“*”、“(”、“\”、“,”、“@”、“"”、“:”、“#”、“_”、“-”、“!”、“&”、“?”、“)”、“{”、“}”、“*”、“.”、“/”

重要说明：CA CA Identity Manager 不会在密码的标点符号字符使用上强加任何限制。 但是，如果您打算使用 Siteminder 密码功能，建议您构造满足 Siteminder 限制的密码。

重置密码或解锁帐户

在用户忘记 Windows 系统上的密码的情况下，您可以配置自助服务，以便提示 Windows 登录屏幕的用户。 对于 Windows VISTA 和 Windows 7 系统，可以通过安装凭据提供程序来使用此功能。

使用此功能，用户通过密码更改要求页面出现的多维数据集 Web 浏览器登录到自助服务。 在填充本页之后，用户单击“返回”回到 Windows 登录屏幕。

安装凭据提供程序

遵循这些步骤:

1. 找到 CA Identity Manager 开通组件下载介质或其他安装介质。
2. 运行“代理”下的安装程序。

   注意：对于 64 位操作系统上的凭据提供程序，请确保选择该软件的 64 位版本。
3. 按照向导提示回答问题。
4. 如果要在 64 位操作系统上安装凭据提供程序，请下载 Microsoft Visual C++ 2008 SP1（64 位）。
5. 安装完成后，配置凭据提供程序。

配置凭据提供程序

您可以使用配置工具配置您安装凭据提供程序的系统。

配置凭据提供程序

1. 在 Windows 浏览器中，转到您安装凭据提供程序的目录。 例如：

   C:\Program Files\CA\Identity Manager\Credential Provider

2. 双击以下可执行文件：

   CAIMCredProvConfig.exe

3. 选择第一个凭据提供程序作为默认选项。

   如果正在使用第二个凭据提供程序（如 Microsoft 密码凭据提供程序），登录屏幕可能不会提供此设置。如果两个提供程序都尝试成为默认提供程序，登录屏幕会选择默认提供程序。

4. 禁用默认凭据提供程序。

5. 填写“凭据提供程序设置”区域中的字段，如下所示：

   Link1 URL

   用户单击“忘记密码”链接时使用的 URL。 该链接应为用于密码重置的 Web 界面的 URL。

   下面是一个链接示例：

   ```
   http://eastern.local:8080/iam/im/environment/ca12/index.jsp?
   task.tag=forgottenpassword&facesViewId=/app/page/screen/
   fp_identify_user.jsp&action.forgottenpassword.identify=1&USER_ID=%use
   rname%
   ```

   对于此 URL，自行注册必须可在该环境中正常工作。 另外，请确认 CA Identity Manager 环境的自助服务 URL 可从您将要安装凭据提供程序的系统上正常工作。 出现的 %username% 将被替换为“登录”对话框的“用户名”字段中的值。

   Link2 **URL**

   用户单击“解锁帐户”链接时使用的 URL。 该链接应为允许用户解除帐户锁定的 Web 界面的 URL。出现的 %username% 将被替换为“登录”对话框的“用户名”字段中的值。

   Link3 URL

   用户单击“新建帐户”链接时使用的 URL。 此链接应为允许用户创建帐户的 Web 界面的 URL。 %username% 标记不是 URL 的一部分。

使用自定义标题

自定义字符串将替换标题栏上或凭据提供程序的“返回”对话框中显示的字符串“技术提供方...”。 字符串的位置取决于 508 节遵从性设置。

Domain

开通域名。

508 节遵从性（使用在菜单中返回）

在菜单中启用返回函数。 如果未选中，则使用“返回”对话框。

禁用所有对话框

阻止安全浏览器产生新的对话框窗口，如弹出对话框、错误对话框以及打印或保存对话框。 启用“*禁用所有对话框*”可以改进系统安全性，但禁用该选项可以进行故障排除。

6. 填写“安全浏览器设置”区域中的字段，如下所示：

   允许列表

   与应始终允许访问的 URL 匹配的正则表达式模式。

   拒绝列表

   与应始终拒绝访问的 URL 匹配的正则表达式模式。

7. （可选）单击“导出”将您的设置导出到其他系统。
8. 单击“确定”保存您的设置。
9. 重新启动系统。

凭据提供程序注册表设置

如果不使用凭据提供程序配置工具，则可以在以下注册表项中编辑 Windows 注册表设置。

```
[HKEY_LOCAL_MACHINE\SOFTWARE\CA\CAIMCredentialProvider]
```

link1_cmd

该链接应该是用户单击链接 1 时要导航到的 URL。

link2_cmd

该链接应该是用户单击链接 2 时要导航到的 URL。例如，可以添加一个链接，该链接指向用于解除帐户锁定的网站。

如果 link2_cmd 为空，则只有 link1_cmd 显示在登录对话框窗口中。

link3_cmd

此链接应加载允许用户创建帐户的 Web 界面的 URL。

comp508

在菜单中启用返回函数。 如果未选中，则使用“返回”对话框

domain

开通域名。

langdir

本地化语言 DLL 的位置。

disablepwdcp

“禁用 Microsoft 密码凭据提供程序”选项。 1 为禁用。 0 为启用。

CredentialProviderInstallPath

安装凭据提供程序的完整目录路径。

configdir

安装凭据提供程序的完整目录路径。

selectdefaultcredential

选择第一个凭据提供程序作为默认选项。 “是”为启用。 “否”为禁用。

多维数据集浏览器注册表设置

多维数据集安全浏览器组件具有若干控制其行为的注册表值。 这些设置位于以下注册表项中：

```
[HKEY_LOCAL_MACHINE\SOFTWARE\CA\Cube]
```

类型

REG_SZ（字符串）

404

计算机在启动时无法联系 CA Identity Manager 时，显示的标准 HTML 文档的路径。

default

Link1 命令或 Link2 命令中不包括任何 URL 时，导航到的默认页面。

allow

显式允许 ACL。 与始终允许访问的 URL 匹配的正则表达式模式。 有关详细信息，请参阅“多维数据集访问控制列表 (p. 99)”。

close

关闭安全浏览器，并使用户返回凭据提供程序的忘记密码对话框。

deny

显式拒绝 ACL。与应始终拒绝访问的 URL 匹配的正则表达式模式。有关详细信息，请参阅“多维数据集访问控制列表 (p. 99)”。

langdir

本地化语言 DLL 的位置。

rejectinvalidcerts

控制凭据提供程序是否仅接受有效的 SSL 证书。 在设置为 no 时，此选项允许过期或无效的 SSL 证书。

此项的有效值是 *yes* 和 *no*。

unreachable

多维数据集遇到连接问题时，重定向到的 URL。

示例值：file:///C:\unreachable.html

usecustomtitle

为凭据提供程序启用自定义标题。

customtitle

这就是您希望在凭据提供程序中显示的标题。

Cube 访问控制列表

Cube ACL 是正则表达式模式，明确允许或拒绝导航到所选 URL 的权限。 ACL 按以下顺序评估：

1. 允许（首先自动允许权限）
2. 拒绝（其次检查拒绝的 URL）

访问控制列表示例

"allow"="(.pdf)"

允许显示所有 PDF 文档。

"deny"="(.doc|.xls)"

拒绝访问 Microsoft Word 和 Excel 文档。

自定义技术提供方消息

您可能会在凭据提供程序的“返回”对话框中或“返回”菜单选项中看到“技术提供方...”消息。 您可以编辑或删除此消息。

自定义技术提供方消息

1. 下载 ResEdit，它是来自 http://www.resedit.net 的免费软件资源编辑器。
2. 启动 ResEdit。
3. 编辑语言文件夹中的文件 1033.dll。
4. 双击字符串表。
5. 删除或修改资源 ID 135（此消息的资源的英文版）。

重置用于 Windows 登录的密码

在 Windows 系统上安装凭据提供程序之后，“忘记密码”链接将显示在标准 Microsoft Windows 登录对话框上。 使用此链接可重置密码或查看提示帮助您记起密码。

重置用于 Windows 登录的密码

1. 在“Windows 安全”对话框中单击“登录”。 将显示“Windows 登录”对话框。
2. 输入有效用户名。
3. 单击“忘记密码”。

   将显示“CA Identity Manager 密码提示”页面。

   如果您记起密码，请返回登录对话框继续操作。否则，请执行步骤 4，对 CA Identity Manager 自助服务进行身份验证。
4. 键入身份验证问题的答案。

   注意：如果您并不知道所有问题的答案，请单击“请求”，以便由管理员重置密码。

   然后系统会提示您在下一屏幕中更改密码。

凭据提供程序的无提示安装

凭据提供程序支持无提示模式下的安装。 支持六个属性

LINK1

是指注册表中的 SOFTWARE\CA\CAIMCredentialProvider\link1_cmd。

LINK2

是指注册表中的 SOFTWARE\CA\CAIMCredentialProvider\link2_cmd。

LINK3

是指注册表中的 SOFTWARE\CA\CAIMCredentialProvider\link3_cmd。

DOMAIN

是指注册表中的 SOFTWARE\CA\CAIMCredentialProvider\domain。

COMP508

是指注册表中的 SOFTWARE\CA\CAIMCredentialProvider\comp508。

USECUSTOMTITLE

是指注册表中的 SOFTWARE\CA\Cube\usecustomtitle。

CUSTOMTITLE

是指注册表中的 SOFTWARE\CA\Cube\customtitle。

REJECTINVALIDCERTS

是指注册表中的 SOFTWARE\ComputerAssociates\Cube\rejectinvalidcerts。

UNREACHABLE

是指无法访问的页面位置。

用于设置这些属性值的语法如下：

```
setup /s /v"/qn LICENSE=Yes INSTALLDIR=\"C:\Program Files\CA\Identity
Manager\Credential Provider\" LINK1=\"<url>\" LINK2=\"<url>\"LINK3=\"<url>\"
COMP508=\"yes\" REJECTINVALIDCERTS=\"yes\" USECUSTOMTITLE=\"yes\"
CUSTOMTITLE=\"custom cp title\""
```

或

```
setup /s /v"/qn LICENSE=Yes INSTALLDIR=\"C:\Program Files\CA\Identity
Manager\Credential Provider\" LINK1=\"<url>\" LINK2=\"<url>\" LINK3=\"<url>\"
COMP508=\"yes\" USECUSTOMTITLE=\"yes\" CUSTOMTITLE=\"custom cp title\"
SELECTDEFAULTCREDENTIAL=\"yes\" UNREACHABLE=\"<url>\""
```

或

```
setup /s /v"/qn LICENSE=Yes INSTALLDIR=\"C:\Program Files\CA\Identity
Manager\Credential Provider\"
LINK1=\"<url>\" LINK2=\" <url>\" LINK3=\"<url>\" COMP508=\"yes\"
USECUSTOMTITLE=\"yes\" CUSTOMTITLE=\"custom cp title\"
SELECTDEFAULTCREDENTIAL=\"yes\" UNREACHABLE=\"file:///[INSTALLDIR]<file
name>\"CUBE_ALLOW=\"\"CUBE_DENY=\"\""
```

[INSTALLDIR]

是指 INSTALLDIR 属性的值。

<url>

指定可解锁帐户或解决忘记密码问题的 URL。

<file name>

定义不可访问的文件名。

CUBE_ALLOW

是指允许多维数据集的 URL 调用。

CUBE_DENY 认

是指限制多维数据集的 URL 调用。

第 6 章： 同步端点上的密码

您可以在 CA Identity Manager 支持的特定端点上安装密码同步代理。 代理在端点上截获密码更改请求，并且将更改提交给配给服务器。

此部分包含以下主题：

Windows 的密码同步

CA Identity Manager 可以截获对本地 Windows 帐户密码的更改，并将新密码传播到用户和属于该用户的所有帐户。

在“密码同步代理”检测到密码更改尝试时，代理会截获请求并将它发送给配给服务器。然后，配给服务器会将新密码传播到用户和与该用户关联的其他帐户。

密码同步有以下要求：

- 必须在要截获密码更改的系统上安装密码同步代理。
- 该系统必须作为已获取端点进行管理。
- 必须在“已获取端点设置”选项卡中，选中“密码同步代理已安装”复选框。
- 管理系统上的帐户必须已被浏览且关联到 CA Identity Manager 用户。
- 环境必须允许来自端点帐户的密码更改。 由具有对管理控制台的访问权限的管理员启用此功能。

重要说明！ 制定密码规则时要小心，以便实现一个密码适用于所有系统。例如，如果 Windows 密码必须是 12 个字符，则接受最多 10 个字符的密码的任何系统都将在同步期间拒绝此更改。

CA Identity Manager 服务器不了解端点上的密码限制。 密码策略用于端点帐户时，应比端点上的密码策略更严格。

安装密码同步代理

您可以在全局用户登录的任何受管理 Windows 计算机上安装密码同步代理。该代理在这些计算机上后台运行。

运行安装程序

注意以下要求：

- 配给服务器必须管理您正在安装代理的系统。
- 创建作为密码更改的管理员的用户：建议名称是 etapwsad。 此用户必须有 PasswordAdministrator 配置文件。
- 安装介质中存在两个 Windows 密码同步代理：32 位 Windows 的一个以及 64 位的一个。64 位 Windows 不支持 32 位密码同步代理。只有 32 位密码同步代理支持 FIPS。

遵循这些步骤:

1. 找到 CA Identity Manager 安装介质。
2. 浏览到 \Agent\PasswordSync or \Agent\PasswordSync-x64。
3. 运行 setup.exe。
4. 对配置向导的回应如下：
   a. 在“主机名”字段中，输入配给服务器系统的名称。
   b. 如果您的配给服务器在安装时使用了非默认端口，则根据需要更改端口。

      用于连接到配给服务器的建议的 LDAP 端口是 20390。
   c. 单击“Find domain”（查找域）按钮以检索配给服务器域。
   d. 如果为故障切换配置了您的配给服务器安装，请遵循屏幕说明添加服务器的逗号分隔列表。
   e. 单击“下一步”。
   f. 在“管理员”字段中，输入 etapwsad 作为密码同步代理的默认全局用户名称。 此用户必须有 PasswordAdministrator 配置文件。 默认情况下该用户不存在。
   g. 在“密码管理员”字段中，请输入管理员密码。
   h. 单击“下一步”。
   i. 从“端点类型”下拉列表，选择您要安装代理的主机的端点类型。
   j. 从“端点名称”下拉列表，选择在用户控制台中创建端点时使用的端点名称。
   k. 单击“配置”。
5. 在提示完成安装和重新启动时单击“完成”。

在用户控制台中更新端点

在用户控制台中，更新端点以表示已安装代理。

遵循这些步骤:

1. 登录到用户控制台。
2. 搜索安装代理的端点。
3. 单击“端点设置”选项卡。
4. 选中“安装密码同步代理”复选框。

启用密码同步的环境

在安装密码同步代理之后，要使环境能够收到在端点上做出的密码更改。 对于此任务，管理员需要对管理控制台和 CA Directory 的访问权限，才能使环境能够接受这些更改。

遵循这些步骤:

1. 对于新用户，您可以采用以下方式使用管理控制台：
   a. 选择“Environment”（环境）。
   b. 单击“Advanced Settings”（高级设置）、“Provisioning”（配给）。
   c. 选中“Enable Password Changes from Endpoint Accounts”（从端点帐户启用密码更改）复选框。
2. 对于现有的用户，在 CA Directory 中将 eTPropagatePassword 属性设置为 1。

配置密码同步代理的其他服务器

要为密码同步代理配置其他服务器，请使用“密码同步代理配置”向导。

添加密码同步代理的其他服务器

1. 运行 *password_sync_folder*\bin 中的 PwdSyncConfig.exe。
2. 输入以下配置信息：

   主机

   指定主要配给服务器的主机名。

   该选项将使用指定的主机名填充“服务器 URL”字段。

   LDAP 端口

   指定计算机连接到配给服务器时使用的端口号。

   CA Identity Manager 使用指定的主机和端口填充“服务器 URL”字段。
3. 单击“Find Domain”（查找域）按钮可获取域列表。
4. 从“域”下拉框中选择域名并单击“下一步”。

5. 使用以下格式将其他服务器的主机名和端口添加在“服务器 URL”字段中：

   ldaps://*primaryhost*:20390,ldaps://*alternatehost1*:20390

6. 单击“下一步”。
7. 填写配置向导中的剩余字段。

密码同步代理如何运行

当全局用户使用任何方式在 Windows 系统上更改其密码时，都会开始传播过程。输入密码之后，将发生以下内容：

1. Windows 操作系统进行检查以确保密码符合其密码策略。 如果 Windows 不接受该密码，更改请求将被拒绝，出现一条错误消息，且不会进行进一步操作（包括同步）。
2. 然后 Windows 系统将该密码更改请求移交给 CA Identity Manager 密码同步代理，如果配置了密码质量检查，该代理则会将该密码提交给配给服务器以进行密码质量检查。 如果该密码不符合 CA Identity Manager 质量规则，更改请求将被拒绝，且出现一条错误消息。 该 Windows 密码保持不变，且不会进行同步。
3. 符合 Windows 和 CA Identity Manager 质量规则的密码会被密码同步代理提交到配给服务器进行传播。
4. 之后 CA Identity Manager 更新该全局用户密码，并将该新密码传播到与该全局用户关联的部分或全部帐户。

注意：Windows 和 CA Identity Manager 的密码策略必须相同或一致，因为显示的错误消息是基于 Windows 密码策略的，即使 CA Identity Manager 拒绝了该请求也是如此。

password_update_timeout 配置参数 (eta_pwdsync.conf) 指定 PSA 等待来自 CA Identity Manager 服务器的密码 - 更改 - 传播确认的时间长度（以秒为单位）。如果 PSA 在这段时间没收到确认，则会像传播成功一样继续，并记录一条警告 (eta_pwdsync.log)，说明无法验证该密码更改传播。 该参数的最小值是零 (0)，表示 PSA 不等待确认。 有关详细信息，请参阅配给管理器帮助中的“eta_pwdsync.conf--Configure Password Synchronization Agent”。

帐户级别密码质量检查

在受管理端点上创建或修改帐户或设置全局用户密码时，将执行密码质量检查。针对帐户的密码质量检查仅限于基于密码中字符的检查。 对于帐户不会进行针对全局用户的、基于最近更改历史（密码更新频率和密码重用频率）的检查，因为 CA Identity Manager 无法截获帐户密码的所有密码更改。 因此，它没有执行这些检查所使用的准确密码更改历史。

帐户密码的检查受下列域配置参数控制：

- 端点类型/检查帐户密码
- 端点类型/检查空帐户密码

上述两个参数值为每个受管理端点指定应执行的检查级别。 端点可以下列方法指定：

ALL
-ALL
<命名空间名称>
-<命名空间名称>
<命名空间名称>：<目录名称>
-<命名空间名称>：<目录名称>

带减号 (-) 的格式禁用该参数。不带减号的格式启用该参数。[-]<命名空间名称> 格式控制所表明端点类型的所有端点，而
<命名空间名称>:<目录名称> 格式控制单个的端点。[-]ALL 格式控制所有端点类型的所有端点。 两个参数的默认值均为 -ALL。

每个参数都可多次指定。 如果多个值指定同一个端点，则使用最后一个值。 您可以将一般规则放在前面，将特定规则放在后面，以覆盖一般规则。

检查帐户密码参数提供的检查等同于全局用户密码质量检查。 为端点启用该参数的情况下，CA Identity Manager 将检查对现有帐户所请求更改中的任何密码，其中包括设置空密码的尝试。 如果在帐户创建期间未提供密码，则不执行密码质量检查。

检查空帐户密码会对创建帐户时的空密码进行附加检查。 如果启用了密码配置文件并且要求至少一个字符的密码，则空密码将导致帐户创建失败。 之所以将该参数与检查帐户密码分隔开来，是因为在一些端点类型中可以接受创建无密码的帐户。

注意：如果提供的密码与当前全局用户密码相匹配，则会忽略同步帐户密码的帐户密码质量检查。

密码质量强制

“密码同步”选项会截获本机系统（例如 Windows NT/ADS）上的密码更改请求，并将这些请求提交给 CA Identity Manager 服务器。 该服务器将全局用户密码与该全局用户关联的帐户密码进行同步。 密码配置文件的 CA Identity Manager 密码质量规则和本机系统密码质量规则 (Windows NT/ADS) 都可用于执行密码质量控制。

配置密码同步

密码同步代理最初在安装期间配置，并且可随时使用“密码同步配置”向导进行重新配置。 进一步配置是可行的。 例如，您可以使用 eta_pwdsync.conf 文件更改密码质量检查的设置，或修改超时的设置。

此文件位于 password_sync_folder\data\ 文件夹。 此配置文件中的所有密钥均已在密码同步代理的安装期间设置。 因此，只在必要时更改这些密钥。 有关详细信息，请参阅此文件内容。

重要说明！ 作为预防措施，在编辑配置文件之前请创建备份。

[Server] 部分

键	说明	默认
host	指定管理密码传播的域服务器。	无
port	指定配给服务器的 LDAP 侦听端口。	20411
use_tls	指定是否将 TLS/SSL 用于密码同步代理和配给服务器之间的安全通信。	是
admin_suffix	指定密码同步代理用来登录到 CA Identity Manager 的管理用户的域后缀。	无
admin	指定密码同步代理用来登录到 CA Identity Manager 的管理用户的帐户名称。	无
password	指定在管理密钥中指定的帐户名称的密码。	无

[eTaDomain] 部分

键	说明	默认
Domain	指定您安装密码同步代理的配给域。	无
etrust_suffix	为总体 CA Identity Manager 产品指定后缀。	无
domain_suffix	为配给域指定域后缀。	无

键	说明	默认
endpoint type	指定您安装密码同步代理的端点类型。	无
endpoint	指定密码同步代理截获密码的端点。	无
endpoint_dn	指定端点的识别名称。	无
container_dn	指定容器的识别名称，这一容器包含要更改密码的帐户。	无
acct_attribute_name	指定帐户的属性名称，例如，针对 Windows NT 的 eTN16AccountName。	取决于端点类型
acct_object_class	指定帐户的 objectClass。	取决于端点类型

[PasswordProfile] 部分

键	说明	默认
profile_enabled	指定是否启用密码配置文件检查功能。	否
profile_dn	指定密码配置向导是否为密码配置文件生成 DN。	eTPasswordProfileName=Password Profile,eTPasswordProfileContainerName=Password Profile,eTNamespaceName=CommonObjects,dc=cai,dc=eta

[Timeout] 部分

键	说明	默认
search_acct_dn	指定在搜索帐户 DN 时的超时值。	120 秒
pwd_update	指定传播密码时的超时值。	400 秒
pwd_quality_check	指定执行密码质量检查时的超时值（以秒为单位）。	1

[Logs] 部分

键	说明	默认
log_file	指定包含来自密码同步代理所记录消息的日志文件。	..\Program files\CA\Identity Manager Password Sync Agent
log_level	指定日志记录的级别。 有效值为： 1－初始文件 2－密码更新成功或失败 3－连接调试 4－跟踪	0，无日志记录

故障转移

如果配给服务器关闭或重载，密码同步代理可以实现对其他服务器的故障切换。故障切换要求多个配给服务器为同一域服务，而此代理使用那些服务器。

"配置代理以使用备用服务器" (p. 105)部分提供了配置说明。

启用日志消息

要了解密码修改被拒绝的原因，请查看从密码同步代理发出的日志消息。 所有日志消息均存储在 eta_pwdsync.log 文件中。默认情况下，该文件位于..\Program files\CA\CA Identity Manager Password Sync Agent 文件夹中。

PSA 日志记录（进入 eta_pwdsync.log 文件）具有以下消息：

- 错误消息，总是进行记录。
- 诊断（过程流、跟踪）消息，可以基于 eta_pwdsync.conf 文件中的 logging_enabled=yes|no 参数值进行启用或禁用。

要更好地诊断问题，请查看同样时间段的 eta_pwdsync.log 和配给服务器日志。

以前的 log_level 配置参数已被取代，但是仍然保留该参数以便实现向下兼容性：log_level=0 转换为了 logging_enabled=no，log_level= 其他任何内容转换为了 logging_enabled=yes。 如果配置文件中同时存在新旧两种参数，logging_enabled=yes|no 的明确设置将覆盖通过旧的 log_level=数字执行的间接设置。

注意：以前 eta_pwdsync.log 中包括了可用连接器的列表，但是该代理现在不再提供该信息。

验证安装

在密码同步代理安装完成之后，请在 Windows 系统上更改密码，以确认与帐户相关联的全局用户密码也会进行更改。

UNIX 和 Linux 的密码同步

CA Identity Manager 可以在 UNIX 或 Linux 系统上截获帐户的密码更改，并且将它传播到与其全局用户关联的所有其他帐户。 针对外部安全系统对密码进行身份验证所用的组件叫做可插入身份验证模块 (PAM)。 使用 PAM，CA Identity Manager 可针对外部安全系统对密码进行身份验证，以便全局用户可以使用他们现有的系统密码登录到 CA Identity Manager。

UNIX 密码同步

提供的密码同步模块可通过 UNIX PAM 框架检测密码更改事件。 UNIX 密码同步模块可向配给服务器发送密码更改通知。 配给服务器可找到关联的全局用户，并自动地将更改传播到其他相关帐户。

支持 PAM 框架的 UNIX 操作系统包括：

- 已启用 PAM 的 AIX v5.3 on Power 平台
- PA-RISC 平台以及 Itanium® 2 平台上的 HP-UX v11.00
- Sparc 和 Intel 平台上的 Solaris v2.6 和更高版本
- s390 或 Intel i386 平台上的 32 位 Linux，带 glibc v2.2 和更高版本

  注意：对于 Linux 平台，test_sync 二进制必须安装在所有用户的 PATH 上，但是只有所有者 root 用户才有执行许可。

  要将此库添加到所有用户的路径中，请在全局 /etc/bashrc 文件中加入以下命令：

  ```
  export PATH=$PATH:/etc/pam_CA_eta
  ```

UNIX PAM 的工作方式

以下过程描述 UNIX PAM 功能：

1. 可因下列理由之一更改 UNIX 用户密码：
   - 用户的决定。
   - 用户只能通过系统设置或手工干预更改密码。
   - 管理员更改了用户的密码。
2. 新密码会提交给 PAM 框架密码服务。
3. PAM 框架的密码服务可调用 PAM 库以更新本地的 UNIX 安全文件。
4. PAM 框架的密码服务可调用 UNIX 密码同步模块 (pam_CA_eta)，以便向配给服务器发送密码更改通知。
5. 配给服务器可更新关联的全局用户以及与全局用户关联的所有帐户的密码。

使用 UNIX 密码同步的要求

以下为使用 UNIX 密码同步功能的要求：

- UNIX 密码同步代理必须安装在您想检测密码更改的 UNIX 系统上。
- UNIX Remote Agent 和 CAM 必须安装在 UNIX 密码同步代理驻留的 UNIX 系统上。
- 该系统必须作为已获取端点进行管理。 在已获取端点属性中，必须选中“密码同步代理已安装”复选框。
- 该管理系统上的帐户必须已浏览且关联到全局用户。
- 环境必须允许来自端点帐户的密码更改。 由具有对管理控制台的访问权限的管理员启用此功能。

安装 UNIX PAM 功能

执行以下程序，以便安装 UNIX PAM。

安装 UNIX PAM 功能

1. 选择与您的 UNIX 平台相对应的程序包文件：

UNIX 操作系统	程序包文件名称
HP-UX v11 PA-RISC	pam_CA_eta-1.1.HPUX.tar.Z
HP-UX Itanium2	pam_CA_eta1.1HPUX-IA64.tar.Z
AIX v5.3 Power	pam_CA_eta-1.1.AIX.tar.Z
Solaris Sparc	pam_CA_eta-1.1.Solaris.tar.Z
Solaris Intel	pam_CA_eta-1.1.SolarisIntel.tar.Z
Linux x86	pam_CA_eta-1.1.Linux.tar.gz
Linux s390	pam_CA_eta-1.1.LinuxS390.tar.gz

2. 使用 FTP，采用二进制模式或支持二进制文件的任何其他文件传输工具，将选中的程序包文件传输到 UNIX 服务器上的临时文件夹 (/tmp) 中。示例传输会话可能显示以下内容：

```
W:\Pam>ftp user01
Connected to user01.company.com.
220 user01 FTP server (Version 1.2.3.4) ready.
User (user01.company.com:(none)): root
331 Password required for root.
Password:
230 User root logged in.
ftp> cd /tmp
250 CWD command successful.
ftp> bin
200 Type set to I.
ftp> put pam_CA_eta-1.1.HPUX.tar.Z
200 PORT command successful.
150 Opening BINARY mode data connection for pam_CA_eta-1.1.HPUX.tar.Z.
226 Transfer complete.
ftp: 117562 bytes sent in 0,09Seconds 1306,24Kbytes/sec.
ftp> quit
```

3. 登录为 UNIX 服务器上的 root 用户，并解压缩程序包文件：

```
# cd /tmp
# zcat pam_CA_eta-1.1.<platform>.tar.Z | tar -xf -
```

在 Linux 上，使用命令：

```
# tar -xzf pam_CA_eta-1.1.<platform-hardware>.tar.gz
```

4. 将配置和 TLS 文件复制到默认配置文件夹：

```
# cd pam_CA_eta-1.1
# mv pam_CA_eta /etc
```

5. 将 pam_CA_eta 模块复制到安全库文件夹：

在 AIX 平台上，使用命令：

```
# cp -p pam_CA_eta.o /usr/lib/security/
```

在 HP-UX 平台上，使用命令：

```
# cp -p libpam_CA_eta.1 /usr/lib/security/
```

在 HP-UX Itanium2 上，使用命令：

```
# cp -p libpam_CA_eta.1 /usr/lib/security/hpux32
```

在 Linux i386 或 s390 上，使用命令：

```
# cp -p pam_CA_eta.so /lib/security/
```

在 Solaris Sparc 或 Intel 上，使用命令：

```
# cp -p pam_CA_eta.so /usr/lib/security/
```

6. （可选）复制测试程序：

```
# cp -p test_* /etc/pam_CA_eta
# cp -p pam_test* (/usr)/lib/security/
```

更多信息

UNIX 密码同步故障排除 (p. 120)

在用户控制台中更新端点

在用户控制台中，更新端点以表示已安装代理。

遵循这些步骤:

1. 登录到用户控制台。
2. 搜索安装代理的端点。
3. 单击“端点设置”选项卡。
4. 选中“安装密码同步代理”复选框。

启用密码同步的环境

在安装密码同步代理之后，要使环境能够收到在端点上做出的密码更改。 对于此任务，管理员需要对管理控制台和 CA Directory 的访问权限，才能使环境能够接受这些更改。

遵循这些步骤:

1. 对于新用户，您可以采用以下方式使用管理控制台：
   a. 选择“Environment”（环境）。
   b. 单击“Advanced Settings”（高级设置）、“Provisioning”（配给）。
   c. 选中“Enable Password Changes from Endpoint Accounts”（从端点帐户启用密码更改）复选框。
2. 对于现有的用户，在 CA Directory 中将 eTPropagatePassword 属性设置为 1。

配置 UNIX 密码同步功能

配置 UNIX 密码同步功能涉及设置下列文件中的参数：

- /etc/pam_CA_eta/pam_CA_eta.conf
- /etc/pam.conf

重要说明！ 因为高权限用户的密码存储在 pam_CA_eta.conf 配置文件中，该文件只能供 root 帐户读取。 请注意，程序包文件的文件设置包括 owner=root 和 mode=500，cp 命令的 -p 开关在安装期间保留这些设置。

配置 pam_CA_eta.conf 文件

执行以下程序，以便配置 pam_CA_eta.conf 文件。

配置 pam_CA_eta.conf 文件

1. 导航到 /etc/pam_CA_eta 文件夹。
2. 编辑 pam_CA_eta.conf 文件。 此配置文件包含自己的文档。

```
#
#   CA - CA Identity Manager
#
#   pam_CA_eta.conf
#
#   Configuration file for the Unix PAM password module "pam_CA_eta"
#

# keyword: server
# description: the CA Identity Manager LDAP server primary and optional
alternate server hostname
# value: a valid hostname and an optional server
# default: no default
server ETA_SERVER ALT_SERVER

#

# keyword: port
# description: the numeric TCP/IP port number of the CA Identity Manager LDAP
server
# value: a valid TCP/IP port number
# default: 20390
# port 20390


# keyword: use-tls
# description: does it use the secured LDAP over TLS protocol ?
# value: yes or no
# default: yes
# use-tls yes
```

```
# keyword: time-limit
# description: the maximum time in seconds to wait for the end of an LDAP
operation.
# value: a numeric value of seconds
# default: 300
# time-limit 300

# keyword: remote-server
# description: identifies whether on premise or cloud Identity Manager
#              server is used.
#              Cloud based server is accessed by proxying the requests
#              through the on-premise CS, requiring use of remote-server
#              set to 'yes'.
# value: yes or no
# default: no
# remote-server no

# keyword: size-limit
# description: the maximum number of entries returned by the CA Identity
Manager server
# value: a numeric value
# default: 100
# size-limit 100


# keyword: root
# description: the root DN of the CA Identity Manager server
# value: a valid DN string
# default: dc=eta
# root dc=eta


# keyword: domain
# description: the name of the CA Identity Manager domain
# value: a string
# default: im
# domain    im


# keyword: user
# description: the CA Identity Manager Global User name used to bind to the
CA Identity Manager server
# value: a valid Global User name string
# default: etaadmin
# user etaadmin


# keyword: password
# description: the clear-text password of the "binding" CA Identity Manager
Global User
# value: the password of the above Global User
# default: no default
password SECRET


# keyword: directory-type
# description: the CA Identity Manager Unix Endpoint type of this Unix server
```

```
# value: ETC or NIS
# default: ETC
# endpoint-type ETC


# keyword: endpoint-name
# description: the CA Identity Manager Unix Endpoint name of this Unix server
# value: a valid Unix Endpoint name string
# default:
# ETC: the result of the "hostname" command (ie: gethostname() system call)
# NIS: "domain [hostname]" where "domain" is the result of the "domainname"
command
#  (ie: getdomainname() system call) and "hostname" the result of the
"hostname"
#    command (ie: gethostname() system call)
# endpoint-name dirname


# keyword: tls-cacert-file
# description: the name of the CA Identity Manager CA certificate file
# value: a valid full path file name
# default: /etc/pam_CA_eta/et2_cacert.pem
# tls-cacert-file /etc/pam_CA_eta/et2_cacert.pem


# keyword: tls-cert-file
# description: the name of the CA Identity Manager client certificate file
# value: a valid full path file name
# default: /etc/pam_CA_eta/eta2_clientcert.pem
# tls-cert-file /etc/pam_CA_eta/eta2_clientcert.pem


# keyword: tls-key-file
# description: the name of the CA Identity Manager client private key file
# value: a valid full path file name
# default: /etc/pam_CA_eta/eta2_clientkey.pem
# tls-key-file /etc/pam_CA_eta/eta2_clientkey.pem


# keyword: tls-random-file
# description: the name of the "pseudo random number generator" seed file
# value: a valid full path file name
# default: /etc/pam_CA_eta/prng_seed
# tls-random-file /etc/pam_CA_eta/prng_seed


# keyword: use-status
# description: this module will exit with a non-zero status code in case of
failure.
# value: yes or no
# default: no
# use-status no


# keyword: verbose
# description: this module will display informational or error messages to
the user.
```

```
# value: yes or no
# default: yes
# verbose yes
```

注意：服务器、域和密码参数没有默认值，需要更新。

配置 pam.conf 文件

/etc/pam.conf 文件是主要的 PAM 配置文件。您必须编辑文件，以便在密码服务堆栈中插入行。在一些 Linux 系统上，pam.conf 文件被替换成 /etc/pam.d，因此您需要编辑 /etc/pam.d/system-auth 文件。

配置 pam.conf 文件

1. 导航到 /etc 目录，或 /etc/pam.d 目录（如果您正在相应的 Linux 系统上配置 PAM 模块）。
2. 编辑 pam.conf 文件，以便在密码服务堆栈中插入密码同步行。 有关特定平台的配置，请参阅下列示例：

   passwd password required /usr/lib/security/pam_unix.so

   passwd password optional /usr/lib/security/pam_CA_eta.so

3. （可选）您可以在 pam_CA_eta 模块行上，添加以下可选的参数：

   config=/path/file

   指示备选配置文件的位置。

   syslog

   将错误和通知消息发送到本地的 syslog 服务。

   trace

   为每次密码更新操作生成跟踪文件。 跟踪文件被命名为 /tmp/pam_CA_eta-trace.<nnnn>，其中 <nnnn> 是密码进程的 PID 编号。

4. 对特定平台实施以下配置更改：

   对于 AIX 系统，在 /etc/pam.conf 文件的底部添加下列行：

```
#
# CA Identity Manager Unix Password Synchronization
#
login   password  optional    /usr/lib/security/pam_CA_eta.so syslog
passwd  password  optional    /usr/lib/security/pam_CA_eta.so syslog
rlogin  password  optional    /usr/lib/security/pam_CA_eta.so syslog
su      password  optional    /usr/lib/security/pam_CA_eta.so syslog
telnet  password  optional    /usr/lib/security/pam_CA_eta.so syslog
sshd    password  optional    /usr/lib/security/pam_CA_eta.so syslog
OTHER   password  optional    /usr/lib/security/pam_CA_eta.so syslog
```

   对于 HP-UX 系统，在 /etc/pam.conf 文件的底部添加下列行：

```
#
# CA Identity Manager Unix Password Synchronization
#
login    password optional    /usr/lib/security/libpam_CA_eta.1 syslog
passwd   password optional    /usr/lib/security/libpam_CA_eta.1 syslog
dtlogin  password optional    /usr/lib/security/libpam_CA_eta.1 syslog
dtaction password optional    /usr/lib/security/libpam_CA_eta.1 syslog
OTHER    password optional    /usr/lib/security/libpam_CA_eta.1 syslog
```

   对于 HP-UX Itanium2，在 /etc/pam.conf 文件的底部添加下列行：

```
#
# CA Identity Manager Unix Password Synchronization
#
login    password optional    /usr/lib/security/$ISA/libpam_CA_eta.1 syslog
passwd   password optional    /usr/lib/security/$ISA/libpam_CA_eta.1 syslog
dtlogin  password optional    /usr/lib/security/$ISA/libpam_CA_eta.1 syslog
dtaction password optional    /usr/lib/security/$ISA/libpam_CA_eta.1 syslog
OTHER    password optional    /usr/lib/security/$ISA/libpam_CA_eta.1 syslog
```

   对于 Sun Solaris 系统，在现有的 pam_unix 行之后添加 pam_CA_eta 行：

```
#
# Password management
#
other   password required       /usr/lib/security/pam_unix.so.1
other   password optional       /usr/lib/security/pam_CA_eta.so syslog
```

对于 Linux 系统，在现有的 pam_cracklib 行与 pam_unix 行之间添加 pam_CA_eta 行：

```
password    required     /lib/security/pam_cracklib.so retry=3 type=
password    optional     /lib/security/pam_CA_eta.so syslog
password    sufficient   /lib/security/pam_unix.so nullok use_authtok md5
shadow
password    required     /lib/security/pam_deny.so
```

5. 对于 AIX 系统，编辑 /etc/security/login.cfg 文件，设置 auth_type = PAM_AUTH。 这会启用 PAM 框架（默认情况下不会启用）。 这是运行时设置，因此无需重新启动系统即可使其生效。

UNIX 密码同步故障排除

您可以使用 syslog 和跟踪消息，通过测试配置、LDAP/TLS 连接、密码同步以及 PAM 框架，排除 UNIX PAM 功能的故障。

更多信息

激活 Syslog 消息 (p. 120)
激活跟踪消息 (p. 120)

激活 Syslog 消息

将 syslog 参数添加到 /etc/pam.conf 文件的 pam_CA_eta 行中，以便允许 pam_CA_eta 模块生成通知和错误消息。 如果使用日志选项，每次 UNIX 帐户更改其密码时，UNIX 管理员都会在 syslog 文件中看见通知消息。 这些消息应当提供了诊断基本问题的足够信息。

您可以在生产系统上永久性地设置此选项，因为它需要的资源不会比运行在无提示服务下时多很多。

激活跟踪消息

如果 Syslog 消息没有提供足够信息，跟踪方式可以提供更多的细节。 对于每次密码更新操作，跟踪模块都会生成名为 /tmp/pam_CA_eta-trace.<nnnn>（其中 <nnnn> 是 passwd 进程的 PID）的文件，为模块使用的大部分函数调用和那些函数使用或返回的数据提供入口。

即使跟踪文件只能供 root 帐户读取，它们也将包含新的明文密码。 鉴于此，此参数不应当永久性地用在生产系统上。

测试配置文件

您可以使用位于 /etc/pam_CA_eta 目录的 test_config 工具，验证配置文件。 首先，您按以下方式设置文件夹结构：

1. 将 pam_CA_eta 文件夹移动到 /etc 下。
2. 将 pam_CA_eta-1.1 下的所有内容复制到 /etc/pam_CA_eta。

示例命令行条目如下所示：

```
/etc/pam_CA_eta/test_config [config=/path/to/config_file]
```

示例会话如下所示：

```
/test_config [config=/path/to/config_file]
# ./test_config
./test_config: succeeded
Trace file is /tmp/test_config-trace.1274
```

正如命令输出显示，系统会生成跟踪文件，其中包含配置文件解析的所有详细信息。

查看 CAM 服务

您可以执行以下程序找出服务启动方。

查看 CAM 服务

1. 使用 Telnet 或 SSH 客户端，以 root 身份登录到您的 UNIX 计算机。
2. 发布以下 UNIX 命令：

   ```
   ps -ef | grep cam
   ```

   此时会出现类似于以下内容的显示内容：

   ```
   root 13822        1 11 11:30:12 ?   0:00 cam

   root 13843 13753  3 11:56:31 pts/5  0:00 grep cam
   ```

注意：如果系统的 root 用户未启动服务，它们看起来会像已启动，但您却无法使用它们。 CA Identity Manager 发布以下消息：“Permission denied: user must be root”（权限被拒: 用户不是 root 用户）。

测试 LDAP/TLS 连接

您可以使用 /etc/pam_CA_eta 目录下的 test_ldap 工具来验证与配给服务器的连接（使用配置文件参数）。 示例命令行条目如下所示：

```
/etc/pam_CA_eta/test_ldap [config=/path/to/config_file]
```

示例会话如下所示：

```
./test_ldap [config=/path/to/config_file]
# ./test_ldap: succeeded
Trace file is /tmp/test_ldap-trace.1277
```

正如命令输出显示，系统会生成跟踪文件，其中包含配置文件解析以及与配给服务器连接的所有详细信息。

测试密码同步

您可以使用位于 /etc/pam_CA_eta 文件夹的 test_sync 工具来验证本地帐户的密码更新已为配给服务器有效地传播。 示例命令行条目如下所示：

```
/etc/pam_CA_eta/test_sync <user> <password> [config=/path/to/config_file]
```

示例会话如下所示：

```
# /etc/pam_CA_eta/test_sync pam002 newpass1234
CA Identity Manager password synchronization started.
:ETA_S_0245<MGU>, Global User 'pam002' and associated account passwords updated
successfully: (accounts updated: 2, unchanged: 0, failures: 0)
CA Identity Manager password synchronization succeeded.
/etc/pam_CA_eta/test_sync: succeeded
Trace file is /tmp/test_sync-trace.2244
```

正如命令输出显示，系统会生成跟踪文件，其中包含配置文件解析、与配给服务器的连接以及帐户更新的所有详细信息。

使用 verbose 模式（通过在配置文件中使用默认的 verbose yes 参数）时，此命令提供关于密码传播的通知消息和可能的错误消息。

测试 PAM 框架

PAM 测试库可用来验证 PAM 框架已正确地检测到密码更改。

测试 PAM 框架

1. 将 pam_test 文件复制到 /usr/lib/security(/hpux32) 文件夹。
2. 为没有参数的 pam_test 库添加密码类行。

   Solaris 的示例如下：

   ```
   other password optional /usr/lib/security/pam_test
   ```

3. 对测试用户发出 passwd 命令，然后搜索 syslog 文件的 pam_test [<pid>] 标记行。

   命令输出显示生成的跟踪文件的名称，例如：

   ```
   pam_test[1417]: Succeeded, trace file is /tmp/pam_test-trace.1417
   ```

在 OS400 上的密码同步

密码同步代理允许在 OS/400 端点系统上进行的密码更改传播到由 CA Identity Manager 管理的其他帐户。 密码同步代理的工作方式如下所示：

1. 在 OS/400 端点系统上安装并且执行代理

   作为安装过程的一部分，程序会注册到 OS/400 系统，以便用户更改它们的密码时，让代理将密码更改发送到配给服务器上。

2. 配给服务器将密码更改传播到关联的帐户。

   代理可以接收通过“更改密码”命令 (CHGPWD) 或“更改密码 (QSYCHGPW) API”启动的密码更改。

3. 代理会将成功或失败操作记录到位于 PWDSYNCH/LOG 的日志文件中。

下列平台支持密码同步代理：

- OS400 V5R2
- OS400 V5R3
- OS400 V5R4

安装密码同步代理

1. 找到配置组件安装介质。
2. 在 \Agent 之下运行密码同步代理安装程序或 OS/400
3. 遵循屏幕上的说明完成安装。

   注意：以下部分包含了端点代理软件链接中的安装说明。

安装 OS400 密码同步代理

要让代理接收密码更改通知，您必须有 *ADDOBJ 权限，并且以下内容是必不可少的：

- 系统值 QPWDVLDPGM 必须被设置成 *REGFAC
- 必须使用命令 WRKREGINF EXITPNT(QIBM_QSY_VLD_PASSWRD) 注册程序
- 环境必须允许来自端点帐户的密码更改。 由具有对管理控制台的访问权限的管理员启用此功能。

仅在进行密码更改时启动代理。 要更改密码，请发出 CHGPWD 命令。

注意：必须针对密码同步对全局用户进行标记。

在 iSeries 上

1. 以拥有 *ALLOBJ 和 *SECADM 权限的用户身份（例如 QSECOFR）登录。
2. 创建名为 PWDSYNCH 的用户：

   ```
   CRTUSRPRF USRPRF(PWDSYNCH) PWDEXP(*YES)
   ```

   注意：出于安全考虑，会使用到期的密码创建用户。
3. 创建 savefile 以将安装程序包存储在您选择的库中（例如 MYLIB）：

   ```
   CRTSAVF MYLIB/PWDSYNCH
   ```
4. 在配有 savefile 的 Windows 计算机上，使用 FTP 将 savefile 传输到 iSeries：

   ```
   ftp <hostname>
   二进制
   cd MYLIB
   put PWDSYNCH.FILE
   ```
5. 在 iSeries 上，从 savefile 提取程序：

   ```
   RSTLIB SAVLIB(PWDSYNCH) DEV(*SAVF) SAVF(MYLIB/PWDSYNCH)
   ```

   此命令会对同步代理解压缩，并将其安装到 PWDSYNCH 库里。
6. 验证安装：

   ```
   DSPLIB PWDSYNCH
   ```

   应当显示下列对象：

对象	类型	属性
PWDSYNCH	*PGM	CLE
CONFIG	*FILE	PF
LOG	*FILE	PF

7. 设置 iSeries，以便使用 PWDSYNCH 作为密码验证 exit 程序：

   ```
   CHGSYSVAL SYSVAL(QPWDVLDPGM) VALUE(*REGFAC)
   ADDEXITPGM EXITPNT(QIBM_QSY_VLD_PASSWRD) FORMAT(VLDP0100) PGMNBR(1)
   PGM(PWDSYNCH/PWDSYNCH) TEXT('eTrust Admin Password Synch Agent')
   ```

8. 在 iSeries 上，指定您的 CA IAM Connector Server 的连接参数：

   ```
   EDTF FILE(PWDSYNCH/CONFIG)
   ```

安装 OS400 密码同步代理

要让代理接收密码更改通知，您必须有 *ADDOBJ 权限，并且以下内容是必不可少的：

- 系统值 QPWDVLDPGM 必须被设置成 *REGFAC
- 必须使用命令 WRKREGINF EXITPNT(QIBM_QSY_VLD_PASSWRD) 注册程序
- 环境必须允许来自端点帐户的密码更改。 由具有对管理控制台的访问权限的管理员启用此功能。

仅在进行密码更改时启动代理。 要更改密码，请发出 CHGPWD 命令。

注意：必须针对密码同步对全局用户进行标记。

在 iSeries 上

1. 以拥有 *ALLOBJ 和 *SECADM 权限的用户身份（例如 QSECOFR）登录。
2. 创建名为 PWDSYNCH 的用户：

   ```
   CRTUSRPRF USRPRF(PWDSYNCH) PWDEXP(*YES)
   ```

   注意：出于安全考虑，会使用到期的密码创建用户。

3. 创建 savefile 以将安装程序包存储在您选择的库中（例如 MYLIB）：

   ```
   CRTSAVF MYLIB/PWDSYNCH
   ```

4. 在配有 savefile 的 Windows 计算机上，使用 FTP 将 savefile 传输到 iSeries：

   ```
   ftp <hostname>
   二进制
   cd MYLIB
   put PWDSYNCH.FILE
   ```

5. 在 iSeries 上，从 savefile 提取程序：

   ```
   RSTLIB SAVLIB(PWDSYNCH) DEV(*SAVF) SAVF(MYLIB/PWDSYNCH)
   ```

   此命令会对同步代理解压缩，并将其安装到 PWDSYNCH 库里。

6. 验证安装：

   ```
   DSPLIB PWDSYNCH
   ```

   应当显示下列对象：

对象	类型	属性
PWDSYNCH	*PGM	CLE
CONFIG	*FILE	PF
LOG	*FILE	PF

7. 设置 iSeries，以便使用 PWDSYNCH 作为密码验证 exit 程序：

```
CHGSYSVAL SYSVAL(QPWDVLDPGM) VALUE(*REGFAC)
ADDEXITPGM EXITPNT(QIBM_QSY_VLD_PASSWRD) FORMAT(VLDP0100) PGMNBR(1)
PGM(PWDSYNCH/PWDSYNCH) TEXT('eTrust Admin Password Synch Agent')
```

8. 在 iSeries 上，指定您的 CA IAM Connector Server (CA IAM CS) 的连接参数：

```
EDTF FILE(PWDSYNCH/CONFIG)
```

在用户控制台中更新端点

在用户控制台中，更新端点以表示已安装代理。

遵循这些步骤:

1. 登录到用户控制台。
2. 搜索安装代理的端点。
3. 单击“端点设置”选项卡。
4. 选中“安装密码同步代理”复选框。

启用密码同步的环境

在安装密码同步代理之后，要使环境能够收到在端点上做出的密码更改。 对于此任务，管理员需要对管理控制台和 CA Directory 的访问权限，才能使环境能够接受这些更改。

遵循这些步骤:

1. 对于新用户，您可以采用以下方式使用管理控制台：
   a. 选择“Environment”（环境）。
   b. 单击“Advanced Settings”（高级设置）、“Provisioning”（配给）。
   c. 选中“Enable Password Changes from Endpoint Accounts”（从端点帐户启用密码更改）复选框。
2. 对于现有的用户，在 CA Directory 中将 eTPropagatePassword 属性设置为 1。

SSL 配置

SSL 用于加密同步代理和配给服务器之间的通信。 因为 SSL 会通过网络发送密码，所以这对于同步代理至关重要。 建议您一定使用 SSL。

要采用 SSL 进行连接，同步代理必须信任配给服务器的证书。 因此，必须将证书安装在 iSeries 计算机上并且完成配置，以便同步代理信任此证书。 由作为 OS/400 可选组件的数字证书管理器执行这些任务。请按照有关数字证书管理器的安装和设置的 OS/400 文档操作。

安装配给服务器证书

要使用 SSL，必须在您的 iSeries 计算机上安装下列操作系统组件：

- 加密访问服务提供商许可程序 (5722-AC3)
- 数字证书管理器（OS/400 的选项 34）
- IBM HTTP Server for iSeries (5722-DG1)

在 iSeries 上

1. 将开通服务器证书从开通服务器计算机上传到 iSeries。 证书可能位于以下路径：

   ```
   C:\Program Files\CA\Identity Manager\Provisioning
   Server\Data\Tls\server\et2_cacert.pem
   ```

2. 登录到 DCM。

   使用 Web 浏览器，转到 http://<hostname>:2001。当出现提示时，以 QSECOFR 身份登录，然后单击“数字证书管理器”。

3. 单击“选择证书存储”并选择 *SYSTEM 证书存储。 如果此存储不存在，请创建名为 *SYSTEM 的存储，然后输入证书存储密码。

4. 使用 DCM 将证书导入为 CA 证书。

   单击“管理证书”、“导入证书”。 选择“证书颁发机构 (CA)”选项，并输入开通服务器证书的文件名。 （这是您在第 1 步中上传证书的位置）。 输入证书的标签“配给服务器”。

5. 在将 CA 证书导入到端点 *SYSTEM 密钥库之后，请确认 IBM Directory 客户端 QIBM_GLD_DIRSRV_CLIENT 能够访问 *SYSTEM 密钥库。 否则，PSA 的 SSL 初始化调用会失败。

6. 配置“目录服务客户端”应用程序以信任开通服务器证书，方法是打开“管理应用程序”、“定义 CA 信任列表”，然后选择“目录服务客户端”。

   如果已在第 4 步中正确地导入证书，配给服务器证书应当在此处列出。

   单击“信任开通服务器证书”，然后单击“确定”。

7. 将 PUBLIC 读取权限授予 SSL 文件，并将读取访问权限授予 *SYSTEM 证书存储：

   (/QIBM/userdata/ICSS/Cert/Server/default.kdb)

   将读取和执行权限授予父文件夹

   (/QIBM/userdata/ICCS/Cert/Server)

   注意：采取用户 PWDSYNCH 的授权不会对 / 文件系统起作用，因此必须将访问权限授予所有用户。

卸载密码同步代理

如果您需要卸载密码同步代理，请按照以下步骤进行操作。

从密码验证出口点中

1. 删除 PWDSYNCH：

   ```
   RMVEXITPGM EXITPNT(QIBM_QSY_VLD_PASSWRD) FORMAT(VLDP0100) PGMNBR(1)
   ```

2. 删除同步代理库：

   ```
   DLTLIB PWDSYNCH
   ```

3. 删除 PWDSYNCH 用户

   ```
   DLTUSRPRF PWDSYNCH
   ```

4. 删除配给服务器证书，方法是按照 SSL 说明登录到 DCM，并对 *SYSTEM 证书存储进行操作：

   单击“Manage Certificates”（管理证书）、“Delete Certificate”（删除证书），然后选择“Certificate Authority (CA)”。

   选中“Provisioning Server”（配给服务器）证书，然后单击“Delete”（删除）。

OS/400 密码代理参数必须正确设置

必须正确设置“pwd_case_action”参数值才能工作。 正确的值包括：

- pwd_case_action = pwd_case_unchanged
- pwd_case_action = pwd_to_uppercase
- pwd_case_action = pwd_to_lowercase

如果 pwd_case_action = [无效值]，则将强制大写密码。

注意：在将标志 pwd_case_action 设置为 OS400 PSA 配置文件中的 pwd_to_uppercase 或 pwd_to_lowercase 时，如果提供的密码对开通服务器的密码策略设置不兼容，则密码可能不被传播回到全局用户。 例如，一些密码策略可能需要至少包含 1 个大写或小写值的密码值。

注意：在配置密码同步代理时，请注意 QPWDLVL（密码级别）系统值

- 在 AS400 系统上，当 QPWDLVL 设为 0（默认值）时，支持包含 1 到 10 个大写字符的密码。
- 当 QPWDLVL 设为 2 或 3 时，允许使用包含 1 到 128 个混合大小写字符的密码。

默认情况下，PSA 将未更改的密码传播到配给服务器。 但您也可以忽略 QPWDLVL 的值，通过将“pwd_case_action”设置为“pwd_to_uppercase”或“pwd_to_lowercase”，强制 PSA 传播仅包含大写字符或仅包含小写字符的密码。

第 7 章： 组

可以创建多种类型的组或这些类型的组合：

- 静态组 - 交互式添加的用户列表
- 动态组 - 属于满足 LDAP 查询（需要 LDAP 目录作为用户存储）的组的用户

  注意：即使组的 directory.xml 中存在此字段，“动态组查询”字段也不包括在创建组任务或其他组任务中。 通过编辑关联的配置文件屏幕，可将“动态组查询”字段包括在任务中。
- 嵌套组 - 包含其他组（需要 LDAP 目录作为用户存储）的组

注意：要查看用户所属的静态组、动态组和嵌套组，请使用“用户”对象的“组”选项卡。 默认情况下，此选项卡显示在“查看用户”和“修改用户”任务中。

此部分包含以下主题：

创建静态组

可以将*静态组*中的一组用户关联起来。 通过在组的成员资格列表中添加或删除单个用户管理静态组。 要查看组的成员资格列表，请使用“成员资格”选项卡，默认情况下，此选项卡包括在“查看和修改组”任务中。

注意：“成员资格”选项卡仅显示显式添加至组中的成员。 并不显示动态添加的成员。

创建静态组：

1. 在用户控制台中，依次选择“组”、“创建组”。
2. 选择创建一个新组或创建某个组的副本，然后单击**确定**。
3. 在“配置文件”选项卡上，输入组名称、组组织、说明和组管理员名称。
4. 单击“成员资格”选项卡。
5. 单击“添加用户”。
6. 搜索要包括在组中的用户。
7. 选中要包括的用户旁边的复选框，然后单击“选择”。
8. 单击“提交”。

创建动态组

您可以通过使用用户控制台定义 LDAP 筛选查询的方式来创建*动态组*，以便在运行时动态确定组员资格，而无需单独搜索并添加用户。

例如，如果要生成列出 NeteAuto 所有美国员工的组，那么可以在用户控制台的“动态组查询”字段中定义一个类似以下内容的 LDAP 搜索筛选：

ldap:///cn=Employees,o=NeteAuto,c=US??sub

您也可以修改此查询以找出美国以外的员工。

静态组、动态组和嵌套组示例 (p. 136)展示了一个由静态组、动态组和嵌套组创建的组的示例。

通过编辑关联的配置文件屏幕，可将“动态组查询”字段包括在任务中。 默认情况下，“创建组”任务中并不包括该字段。

注意：要启用动态组，系统管理员需要在目录配置文件 (directory.xml) 中配置支持：

- 在“目录组行为”部分中，添加如下 GroupTypes 元素：

  <GroupTypes type=*type*>

  type 可以是 NESTED (p. 134)、DYNAMIC 或 ALL。

  GroupTypes 区分大小写。
- 将 %DYNAMIC_GROUP_MEMBERSHIP% 常用属性映射到用户存储中存在的物理属性。

创建动态组：

1. 在用户控制台中，依次选择“组”、“创建组”。
2. 选择创建一个新组或创建某个组的副本，然后单击**确定**。
3. 在“配置文件”选项卡上，输入组名称、组组织、说明和组管理员名称。
4. 在“动态组查询”字段中输入一个 LDAP 搜索筛选，如下例所示：

   ldap:///cn=Employees,o=NeteAuto,c=US??sub
5. 单击“提交”。

注意：只有具有“修改组”任务的管理员才能更改组的动态成员资格。

动态组查询参数

您可以在搜索中使用以下动态查询参数：

ldap:///*<search_base_DN>*??*<search_scope>*?*<searchfilter>*

- *<search_base_DN>* 是在 LDAP 目录中进行搜索的起始点。如果您未在查询中指定基本 DN，则该组的组织为默认的基本 DN。
- *<search_scope>* 指定搜索的范围，其中包括：
  - sub－返回基本 DN 及以下级别的条目
  - one－返回比您在 URL 中指定的基本 DN 低一个级别的条目。（默认）
  - base－使用 one 代替，作为搜索选项时忽略 base

  使用 one 或 base 仅获取基本 DN 组织中的用户。

  使用 sub 获取基本 DN 组织以及树中的所有下级组织下的所有用户。
- *<searchfilter>* 是您希望应用到搜索范围内的条目的筛选。 输入搜索筛选时，请使用标准 LDAP 查询语法，如下所示:

  (<逻辑运算符><比较><比较...>)
  - <逻辑运算符> 为下面任一项：

    逻辑或：|

    逻辑与：&

    逻辑非：!
  - <比较> 表示 <属性><运算符><值>

  例如：

  (&(city=boston)(state=Massachusetts))

  默认搜索筛选为 (objectclass=*)。

创建动态查询时，请注意以下事项：

- “ldap”前缀必须为小写，例如：

  ldap:///o=MyCorporation??sub?(title=Manager)
- 不能指定 LDAP 服务器主机名或端口号。 所有搜索发生在与环境关联的 LDAP 目录内。

下表包括 LDAP 查询示例：

说明	查询
所有经理用户。	ldap:///o=MyCorporation??sub?(title=Manager)

说明	查询
纽约西部分支机构的所有经理	ldap:///o=MyCorporation??one?(&(title=Manager) (roomNumber=NYWest))
所有配有手机的技术人员	ldap:///o=MyCorporation??one?(&(employeetype=technician) (mobile=*))
员工编号在 1000 至 2000 之间的所有员工	ldap:///o=MyCorporation, (& (ou=employee) (employeenumber >=1000) (employeenumber <=2000))
所有在公司供职超过 6 个月的帮助中心管理员	ldap:///o=MyCorporation,(& (cn=helpdeskadmin) (DOH => 2004/04/22) **注意：**此查询要求您为用户的入职日期创建一个 DOH 属性。

注意： > 和 <（大于和小于）比较按词典编纂顺序而非算术顺序进行。 有关其用法的详细信息，请参阅 LDAP 目录服务器相关文档。

创建嵌套组

如果用户存储为 LDAP 目录，则可以将一个组添加为另一个组的成员。该组称为*嵌套组*。

包含嵌套组的组称为*父组*。 嵌套组的成员将成为父组的成员。 但父组的成员不会成为嵌套组的成员。

电子邮件分发列表中，一个列表可成为另一个列表的成员，嵌套组与此类似。通过嵌套组，您可以将组和用户添加为组的成员。 通过将组嵌套在另一个组的成员资格列表中，您可以包括所有的嵌套组成员。

例如，如果为一家公司的生产、设计、运输和会计部门创建了独立的组，您可以通过将所有独立部门的组嵌套为公司父组的成员来为整个公司建立一个父组。 这样，您对生产、设计、运输和会计嵌套组所做的任何更改都会自动地反映在整个公司的嵌套组中。 嵌套在其他组中的组可以为动态组，并且/或者可以包含其他嵌套组。

静态组、动态组和嵌套组示例 (p. 136)中的图展示了一个由静态组、动态组和嵌套组创建的父组的示例。

创建嵌套组之前，需要注意以下几点：

- 只有具有“修改组成员”任务的管理员才能从用户控制台向组的静态成员列表中添加嵌套组或更改其中的嵌套组。
- 只有具有相应的管理员权限的用户才能修改、添加或删除组的成员。

  例如，如果父组 A 是由嵌套组 B 和 C 创建的，则组 A 的管理员只能修改组 A 的成员，而不能修改组 B 和 C 的成员。 组 B 和 C 只能由其相应的管理员修改。
- 要启用嵌套组，系统管理员需要在目录配置文件 (directory.xml) 中配置嵌套组支持：
  - 在“目录组行为”部分中，添加如下 GroupTypes 元素：

    <GroupTypes type=*type*>

    type 可以是 NESTED (p. 132)、DYNAMIC 或 ALL。

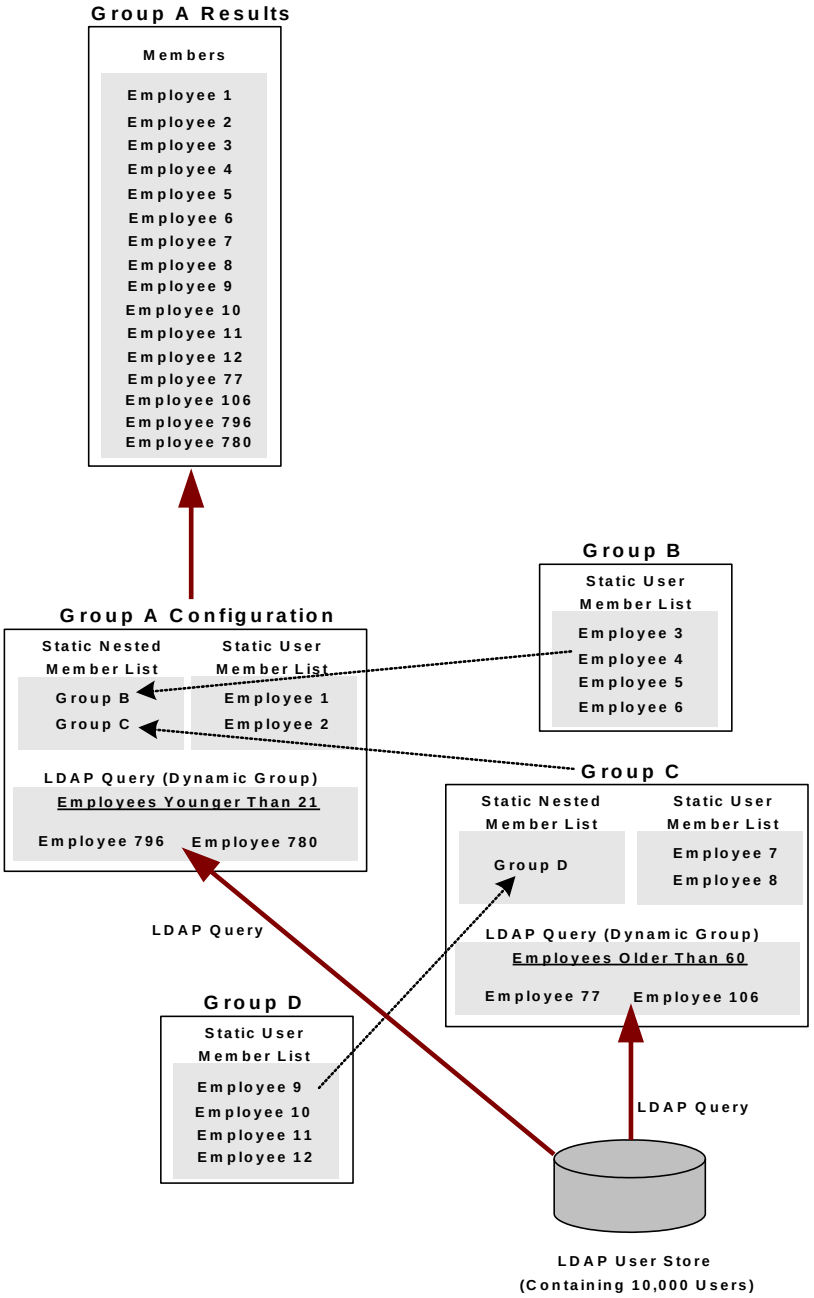
    GroupTypes 区分大小写。
  - 将 %NESTED_GROUP_MEMBERSHIP% 常用属性映射到用户存储中存在的物理属性。

创建嵌套组：

1. 在用户控制台中，依次选择“组”、“创建组”。
2. 选择创建一个新组或创建某个组的副本，然后单击**确定**。
3. 在“配置文件”选项卡上，输入组名称、组组织、说明和组管理员名称。
4. 在“成员资格”选项卡上：
   a. 单击“添加组”为此组添加一个嵌套组。
   b. 搜索现有组。
   c. 选中要包括的组旁边的复选框，然后单击“选择”。
   d. 单击“提交”。

静态组、动态组和嵌套组示例

组可能十分复杂，由动态、静态或嵌套组组合而成。下图展示了一个由静态组、动态组和嵌套组创建的父组示例。



在上图中：

- 父组 A 包含了嵌套组 B 和 C、两个静态用户和一个列出了所有 21 岁以下员工的动态 LDAP 查询。
- 组 B 由四个静态用户组成。
- 父组 C 包含了嵌套组 D、两个静态用户和一个列出了所有 60 岁以上员工的动态 LDAP 查询。
- 组 D 包含了四个静态用户。
- 图的上部列出了由嵌套组、动态查询以及组 B、C 和 D 的静态用户成员列表产生的组 A 成员。

组管理员

在“创建组”或“修改组”任务的“管理员”选项卡上，您可以将用户和组指定为组的管理员。 将某个用户分配为组管理员时，请确保该管理员的角色具有管理该组的相应作用域。 例如：

1. 使用“修改组”将一个用户分配为组管理员。
2. 为该用户分配带有组管理任务（如“修改组成员”）或用户管理任务（带有“组”选项卡）的管理角色。
3. 确认此角色具有该组的相应作用域。
   a. 对分配有组管理任务的角色使用“查看管理角色”。
   b. 在“成员”选项卡上，确认存在带有以下项的策略：

      组管理员符合的成员规则

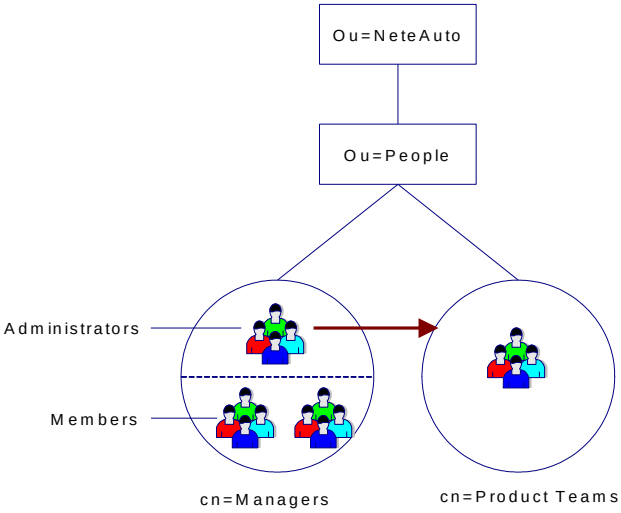
      包括该组的作用域规则

      包括一些要添加到该组的用户的作用域规则

注意：要使组成为其他组的管理员，系统管理员需要在目录配置文件 (directory.xml) 中配置组管理员支持：

- 在“目录 AdminGroups 行为”部分中，设置 AdminGroupTypes type=ALL。AdminGroupTypes 区分大小写。
- 将 %GROUP_ADMIN_GROUP% 常用属性映射到用户存储中存在的物理属性。

在您将组分配为管理员时，只有该组的管理员会成为要创建或修改的组的管理员。 您指定的管理员组的成员不会具有管理该组的权限。 下图显示了作为另一个组的管理员的组。



在该示例中：

- “经理”组是“产品团队”组的管理员。
- “经理”组的管理员可以管理“产品团队”组。而“经理”组的成员不能对该组进行管理。

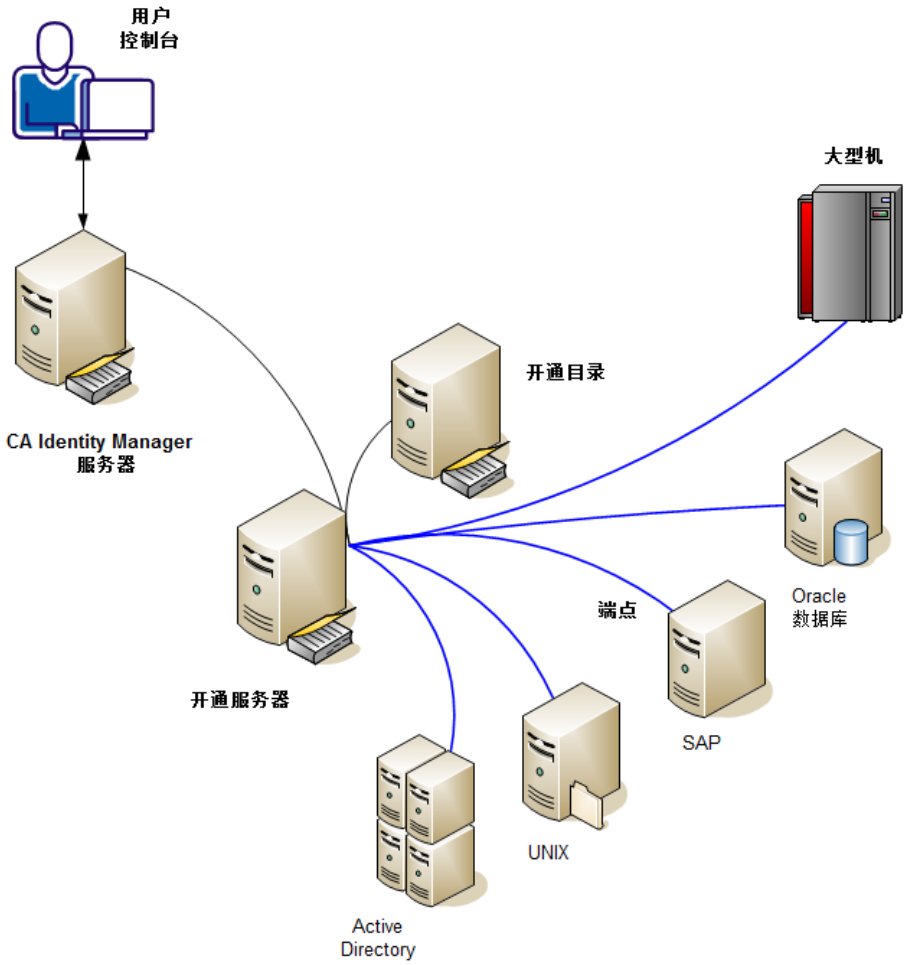
第 8 章： 受管理的端点帐户

在 CA Identity Manager 中，如果 CA Identity Manager 安装有配给服务器，那么您可以管理端点系统中的帐户。 您可以管理如 Exchange、Windows NT 或 Oracle 等帐户，也可以管理孤立和系统帐户（当前未与 CA Identity Manager 关联的帐户）。

此部分包含以下主题：

集成管理端点

借助 CA Identity Manager，您可以通过一个用户界面（即用户控制台）管理多个系统中的帐户。 帐户位于被称为管理端点或端点的系统上。 在下面的示例中，您管理五个端点上的用户。



您可以将任意端点组合上的帐户分配给用户。 集成端点时，CA Identity Manager 将每个端点帐户与配给目录中的用户关联。

以下步骤介绍了如何集成端点，以便可以通过用户控制台管理端点帐户。

1. 导入角色定义文件 (p. 141)
2. 创建关联规则
3. 将端点添加到环境中
4. 创建浏览和关联定义
5. 浏览和关联端点

导入角色定义文件

从应用于新端点的文件中导入角色定义。 此步骤需要访问管理控制台。

遵循这些步骤:

1. 从管理控制台中单击“环境”。
2. 选择要在其中添加端点的环境。
3. 单击“Role and Task Settings（角色和任务设置）”。
4. 单击“导入”。
5. 在“端点类型”下选择端点。
6. 单击“完成”。

   导入状态将显示在当前窗口中。
7. 单击“继续”退出。
8. 重新启动环境，以便更改生效。

创建关联规则

托管管理员或具有“配置关联属性”任务的管理员可以创建浏览端点时使用的规则。 “执行浏览和关联”任务将在任务的关联部分使用这些规则。

关联规则决定端点帐户属性如何映射到用户控制台中的用户属性。例如，在“访问控制”中，存在名为 AccountName 的属性。 您可以创建一条规则，将其映射到用户控制台中的 FullName。 如果规则导致两条映射应用于一个用户属性，则将使用第一个参数值。

遵循这些步骤:

1. 登录到用户控制台。
2. 依次单击“系统”、“配给配置”、“配置关联属性”。
3. 单击“添加”。
4. 定义关联规则，如下所述：
   a. 选择全局用户属性列表。

      此值是指列入配给目录的用户属性。
   b. 启用“设置特定帐户属性”复选框。
   c. 选择端点类型。
   d. 选择适用于全局用户属性的帐户属性。

e. 填写子字符串字段（可选）。

如果“子字符串源”字段为空，将从字符串的起始部分开始处理。
如果“子字符串目标”字段为空，将从字符串的结尾部分开始处理。

5. 单击“确定”。
6. 单击“提交”。

注意：无论何时更改关联规则，请务必浏览端点，即使之前已经浏览过该端点。

关联规则示例

下面的示例说明了 Active Directory 端点的示样设置。

```
GlobalUserName
FullName=LDAP Namespace:globalFullName
FullName=ActiveDirectory:DisplayName
 CustomField01=ActiveDirectory:Telephone
```

在关联 Active Directory 容器中的帐户时，每个之前未关联的帐户均会发生如下操作：

1. 配给服务器将第一个参数值 (GlobalUserName) 与 Active Directory 端点帐户属性 (NT_AccountID) 进行比较。 服务器尝试寻找名字与该帐户的 NT_AccountID 属性值匹配的唯一全局用户。 如果找到唯一匹配，配给服务器将帐户与全局用户关联。如果找到多个匹配，配给服务器执行步骤 5。如果找不到匹配，配给服务器执行下一个步骤。
2. 配给服务器考虑第二个参数值 (FullName=LDAP Namespace:globalFullName)。此值特定于其他端点类型，因此被跳过，配给服务器执行下一个步骤。
3. 配给服务器考虑第三个参数值 (FullName=ActiveDirectory:DisplayName)。 此值特定于 Active Directory，因此会使用该值。 服务器尝试寻找 FullName 与该帐户的 DisplayName 属性值匹配的唯一全局用户。如果找到唯一匹配，配给服务器将帐户与全局用户关联。 如果找到多个匹配，配给服务器执行步骤 5。 如果找不到匹配，配给服务器执行步骤 4。
4. 配给服务器考虑最后一个参数值 (CustomField01=ActiveDirectory:Telephone)。此值特定于 Active Directory，因此会使用该值。 服务器尝试寻找 Custom Field #01 属性等于该帐户的 Telephone 属性值的唯一全局用户。这里不显示使用系统任务的全局属性指定给自定义全局用户属性的名字。 如果找到唯一匹配，配给服务器将帐户与全局用户关联。 如果找到多个匹配，配给服务器执行步骤 5。 如果找不到匹配，配给服务器执行下一个步骤。
5. 配给服务器将帐户与 [默认用户] 对象关联。 如果 [默认用户] 对象不存在，服务器将创建一个对象。

将端点添加到环境中

将端点添加到要在其中管理该端点的环境中。 任何具有“创建端点”任务的管理员均可执行此步骤。

遵循这些步骤:

1. 依次选择“端点”、“管理端点”、“创建端点”。
2. 选择端点类型。
3. 填写字段完成各个选项卡。

   必填字段开头具有红色圆圈。

   注意：避免在端点名称中使用 # 符号，因为无法搜索该字符。
4. 单击“提交”。

现在，即可以创建浏览和关联定义 (p. 143)以管理其帐户。

创建浏览和关联定义

要添加端点中存在的用户，请为该端点创建浏览和关联定义。 任何具有“创建浏览和关联定义”任务的管理员均可创建该定义。

遵循这些步骤:

1. 在环境中，依次单击“端点”、“浏览和关联定义”、“创建浏览和关联定义”。
2. 单击“确定”开始新的定义。
3. 使用任何有意义的名称填写浏览和关联名称。
4. 如果存在端点和容器，请单击“选择容器/端点/浏览方法”进行选择。 对于大型端点，容器搜索可能会花费一段时间；可使用搜索筛选来缩小搜索范围。
5. 单击容器的浏览方法。 浏览和关联过程包括选择的容器及其子容器。 对于目录容器，包括子树中的所有容器。

6. 单击要执行的浏览/关联操作：
   - **浏览受管理对象的目录**－查找那些存储在端点但不在配给目录中的对象。
   - **关联用户与帐户**－将在浏览功能中发现的对象与配给目录中的用户进行关联。 关联存在两个选项。
     - **使用现有用户**

       对于将每个帐户与之前创建的用户相匹配的关联规则 (p. 141)，请使用此选项。

       如果发现了某用户，则将帐户与该用户关联。 如果找到多个用户，则帐户与默认用户关联。 如果未发现用户，则此选项创建用户（如果知道所有必需属性）并将帐户与该用户关联；否则，它将帐户与默认用户关联。

     - **根据需要创建用户**

       在主端点上关联帐户时，请使用此选项。 该选项假设端点上的帐户名称与用户完全一样。 关联匹配算法未与此选项一起使用。 相反，每个帐户与具有相同名称的用户相关联。 如果用户尚不存在，将创建该用户。 没有帐户与默认用户关联。
   - **更新用户字段**－如果对象字段和用户字段存在映射，那么会使用对象字段中的数据更新用户字段。

     使用不可选的属性（如全名、地址和电话号码）创建用户。 初次获得端点时，通过该选项可使用帐户属性值设置这些用户属性。在随后的浏览和关联过程中，请使用此选项刷新用户属性，以应用帐户属性更改，或许会使用除 CA Identity Manager 之外的其他工具。
7. 单击“提交”。

现在，具有“执行浏览和关联” (p. 144)任务的管理员即完成了端点的集成。

浏览和关联端点

托管管理员或具有“执行浏览和关联”任务的其他管理员可执行此过程。 任务的浏览阶段会确定端点中的帐户。 关联阶段会将帐户与 CA Identity Manager 中的用户匹配或创建帐户。

遵循这些步骤:

1. 在环境中，依次单击“端点”、“执行浏览和关联”。
2. 选择“立即执行”立即运行浏览和关联，或选择“排定新作业 (p. 347)”稍后或按周期排定运行浏览和关联。

   注意：该操作要求客户端浏览器与服务器中的浏览器所在时区相同。 例如，如果客户端时间为星期二下午 10:00，而服务器的时间为上午 07:00，那么浏览和关联定义将不会工作。

3. 单击要执行的浏览和关联定义。
4. 单击“提交”。

   端点中存在的用户帐户即基于所创建的浏览和关联定义在 CA Identity Manager 中创建或更新。
5. 验证任务是否成功，如下所述：
   a. 依次单击“系统”、“查看提交的任务”。
   b. 如下填写任务名称字段：执行浏览和关联
   c. 单击“搜索”。

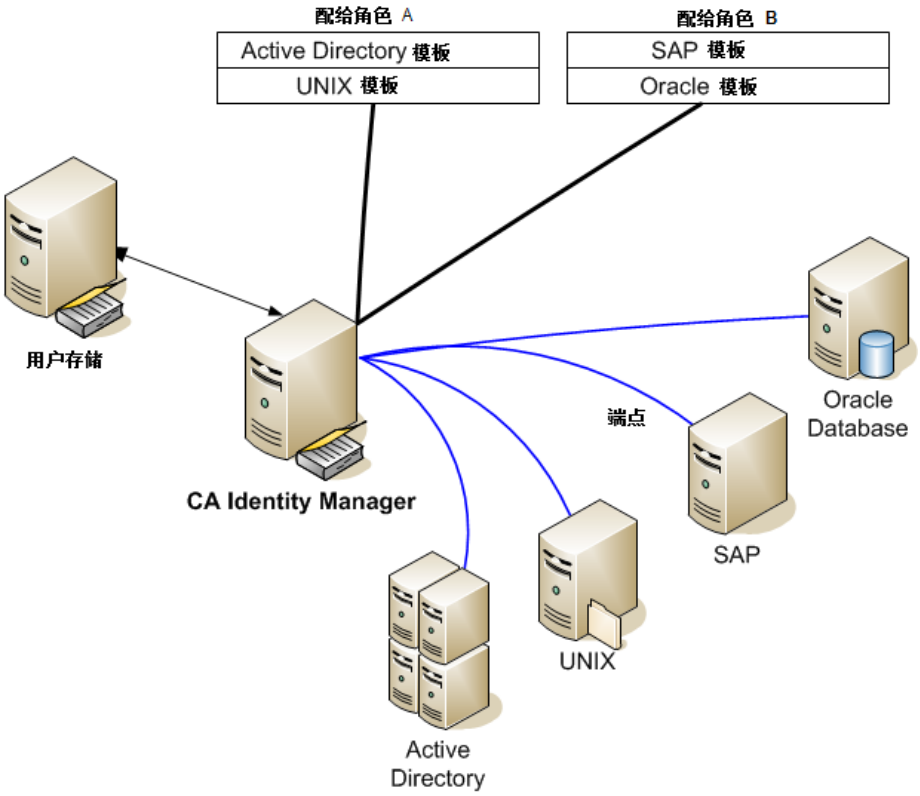
   结果即会显示任务是否成功。

注意：在“查看提交的任务”(VST) 中查看任务状态时，您可以中止“浏览和关联”任务。 中止任务将停止处理任务，将该任务保持在中止时的状态。 会发送任何一个生成的通知，以便所有系统保持同步。

同步用户、帐户和角色

将多个端点和帐户集成到一个用户管理系统会导致同步丢失。 分配给用户的配给角色或帐户模板可能与该用户的实际帐户不同。

例如，设想一个包含两个配给角色的情况，其中一个角色拥有 Active Directory 和 UNIX 帐户模板，另一个拥有 SAP 和 Oracle 模板。 用户 john_smith 拥有包含 Active Directory 和 UNIX 帐户模板的配给角色 A，但该用户仅拥有 Active Directory 帐户。 UNIX 帐户模板可能是在分配给该用户之后才添加到角色中的。 因此，管理员需要同步该用户和当前的角色定义。



以下情况是用户与配给角色或帐户模板同步丢失的其他原因：

- 由于网络中的硬件或软件问题，创建必要帐户的之前尝试失败，导致帐户缺失。
- 配给角色和帐户模板出现变化，从而创建了额外帐户或导致帐户缺失。
- 帐户创建后被分配给帐户模板，因此存在帐户，但是与其帐户模板不同步。
- 因为被指定稍后创建帐户，因此新帐户创建推迟。
- 获得了新端点。 在浏览和关联过程中，配给服务器未自动将配给角色分配给用户。 您需要更新角色以指明端点上需要帐户的用户。 在用户同步时，与用户关联的任何帐户均被列为额外帐户。

- 通过将帐户复制到用户的方式，将现有帐户分配给用户。
- 通过将用户分配给角色之外的其他方式为用户创建帐户。 例如，将用户复制到该用户配给角色中不包含的帐户模板。 帐户被列为额外帐户或具有额外帐户模板的帐户。如果将用户复制到端点以使用默认帐户模板创建帐户，则该帐户可能成为额外帐户。

以下章节将介绍如何执行三种类型的同步操作：

1. 将用户与角色同步 (p. 147)。
2. 将用户与帐户模板同步 (p. 147)。
3. 将端点帐户与帐户模板同步 (p. 148)。

将用户与角色同步

此任务可创建、更新或删除帐户，以便帐户与分配给用户的配给角色保持一致。例如，管理员使用端点上的内置工具添加或删除帐户，但是您尚未重新浏览该端点以更新配给目录。 因此，用户具有额外或缺失的帐户。 另外，此任务还可确保每个帐户都属于正确的帐户模板。

遵循这些步骤:

1. 登录到用户控制台。
2. 依次选择“任务”、“用户”、“同步”、“检查角色同步”。
3. 选择用户。

   系统将显示一个页面，其中列出了预期帐户、额外帐户和缺失帐户。
4. 单击“同步”使帐户与此角色中的模板匹配。
   a. 您可以选中复选框在端点上创建帐户。如果用户有多个帐户模板限定的都是同一个帐户，则该帐户是通过合并所有相关帐户模板创建的。

      此帐户会分配给当前与该帐户不同步的那些帐户模板。
   b. 您可以选中复选框删除额外帐户。不过，用户可能有拥有这些帐户的正当理由。 如果是这种情况，请不要选中此选项。

      在某些端点上，帐户删除功能被禁用；因此，无法删除帐户。

将用户与帐户模板同步

此任务可将端点帐户的属性与用户的关联帐户模板同步。 不过，完全同步取决于以下因素：

- 帐户完全同步出现在两种情况下。 帐户模板使用强同步 (p. 149)，或者两个或更多帐户模板被添加到帐户。
- 如果帐户模板使用弱同步 (p. 149)，则此任务将启动仅涉及此模板的帐户同步。 如果在此更新前，帐户之前没有与其他帐户模板保持帐户同步，更新后将仍然如此。

遵循这些步骤:

1. 登录到用户控制台。
2. 依次选择“任务”、“用户”、“同步”、“检查帐户模板同步”。
3. 选择用户。

   系统将显示一个页面，其中列出了预期帐户、额外帐户和缺失帐户。
4. 单击“同步”使帐户与模板匹配。

   a. 您可以选中复选框在端点上创建帐户。如果用户有多个帐户模板限定的都是同一个帐户，则该帐户是通过合并相关帐户模板创建的。

      此帐户会分配给与该帐户不同步的帐户模板。新创建的帐户不需要执行帐户同步。

   b. 您可以选中复选框删除额外帐户。不过，用户可能有拥有这些帐户的正当理由。 如果是这种情况，请不要选中此选项。

      在某些端点上，帐户删除功能被禁用；因此，无法删除帐户。

仅针对新帐户的属性

在帐户模板中，某些属性仅在创建帐户时适用。 例如，密码属性是定义新帐户密码的规则表达式。 该规则表达式从不更新帐户的密码。对密码规则表达式的更改仅影响在设置规则表达式之后创建的帐户。

与之相似，只读帐户属性的模板规则表达式也只影响在设置规则表达式之后创建的帐户。 更改这种规则表达式对现有帐户没有任何影响。

将端点帐户与帐户模板同步

此任务可在关联帐户模板修改后同步端点帐户。 例如，Active Directory 帐户或许没有组，但是关联帐户模板被定义为包括组。

遵循这些步骤:

1. 登录到用户控制台。
2. 依次选择“任务”、“端点”、“管理端点”、“检查端点帐户同步”。
3. 选择端点。

   系统将显示一个页面，其中列出了该端点上的帐户、关联帐户模板以及不同步的属性。
4. 单击“同步”使这些帐户的属性与帐户模板中定义的属性匹配。

   对帐户模板所做的更改将影响现有的帐户，如下所述：

   - 如果更改功能属性的值，则会更新相应的帐户属性以与该帐户模板属性值同步。 请参阅弱同步和强同步的说明。

- 某些帐户属性由连接器指定为在帐户模板发生变化时不进行更新。示例中列出的是端点类型仅允许在帐户创建过程中设置的某些属性以及密码属性。

更新哪些属性

当您更改帐户模板中的功能属性时，帐户的相应属性也会发生更改。 此更改会对帐户的属性产生影响。 产生的影响基于以下因素：

- 该帐户模板定义为使用弱同步还是强同步。
- 该帐户是否属于多个帐户模板。

弱同步

*弱同步*可确保用户具有其帐户的最少功能属性。 在多数端点类型中弱同步是默认值。 如果更新使用弱同步的模板，CA Identity Manager 将更新功能属性，如下所述：

- 如果在帐户模板中更新了数字字段，且该新数字大于该帐户中的数字，CA Identity Manager 则会更改帐户中的值以与新数字匹配。
- 如果之前在帐户模板中没有选中，但您在之后选中了该复选框，CA Identity Manager 则会在未选中复选框的任何帐户中更新该复选框。
- 如果在帐户模板中更改了列表，CA Identity Manager 则会更新所有帐户以包括未包括在该帐户列表值中的新列表中的任何值。

如果帐户属于其他帐户模板（无论这些模板使用弱同步还是强同步），CA Identity Manager 则仅会参考正在更改的模板。 此操作比检查每个帐户模板更有效。 因为弱同步仅将功能添加到帐户，所以通常不需参考那些其他帐户模板。

注意：从弱同步帐户模板传播时，将要删除或降低功能的更改会保持某些帐户的状态，而不同步。 请记住，使用弱同步，从不会删除或降低功能。 在不参考帐户的其他模板的情况下，传播不会考虑弱同步是否充分。

在这种情况下，请使用“将用户与帐户模板同步”让帐户与其帐户模板保持同步。

强同步

强同步可确保帐户具有与在帐户模板中指定的那些帐户属性完全相同的帐户属性。

例如，假设您将一个组添加到现有 UNIX 帐户模板中。最初，帐户模板使帐户成为“人员”组的成员。 现在，您希望帐户同时成为“人员”和“系统”两个组的成员。当每个帐户都是“人员”组和“系统”组（且没有其他组）的成员时，与帐户模板关联的所有帐户即被视为同步。任何不在“人员”组中的帐户会被添加到两个组中。

要考虑的一些其他因素包括以下内容：

- 如果帐户模板使用强同步，则属于除“人员”组和“系统”组之外的其他组的任何帐户会被从这些额外组中删除。
- 如果帐户模板使用弱同步，则帐户会被添加到“人员”组和“系统”组中。已定义其他组的任何帐户仍然是这些组的成员。

注意：定期同步帐户和其模板，以便确保帐户保持与其帐户模板同步。

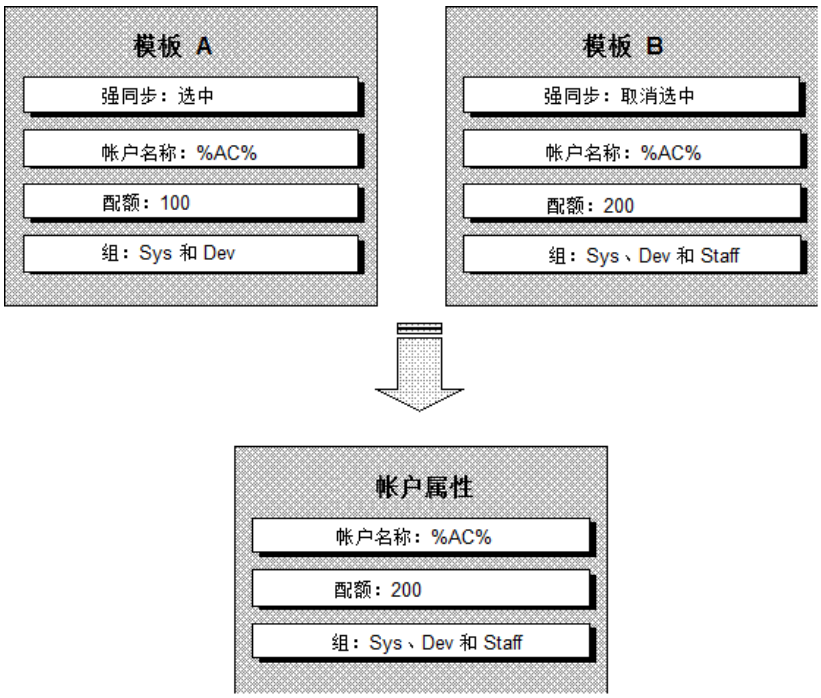
带有多个模板的帐户

同步还取决于帐户是否属于多个帐户模板。 如果帐户只有一个帐户模板，并且该模板使用强同步，则每个属性均会更新，以精确匹配帐户模板属性值所求得的结果。 结果与属性是初始属性时的结果一样。

一个帐户可能属于多个帐户模板，就像一个用户属于多个开通角色，每个角色都规定了在同一管理端点上的某一访问级别。 在这种情况下，CA Identity Manager 会将这些帐户模板合并为一个有效的帐户模板，其规定来自单个帐户模板的功能超集。 如果所有单个帐户模板均为弱同步，则此帐户模板本身被视为使用弱同步；如果任何单个帐户模板为强同步，则此帐户模板本身被视为使用强同步。

注意：通常，对于控制一个帐户的帐户模板，将仅使用弱同步或仅使用强同步，具体取决于您公司的角色是否完全定义了用户所需的访问权限。 如果用户不适合定位明确的角色，您需要一定的灵活性，以便向用户帐户授予其他能力，则使用弱同步。如果您可以定义角色以精确指定用户需要的访问，则使用强同步。

下列示例说明如何将多个帐户模板合并为一个有效的帐户模板。 在本例中，一个帐户模板被标记为弱同步，另一个为强同步。 因此，通过合并两个帐户模板而创建的有效帐户模板被视为强同步帐户模板。 整数“配额”属性取两个帐户模板中较大的值，多值“组”属性取两者的联合值。



反向同步端点帐户

虽然创建、删除和修改帐户是 CA CA Identity Manager 的责任，但是防止端点系统用户独立地执行这些操作也是不可能的。由于紧急原因或恶意原因（如黑客）会导致该情况发生。 反向同步确保对每个端点上用户具有的帐户进行控制，方法是通过识别 CA Identity Manager 帐户和端点上帐户之间差异。

例如，如果使用外部工具在 Active Directory 域中创建了帐户，CA CA Identity Manager 必须意识到这种潜在的安全问题。此外，绕过 CA CA Identity Manager 会引起缺乏批准流程以及审核报告。

CA CA Identity Manager 和管理端点之间差异的两种类型如下所示：

- 检测到新帐户
- 现有帐户中的更改

您可以通过定义策略处理更改来对待这两种情况。 然后，使用“浏览和关联”更新 CA CA Identity Manager 来触发执行策略。

反向同步如何工作

用端点帐户反向同步发生如下：

1. 管理员或恶意用户创建或修改端点中的帐户。
2. 当浏览和关联在该端点上运行时，将检测新的或修改的帐户。
3. 配给服务器将通知发送到 CA Identity Manager 服务器。
4. CA Identity Manager 服务器搜索与该端点中的更改相匹配的反向同步策略。
5. 如果找到匹配策略，则执行。 如果一个以上的策略应用于该帐户并且那些策略有同样的范围，最高优先级策略则运行。
6. 根据策略，会发生以下操作之一：
   - 对于新帐户，策略接受、删除或挂起帐户或将其发送进行工作流批准。
   - 对于修改的帐户，策略接受值，恢复到最后的已知值，或将其发送进行工作流批准。
7. 如果选择工作流，则会生成工作流的新事件并设置批准人。 然后，会发生以下操作之一：
   - 对于新帐户，批准人可以接受、删除或挂起帐户，或将其分配给用户。
   - 对于修改的帐户，工作流流程与在用户控制台中更改值一样（除了拒绝值在该端点被恢复）。

映射端点属性

要对端点帐户中的属性使用反向同步，首先应将该属性映射到用户控制台中可见的属性。 默认情况下会映射一些属性，如帐户名和密码。 其他属性则不会被映射。例如，Active Directory 属性组成员资格不会被映射。 对于一些端点类型，不会映射任何属性。

检查属性是否可以映射

1. 在用户控制台中，单击“端点”，或单击“任务”、“端点”。
2. 依次单击“反向修改”、“创建反向同步修改的帐户策略”。
3. 选择创建新策略或策略副本。
4. 单击“端点类型”，并选择端点，如 Active Directory。
5. 单击“属性名称”以显示可以映射的属性的列表。
6. 单击“取消”。

   您可以取消策略，因为您现在只是用其来检查哪些属性可以映射。

重要说明！ 某些属性只能通过端点上的本地工具进行管理。因此，如果端点用户修改此类属性，则在触发反向同步策略时，反向事件将失败。 然而，对该反向事件中的其他属性所做的更改不可反向，因此，请避免映射只能在端点中进行管理的属性。

为反向同步映射端点属性

1. 单击“端点”、“修改端点”。
2. 搜索并选择需要反向同步的端点。
3. 单击“属性映射”选项卡。
4. 选择“使用自定义设置”。
5. 单击“添加”添加新的自定义属性。
6. 选择可用的自定义属性。 例如，如果您的环境中未使用 CustomField 10，则使用它。
7. 将自定义属性映射为要管理的帐户属性名称。
8. 重复步骤 5 至 7，在所需的所有帐户属性和所选的自定义属性之间添加映射。

   您可以为要管理的所有属性使用相同的自定义属性（示例中的 CustomField 10）。
9. 单击“提交”。

创建此端点的基准值

映射完端点的所有值后，即可浏览该端点。 对于此操作，需先禁用入站通知，然后在浏览完成后再将其启用。 禁用通知能够消除不必要的通知。 否则，在执行浏览操作过程中，具有新属性值的每个帐户都将生成一个通知。

1. 在配给管理器中，禁用入站通知如下：
   a. 单击“系统”、“域配置”、“CA Identity Manager 服务器”、“启用通知”。
   b. 选择“否”。
   c. 重新启动配给服务器来确保更改生效。
2. 在用户控制台中，单击“端点”、“执行浏览和关联”。

   选择取消选定关联的浏览和关联定义。

   该操作可以使用新的端点属性数据重新填充用户存储属性。 如果端点大的话，该任务可能需要一点时间。
3. 在配给管理器中重新启用入站通知。
4. 重新启动开通服务器。

在为该端点执行下一个浏览和关联操作时，会生成修改帐户通知。 如果为映射为全局用户属性的属性发生更改且策略应用于该属性，则生成通知。

更多信息：

功能属性和初始属性 (p. 176)

用于反向同步的策略

在端点上创建或修改帐户时，反向同步策略可以采取适当操作作为响应。例如，用户在公司域中，在几个 OU 中创建一些 Active Directory 帐户。 此外，用户修改一些 Microsoft Exchange 帐户。您可以检测新的和更改的帐户，并提供适当操作作为使用反向同步帐户策略的响应。

可以使用反向同步执行下列操作：

- 配置接受新帐户、拒绝新帐户或将其发送进行工作流批准的策略。
- 配置接受对属性更改、将其恢复到原始属性或将其发送进行工作流批准的策略。
- 当将帐户发送进行工作流批准时，批准人可以执行下列的操作之一：
  - 拒绝它（从端点将其删除/挂起，或者更改值以匹配 CA Identity Manager 用户存储值）
  - 接受它并更新 CA Identity Manager 用户存储以匹配帐户
  - 将其分配给用户控制台的用户（在帐户创建的情况下）

为新帐户创建策略

如果要为在端点上检测到新帐户定义流程，要创建应用于新帐户的帐户策略。当“关联”选项包含在浏览和关联定义中时，新帐户策略在检测到帐户时会运行。如果仅在运行浏览时发现帐户，策略则在下次浏览该端点时包括“关联”选项时运行。

为新帐户创建策略

1. 在用户控制台中，单击“端点”，或单击“任务”、“端点”。
2. 依次单击“反向新建”、“创建反向同步新帐户策略”。
3. 为该策略输入名称和说明。
4. 输入以下参数：
   - 优先级 - 策略的优先级。最高优先级的策略是具有最小数字的策略。如果两个策略具有相同的优先级和相同的范围，任何一个策略则可运行。因此，确保设置不同的优先级。
   - 端点类型 - 所有端点或特定端点类型。
   - 端点 - 特定的端点名称。 如果端点类型是“所有”，唯一的选择是“所有”端点。
   - 容器 - 帐户所在的容器。该字段仅适用于分级端点。输入容器作为节点列表，以端点结束。 例如，针对路径为“ou=child,ou=parent,ou=root,dc=domain,dc=name”的 AD OU，正确的格式为“child,parent,root”。
   - 关联用户 - 根据是否在配给目录中发现关联用户，控制运行策略的时间。

5. 选择下列操作之一：
   - 接受 - 不对帐户采取操作。 如果两个策略存在，该选项将十分有用，一个是拒绝所有新帐户的策略，一个是接受在某个 OU 下创建的帐户的较高优先级策略。 因此，如果帐户在该 OU 创建，则会接受它。 由于是较低优先级，所以拒绝优先级不会运行。
   - 删除 - 从端点中删除帐户。
   - 挂起 - 帐户保留在端点中，但为挂起。
   - 发送以获批准 - 提交更改以获工作流批准。
6. 如果将“操作”设置为“发送以获批准”，请执行下列步骤：
   a. 单击工作流流程旁边的图标。
   b. 选择工作流流程。
   c. 单击“确定”。
7. 单击“提交”。

如果将工作流流程分配给了策略，则需要创建批准任务 (p. 156)。

为修改的帐户创建策略

只要帐户属性是在属性映射中定义 (p. 152)，那么端点帐户中的任何帐户属性可由“反向同步”管理。

如果要在现有端点帐户和其在 CA Identity Manager 中的已知值之间出现差异时定义流程，则可以创建应用于现有帐户的帐户策略。 如果属性为多值，可能会是已经添加或删除多个值。 在这种情况下，策略分别应用于各个值，或可以为不同值创建不同策略。

为修改的帐户创建策略

1. 在用户控制台中，单击“端点”，或单击“任务”、“端点”。
2. 依次单击“反向修改”、“创建反向同步修改的帐户策略”。
3. 为该策略输入名称和说明。
4. 输入以下参数：
   - 优先级 - 策略的优先级。最高优先级的策略是具有最小数字的策略。如果两个策略具有相同的优先级和相同的范围，任何一个策略则可运行。因此，确保设置不同的优先级。
   - 端点类型 - 所有端点或特定端点类型。
   - 端点 - 特定的端点名称。 如果端点类型是“所有”，唯一的选择是“所有”端点。
   - 容器 - 帐户所在的容器。该字段仅适用于分级端点。输入容器作为节点列表，以端点结束。 例如，针对路径为“ou=child,ou=parent,ou=root,dc=domain,dc=name”的 AD OU，正确的格式为“child,parent,root”。

- 属性 - 物理名称。
- 值 - 值的字符串表示，可能包含 *（星号）作为通配符。 通配符是指更改中的任何值。

5. 选择下列操作之一：
   - 接受 - 更新 CA Identity Manager 用户存储中的帐户值匹配端点帐户中的值。
   - 拒绝 - 将属性恢复为原始值，而不影响对该帐户属性的其他更改。
   - 发送以获批准 - 提交更改以获工作流批准。
6. 如果将“操作”设置为“发送以获批准”，请执行下列步骤：
   a. 单击工作流流程旁边的图标。
   b. 选择工作流流程。
   c. 单击“确定”。
7. 单击“提交”。

如果将工作流流程分配给了策略，则需要创建批准任务 (p. 156)。

创建用于反向同步的批准任务

针对具有“发送到工作流”操作的策略，创建反向批准任务。 考虑以下创建任务的说明：

- 对于批准新帐户的任务，您有两种选择。
  - 可以为帐户创建一般的批准屏幕。 任务的配置文件屏幕仅显示有关帐户的一般信息。 “批准反向新帐户”任务以这种方式操作。
  - 如果批准人需要查看新帐户的详细信息，那么该屏幕必须为端点类型所特有。 因此具有该屏幕的批准任务仅应用于该端点类型所特有的策略。任务必须包括“反向批准”选项卡。
- 对于批准帐户修改的任务，批准屏幕必须为端点类型所特有，以便批准人可以查看更改的值。

反向批准任务等同于用于帐户更改的批准任务。 如果特定端点类型的批准任务已经存在，则可以使用该任务。 对于新帐户，需要其他的反向批准选项卡。 如果端点类型的现有批准任务不存在，则使用以下步骤。

创建用于反向同步的批准任务

1. 在用户控制台中，依次单击“任务”、“角色和任务”，或单击“角色和任务”。
2. 依次单击“管理任务”、“创建管理任务”。
3. 选择该端点的修改任务。

   该名称将始于该端点类型的修改和状态名称。 修改 Active Directory 帐户是一个示例。
4. 在“配置文件”选项卡中做以下更改：
   - 更改新任务的名称。
   - 更改任务标签。
   - 将操作更改为“批准事件”。
5. 在“选项卡”选项卡中做以下更改：
   a. 删除所有关系选项卡。
   b. 如果任务是批准新帐户，则添加“反向批准”选项卡。将该选项卡移动到第一个选项卡。
   c. 复制选项卡上的批准屏幕，并根据需要进行编辑。

      注意：在批准任务中使用某些帐户屏幕时，您可能会遇到问题。如果是这样的话，请修改选项卡的默认帐户屏幕，使其在任务中正常工作。
6. 单击“提交”。
7. 如果任务用于新帐户批准，则将任务添加到批准人所属的角色中。 角色定义用户范围，用于搜索可以分配新帐户的用户。

执行反向同步

使用“执行浏览和关联”任务时，反向同步就会发生。 使用该任务可以更新 CA Identity Manager 带有端点上新的或更改帐户的配给存储。

执行反向同步

1. 创建包括“关联”选项的浏览和关联定义。 需要关联来检测新帐户。
2. 依次单击“任务”、“端点”、“执行浏览和关联”。
3. 选择应用于带有新的或更改帐户端点的定义。

   注意：在与现有用户关联时，用户必须存在于配给目录，否则用户与该目录中的默认用户关联。 CA Identity Manager 用户存储不在浏览和关联任务的范围里。
4. 单击“提交”。

如果策略没有工作流流程，则根据策略中的定义已经处理帐户。

注意：如果多个属性在由反向同步策略检测到的帐户中被拒绝，那么所有操作都会放入一个事件。 然而，如果该事件由于属性之一的问题而失败，则不会更新属性。

如果工作流是策略的一部分，那么由反向同步生成的任何批准会出现在“工作流”、“查看我的工作列表”供批准人查看。

对于新帐户，批准人有以下选择：

- 通过选择“删除”或“挂起”，然后单击“拒绝”，批准人可以选择在端点中挂起或删除帐户。
- 否则，批准人可以通过单击“批准”接受新帐户。

  如果批准人没有在“关联用户”字段中选择用户，则将帐户分配给默认用户。 如果在批准任务中填充了“关联用户”字段，该帐户则与该用户关联。 如果能够发现用户，“关联用户”字段则包含由关联机制找到的建议用户。

对于修改的帐户，批准人有以下选择：

- 对于每个帐户，批准人都会查看哪些值被更改，并且可以批准或拒绝他们正如在帐户管理屏幕中发动的更改一样。
- 批准人将对功能属性的更改（如 Active Directory 组）视为单独的批准事件。

验证反向同步是否成功

1. 转到“系统”、“查看提交的任务”。
2. 如下完成任务名称字段：配置活动
3. 单击“搜索”。

结果显示反向同步事件是否成功完成。

展开端点上的自定义属性

配给服务器可以管理自定义端点属性。要使 CA CA Identity Manager 能够读取与配给角色相关联的自定义端点属性，还需要一些步骤。

展开端点上的自定义属性

1. 如果该连接程序是在 CA CA Identity Manager r12.5 之前创建的，则从分析程序表生成元数据。

   请参阅《*Programming Guide for Java Connector Server*》（《Java Connector Server 编程指南》）。

2. 按照以下方式使用 Connector Xpress：

   a. 将元数据安装在命名空间节点中。

   b. 使用角色定义生成器生成 JAR 文件、属性文件和角色定义文件。

      有关详细信息，请参阅《*Connector Xpress Guide*》（《Connector Xpress 指南》）。

3. 将 JAR 文件复制到此位置：

   - (Windows) *app server home*/iam_im.ear/user_console.war/WEB-INF/lib
   - (UNIX) *app server home*\iam_im.ear\user_console.war\WEB-INF\lib

     注意：对于 WebSphere，请将 JAR 文件复制到：WebSphere_home/AppServer/profiles/*Profile_Name*/config/cells/*Cell_name*/applications/iam_im.ear/user_console.war/WEB-INF

4. 将属性文件复制到此位置：

   - (Windows) *app server home*/iam_im.ear/custom/provisioning/resourceBundles
   - (UNIX) *app server home*\iam_im.ear\custom\provisioning\resourceBundles

     注意：对于 WebSphere，请将属性文件复制到：

     WebSphere_home/AppServer/profiles/*Profile_Name*/config/cells/*cell_name*/applications/iam_im.ear\custom\provisioning\resourceBundles

5. 如果您有群集，则对于每个节点重复上面两个步骤。
6. 重新启动应用程序服务器。
7. 按照以下方式导入角色定义文件：

   a. 在管理控制台中，选择“环境”。

   b. 选择“角色”和“任务”设置。

   c. 单击“导入”。

   d. 选择端点类型并且单击“完成”。

帐户任务

在用户控制台中，您可以创建、修改、查看和删除与 Identity Manager 用户关联的端点帐户。 您也能将未与 CA CA Identity Manager 关联的其他端点帐户分配给用户。

端点帐户有四种类型：

已配给

为用户分配配给角色时创建的帐户

例外

为用户分配帐户模板时创建的帐户

孤立

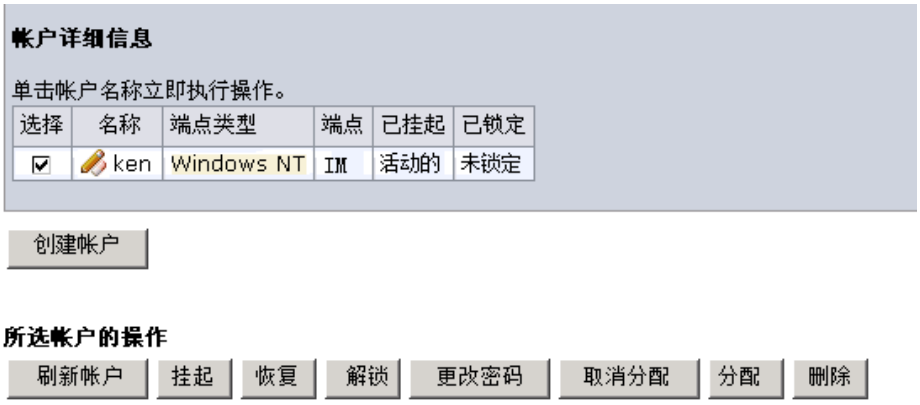
端点系统上创建的、未与任何 CA Identity Manager 用户关联的帐户

系统

端点系统上创建的、未与任何 CA Identity Manager 用户关联的，并且用于管理该端点系统的帐户

查看或修改端点帐户

允许您查看用户配置文件的任务（如“查看用户”或“修改我的配置文件”）包括一个列出该用户端点帐户的“帐户”选项卡。



对于每个帐户，Identity Manager 会显示帐户名称、帐户所在端点和帐户状态等信息。 对于修改任务，还提供了用于更改用户密码以及锁定或挂起帐户的附加选项。

在本例中，“帐户”选项卡包括一个“搜索”按钮，其意味着该选项卡已配置为搜索屏幕。 您可以将该选项卡配置为使用列表屏幕、搜索屏幕或两者同时使用。

- 如果两种屏幕均已配置，则由搜索屏幕确定搜索结果中的字段。
- 如果仅配置了列表屏幕，则由其确定搜索结果中的字段。
- 如果两种屏幕均未配置，则“帐户”选项卡使用静态列表显示，这意味着“帐户”选项卡无法自定义显示列。

有关可在“帐户”选项卡上提供的其他选项的详细信息，请参阅用户控制台帮助中的“配置帐户”选项卡。

创建已配给的帐户

为 CA Identity Manager 用户创建端点帐户的推荐方法是将开通角色分配给该用户。 该用户将接收该帐户，以及在帐户模板中为该角色定义的属性。 必要时，更改帐户模板（如 Exchange 帐户的邮箱大小）会更新端点帐户。

创建已配给帐户

1. 在用户控制台中，选择“管理用户”，“修改用户”。
2. 选择要修改的用户。
3. 单击“配给角色”选项卡。
4. 单击“添加配给角色”。
5. 选择角色。
6. 单击“提交”。

创建例外帐户

对用户使用“修改用户”时您可以在“帐户”选项卡上直接创建帐户。 该帐户称为例外帐户。 然而，因为该帐户不涉及任何配给角色，所以角色与用户的同步不更新该帐户。

创建例外帐户

1. 在用户控制台中，选择“用户”，“修改用户的端点帐户”。
2. 选择要修改的用户。
3. 单击“创建”。
4. 选择端点。
5. 选择容器（如果该端点类型需要）。
6. 完成每个选项卡中的字段。
7. 单击“提交”。

分配孤立帐户

在用户控制台中，您可以管理孤立帐户，即未与 CA Identity Manager 用户关联的帐户。

为孤立帐户创建默认用户

如果配给目录与 CA Identity Manager 用户存储分离，则在 CA Identity Manager 用户存储中创建配给服务器默认用户。 该默认用户将用于孤立帐户。

1. 在用户控制台中，单击“用户”。
2. 单击“管理用户”、“创建用户”。
3. 按照以下方式命名该用户，包括括号：
   `[default user]`

   您现在就可以将孤立帐户分配给用户了。

分配孤立帐户

1. 在用户控制台中，单击“端点”，
2. 单击“管理孤立帐户”。
3. 搜索并选择一个用户。
4. 单击一个用户以便分配给该孤立帐户。

分配系统帐户

在用户控制台中，您可以管理系统帐户，即用于管理端点系统的端点帐户。

要将系统帐户分配给用户，可以基于“管理系统帐户”任务创建一个管理任务。该新任务具有一个适用于特定端点的特定 CA Identity Manager 用户。 您可以为每个类型的端点都创建一项任务。

配置分配系统帐户的任务

1. 在用户控制台中，依次单击“角色和任务”、“管理任务”、“创建管理任务”。
2. 在“管理系统帐户”上建立新任务。

   例如，您可以创建一个名为“*管理 Oracle 系统帐户*”的任务，以便在 Oracle 端点类型中分配系统帐户。
3. 在“搜索”选项卡上，单击“浏览”按钮以编辑搜索屏幕。 在该屏幕上，输入一个搜索筛选，以便搜索到一个将该系统帐户分配给的用户。
4. 提交任务。
5. 将该任务包括在某个角色中。
6. 将该角色分配给应将端点系统帐户分配给用户的一个用户。

   具有该角色的用户可以执行新的任务，将系统用户分配给 CA Identity Manager 用户。

移动帐户任务屏幕

使用该任务屏幕来将帐户从端点的一个容器转移到另一个。 该屏幕上的字段如下所列：

移动帐户详细信息

指定要移动的帐户、父容器、目标容器、端点以及端点类型。

选择“容器”按钮

单击搜索属于该端点的可用帐户容器。

删除端点帐户

您可以以两种方式删除端点帐户：

1. 使用“配给角色”选项卡上的“修改用户”任务删除创建该帐户的角色。
2. 使用“修改用户的端点帐户”任务，删除该帐户。

使用“修改用户的端点帐户”删除帐户

1. 在用户控制台中，选择“用户”，“修改用户的端点帐户”。
2. 选择要修改的用户。
3. 根据端点类型搜索帐户。
4. 选择帐户。
5. 单击“删除”按钮。

在使用配给管理器时，会按照以下方式重新创建已删除的帐户：

- “Synchronize User with Roles”（同步用户与角色）会重新创建已配给的帐户（用户拥有配给角色时创建的帐户）。
- “Synchronize User with Account Templates”（同步帐户与帐户模板）会重新创建例外帐户（如果帐户有帐户模板）和已配给的帐户。

更改端点帐户的密码

您可以在不知道当前密码的情况下更改端点帐户的密码。

更改端点帐户的密码

1. 在用户控制台中，选择“用户”，“修改用户的端点帐户”。
2. 选择要修改的用户。
3. 根据端点类型搜索帐户。
4. 选择一个或多个帐户。
5. 单击“更改密码”按钮。
6. 输入新密码。

   CA CA Identity Manager 密码策略验证该新密码。
7. 单击“提交”。

针对若干帐户执行操作

您可以针对一个或多个帐户执行若干其他操作。例如，您可以恢复挂起的帐户，在用户输入错误密码时解锁帐户，或分配或取消分配用户的帐户。 这些操作适用于所有选定的帐户，并且过程相同。

针对若干帐户执行任务

1. 在用户控制台中，选择“用户”，“修改用户的端点帐户”。
2. 选择要修改的用户。
3. 根据端点类型搜索帐户。
4. 选择一个或多个帐户。
5. 单击“所选帐户的操作”下面的任何按钮。
6. 响应出现的对话框并单击“提交”。

高级帐户操作

在配给管理器中，您可以对帐户执行大量的其他操作：

- 将帐户与不同全局用户关联在一起
- 自动地浏览帐户
- 删除帐户
- 使用删除未决
- 重新创建已删除的帐户

更改帐户的全局用户

以下示例说明了需要将帐户与不同的全局用户关联起来的情况：

- 您拥有两个同名全局用户，CA CA Identity Manager 会将帐户与错误的人关联起来
- CA CA Identity Manager 将帐户与 [默认用户] 对象关联起来，而您希望将它与另一个全局用户对象关联在一起
- 您使用“新建”创建了帐户，现在您希望将它与全局用户关联在一起

要将帐户与配给管理器的不同全局用户关联在一起，请将帐户拖放到正确的全局用户上。

自动浏览的工作原理

除非您浏览端点，否则 CA CA Identity Manager 不会察觉到使用端点自带工具的帐户或其他对象的增加或减少。浏览过程注意到已经发生的添加和删除操作（以及某些情况下的修改操作），会将这些更改应用于配给目录中的对象的 CA Identity Manager 表示。

不过，如果在此次浏览发生之前，您已使用配给管理器来尝试创建同名对象，CA CA Identity Manager 会注意系统已经存在使用该名称的对象，并会报告此错误。然后 CA CA Identity Manager 会浏览该对象，在配给目录中创建对它的表示。您可以立即开始处理该对象。 当对象未存在于配给目录中时，如果执行添加、移动或重命名操作从端点生成了已经存在的错误，则系统会自动生成单一对象浏览。

您可以将自动浏览与《*Provisioning Reference Guide*》中描述的同步/自动关联域配置参数相结合。 在这些功能协同工作时，它们首先会将通过帐户模板创建帐户的尝试处理为创建新帐户的尝试。 然后，使用下列步骤进行处理：

- 注意未浏览过的帐户
- 自动地浏览该帐户
- 将帐户自动关联到全局用户
- 将帐户模板添加到帐户中，就好像它是与此全局用户相关联的现有帐户。

删除帐户

如果必须删除帐户，您可以在配给管理器中使用以下方式：

- 右键单击帐户，然后选择“删除”
- 右键单击全局用户并且选择“删除用户和帐户”
- 运行“删除帐户”向导
- 使全局用户与配给角色保持同步，并且指定您想要删除额外帐户

在您从配给角色中删除全局用户时，配给管理器为帐户删除提供这些选择：

- 如果您决定删除这些帐户，CA Identity Manager 会从配给目录中删除帐户。
- 如果决定不删除帐户，您可以使用“用户与角色同步”选项并且选择“删除帐户”。

在删除帐户之前从配给角色中删除全局用户时，您可以列出全局用户的帐户。右键单击全局用户并选择“List Accounts”（列出帐户）。

- 帐户列表显示每个帐户所属的配给角色。 如果帐户属于一个配给角色，在您从该角色中删除该用户，并且接受删除帐户的用户同步操作时，该帐户将被删除。
- 如果帐户不属于配给角色即为额外帐户，由“Check User Synchronization”（检查用户同步）报告。 如果您选择全局用户的“将用户与角色同步”菜单项，帐户将被删除。

使用删除未决

系统会逐端点地配置 CA CA Identity Manager，因此在管理员启动通常要删除帐户的删除或同步操作时，端点上的帐户将不会被删除。 相反，帐户在 CA CA Identity Manager 中将被置于“删除未决”状态，在管理端点上将被置于“挂起”状态。

可以在配给管理器中将“删除未决”帐户标示在帐户属性的“统计信息”选项卡上。挂起的帐户提供了“删除未决”挂起原因以及它进入此状态的时间戳。 “删除未决”状态和“挂起”时间戳的存储允许撰写实用程序，以确定这些“删除未决”帐户，并且稍后将其从“配给服务器”和管理端点删除。

重新创建已删除的帐户

如果您使用 CA Identity Manager 之外的工具删除管理端点的帐户，“检查帐户同步”功能会将帐户报告为缺失，因为它存在于“配给目录”中，但不在管理端点上。发生这一情况时，通过“将帐户与帐户模板同步”功能在端点重新创建帐户，方法是使用关联到帐户的帐户模板。

如果帐户被重新创建，CA Identity Manager 会将其记录为已重新创建。这些帐户可以独立于已更新帐户进行标识，因为管理员需要了解功能属性（例如密码）之外的属性是否已经被设成帐户模板初始值。

第 9 章： 配给角色

此部分包含以下主题：

配给角色和帐户模板

要简化帐户管理，请使用在配给角色中使用的帐户模板来创建并维护帐户。 一个配给角色包含一个或多个帐户模板。 将该角色应用到用户时，该用户会收到由模板定义的帐户。

这些模板对特定端点类型上的帐户提供了基础。 这些模板提供的功能类型与 eTrust Admin 中提供的配给策略相同。

使用帐户模板，您可以：

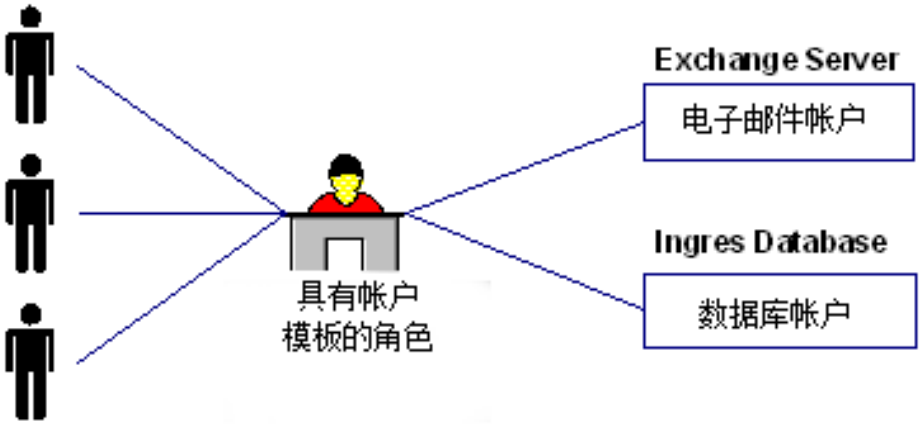
- 在创建 CA CA Identity Manager 用户帐户时控制这些用户在端点中拥有哪些帐户属性
- 使用规则字符串或值定义属性
- 合并不同配给角色中的帐户属性，以便用户在某个特定的端点上只有一个帐户，并带有所有必需的帐户属性
- 在全局用户更改配给角色时创建或更新帐户属性
- 同步帐户属性，以便全局用户只有他们所需的属性
- 执行查询以了解在同步操作中应创建、更新或删除哪些帐户
- 确定哪些帐户属性可与配给角色同步，哪些不能同步

创建角色以分配帐户

在多数组织中，管理员花费大量时间为用户提供不同系统和应用程序的登录帐户。 为了简化这项重复性活动，您可以创建配给角色，即包含帐户模板的角色。 模板定义了在一种类型的帐户中存在的属性。 例如，Exchange 帐户的帐户模板定义了邮箱大小等属性。 帐户模板还定义了用户属性如何映射到帐户。

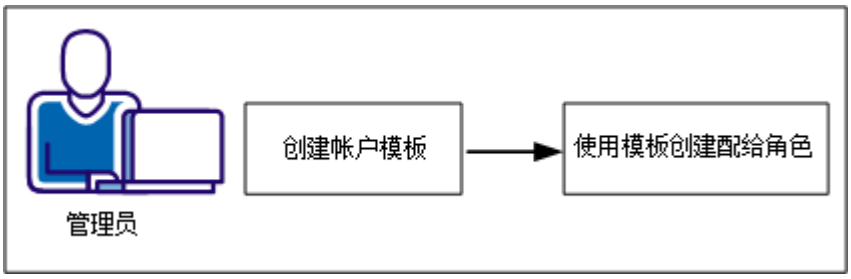
来看一个例子，Forward, Inc 的每个员工都需要访问数据库和电子邮件。 管理员不想只能以一次一个的方式为每位员工创建数据库帐户和电子邮件帐户。因此，管理员为该公司创建了配给角色。该角色包含用于 Microsoft Exchange 服务器的帐户模板（以提供电子邮件帐户）和用于 Oracle 数据库的模板。 在本例中，Exchange 服务器和 Oracle 数据库都称为端点，即帐户所在的系统或应用程序。

注意：Forward, Inc. 是虚构的公司名，完全只是用于演示目的，而不是指实际的公司。



创建角色之后，业务管理员（如管理人员或支持人员）可以将这些角色分配给用户，以便为其提供端点中的帐户。 用户收到角色之后，便可登录到端点。

创建包括帐户模板的配给角色这一过程分两步，具体如下：



以下部分说明如何创建可以用于分配帐户的角色：

1. 创建帐户模板 (p. 171)
2. 创建配给角色 (p. 171)

创建帐户模板

要简化帐户管理，请使用在配给角色中使用的帐户模板来创建并维护帐户。 一个配给角色包含一个或多个帐户模板。 将该角色应用到用户时，该用户会收到由模板定义的帐户。

这些模板对特定端点类型上的帐户提供了基础。

使用帐户模板，您可以：

- 在创建用户帐户时控制这些用户在端点中拥有哪些帐户属性
- 使用规则字符串或值定义属性
- 合并不同配给角色中的帐户属性，以便用户在某个特定的端点上只有一个帐户，并带有所有必需的帐户属性
- 在全局用户更改配给角色时创建或更新帐户属性

每个端点类型的默认帐户模板都是与 CA Identity Manager 服务器一起安装的。在配给角色中，您可以使用默认帐户模板，也可以针对您已配置的任意端点创建自己的帐户模板。

创建帐户模板

1. 导航到“端点”（可能列在“任务”下），然后依次单击“帐户模板”、“创建帐户模板”。
2. 选择该模板的端点类型。
3. 如果适用的话，将“端点名称”定义为该端点或本地主机的系统名称。
4. 在“端点”选项卡上选择一个要用的端点。
5. 完成填写各个选项卡的字段，或者使用默认值。

   每个端点类型都有一组不同的选项卡。 单击“帮助”可获取字段定义。
6. 单击“提交”。

注意：如果指定多个端点，在搜索帐户模板的端点对象时，则返回相关对象的通用子集（交集）。 示例是存在于与帐户模板关联的每个选定端点上的 Active Directory 组。 在搜索结果显示除对象名之外的属性时，它显示与第一个端点关联的对象属性值。 示例是 PeopleSoft 连接器中语言对象的说明属性。

创建配给角色

要创建配给角色，请先确定以下角色要求：

- 哪些用户需要其他帐户
- 哪些帐户与角色相关联
- 谁是该角色的成员、管理员和所有者

创建配给角色

1. 在用户控制台中，依次导航到“角色和任务”、“开通角色”和“创建开通角色”。

   有关每个选项卡的详细信息，请单击屏幕中的“帮助”链接。

2. 填写“配置文件”选项卡。 只有“名称”字段为必填字段。

   注意：可以在“配置文件”选项卡指定自定义属性，以便用于指定配给角色的有关附加信息。 可以使用这些附加信息帮助在含有很多角色的环境中进行角色搜索。

3. 填写“帐户模板”选项卡。

   a. 单击一种端点类型，例如 ActiveDirectory。

   b. 单击一个帐户模板。

      您可以单击的模板取决于端点类型。

   c. 根据需要为不同的端点类型添加更多帐户模板。

4. 如果要在“配给角色”选项卡中嵌套配给角色，请填写此选项卡。

   此步骤要求您已经为此环境启用嵌套角色 (p. 175)。

5. 填写“管理员”选项卡，在其中添加管理员规则，用于控制哪些人员可以管理此角色的成员和管理员。

6. 填写“所有者”选项卡，在其中添加所有者规则，用于控制哪些人员可以修改此角色。

7. 单击“提交”。

8. 要验证是否已创建角色，请依次单击“配给角色”、“查看配给角色”。

角色和模板任务

在用户控制台中，可以通过选择角色和任务并选择配给角色下的任务创建并管理配给角色。 标准操作的任务有：使用户成为角色成员、修改或删除角色。

创建配给角色之前，您需要一个要包括该角色的帐户模板或一个要导入的配给角色。 您可以导入在配给管理器或 eTrust Admin 中创建的角色。 但是，CA Identity Manager 不支持在 eTrust Admin 创建的嵌套角色。

导入配给角色

虽然您可在用户控制台中管理配给角色，但是某些配给角色可能已在配给管理器或外部应用程序中创建。 对于这些开通角色，您可以将角色所有者重置为 CA Identity Manager 管理员，以便您可以在用户控制台中进行管理。

导入配给角色

1. 以具有系统管理员角色的用户身份登录用户控制台。 依次单击“任务”和“角色和任务”。
2. 单击“配给角色”，“重置配给角色所有者”，然后选择一个在配给管理器中创建的配给角色。
3. 填写“所有者”选项卡，在其中添加所有者规则，用于控制哪些人员可以修改此角色。
4. 单击“提交”。

此时，您可以使用配给角色类别中的任务对角色进行修改、分配或查看。

为配给角色分配新的所有者

您可以选择一个或多个配给角色，然后分配所有者策略以便控制有权修改角色的用户。

为配给角色分配新的所有者

1. 以具有系统管理员角色的用户身份登录用户控制台。
2. 依次单击“任务”、“角色”，或单击“角色和任务”。
3. 依次单击“配给角色”、“创建配给角色的所有者策略”。
4. 选择一个或多个配给角色。
5. 填写“所有者”选项卡，在其中添加所有者规则，用于控制哪些人员可以修改此角色。
6. 单击“提交”。

满足新的所有者策略的用户可以修改选定的配给角色。

配给角色创建的帐户的密码

在分配给用户配给角色时，如果 CA Identity Manager 用户的密码不满足端点的密码要求，则该用户的帐户创建就会失败。 此情况包括创建具有临时密码的新用户。

因此，设置匹配或比端点密码要求更严格的密码策略。 通过使用 CA Identity Manager 密码策略或配给密码配置文件，您可以设置密码策略。 如果两种方式都被使用，则策略必须匹配。

配给角色事件处理顺序

某些默认的 CA Identity Manager 任务包括若干个*事件*，这些事件是 CA Identity Manager 完成某项任务所执行的操作，这些操作可确定配给角色成员资格。 例如，默认的“修改用户”任务包括 AssignProvisioningRoleEvent 和 RevokeProvisioningRoleEvent。 分配或吊销配给角色可能会在端点上添加或删除帐户。 某些情况下，端点可能会要求所有“添加”操作必须发生在“删除”操作之前。

要强制 CA Identity Manager 首先处理“添加”操作，请在管理控制台中启用“配给角色成员资格事件累计”设置。 启用该设置后，CA Identity Manager 会将所有的“添加”和“删除”操作累计到单个事件中，称为 AccumulatedProvisioningRolesEvent。 例如，如果“修改用户”任务将一个用户分配给三个配给角色，然后将该用户从其他两个配给角色中删除，则会生成 AccumulatedProvisioningRolesEvent，其中包含五个操作：3 个添加操作和 2 个删除操作。

执行该事件后，所有的“添加”操作都会被合并到单个操作中，然后发送到配给服务器进行处理。 “添加”操作处理完成后，CA Identity Manager 即会将“删除”操作合并到单个操作中，然后将该操作发送到配给服务器。

启用该设置会对 CA Identity Manager 的下列功能产生影响：

- **用户任务中的配给角色选项卡**

  当管理员使用“配给角色”选项卡将用户添加到配给角色或将其从中删除时，CA Identity Manager 会将这些操作累计到单个事件中。

- **身份策略**

  “身份策略”评估所生成的所有配给角色成员资格事件（AssignProvisioningRoleEvent 或 RevokeProvisioningRoleEvent）都会累计到单个的 AccumulatedProvisioningRolesEvent 中。 CA Identity Manager 像处理其他任何次要事件那样执行该事件。 例如，某个身份策略集包括两个身份策略：策略 A 吊销配给角色 A 中的成员资格，而策略 B 使用户成为配给角色 B 的成员。 如果 CA Identity Manager 确定某用户不再满足策略 A 但开始满足策略 B，则会生成包含两个操作（一个是删除操作，另一个是添加操作）的 AccumulatedProvisioningRolesEvent。 首先执行“添加”操作，然后执行“删除”操作。

- **查看提交的任务**

  要查看 AccumulatedProvisioningRolesEvent 以及每个操作的状态，请使用“查看提交的任务”任务来查看事件详细信息。

  如果其中一个操作失败，该事件的状态则为失败，这使该任务也进入失败状态。

- **工作流**

  您可以将工作流流程与 AccumulatedProvisioningRolesEvent 相关联。 在这种情况下，批准人可以批准或拒绝整个事件，也就是批准或拒绝每个单独的事件。

  还需要其他配置来启用 AccumulatedProvisioningRolesEvent 内各个事件的工作流。

- **审核**

  CA Identity Manager 审核 AccumulatedProvisioningRolesEvent 以及每个单独事件的相关信息。

启用配给角色成员资格事件累计

CA CA Identity Manager 在管理控制台上提供了一个配置设置，可用于将一个配给角色成员资格事件的所有“添加”和“删除”操作组合到一个操作中。 一旦组合完成，CA CA Identity Manager 会将“添加”操作作为单一操作处理，然后再处理“删除”操作。

该设置可以执行某些端点类型要求的事件排序。

注意：默认情况下禁用该功能。

启用配给角色成员资格事件累计

1. 访问 Identity Manager 管理控制台。
2. 单击“环境”。
3. 选择要配置的环境。
4. 依次打开“高级设置”、“配给”。
5. 选择“启用配给角色成员资格事件累计”复选框。
6. 重新启动应用程序服务器。

在环境中启用嵌套角色

您可以在一个配给角色中包括另一个配给角色。 被包括的角色称为嵌套角色。

例如，您可以创建员工配给角色。 员工角色将提供所有员工都需要的帐户（如电子邮件帐户）。 将员工角色包括在部门特定的配给角色（如财务角色和销售角色）中。 部门配给角色将提供仅与该部门相关的帐户。 角色的这种组合为每个用户提供正确的帐户。

在环境中启用嵌套角色

1. 在管理控制台中，选择“环境”。
2. 依次单击“角色”和“任务”设置、“导入”。
3. 选择“嵌套的配给角色支持”。

4. 单击“完成”。
5. 重新启动环境。

在配给角色中包括角色

在配给角色中包括角色

1. 依次导航到“角色和任务”、“开通角色”、“修改开通角色”。
2. 通过单击“添加角色”填写“配给角色”选项卡，然后选择配给角色。

   由于性能原因，建议将角色嵌套限制为三个级别。 例如，您要将另一个角色（第二级角色）包括在当前配给角色（第一级角色）中，第二级角色又可以包含一个第三级角色。 建议第三级角色不再包含角色。
3. 通过修改所有者规则来完成所有者策略。

   作用域必须等于或大于您添加的角色的作用域。
4. 单击“提交”。

帐户模板中的属性

帐户模板中的属性确定了如何在帐户中定义属性。

功能属性和初始属性

帐户模板包括两种类型的属性：

- *功能属性*表示帐户信息，如存储大小、数量、频率限制或组成员身份。 配给管理器将所有帐户模板屏幕中的功能属性进行加粗以方便识别。
- *初始属性*表示为帐户最初设置的所有信息，如帐户名称、密码和帐户状态以及个人信息（如姓名、地址和电话号码）。

在同步所有功能属性时，会认为帐户与其帐户模板同步。 这些属性因端点类型的不同而异，如组成员身份、权限、配额、登录限制；这些属性在登录帐户时控制用户可执行哪些操作。

同步不更新其他帐户属性。 这些属性是在帐户创建期间从帐户模板初始化的，也可在传播功能期间更新。 配给服务器提供两种传播功能（更改帐户模板时帐户立即更新，以及更改全局用户属性时帐户的更新）。

找到功能属性和初始属性

要找出哪些属性定义为功能属性以及哪些是初始属性，您需要生成 eTACapability.txt 文件。 在 Windows 命令提示符下输入以下命令：

```
PS_HOME\dumpptt.exe -c > eTACapability.txt
```

PS_Home

指定 C:\Program Files\CA\Identity Manager\Provisioning Server\bin

即会为您已安装的所有连接器生成一个文件版本。

帐户模板中的规则字符串

在创建帐户模板时，可使用规则字符串来定义多个帐户属性的格式。 规则字符串是实际值的变量。当您要生成因帐户而异的属性时，规则字符串会非常有用。对规则进行评估时，CA Identity Manager 将使用用户对象中指定的数据替换在帐户模板中输入的规则字符串。

注意：对于在浏览过程中创建的帐户或创建时不带配给角色的帐户，不会进行规则评估。

下表列出 CA Identity Manager 中的规则字符串：

规则字符串	说明
%AC%	帐户名称
%D%	格式为 *dd/mm/yyyy* 的当前日期（该日期为不涉及全局用户信息的计算值）。 该规则字符串与下面内容相同： %$$DATE()% %$$DATE%
%EXCHAB%	在 Exchange 地址簿中隐藏邮箱
%EXCHS%	邮箱主服务器名
%EXCMS%	邮箱存储名
%GENUID%	数字型 UNIX/POSIX 用户标识符。 只要设置了全局用户的 UID 值，该规则变量就与 %UID% 相同。 然而，如果全局用户没有分配的 UID 值，但启用了 UID 生成功能（系统任务的全局属性），则会发生几项操作。下一可用 UID 值将分配给全局用户，并用作该规则变量的值。
%P%	密码
%U%	全局用户名

规则字符串	说明
%UA%	完整地址（由街道、城市、省/自治区/直辖市和邮政编码生成）
%UB%	楼宇
%UC%	城市
%UCOMP%	公司名称
%UCOUNTRY%	国家/地区
%UCU*xx*% 或 %UCU*xxx*%	自定义字段（*xx* 或 *xxx* 表示“系统任务”框架中“自定义用户字段”选项卡上指定的 2 位或 3 位数字的字段 ID）
%UD%	说明
%UDEPT%	部门
%UE%	电子邮件地址
%UEP%	主要电子邮件地址
%UES%	次要电子邮件地址
%UF%	名字
%UFAX%	传真号
%UHP%	主页
%UI%	英文名缩写
%UID%	数字型 UNIX/POSIX 用户标识符
%UL%	姓氏
%ULOC%	位置
%UMI%	中间名首字母
%UMN%	中间名
%UMP%	手机号码
%UN%	全名
%UO%	办公室名称
%UP%	电话号码
%UPAGE%	传呼机号码
%UPC%	邮政编码
%UPE%	电话分机号码

规则字符串	说明
%US%	省/自治区/直辖市
%USA%	街道地址
%UT%	职位
%XD%	生成格式为 XML dateTimeValue、固定长度字符串格式的当前时间戳。 在 dateValue 或 timeValue 属性中，您可以编写一个子字符串表达式 (:offset,length) 来提取 dateTimeValue 的日期或时间部分。 例如：%XD:1,10% 会生成 YYYY-MM-DD；%XD:12,8% 会生成 HH:MM:SS。

属性值

要对帐户属性使用特定的常量值，请在帐户模板字段中输入值，而不是输入规则字符串。 例如，可以输入指定频率限制或数量大小的值。

如果该常量属性值必须包含多个百分号，则请每次输入两个百分号 (%%)。CA CA Identity Manager 在构建帐户属性值时会将它们转换为一个百分号 (%)。 如果帐户模板值仅包含一个百分号，CA CA Identity Manager 则不会产生错误。 该规则说明，如果需要字面值 25%，则必须指定 25%%。但是，作为特例，也接受 25%。

高级规则表达式

为了比简单的全局用户属性替换更加灵活，您可以输入高级规则表达式，其中包括以下内容：

- 使用 Offset 和 Length 的规则表达式子字符串
- 规则字符串和值的组合
- 用于为多值帐户属性设置多个值的规则表达式
- 其他全局用户属性的规则变量
- 内置函数的调用
- 客户编写的程序出口函数的调用

组合规则字符串和值

您可以将多个规则字符串和多个常数值组合到一个帐户模板属性值中。 例如，如果没有 %UI% 规则字符串，您则可以通过串联多个规则表达式来获得同样的效果，如下所示：

```
%UF:,1%%UMI:,1%%UL:,1%
```

%UA% 规则字符串相当于以下内容：

```
%USA%, %UC%, %US%, %UPC%
```

您也可以将一个规则字符串与一个常数值进行组合，以创建一个 UNIX 主端点属性，如下所示：

```
/u/home/%AC%
```

规则子字符串

以下内容是用于创建规则变量的子字符串值的语法：

```
%var[:offset,length]%
```

var

表示先前所显示表中定义的预定义规则变量的名称。

offset

（可选）定义子字符串后缀的开始偏移量。 数字 1 表示第一个字符。

length

（可选）定义子字符串后缀的结束偏移量。 长度值星号 (*) 表示到值的结尾。

例如，要将某个帐户属性设置为全局用户“楼宇”属性的前 4 个字符，请使用以下内容来定义该变量：

```
%UB:1,4%
```

如果“楼宇”属性为空或少于四个字符，则最终生成的帐户属性值将少于四个字符。

多值规则表达式

大多数规则表达式都是单值的。 它们始于一个用户属性值（可能为空），也会生成一个帐户属性值（也可能为空）。 然而，有时您可能想将空的用户属性视为 0 个值。 有时您可能想生成多个值来填充一个多值帐户属性值。

通过使用下列的规则语法，可以对一个用户属性可能包括的零个或多个值进行操作：

%*var*%

在规则表达式的第一个百分号 % 之后紧挨着的可选多值标志星号 (*) 表示该规则表达式的结果应当是 0 个、1 个或多个值，具体取决于所引用用户属性包含多少值。

大多数用户属性值都是单值的，因此它们只可能包括 0 个或 1 个值。 然而，自定义属性（CustomField01 到 CustomField99）是多值属性，因此引用这些属性的规则变量可能包含 0 个、1 个或多个值。

如果某个用户属性具有多个值，但您在规则表达式中未包括星号 (*)，则该规则评估的结果将是第一个值的结果。 而在大多数情况下属性值通常是无序的，因此 CA Identity Manager 首先考虑的值可能无法预测。

如某个用户属性具有多个值，并且您在规则表达式中包括了 *，则会为该帐户属性生成多个值。 如果基于帐户模板属性设置的帐户属性本身不是多值的，则请不要在该帐户模板中定义这样的多值规则表达式。

您可以将 ADS 端点类型中的扩展帐户属性设置为多值；然后使用该多值规则表达式语法来设置该属性。例如，某个环境定义了一个名为 patents 的扩展 ADS 帐户属性和三个也命名为 patents 的自定义用户属性。

某个 ADS 帐户模板对于该 patents 属性可以定义规则字符串 %*UCU03%。 然后，您可以通过添加一个或多个值，来更改某个用户的 patents 属性。将这些更改应用于该用户时，要选择更新该用户帐户的选项。 此操作将参考该帐户的帐户模板，查找规则变量 %*UCU03%，并且知道要将该用户的所有 patents 均复制到该帐户的 patents 属性。

与之相似，在帐户创建期间也会评估规则字符串。 而且在帐户模板更改期间，如果该规则字符串已发生更改，则可以选择对于关联到该帐户模板的所有帐户重新评估该规则。

%*var*% 语法对于引用单值用户属性的变量 *var* 来说也是有意义的。 上述情况仅适用于涉及串联，以及对于用户未设置所引用属性的情况。

可选的多值标志星号 (*) 表示：如果用户属性没有值，包含 *var*% 规则变量的规则则会评估为无值。 这不同于单值规则表达式 %*var*%，该单值规则表达式总是评估为一个值，即使是空字符串也是如此。

要了解该差异，请看下面的规则字符串：

```
(310)%UP%
 (310)%*UP%
```

这两个规则字符串好像都是在电话号码后面附加地区代码 310。 然而，它们其实是不同的，因为如果用户对于其电话号码没有值，则第一个规则会评估为帐户值 (310)。第二个规则字符串则不会生成任何值并且将帐户属性保持为未设置状态。

另一方面，请看下面规则字符串，这两个规则字符串好像都是要在电话号码后面附加电话分机：

```
%UP% %UPE%
%UP% %*UPE%
```

如果每个人都有电话号码，但是一些人没有分机号，则第一个规则字符串将对于每个没有分机号的用户生成包括电话号码的值。 第二个规则字符串则不生成值。 在这种情况下，请使用带 %UPE% 的第一个规则。

显式全局用户属性规则

每个用户拥有的属性都比以前规则表中所列出的内容要多很多。 您可能不需要创建引用其他这些属性的规则表达式。 但如果这种需求出现，则可以使用以下语法来引用某个特定的用户属性：

```
%#ldap-attribute%
```

例如，如果必须确定用户“已挂起”字段的值，则应确定该字段相应的 LDAP 属性名称（eTSuspended），并创建评估为 0 或 1（与 eTSuspended 相同）的规则表达式：

```
%#eTSuspended%
```

还例如，您可以使用下列规则表达式获得用户的分配配给角色：

```
%*#eTRoleDN%
```

这些配给角色是 LDAP 完全可分辨名称值。 也许这些值与内置函数 RDNVALUE（见下表）结合起来会更有用一些。 请注意多值指示标志星号 (*)，这是为了将该用户的所有已分配配给角色获取为多个值。

子字符串语法也适用于这些规则表达式，因此您可以使用 %#eTTelephone:6,*% 来表示与 %UP:6,* 相同的意思。 每个字符串都要求 CA CA Identity Manager 去掉用户电话字段的前五个字符。

内置规则函数

您可以在规则表达式中使用内置规则函数来对值进行各种变化。 内置规则函数调用的一般形式为

```
%[*]$$function(arg[,…])[:offset,length]%
```

其中，多值指示器星号 (*) 以及 Offset 和 Length 子字符串的指定也是可选的。

常用的内置函数如下所示：

内置规则函数	说明
ALLOF	将所有参数合并到一个多值属性中。 保留顺序但会删除重复。 例如，如果用户属性设置为以下内容： eTCustomField01: { A, B } eTCustomField02: { A, C } 则规则： %*ALLOF(%*UCU01%,%*UCU02%)% 会评估为三个值 { A, B, C }。
DATE	评估为 *dd/mm/yyyy* 格式的当前日期。规则表达式 %D% 相当于以下内容之一： %$$DATE()% %$$DATE%
FIRSTOF	返回任何参数的第一个值。 如果不设置属性则用于插入默认值： %$$FIRSTOF(%UCU01%,'unknown')% %$$FIRSTOF(%LN%,%UCU01%,%U%)% 如果未设置任何值，结果则是没有值。要在参数中输入常量字符串，请将其放在单引号中。
INDEX	返回多值属性的一个值。 索引 1 是第一个值。 如果索引大于值的数目，结果则是未设置（空）值。 下列规则相当于以下内容： %$$INDEX(%*UCU01%,1)% %$$FIRSTOF(%*UCU01%)%

内置规则函数	说明
NOTEMPTY	返回其中一个参数的单一值，但如果未设置该设置时则会报告失败。 示例 1： 如果用户没有指定的 UID 属性，则使得帐户创建或更新失败： %$$NOTEMPTY(%UID%)% 示例 2： 使用名字，除非没有设置名字，在这种情况下使用姓氏。 如果都没设置，则帐户创建或更新失败。 %$$NOTEMPTY(%$$FIRSTOF(%UF%, %UL%)%)%
PRIMARYEMAIL	返回从多个电子邮件地址提取的主要电子邮件地址。 表达式 %UE% 相当于以下内容： %$$PRIMARYEMAIL(%UEP%)%
RDNVALUE	将属性值视作 LDAP 可分辨名称，并从该 DN 提取对象的通用名称： %*$$RDNVALUE(%#eTRoleDN%)% 该表达式将返回所有分配的配给角色的通用名称。 如果用户属于具有相同通用名称的两个配给角色，则列出该角色名称一次。
TOLOWER	将大写文本转化成小写： %$$TOLOWER(%AC%)%
TOUPPER	将小写文本转化成大写： %$$TOUPPER(%U%)%

内置规则函数	说明
TRIM	删除属性值中的前导和结尾空白字符。 例如，“%UF %UL%”通常会创建一个以空白字符分隔的名字和姓氏组成的值。 然而，如果用户的名字属性为空，该规则则生成一个以空白结束的值。 但使用 “%$$TRIM(%UF% %UL%)% 将确保帐户属性值中不存在前导和结尾空白，即使未设置名字或姓氏中的一个也是如此。

配给角色性能

将 CA Identity Manager 用于配给服务器时，您可能想考虑一些配给性能增强问题。

JIAM 对象缓存

Identity Manager 使用 Java IAM (JIAM) API 与配给服务器进行通信。 为了改进通信性能，您可以为从配给服务器检索的对象配置缓存。

启用 JIAM 缓存

启用 JIAM 缓存

1. 通过管理控制台访问环境设置。 单击“高级设置”，“杂项”。
2. 为 JIAM 缓存配置用户定义属性。
   - **属性** — JIAMCache
   - **值** — true
3. 单击“添加”。
4. 单击“保存”。

   此时该用户定义属性得以保存。

定义 JIAM 缓存 TTL（生效时间）

JIAM 缓存存储信息的时间为数据到期之前的一个指定时间段。 该时间段称为生效时间 (TTL)。 您可以设置 JIAM 缓存 TTL 值（以秒为单位）来定义数据存在于缓存中的时间。

要从本地缓存数据获取最大利益，您要在性能提升和数据的及时性之间进行权衡。 我们建议 TTL 最小值为 1 天，最大值为 7 天。 请参见下表了解要使用的生效时间值：

所需生命周期	TTL 设置（秒）
24 小时（1 天）	86,400
72 个小时（3 天）	259,200
120 个小时（5 天）	432,000
168 个小时（7 天）	604,800

定义 JIAM 缓存 TTL

1. 通过管理控制台访问环境。 单击“高级设置”，“杂项”。
2. 为 JIAM 缓存 TTL 配置用户定义属性。
   - **属性** — JIAMCacheTTL
   - **值** — 数据在 JIAM 缓存中的秒数

     默认值：300
3. 单击“添加”。
4. 单击“保存”。

   此时该用户定义属性得以保存。

会话缓冲池

为了改进性能，当 Identity Manager 与配给服务器进行通信时，可能会预先分配一些会话进行缓冲。

有关电子邮件通知的详细信息，请参阅 *管理控制台联机帮助*。

用于现有环境的配给任务

如果要导入自定义角色定义并且想在环境中启用配给，则必须*同时*在管理控制台中导入“仅配给”角色定义。 这些角色定义位于以下文件夹：

```
iam_im.ear\management_console.war\WEB-INF\Template\environment
```

注意：有关导入角色定义的详细信息，请参阅《*Configuration Guide*》（《配置指南》）。

第 10 章： 管理服务（基本访问请求）

此部分包含以下主题：

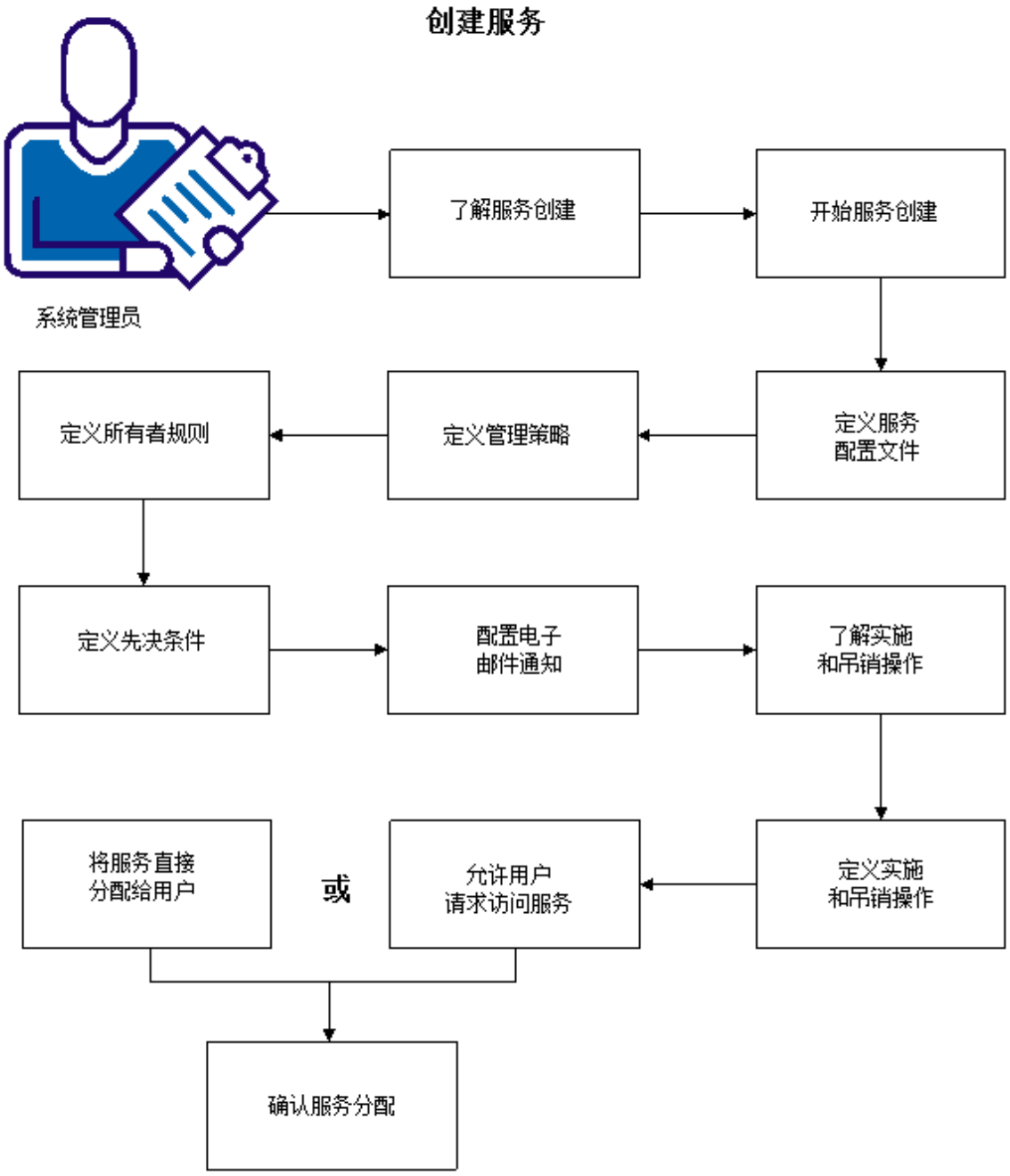
创建服务

服务可简化权利管理。服务将用户的指定业务角色所需的所有权利（包括任务、角色、组以及属性）捆绑在一起。 服务通过 CA CloudMinder 用户控制台中的访问请求任务提供给用户。 通过访问请求任务，用户或管理员可以请求、分配、吊销和续订服务。

管理员可以通过服务将用户权利合并到一个数据包中，并作为一个集合进行管理。 例如，所有新销售员工都需要访问定义的一系列任务和特定端点系统上的帐户。 他们还需要访问添加到其用户帐户配置文件中的特定信息。 管理员创建名为“销售管理”的服务，包含新销售员工所需的所有任务、角色、组以及配置文件属性信息。 当管理员将“销售管理”服务分配给用户时，该用户会收到由该服务定义的一整套角色、任务、组和帐户属性。

用户可以访问服务的另一种方式是自己请求访问。 在用户控制台中，每个用户都有一个可供其请求的服务列表。 通常，此列表由具有适当权限的管理员在服务创建过程中使用标记为“自行订阅”的服务填充。 从可用服务列表中，用户可以请求访问其所需的服务。 用户请求访问服务时，请求将自动履行，关联权利将立即分配给用户。 具有适当权限的管理员也可以将服务履行配置为需要工作流审批，或生成电子邮件通知。

下图说明了创建服务要了解的信息以及执行的步骤。


创建服务
系统管理员
了解服务创建
开始服务创建
定义服务
配置文件
定义管理策略
定义所有者规则
定义先决条件
配置电子
邮件通知
了解实施
和吊销操作
定义实施
和吊销操作
允许用户
请求访问服务
或
将服务直接
分配给用户
确认服务分配

以下主题将介绍如何创建服务并将服务提供给用户：

1. 了解服务创建 (p. 192)。
2. 开始服务创建 (p. 193)。
3. 定义服务配置文件 (p. 193)。
4. 定义服务的管理策略 (p. 194)。
5. 定义服务的所有者规则 (p. 195)。
6. 定义服务的先决条件 (p. 195)。
7. 为服务续订配置电子邮件通知。 (p. 196)
8. 了解履行和吊销操作 (p. 197)。
9. 定义服务的履行和吊销操作。 (p. 197)
10. 允许用户请求对服务的访问。

    在用户控制台中，依次单击“我的访问”、“请求和查看访问”后，用户将看到可供请求的服务列表。 通常，此列表中显示的服务是具有适当权限的管理员在服务创建过程中标记为“自行订阅”的服务。
11. 将服务直接分配给用户 (p. 74)。
12. 确认服务分配。

了解服务创建

创建服务之前，请考虑创建和履行服务所需的先决条件信息和权利。

请考虑以下问题：

1. 此服务解决什么业务需求？ 例如，您可以创建一项将 Salesforce.com 上的帐户提供给所有新员工的服务。
2. 服务的成员需要特定管理角色吗？ 如果需要，创建或确定这些管理角色。
3. 服务的成员必须获得一个或多个端点的访问权限吗？ 如果需要，创建或确定这些端点。
4. 如果服务的成员需要访问端点，请创建或确定关联的配给角色和帐户模板。
5. 服务的成员必须是特定组的成员吗？ 如果是，创建或确定这些组。
6. 用户成为服务成员时，必须引用或修改特定用户属性吗？ 例如，用户收到 Salesforce.com 服务时，有必要确认该用户的部门属性是否设置为了“销售”吗？ 如果有必要，创建或确定这些用户属性。

创建或确定这些先决条件后，您即可以开始创建服务 (p. 193)。

开始服务创建

从用户控制台创建服务。

遵循这些步骤:

1. 登录到具有服务管理权限的帐户。

   例如，某环境的第一位用户具有“系统管理员”角色，而该角色具有“创建服务”任务。

2. 从导航菜单，选择“服务”，它可能列在“任务”下。
3. 依次单击“管理服务”、“创建服务”。
4. 定义服务配置文件。

定义服务配置文件

在“配置文件”选项卡上，定义服务的基本特征。

遵循这些步骤:

1. 输入名称和标记。 标记是服务的唯一标识符。

   注意：标记只能包含字母数字和下划线字符，且不能以数字开始。 一旦创建了标记名称，该名称就无法更改或重新使用，即使稍后删除服务也不例外。

2. 如果要在服务创建之后立即提供给用户，请选择“已启用”。
3. 如果要将服务显示在可供用户请求的服务列表中，请选择“自行订阅”。 启用“自行订阅”后，用户可通过用户控制台请求访问此服务。
4. （可选）增加一个或多个类别。 键入类别名称，然后单击向上箭头，将其添加到服务中。

   类别会将其他信息添加到服务中。 可以使用这些其他信息帮助在包含很多项服务的环境中搜索服务。

5. 如果想在用户请求服务时收集其他用户数据，请指定服务运行时用户数据屏幕。

   使用服务运行时用户数据屏幕有助于确保系统中存在履行服务必需的所有用户数据。 例如，要履行在 Google Apps 中创建帐户的服务，需要有效的电子邮件地址。如果 CA CloudMinder 用户存储中不存在用户的电子邮件地址，用户需要在请求服务时提供。

a. 单击“浏览”。

此时将显示可用的配置文件屏幕列表。 这些屏幕通常用于收集用户数据。

b. 选择包含要收集的用户数据的配置文件屏幕。 选择以下选项之一：

- 单击“选择”以收集包含在该屏幕内的所有用户数据。

OR

- 单击“复制”以自定义要收集的用户数据。 为新屏幕指定名称和唯一标记。 添加、编辑或移除用户数据元素，然后单击“确定”。

OR

- 单击“编辑”以更改包含在该屏幕内的用户数据。 添加、编辑或移除用户数据元素，然后单击“确定”。

重要说明！ 如果编辑用户数据屏幕，则所做更改将应用于用户控制台中使用该屏幕的任何位置。 因此，请考虑复制和自定义配置文件屏幕。

c. 单击“选择”。

用户请求服务时，将收集所选的用户数据元素。

注意：如果用户请求服务时系统中存在所需数据，则数据将预填充在配置文件屏幕中。

6. 定义服务的管理策略 (p. 194)。

定义服务的管理策略

在“管理员”选项卡上，定义可作为此服务的成员和管理员添加或移除用户的人员。 管理策略包含管理和作用域规则以及至少一项管理员权限（管理成员或管理管理员）。

管理规则定义可以管理此服务的人员。 作用域规则限制哪些用户可以成为管理员。 例如，管理规则可以允许“销售”组的所有成员管理服务。 然后，作用域规则可以将这些用户仅局限于马萨诸塞州波士顿的“销售”组的成员。

遵循这些步骤:

1. 在“管理员”选项卡上，单击“添加”。

将显示“管理策略”屏幕。

2. 定义哪些用户可以管理此服务的管理规则。 例如，您可以指定“销售”组的成员用户，或具有“销售经理”特定职位配置文件属性的人员。

单击向左箭头以编辑规则的先前指定的部分。

3. 定义作用域规则以限制哪些用户可以管理该服务。 例如，如果在您的管理规则中指定的用户是“销售”组的成员，那么您可以将该规则的作用域限制为仅作用于马萨诸塞州波士顿这个城市的用户。

   注意：您可以为每个服务添加多个使用不同规则和不同权限的管理策略。

4. 如果您希望允许管理员添加或删除该服务的成员，请单击“可以管理该服务的成员”。
5. 单击“确定”。
6. 要进一步编辑策略，请单击“编辑”图标。 要删除策略，请单击减号图标。
7. 定义服务的所有者规则。 (p. 195)

定义服务的所有者规则

在“所有者”选项卡上，定义谁可以成为服务所有者的相关规则。 所有者是可以修改服务的用户。

遵循这些步骤:

1. 在“所有者”选项卡上，单击“添加”。

   系统将显示“所有者规则”屏幕。

2. 定义用来确定哪些用户可以拥有该服务的所有者规则。 例如，您可以指定“销售”组的成员用户，或具有“销售经理”特定职位配置文件属性的人员。

   单击向左箭头以编辑规则的先前指定的部分。

3. 单击“确定”。
4. 定义服务的先决条件。 (p. 195)

定义服务的先决条件

在“先决条件”选项卡上，定义用户在请求该服务前必须先拥有的服务。 只有当指定的用户是所有先决服务的成员时，该服务才会显示在该用户的可用服务列表中。

为先决服务设置持续时间后，该持续时间将适用于您正定义的服务。 例如，服务 A 是服务 B 的先决条件。 服务 A 的持续时间为一周。 服务 B 也在一个星期内到期。

遵循这些步骤:

1. 在“先决条件”选项卡上，单击“添加服务”。

   此时显示一个搜索屏幕。

2. 搜索您想将其指定为该服务的先决条件的服务。

   要显示您有管理权限的所有服务的列表，请单击“搜索”而不修改搜索条件。

3. 选择一项服务，然后单击“选择”。

   系统将显示该服务的先决条件的更新列表。

为服务续订配置电子邮件通知

有些服务将在一个特定的时间段之后到期。

在“电子邮件”选项卡上，您可以配置电子邮件通知，提醒服务成员在其会员资格到期前进行续订。然后成员可以使用“续订服务”任务来续订他们的访问权限。

CA CloudMinder 可提供包括动态内容的默认电子邮件模板。 该内容会在发送电子邮件时自动填充。 在电子邮件通知编辑器中显示在大括号 ({}) 中的动态内容可以向电子邮件添加特定的用户名、服务名称和到期日期。

您可以在编辑器中修改电子邮件通知的内容。 例如，您可以修改正文或主题文本、更改字体或删除动态内容。

配置电子邮件通知时要注意以下事项：

- 如果要在电子邮件通知中包括动态内容，请不要修改大括号 ({ }) 内的文本。
- 如果服务具有到期的先决服务，则仅为该先决服务发送电子邮件通知，即使为两种服务都配置了电子邮件通知也是如此。

遵循这些步骤:

1. 在“电子邮件”选项卡上，选中“服务到期之前发送给用户的电子邮件通知”复选框以启用通知。
2. （可选）使用编辑器中的控件自定义电子邮件通知。

   电子邮件通知编辑器支持 HTML。单击工具栏中的“Toggle HTML Source”按钮 (<>) 可以将 HTML 内容添加到电子邮件通知的正文中。

3. 了解履行和吊销操作。 (p. 197)

了解履行和吊销操作

在“操作”选项卡上，您可以定义要在分配或吊销服务时添加、修改或删除的权利和信息（任务、角色、组以及属性）。 简而言之，服务操作可定义服务执行的操作。

CA CloudMinder 使用 Policy Xpress 策略定义履行和吊销操作在什么情况下发生。 CA CloudMinder 可预配置该策略，以便不管用户何时请求服务，都能获得适当的条件和数据。 该服务会自动履行或吊销。

管理员必须定义履行或吊销服务时系统执行的操作。 例如，创建服务时，管理员可以为服务成员指定“销售经理”管理角色、Salesforce.com 配给角色和“销售”组。 同样，管理员也可以指定在吊销服务时删除这些权利。

定义服务的履行和吊销操作

在“操作”选项卡上，您可以定义在将服务分配给用户或从用户删除服务时系统添加、修改或删除的权利和信息。

遵循这些步骤:

1. 单击“操作”选项卡。

   系统将显示“履行和吊销操作”屏幕。

2. 单击“管理实施操作”或“管理吊销操作”按钮。

   此时将显示“创建 Policy Xpress 策略”屏幕。

   将预先定义以下字段以创建操作规则：

   名称

   提供操作规则的友好名称。 该名称必须唯一。

   说明

   定义操作规则的含义。

   优先级

   定义在多个操作规则匹配的情况下要执行哪个操作规则。该字段在定义默认操作时十分有用。 例如，如果您有多个规则，每一个规则为一个部门名称，则可以通过添加没有条件但为较低优先级（如 10，而其他优先级是 5）的其他规则来设置默认值。 如果不匹配任何部门的规则，那么将使用默认值。

3. 指定在“操作规则条件”下匹配的条件。
4. 单击“添加操作”下的“匹配时添加操作”按钮

   系统将显示“匹配时添加操作”屏幕。 在该屏幕上，您可以定义规则相匹配时系统执行的操作。
5. 输入定义操作用途的友好名称。

   例如，输入“添加销售经理管理角色”。
6. 选择您希望系统执行的操作的类别。

   例如，要添加角色，请选择“角色”类别。
7. 选择您希望系统执行的操作的类型。

   例如，要添加或删除管理角色，请选择“设置管理角色”类型。
8. 选择您希望系统执行的功能。

   例如，要添加管理角色，请选择“添加”功能。

   注意：选择功能时，将显示该功能的说明。 该说明可以帮助您确定选择的功能是否产生您想要的系统行为。
9. 定义您希望系统执行的特定操作。

   例如，要添加名为“销售经理”的管理角色，请输入角色名称，或单击“浏览”按钮并从可用的管理角色列表中选择“销售经理”。
10. 单击“确定”。

    重复该步骤，直到您为该服务添加了所有需要的操作。
11. 单击“确定”。

    系统会将指定的履行和吊销操作与服务关联。 当用户获得服务时，会添加、修改或删除关联的权利和信息。
12. 您可以立即将服务分配给用户 (p. 74)。

将服务分配给用户

您可以将服务直接分配给个别用户。 该用户成为该服务的*成员*。

遵循这些步骤:

1. 依次导航到“服务”、“请求和查看访问”。

   此时显示一个您可以管理的服务的列表。
2. 选择要分配给用户的服务，然后单击“选择”。

   此时显示一个分配给服务的用户的列表。
3. 单击“请求访问”。

4. 搜索您要给其分配服务的用户。

   要显示您有管理权限的所有用户的列表，请单击“搜索”而不修改搜索条件。

5. 选择一个用户，然后单击“选择”。

   此时显示一个分配给服务的用户的更新列表。

6. 单击“保存更改”。

   用户会收到指定的服务。用户收到包括在该服务中的所有应用程序、角色、组和属性。

确认服务分配

在将服务分配给用户后，请确认与该服务关联的所有任务均已成功完成。

遵循这些步骤:

1. 依次导航到“服务”、“查看服务访问请求历史”。

   此时显示一个搜索屏幕。

2. 搜索您分配给用户的服务。

   要显示您有管理权限的所有服务的列表，请单击“搜索”而不修改搜索条件。

   此时显示一个您可以管理的服务的列表。

3. 选择您分配的服务，然后单击“选择”。

   此时显示与服务关联的操作的历史记录。

4. 单击“上次更改”以先看最近的操作。

5. 确认上述用户成功收到服务。

6. 单击“关闭”。

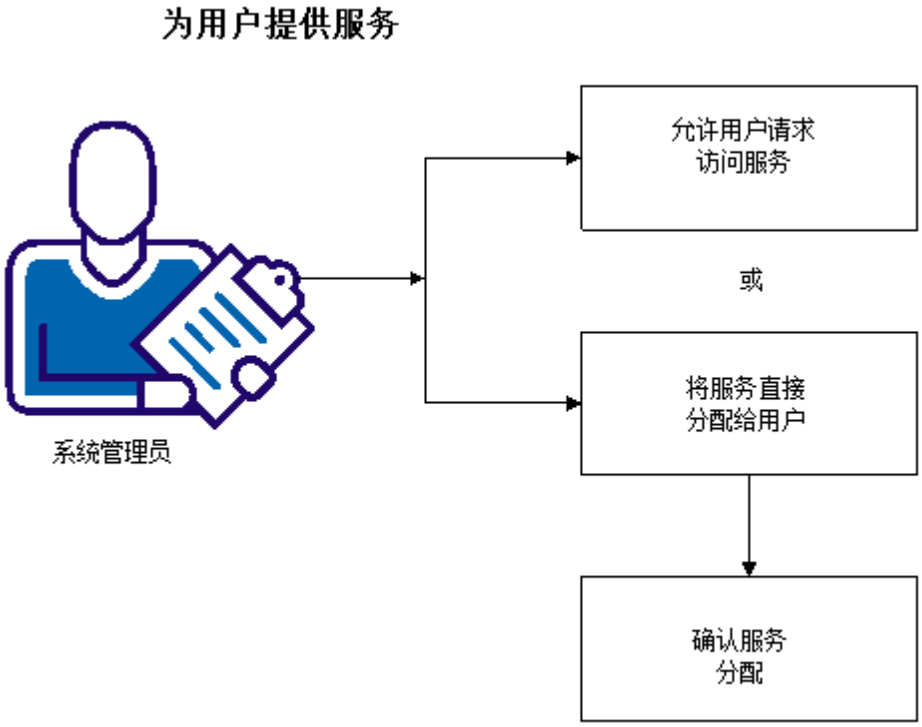
将服务提供给用户

服务可简化权利管理。 服务将用户针对指定业务角色所需的所有权利捆绑到一起。 在用户控制台中，通过“访问请求”任务，可将服务提供给用户。 通过“访问请求”任务，用户或管理员可以通过用户界面请求、分配、吊销和续订服务。

通过服务，系统管理员可将用户活动和信息（任务、角色、组以及属性）合并为一个包，作为一个集合来进行管理。 例如，所有新销售员工需要访问一组定义的任务、特定端点系统帐户以及添加到其用户帐户配置文件中的特定信息。系统管理员可创建一项名为“销售管理”的服务，其中包含新销售员工的所有必需任务、角色、组以及配置文件属性信息。 当管理员将“销售管理”服务分配给用户时，该用户会收到由该服务定义的一整套角色、任务、组和帐户属性。

用户可以访问服务的另一种方式是自己请求访问。 在用户控制台中，每个用户都有一个可供其请求的服务列表。 该列表包含由具有适当权限的系统管理员通常在服务创建期间标记为“自行订阅”的服务。 从可用服务列表中，用户可以请求访问其所需的服务。当用户请求访问服务时，请求会自动履行。关联的任务、角色、组和属性会立即分配给用户。 具有适当权限的 CA CloudMinder 管理员还可以将服务实施配置为需要工作流批准，或生成电子邮件通知。

下图显示要了解的信息以及要执行的步骤，以便将服务提供给用户。



您可以使用下列方式将服务提供给用户：

1. 允许用户自己请求访问。

   在 CA CloudMinder 用户控制台中，用户依次单击“我的访问”、“请求及查看访问”后，会看见一个可供其请求的服务列表。 该列表中显示的服务是具有适当权限的 CA CloudMinder 管理员通常在服务创建期间标记为“自行订阅”的服务。

   用户请求访问时，系统将服务分配给用户。 用户收到与该服务关联的所有应用程序、角色、组和属性。 如果该服务包括应用程序的启动角色，应用程序的图标和链接则出现在用户控制台主页中。

2. 将服务直接分配给用户 (p. 74)。
3. 如果您将服务直接分配给用户，请确认服务分配 (p. 201)。

将服务分配给用户

您可以将服务直接分配给个别用户。 该用户成为该服务的*成员*。

遵循这些步骤:

1. 依次导航到“服务”、“请求和查看访问”。

   此时显示一个您可以管理的服务的列表。

2. 选择要分配给用户的服务，然后单击“选择”。

   此时显示一个分配给服务的用户的列表。

3. 单击“请求访问”。

4. 搜索您要给其分配服务的用户。

   要显示您有管理权限的所有用户的列表，请单击“搜索”而不修改搜索条件。

5. 选择一个用户，然后单击“选择”。

   此时显示一个分配给服务的用户的更新列表。

6. 单击“保存更改”。

   用户会收到指定的服务。用户收到包括在该服务中的所有应用程序、角色、组和属性。

确认服务分配

在将服务分配给用户后，请确认与该服务关联的所有任务均已成功完成。

遵循这些步骤:

1. 依次导航到“服务”、“查看服务访问请求历史”。

   此时显示一个搜索屏幕。

2. 搜索您分配给用户的服务。

   要显示您有管理权限的所有服务的列表，请单击“搜索”而不修改搜索条件。

   此时显示一个您可以管理的服务的列表。

3. 选择您分配的服务，然后单击“选择”。

   此时显示与服务关联的操作的历史记录。

4. 单击“上次更改”以先看最近的操作。

5. 确认上述用户成功收到服务。

6. 单击“关闭”。

修改服务

作为系统管理员，您可以修改之前创建的服务。 例如，您可以通过将角色添加到服务中，更改服务授予服务成员的权利。 您还可以针对服务、服务先决条件和其他管理详细信息，调整管理员和所有者规则。

如果 CA CloudMinder 已履行给定用户的服务，则对该服务所做的任何更改不会传播到该用户。 如果您决定修改某项服务，则在您更改之前，收到该服务的用户拥有原始权利。 在您更改之后，收到该服务的用户拥有修改后的服务授予的权利。 例如，考虑以下情形：

作为系统管理员，您创建了“销售经理”服务，其将“销售经理”角色和“销售”组授予服务成员。 用户请求“销售经理”服务，CA CloudMinder 通过将适当角色和组授予用户履行了该服务。 您决定修改“销售经理”服务，以包括“员工经理”角色。 然后，服务的现有成员不会收到“员工经理”角色。 只有“销售经理”服务的新成员才会收到“员工经理”角色，除此之外，新成员还会收到“销售经理”角色和“销售”组。

因此，只有当服务没有成员时，才考虑修改服务。 也就是说，只有当用户没有请求并收到服务且管理员也没有将服务分配给用户时，才修改服务。

您可以修改服务的管理信息、管理员和所有者规则、服务先决条件以及权利（任务、角色、组以及属性）。

遵循这些步骤:

1. 登录到具有服务管理权限的 CA CloudMinder 帐户。

   例如，某环境的第一位用户具有“系统管理员”角色，而该角色具有“修改服务”任务。

2. 从导航菜单，依次选择“任务”、“服务”。
3. 依次单击“管理服务”、“修改服务”。

   此时显示一个搜索屏幕。

4. 搜索要修改的服务。

   要显示您具有管理权限的所有服务的列表，请单击“搜索”而不要修改搜索条件。

5. 选择一项服务，然后单击“选择”。

   此时显示确认消息。

6. 单击“是”。
7. 单击“提交”。

   CA CloudMinder 即会将更改应用于服务。

向“请求和查看访问”添加搜索

“请求和查看访问”任务会显示服务列表；但是，不存在用于搜索更多服务的字段。 添加搜索字段：

1. 依次选择“角色和任务”、“管理任务”、“修改管理任务”。
2. 搜索“请求和查看访问”。
3. 在“服务”类别中选择任务。
4. 单击“选项卡”。
5. 在选项卡下，单击“管理访问”左侧的编辑图标。
6. 单击“列表屏幕”行上的“浏览”。
7. 配置要应用以添加正确搜索的选项。
8. 选择所需的屏幕，然后单击“编辑”按钮以编辑屏幕。
9. 在“配置标准列表屏幕”中，导航到“选择用户可以搜索的字段:”部分。
10. 选择搜索字段并配置搜索字段名称。
11. 单击“确定”保存更改。

有关服务请求的信息（如服务请求持续时间以及用户数据）将显示在服务请求批准工作流项中。 此外，如果您将基于 AddServiceToUserEvent 策略的工作流分配给“请求和查看访问”任务，系统将通过电子邮件发送此信息。

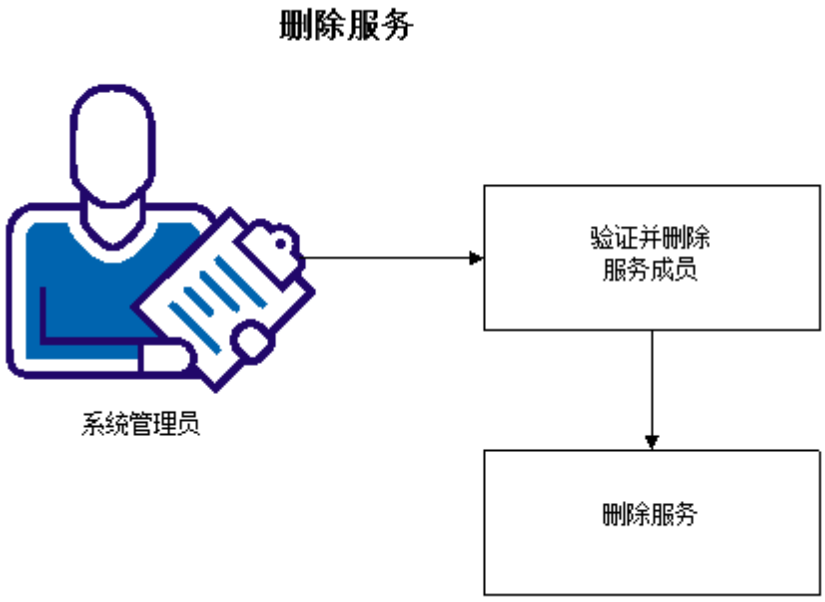
删除服务

系统管理员可以删除服务。 已删除的服务将从系统中完全移除。

如果为服务分配了用户，则无法删除该服务。 删除服务之前，请首先检查并移除所有分配的用户或*成员*。

注意：同样，如果用户是服务的成员，也将无法删除该用户。 首先，将用户从服务成员中移除，然后再删除该用户。

下图说明了删除服务要了解的信息以及执行的步骤。



以下主题将介绍如何删除服务：

1. 验证并移除服务成员 (p. 204)
2. 删除服务 (p. 205)

验证并移除服务成员

删除服务之前，请首先检查并移除现有成员。

遵循这些步骤:

1. 登录到具有服务管理权限的 CA CloudMinder 帐户。

   例如，某环境的第一位用户具有“系统管理员”角色，而该角色具有“修改服务”任务。

2. 依次选择“任务”、“服务”、“请求和查看访问”。

   此时显示一个您可以管理的服务的列表。

3. 选择要删除的服务，然后单击“选择”。

   此时显示一个分配给服务的用户的列表。

4. 如果服务具有成员，请清除所有用户旁边的复选框。
5. 单击“保存更改”。

   此时显示确认消息。

6. 单击“是”。

   CA CloudMinder 即会移除服务中的成员。

删除服务

您可以删除没有服务成员的服务。

删除服务

1. 使用具有服务管理权限的帐户登录到 CA CloudMinder。

   例如，某环境的第一位用户具有“系统管理员”角色，而该角色具有“删除服务”任务。

2. 从左侧窗格或通过选择“任务”导航到“服务”。
3. 依次单击“管理服务”、“删除服务”。

   此时显示一个搜索屏幕。

4. 搜索要删除的服务。

   要显示您具有管理权限的所有服务的列表，请单击“搜索”而不要修改搜索条件。

5. 选择该服务，然后单击“选择”。

   此时显示确认消息。

6. 单击“是”。

   服务即会删除。

续订服务访问

部分服务在一段时间后会到期。 为防止用户访问中断，管理员可以为用户续订服务。

您可以使用以下方式之一续订服务：

- 选择服务，然后选择要续订的用户访问
- 选择用户，然后选择要续订的服务

注意：最终用户也可以通过使用“续订访问”任务续订访问，具体视环境的配置方式而定。

下面的步骤介绍了如何通过首先选择服务续订访问。 如果您想首先选择用户，请使用“用户”类别中的“用户访问请求”、“管理用户续订请求”任务。

遵循这些步骤:

1. 在用户控制台中，依次单击“服务”、“续订访问”。
2. 搜索并选择要续订的服务。

   用户控制台将显示当前具有所选服务访问权限的用户列表及其访问的到期日期。
3. 在“访问请求”列中，选择续订的持续时间，然后单击“确定”。

   “持续时间”字段中的选项在创建服务时确定。
4. 单击“保存更改”。

您可以使用用户控制台中的“查看访问请求历史”查看服务续订的状态。

第 11 章： 同步

此部分包含以下主题：

服务器之间的用户同步

您在 Identity Manager 中配置同步，以便确保企业目录和配给目录的用户有匹配数据。 要处理任何一个目录的更改，您需要配置入站和出站同步。

入站同步

*入站同步*使 CA Identity Manager 用户与在配给目录中发生的更改一起更新。 配给目录中的更改包括通过具有到配给服务器的连接器的系统所做的更改。 同步使用在管理控制台的“Provisioning”（配给）屏幕上定义的映射。

入站同步的故障切换

只有当 URL 命名的应用程序服务器未运行时，才会发生备选 Identity Manager 服务器 URL 的故障切换。 如果应用程序服务器正在运行并且接受通知，但是遇到配置错误（如未知环境或环境未启动），这些错误将阻止通知的传递。 这些问题必须得到妥善的解决，然后才能正常实现入站通知功能。

出站同步

*出站同步*涉及使用 Identity Manager 在配给目录中创建并更新用户。

通过 Identity Manager 创建全局用户

系统只针对配给相关事件（如将配给角色分配给用户）在配给目录中创建用户。在您使用管理任务来创建用户的时候，除非该任务分配角色，或包括分配角色的身份策略，否则不会在配给目录中创建用户。

如果 Identity Manager 中的用户创建触发了配给目录中的用户创建，Identity Manager 会将带临时密码的电子邮件发送给在配给目录中定义的新用户电子邮件地址。 用户可以使用该密码登录到用户控制台，不过这之后用户需要变更为新密码。 因此，密码在用户存储和配给目录之间是同步的。

如果用户没有电子邮件地址，则除非更改用户存储中的密码，或者由 CA Identity Manager 管理员更改配给管理器中的用户密码，否则用户无法访问用户控制台。

注意：为了通过电子邮件发送临时的密码，“环境”必须启用电子邮件通知，电子邮件通知必须配置 CreateProvisioningUserNotificationEvent。（请参阅*《配置指南》*。）

使用 Identity Manager 更新全局用户

当您使用修改用户的管理任务时，将在配给目录中更新用户。 如果不存在全局用户，就不会出现同步。

出站映射会将 Identity Manager 用户事件和影响配给目录的出站事件相匹配。

Identity Manager User Event	Outbound Event
☐ DeleteUserEvent	POST_DELETE_GLOBAL_USER
☐ DisableUserEvent	POST_DISABLE_GLOBAL_USER
☐ EnableUserEvent	POST_ENABLE_GLOBAL_USER
☐ ModifyUserEvent	POST_MODIFY_GLOBAL_USER
☐ ResetPasswordEvent	POST_CHANGE_GLOBAL_USER_PWD

如果配给目录中存在某用户，而 Identity Manager 中没有，您可以在用户控制台中创建该用户。 如果您已经为创建任务提供了映射属性，并且用户有同样的用户 ID，则配给用户的属性将在配给目录中更新。 现在，您可以通过 Identity Manager 管理该用户。

注意：如果某事件更新用户属性，而您希望将这些值同步到 CA Identity Manager，则您需要将事件映射到出站事件：POST_MODIFY_GLOBAL_USER。

使用 Identity Manager 删除全局用户

默认情况下会为“删除用户”事件配置出站同步。如果您在 Identity Manager 中删除用户，则该用户还会从配给目录和所有端点帐户中删除。

如果 CA Identity Manager 无法删除管理端点的用户帐户，它会删除剩余帐户中的该用户，但是不会自配给目录中删除该用户。

例如，假定用户 A 有 UNIX 帐户和 Exchange 帐户，它们会在配给服务器中进行管理。 如果在 Identity Manager 中删除用户 A，配给服务器会尝试删除该用户的帐户。 如果因通信错误导致配给服务器无法删除 Exchange 帐户，它会删除用户 A 的 UNIX 帐户，但是不会从配给目录中删除用户。 然而，用户 A 不会在用户存储中被还原。

启用密码同步

配给服务器允许在 Identity Manager 用户和关联的端点用户帐户之间实现密码同步。 要实现由端点发起的更改，需要两个配置：

- 端点必须配置为捕获由端点启动的更改，并将更改转发给配给服务器。

  注意：有关如何为密码同步配置端点的详细信息，请参阅《*CA CA Identity Manager Administration Guide*》。

- 应当为全局用户激活“启用密码同步代理”属性。

启用密码同步

1. 在管理控制台中，依次选择“Advanced Settings”（高级设置）、“Provisioning”（配给）。
2. 选中“Enable Password Changes from Endpoint Accounts”（从端点帐户启用密码更改）。
3. 单击“Save”（保存）。
4. 重新启动应用程序服务器。

在创建或修改用户任务中实现用户同步

在创建或修改用户的任务的“配置文件”选项卡上，同步控制将确保对 Identity Manager 所做的更改也应用于全局用户。 如果您创建了对用户进行创建或修改的管理任务，并且您提供了身份策略，请按以下方式设置同步控制：

- 将“用户同步”设为“任务完成时”。
- 将“帐户同步”设为“任务完成时”。

注意：要获得最佳性能，请选择“任务完成时”。 但是，如果为包括多个事件的任务选择了“任务完成时”选项，则 Identity Manager 直到完成任务中的所有事件之后才会进行同步。 如果其中一个或多个事件需要工作流批准，则可能需要几天时间。为防止 Identity Manager 直到完成所有事件之后才应用身份策略，请选择“每个事件时”选项。

如果将属性添加到管理用户的管理任务中，您需要在管理控制台“Provisioning”（配给）屏幕中更新“Attribute Mappings”（属性映射）。对于 Identity Manager 的每个用户属性，都存在默认配给属性。

User Attribute	Provisioning Attribute
%ADMIN_ROLE_CONSTRAINT%	%ADMIN_ROLE_CONSTRAINT%
%EMAIL%	%EMAIL%
%ENABLED_STATE%	%ENABLED_STATE%
%FIRST_NAME%	%FIRST_NAME%
%FULL_NAME%	%FULL_NAME%
%IDENTITY_POLICY%	%IDENTITY_POLICY%
%LAST_NAME%	%LAST_NAME%
%PASSWORD%	%PASSWORD%
%PASSWORD_DATA%	%PASSWORD_DATA%
%USER_ID%	%USER_ID%

同步任务

您可以执行以下同步类型：

用户同步

确保每个用户对于相应的管理端点都有必要的帐户，且每个帐户在被用户的配给角色调用时都会分配到相应的帐户模板。

帐户同步

确保帐户的功能属性值是由帐户所分配的帐户模板表示的相应值。帐户同步可强可弱。 弱同步可确保帐户功能属性至少满足其帐户模板要求的最低功能。 强同步可确保帐户功能属性精确满足其帐户模板要求的功能。如果帐户至少属于一个选中了“使用强同步”复选框的帐户模板，帐户同步是强同步。

没有相应的“使用强同步”复选框管理用户同步，但是系统存在类似的概念。 在您对用户使用“角色”菜单项执行“同步用户”时，系统会向您提供两个同步选项：

- 添加缺失的帐户以及帐户模板分配。
- 删除额外帐户以及帐户模板分配。
- 通过仅选中“添加”复选框（类似于“弱帐户同步”），可以让全局用户至少拥有分配的配给角色需要的所有帐户，不过您必须允许用户拥有当前配给角色未规定的其他帐户。

选中“添加”和“删除”复选框（类似于“强帐户同步”），使配给角色精确定义用户应当拥有哪些帐户。 所有其他帐户都已删除。

基于配给角色被定义的精确程度，选择“弱/强帐户同步”或“弱/强用户同步”。如果您的用户属于明确定义的配给角色（帐户访问权限与那些角色有关），您将“使用强同步”。

注意：一些端点类型会将强同步设成默认。 有关详细信息，请参阅*《连接器指南》*。

用户同步和帐户同步是您必须单独执行的独立任务。通常，您先执行用户同步，以确保创建了所有必要的帐户，然后执行帐户同步，以便配给服务器分配或更改帐户属性的值。

配给服务器向对象提供两组同步菜单选项：

- 选中同步菜单选项，验证同步，并返回不符合配给角色或帐户模板的帐户的列表。
- “同步”菜单选项使全局用户与配给角色或者帐户与帐户模版保持同步。

如果您先执行检查同步功能，配给服务器告诉您同步功能将执行什么更正。 如果检查同步功能未找到问题，同步功能将不会运行。

用户为什么变得不同步

以下是用户与他们的配给角色或帐户模板不同步的一些原因：

- 由于网络中的硬件或软件问题，先前所做的创建必要帐户的尝试失败了，因此导致帐户缺失。
- 配给角色和帐户模板可能更改，从而创建了额外的或缺失的帐户。
- 帐户创建后被分配给帐户模板，因此存在与其帐户模板不同步的帐户。
- 因为被指定稍后创建帐户，因此新帐户创建推迟。
- 获得了新端点。 在浏览和关联过程中，配给服务器未自动将配给角色分配给用户，因此您必须更新角色，以便指出哪些用户应当拥有新端点上的帐户。在用户同步时，与用户关联的任何帐户均被列为额外帐户。
- 通过将帐户复制到用户，从而执行手工关联并建立额外的帐户，可将现有帐户分配给用户。
- 通过将用户分配给角色之外的其他方式为用户创建帐户。 例如，如果您将用户复制到不是位于用户的任何配给角色的帐户模板，帐户会被列为额外的帐户或具有额外帐户模板的帐户。 如果将用户复制到端点以使用端点的默认帐户模板创建帐户，则该帐户可能成为额外帐户。

用户同步

用户同步可创建、更新或删除帐户，以便帐户与分配给用户的配给角色保持一致。 因此，如果管理员通过使用内置工具添加或删除管理端点上的帐户，并且您近期没有对端点执行再浏览以更新配给目录，则在用户实际上可能有额外的或缺失的帐户时，“用户同步”却可能指示不存在问题。

用户与角色同步

您可以检查用户的同步情况来列出额外帐户或缺失的帐户模板和帐户。 在您请求使用户与角色保持同步时，配给服务器可确保用户拥有该人的配给角色需要的所有帐户，并且可确保每个帐户各属于正确的帐户模板。

- 对于这项任务，您可以选中复选框在端点上创建帐户。 如果用户配给角色中有多个帐户模板限定的都是同一个帐户，则该帐户是通过合并所有相关帐户模板创建的。
- 在用户与角色同步期间，您可以选择删除额外帐户。 您可能认为，除配给角色需要的那些帐户之外，您的用户有合理原因拥有其他帐户。 如果情况如此，您不应当选择这个删除选项。

  如果被删除的帐户驻留在管理端点，该端点禁用了帐户删除，则帐户实际上不会被删除。

创建帐户

因为配给角色包含帐户模板，并且帐户模板被关联到端点，用户应该拥有列出在每个端点上且拥有正确的帐户属性的帐户。

对于这项任务，您可以选中复选框在端点上创建帐户。 如果用户配给角色中有多个帐户模板限定的都是同一个帐户，则该帐户是通过合并所有相关帐户模板创建的。

此帐户会分配给当前与该帐户不同步的那些帐户模板。 新创建的帐户不需要执行帐户同步。

删除帐户

在用户与角色同步期间，您可以选择删除额外帐户。 您可能认为，除配给角色需要的那些帐户之外，您的用户有合理原因拥有其他帐户。 如果情况如此，您不应当选择这个删除选项。

如果被删除的帐户驻留在管理端点，该端点禁用了帐户删除，则帐户实际上不会被删除。

将帐户模板添加到帐户中

如果帐户被分配的帐户模板少了一个或多个，支持帐户模板同步的用户会将现有的帐户分配给那些帐户模板。 在帐户被分配给一个或多个新建帐户模板时，自动运行帐户同步，以将帐户的功能属性更新到由帐户模板指定的功能。

在帐户从具有帐户模板同步的用户那里得到更新之后，帐户与其帐户模板可能处于同步模式，也可能不处于同步模式。 如果添加的帐户模板之一是强同步帐户模板，或者如果两个或更多帐户模板被添加到帐户，实现了角色同步的用户将开始对帐户进行完整的帐户同步。 不过，如果仅仅添加了一个弱同步帐户模板，通过帐户模板同步实现的用户同步会启动仅仅涉及这一个帐户模板的帐户同步。 如果在此更新前，帐户没有与它的其他的帐户模板保持帐户同步，更新后将仍然如此。

从帐户中删除帐户模板

实现了角色同步的用户也能用于从帐户中删除额外的帐户模板。 只有您选择了“删除”选项，才能实现这一操作。 在用户同步确定帐户需要被更新以删除一个或多个额外的帐户模板时，帐户同步会自动地在帐户上运行，以使其功能属性与帐户上剩余的帐户模板保持同步。

发生在从帐户中删除帐户模板时的这一帐户同步：如果剩余的帐户模板的任何一个被标记为强同步，将使用强同步；如果剩余的所有帐户模板被标记为弱同步，则使用弱同步。

使用弱同步还是强同步将影响之前在将帐户模板分配给帐户时获得的帐户功能是否会在稍后删除该帐户模板时被解除。 对于强同步，如果帐户剩下的帐户模板中没有一个规定该功能，由帐户模板所授予的功能（如组成员资格或更高配额）将被解除（删除组成员资格或降低配额）。 不过，对于弱同步，通常帐户不会变更，因为配给服务器不区分按需加载的额外功能与通过帐户模板授予的功能。

SyncRemoveValues 属性指定的特定多值功能属性是此规则的一个例外。 代表被分配给帐户的值集合的简单多值属性（如组成员资格列表）通常会被列为 SyncRemoveValues 属性。 对于这些属性，从帐户中删除帐户模板时发生的弱同步操作将删除要删除的帐户模板规定的值，除非剩余帐户模板之一也规定了该值。

例如，如果您创建了帐户模板，每个帐户模板就会将唯一的组成员资格分配给您的帐户，此 SyncRemoveValues 功能将意味着，在您更改全局用户的配给角色，以便不再要求获得特定的帐户模板时，帐户将被更新，以不再属于该帐户模板规定的组。 您会注意到，这与强同步不完全一样，因为赋予帐户的超出帐户模板规定的组成员资格会被保留。

对于未指定为 SyncRemoveValues 属性的所有单值属性和特定多值属性，从帐户中删除帐户模板时的弱同步操作与正常的弱同步操作是同样的：功能从未被删除。

如果您希望功能永不被弱同步删除，可以通过将域配置参数“Synchronize/Remove Account Template Values from Accounts”（从帐户同步/删除帐户模板值）设置为“No”（否）来禁用 SyncRemoveValues 功能。

帐户模板同步

对帐户模板所做的更改将影响现有的帐户，如下所述：

- 如果更改功能属性的值，需要的话，会更新相应的帐户属性以与该帐户模板属性值同步。 请参阅弱同步和强同步的说明。
- 某些帐户属性由连接器指定为在帐户模板发生变化时不进行更新。 示例中列出的是端点类型仅允许在帐户创建过程中设置的某些属性以及密码属性。

更新哪些属性

当您更改帐户模板中的功能属性时，帐户的相应属性也会发生更改。 此更改会对帐户的属性产生影响。 产生的影响基于以下因素：

- 该帐户模板定义为使用弱同步还是强同步。
- 该帐户是否属于多个帐户模板。

弱同步

*弱同步*可确保用户具有其帐户的最少功能属性。 在多数端点类型中弱同步是默认值。如果更新使用弱同步的模板，CA Identity Manager 将更新功能属性，如下所述：

- 如果在帐户模板中更新了数字字段，且该新数字大于该帐户中的数字，CA Identity Manager 则会更改帐户中的值以与新数字匹配。
- 如果之前在帐户模板中没有选中，但您在之后选中了该复选框，CA Identity Manager 则会在未选中复选框的任何帐户中更新该复选框。
- 如果在帐户模板中更改了列表，CA Identity Manager 则会更新所有帐户以包括未包括在该帐户列表值中的新列表中的任何值。

如果帐户属于其他帐户模板（无论这些模板使用弱同步还是强同步），CA Identity Manager 则仅会参考正在更改的模板。 此操作比检查每个帐户模板更有效。 因为弱同步仅将功能添加到帐户，所以通常不需参考那些其他帐户模板。

注意：从弱同步帐户模板传播时，将要删除或降低功能的更改会保持某些帐户的状态，而不同步。 请记住，使用弱同步，从不会删除或降低功能。 在不参考帐户的其他模板的情况下，传播不会考虑弱同步是否充分。

在这种情况下，请使用“将用户与帐户模板同步”让帐户与其帐户模板保持同步。

强同步

强同步可确保帐户具有与在帐户模板中指定的那些帐户属性完全相同的帐户属性。

例如，假设您将一个组添加到现有 UNIX 帐户模板中。最初，帐户模板使帐户成为“人员”组的成员。现在，您希望帐户同时成为“人员”和“系统”两个组的成员。当每个帐户都是“人员”组和“系统”组（且没有其他组）的成员时，与帐户模板关联的所有帐户即被视为同步。任何不在“人员”组中的帐户会被添加到两个组中。

要考虑的一些其他因素包括以下内容：

- 如果帐户模板使用强同步，则属于除“人员”组和“系统”组之外的其他组的任何帐户会被从这些额外组中删除。
- 如果帐户模板使用弱同步，则帐户会被添加到“人员”组和“系统”组中。已定义其他组的任何帐户仍然是这些组的成员。

注意：定期同步帐户和其模板，以便确保帐户保持与其帐户模板同步。

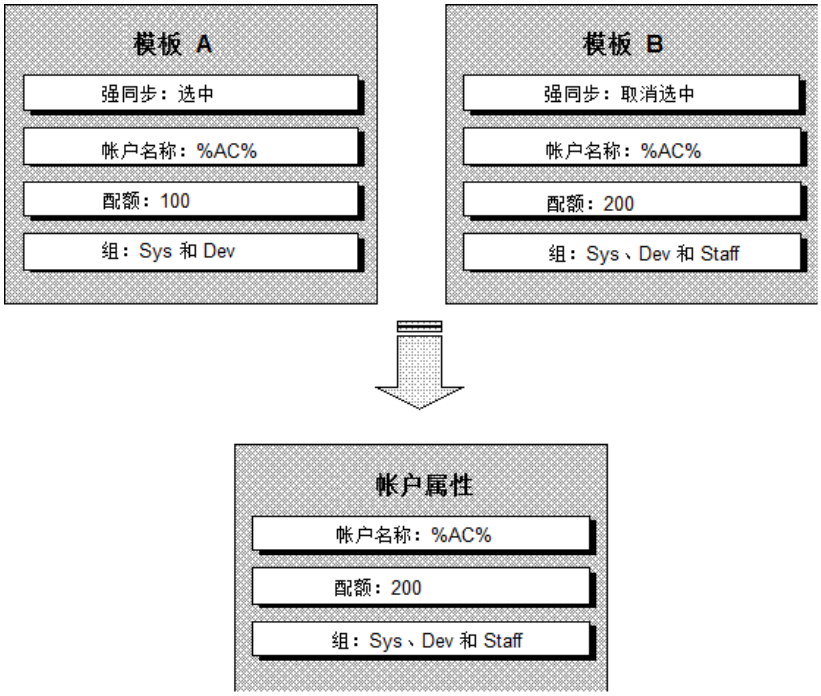
带有多个模板的帐户

同步还取决于帐户是否属于多个帐户模板。如果帐户只有一个帐户模板，并且该模板使用强同步，则每个属性均会更新，以精确匹配帐户模板属性值所求得的结果。结果与属性是初始属性时的结果一样。

一个帐户可能属于多个帐户模板，就像一个用户属于多个开通角色，每个角色都规定了在同一管理端点上的某一访问级别。在这种情况下，CA Identity Manager 会将这些帐户模板合并为一个有效的帐户模板，其规定来自单个帐户模板的功能超集。如果所有单个帐户模板均为弱同步，则此帐户模板本身被视为使用弱同步；如果任何单个帐户模板为强同步，则此帐户模板本身被视为使用强同步。

注意：通常，对于控制一个帐户的帐户模板，将仅使用弱同步或仅使用强同步，具体取决于您公司的角色是否完全定义了用户所需的访问权限。如果用户不适合定位明确的角色，您需要一定的灵活性，以便向用户帐户授予其他能力，则使用弱同步。如果您可以定义角色以精确指定用户需要的访问，则使用强同步。

下列示例说明如何将多个帐户模板合并为一个有效的帐户模板。 在本例中，一个帐户模板被标记为弱同步，另一个为强同步。 因此，通过合并两个帐户模板而创建的有效帐户模板被视为强同步帐户模板。 整数“配额”属性取两个帐户模板中较大的值，多值“组”属性取两者的联合值。



仅针对新帐户的属性

在帐户模板中，某些属性仅在创建帐户时适用。 例如，密码属性是定义新帐户密码的规则表达式。 该规则表达式从不更新帐户的密码。 对密码规则表达式的更改仅影响在设置规则表达式之后创建的帐户。

与之相似，只读帐户属性的模板规则表达式也只影响在设置规则表达式之后创建的帐户。 更改这种规则表达式对现有帐户没有任何影响。

帐户同步

帐户同步可更新功能属性以确保帐户拥有帐户模板指定的功能。此同步不会影响帐户的初始属性。

要将帐户模板的功能属性更改与其帐户同步，请使用在此部分中讨论的同步菜单选项之一。

检查帐户同步

您可以检查端点和用户的帐户同步。 通过此操作可返回未遵守帐户模板的帐户的列表。 下表描述当您检查帐户对每个对象的同步时发生的情况：

对象	同步
端点	端点上每个帐户的帐户属性，可确保它们与关联的帐户模板保持一致。
全局用户	用户每一个帐户的帐户属性，可确保它们与关联的帐户模板保持一致。

使帐户同步

您可以对端点、用户和帐户模板执行帐户同步。 下表列出了每个对象上的帐户同步造成的影响：

对象	同步
端点	端点上的每个帐户与其关联的帐户模板。
全局用户	全局用户的每个帐户与关联到它的每个帐户模板。

第 12 章： 工作流

此部分包含以下主题：

工作流概述

通过 CA Identity Manager 工作流功能，工作流流程可以控制 CA Identity Manager 任务。*工作流流程*是一个或多个步骤，必须执行这些步骤 CA Identity Manager 才能完成工作流控制下的任务。 *作业*是工作流流程的运行时实例。

WorkPoint Designer 是 Workpoint LLC 公司（Planet Group, Inc. 的子公司）的软件，与 CA Identity Manager 集成。 通过 WorkPoint Designer，可以管理工作流流程和工作流作业。

工作流流程包括称为*活动*的一个或多个步骤，必须执行这些步骤才能完成某业务任务，例如创建或修改员工用户帐户。 通常，工作流流程包括一个或多个手工活动，这些活动需要授权的用户或参与人批准或拒绝任务。

*参与人*是授权执行工作流活动的人员。 在 CA CA Identity Manager 中，参与人还称为*批准人*，因为他们必须批准或拒绝工作流控制下的任务。 *参与人确定程序*是一个规则或一组标准，用于确定哪些人员是参与人。

在 CA Identity Manager 中，工作流中单个手工活动称为*工作项*。

*工作列表*是工作流生成的批准任务列表或*工作项*列表，显示在授权批准任务的参与人的用户控制台中。

WorkPoint 流程图

通常，CA Identity Manager 任务触发 CA Identity Manager 事件。 例如，要创建用户，管理员需选择“创建用户”任务。启动该任务后，将触发事件“创建用户事件”。

下图是显示在 WorkPoint Designer 中的一个简单工作流流程（预定义流程“创建用户批准流程”）的示例。 如果“创建用户”是工作流控制下的任务，则“创建用户事件”将调用该流程。

该流程包括“批准创建用户”这一手工活动，该活动与同名的 CA Identity Manager 工作流批准任务相对应。 参与人必须批准或拒绝批准任务，通常在工作流控制下的任务运行完成之前通过单击用户控制台中的按钮来执行。

工作流和电子邮件通知

当您启动任务时，CA CA Identity Manager 将提交任务进行处理，并如下显示确认消息：

确认：任务已完成。

不过，如果该任务在工作流控制下且需要批准，则会显示如下消息：

警告：任务未决。

除了屏幕上的消息外，CA CA Identity Manager 还可以在以下情况下自动生成电子邮件通知：

- 需要工作流批准人批准或拒绝的事件或任务处于未决状态。
- 批准人批准事件或任务。
- 批准人拒绝事件或任务。
- 事件或任务已完成。

更多信息：

电子邮件通知 (p. 301)

WorkPoint 文档

有关工作流概念的一般信息以及有关 WorkPoint Designer 中工作流流程、活动和作业的说明，请参阅 WorkPoint 文档。 要执行此操作，请打开以下 HTML 页面：

管理工具\WorkPoint\docs\designer\default.htm

管理工具

定义 CA Identity Manager 管理工具的安装目录。默认安装目录如下所示：

- **Windows：**<安装路径>\tools
- **UNIX：**<安装路径 2>/tools

注意：Workpoint 是随 CA CA Identity Manager 安装的第三方产品。CA CA Identity Manager 支持 Workpoint 中的部分功能。 例如，CA CA Identity Manager 不支持 WpConsole。 但是，Workpoint 文档描述了该产品中的所有功能。 Workpoint 文档的某些部分不适用于 CA CA Identity Manager 用户。

工作流控制方法

CA Identity Manager 提供了两种将任务置于工作流控制下的方法。

模板方法

CA Identity Manager 包括可用于将任务置于工作流控制下的工作流流程模板。 通过*模板方法*，您可以使用这些模板完全在用户控制台中配置和管理工作流。 已在 CA Identity Manager r12 中引进了这些常规流程模板，并可以对其进行配置，以控制大多数 CA Identity Manager 任务和事件。

模板方法实现了以下新功能：

- 任务级和事件级工作流控制
- 简化了适用于工作流批准人的参与人确定程序配置
- 工作项指派，通过允许用户指派其他用户批准工作项从而包括“不在办公室”方案
- 工作项重新分配，用于将正在运行的任务重新分配给其他用户进行批准

WorkPoint 方法

CA Identity Manager 还包括一组预定义的工作流流程，其中包括对应于特定 CA Identity Manager 任务的默认事件映射。 *WorkPoint 方法*需要您配置和自定义这些 WorkPoint Designer 中的流程。这些预定义的流程与 CA Identity Manager r12 之前的版本兼容。

WorkPoint 方法也实现以下新功能：

- 任务级和事件级工作流控制
- 工作项指派，通过允许用户指派其他用户批准工作项从而包括“不在办公室”方案
- 工作项重新分配，用于将正在运行的任务重新分配给其他用户进行批准

注意：为了提高灵活性和易用性，CA 建议尽可能使用模板方法。

更多信息：

使用工作流控制 - 模板方法 (p. 221)

使用工作流控制 - 模板方法

已在 CA Identity Manager r12 中引进了模板方法，该方法用于在用户控制台中配置工作流流程模板，且不必打开 WorkPoint Designer。

模板方法的优势是：

- 多阶段流程模板可以满足多数工作流需要，而不需要在 WorkPoint Designer 中进行自定义。
- 模板支持任务级和事件级的工作流控制。
- 可以将同一工作流流程模板配置为用于多个不同的任务，而且流程设计本身保持不变。
- 可以在用户控制台中轻松地指定参与人确定程序。
- 可以在用户控制台中执行工作项指派。

先决条件：启用工作流

您必须启用工作流才能用它来控制 CA Identity Manager 任务。 默认情况下，禁用工作流。

遵循这些步骤:

1. 在管理控制台中，选择“环境”。
2. 依次进入“高级设置”、“工作流”。
3. 选中“启用”复选框，然后单击“保存”。

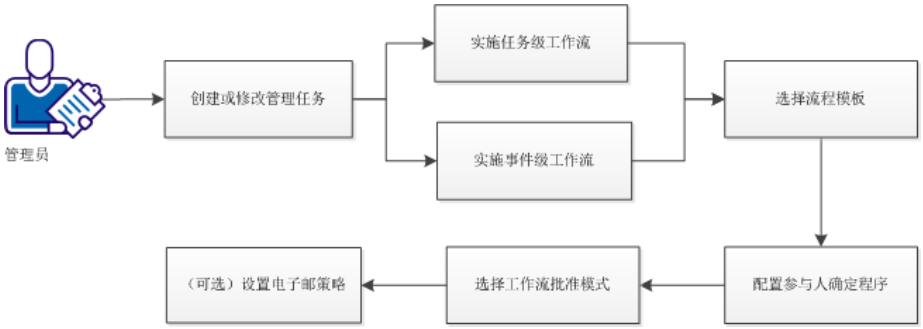
   注意：仅当您使用 WorkPoint 方法配置工作流时，才会应用该屏幕上的“事件映射”。 如果您使用模板方法（推荐），请勿使用该管理控制台将事件映射至流程。
4. 重新启动应用程序服务器。
5. （可选）配置 WorkPoint 管理工具 (p. 239)。

更多信息：

将流程全局映射到事件 (p. 245)
工作流控制方法 (p. 221)

将管理任务放置在工作流控制下 - 模板方法

作为管理员，您可以使用模板方法将管理任务放置在工作流控制下。



遵循这些步骤:

1. 在用户控制台中，依次选择“角色和任务”、“管理任务”、“修改 (或创建) 管理任务”。
2. 搜索您要将其置于工作流控制下的任务，然后单击“选择”。
3. 请执行下列操作之一：
   - 通过单击“配置文件”选项卡的“工作流流程”编辑按钮，实施任务级工作流 (p. 224)。
   - 通过在“事件”选项卡上选择一个或多个事件，实施事件级工作流 (p. 226)。
4. 选择流程模板 (p. 228)。
5. 配置参与人确定程序 (p. 231)。
6. 选择工作流批准模式。
7. （可选）为工作流流程设置电子邮件策略 (p. 236)。

   注意：如果您选择 EscalationApproval 流程，则显示名为“批准超时 (分钟)”的字段。该字段指定以分钟计且不得为空。默认情况下，时间设置为 60 分钟。

配置工作流控制之后，具有适当角色的用户执行管理任务，指定的工作流参与人会批准或拒绝任务或事件。

基于任务或事件的工作流

CA Identity Manager 可以将工作流流程与任务或事件相关联。这表示参与人可以批准或拒绝整个 CA Identity Manager 任务或任务中的特定事件。

例如，某些 CA Identity Manager 任务生成了多个事件，而批准人可能需要在决定批准或拒绝请求之前查看所有事件。 这在任务级工作流下是可行的。 当工作流流程与任务内的特定事件关联时，批准人将无法看到包含所提请求的整体任务上下文。

任务级工作流

通过任务级工作流，批准人可以在决定批准或拒绝请求之前查看所有事件。 在处理任何任务活动之前执行任务级工作流。 工作流流程作业开始之前，不执行任何事件或嵌套任务。

如果拒绝了任务级工作流，则不会执行任务的任何部分。

注意：配置为由任务级工作流控制的任务也可以同时配置为由事件级工作流控制。 并发事件级工作流可以全局应用，也可以应用于特定任务。

更多信息

事件级工作流 (p. 226)
全局流程到事件的映射 (p. 244)

任务级流程属性

与任务级工作流兼容的工作流流程在 WorkPoint Designer 内都定义特定的属性。该流程级别用户数据属性称为 TASK_LEVEL，默认情况下，在以下流程模板中设置为 true：

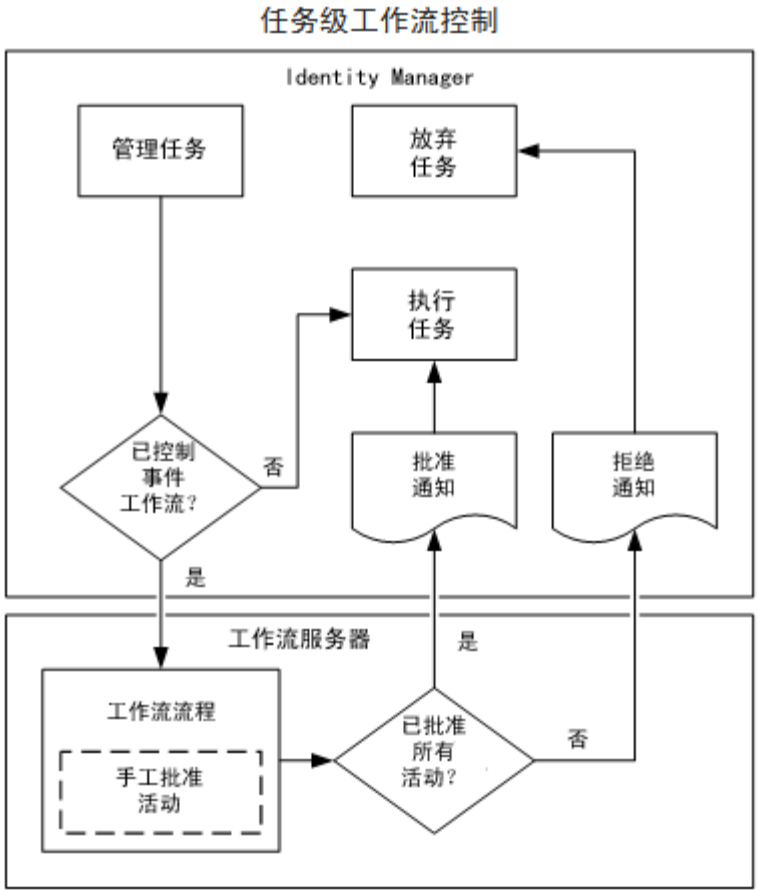
- SingleStepApproval
- TwoStageApprovalProcess
- EscalationApproval

在您选择任务级工作流的管理任务时，只有这些流程模板可用。

注意：虽然 TASK_LEVEL 被设置为 true，但是流程模板仍然可以用于事件级工作流。 请勿更改此 TASK_LEVEL 属性值。

任务级控制图

下图说明了当启动典型的事件级工作流流程时，CA Identity Manager 和工作流服务器之间的交互。



更多信息：

事件级控制图 (p. 227)

如何配置任务级工作流

在处理任何任务活动之前执行任务级工作流。 工作流流程作业开始之前，不执行任何事件或嵌套任务。

配置任务级工作流

1. 在用户控制台中，依次选择“角色和任务”、“管理任务”、“修改 (或创建) 管理任务”。

   将显示“选择管理任务”屏幕。

2. 搜索您要将其置于工作流控制下的任务，然后单击“选择”。

   将显示“修改 (或创建) 管理任务”屏幕。

3. 在“配置文件”选项卡中，确认已选中“启用工作流”。
4. 在“配置文件”选项卡上，单击“工作流流程”按钮。

   将显示“任务级工作流配置”选项卡。
5. 从“工作流流程”列表中选择以下流程模板之一：
   - 一步批准
   - 两个阶段批准流程

   “任务级工作流配置”选项卡将展开。
6. 根据流程模板的需要配置参与人确定程序。

   参与人请求将添加至该流程。
7. 单击“确定”。

   CA Identity Manager 将保存任务级工作流配置。
8. 单击“提交”。

   CA Identity Manager 处理任务修改。

事件级工作流

可将事件映射到工作流流程。 当触发映射至工作流流程的事件时，工作流流程即开始。 触发事件的任务将被置为挂起状态，并将其视为在工作流控制下。

工作流流程可以要求参与人在完成该流程之前批准或拒绝事件或任务。 完成需要参与人进行手工工作流批准的任务，比完成不在工作流控制下的任务所花费的时间长。

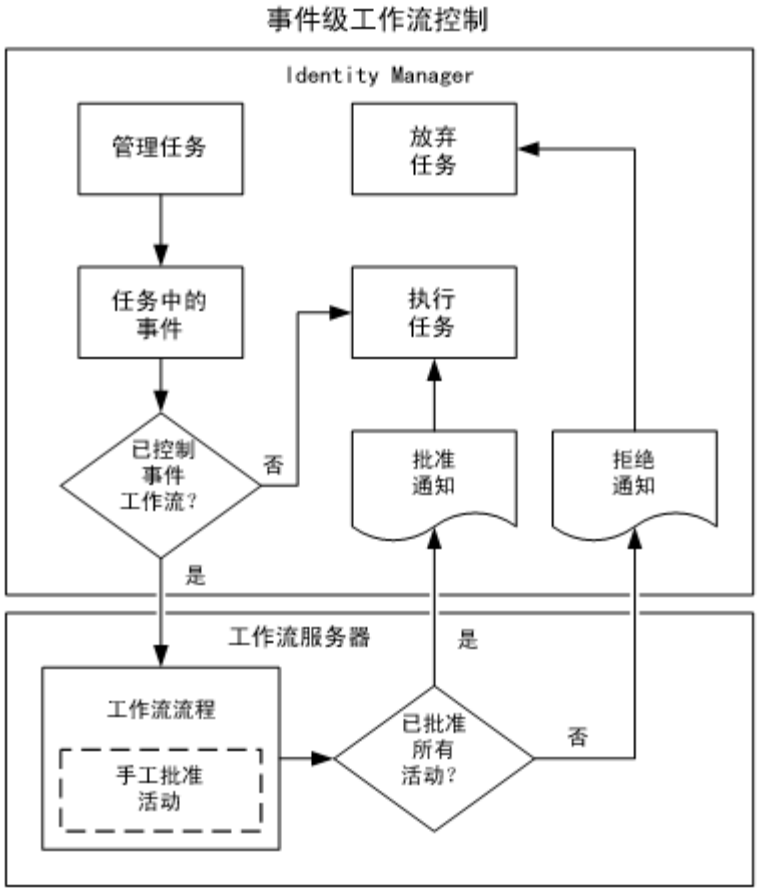
执行工作流流程中的所有活动后，映射至工作流流程的事件将从工作流控制中释放。 由指定任务触发的所有事件均从工作流控制释放后，工作流控制的任务即完成。

当任务在工作流控制下时，任务屏幕的内容将保存在任务永久数据库中。 工作流作业状态（与工作流相关的数据）将存储在 WorkPoint 数据库中。

注意：“事件”选项卡列出由任务中的每个选项卡生成的事件。 将新选项卡添加到任务后，必须首先使用“修改管理任务”提交并重新打开该任务，之后这些新事件才会显示在“事件”选项卡中。

事件级控制图

下图说明了当启动典型的事件级工作流流程时，CA Identity Manager 和工作流服务器之间的交互。



更多信息：

任务级控制图 (p. 225)

如何配置事件级工作流

当触发映射至工作流流程的事件时，事件级工作流即开始。 触发事件的任务将被置为挂起状态，直至参与人批准或拒绝任务。

配置事件级工作流

1. 在用户控制台中，依次选择“角色和任务”、“管理任务”、“修改 (或创建) 管理任务”。

   将显示“选择管理任务”屏幕。

2. 搜索您要将其置于工作流控制下的任务，然后单击“选择”。

   将显示“修改 (或创建) 管理任务”屏幕。

3. 在“配置文件”选项卡中，确认已选中“启用工作流”。
4. 在“事件”选项卡上，选择要映射至流程模板的事件。

   将显示工作流映射屏幕。
5. 从“工作流流程”列表中选择以下流程模板之一：
   - 一步批准
   - 两个阶段批准流程

   工作流映射屏幕将展开。
6. 根据流程模板的需要配置参与人确定程序。

   参与人请求将添加至该流程。
7. 单击“确定”。

   CA Identity Manager 将保存该事件级工作流配置。
8. 对您要将其置于工作流控制下的每个事件，请重复步骤 3 - 6。
9. 单击“提交”。

   CA Identity Manager 处理任务修改。

注意：“工作流流程”列表包括与模板方法和 WorkPoint 方法配合使用的流程：

- 当选择模板方法流程（“一步批准”或“两个阶段批准流程”）时，页面将展开以启用参与人确定程序配置。
- 当选择 WorkPoint 方法流程时，页面将不展开。 在 WorkPoint Designer 中配置参与人确定程序。

流程模板类型

工作流流程模板具有以下特点：

- 在 WorkPoint Designer 中定义。
- 具有手工活动，对应于 CA Identity Manager 批准任务。
- 包括一些特殊属性，这些属性包含识别参与人（也称为批准人）的信息。

工作流流程模板不包括用于选择特定参与人的信息。 这些信息在用户配置工作流及其参与人确定程序之后由 CA Identity Manager 提供。 这些信息将被映射至由事件级工作流控制的事件，以及由任务级工作流控制的任务。

使用模板方法时，所有工作流和参与人配置均在用户控制台中完成。

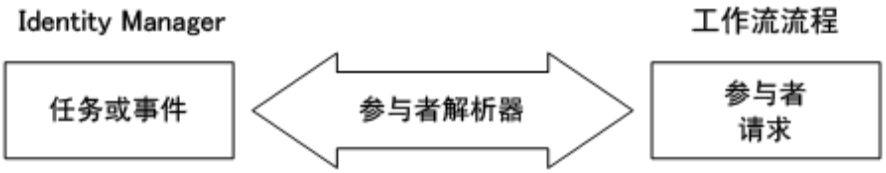
以下是使用模板方法的三个流程模板：

- SingleStepApprovalProcess
- TwoStageApprovalProcess
- EscalationApprovalProcess

流程模板的工作方式

工作流流程模板包含多个请求参与人列表的位置。 将模板映射至 CA Identity Manager 任务或事件时，需要为这些列表配置参与人确定程序。

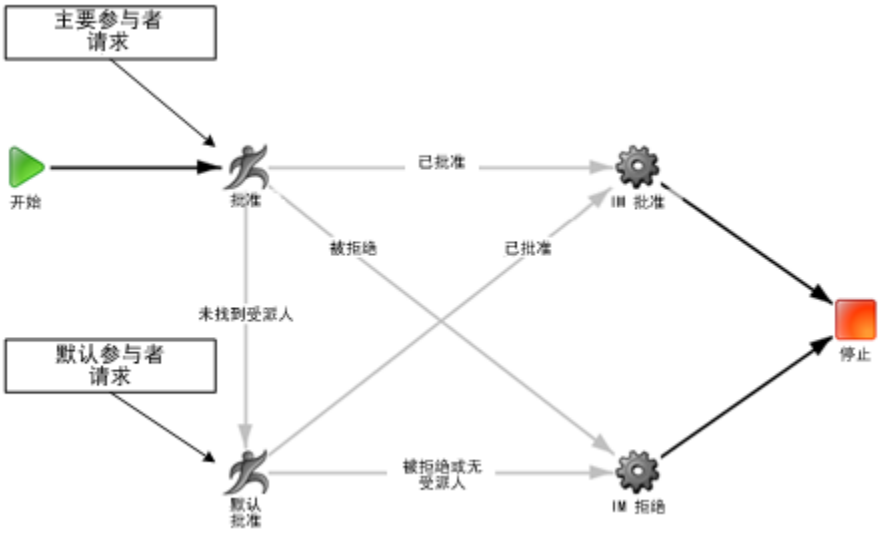
在运行时，如下图所示，CA Identity Manager 基于您的配置信息向工作流流程提供参与人列表：



单阶段模板图

下图说明了在 WorkPoint Designer 中显示的“单阶段批准”流程模板。该流程模板包括两个手工活动：

- 用于主参与人的批准节点。 如果该用户批准或拒绝请求，则流程将完成运行。
- 用于默认参与人的批准节点。 如果主参与人未找到或未响应，则该用户可以批准或拒绝任务。

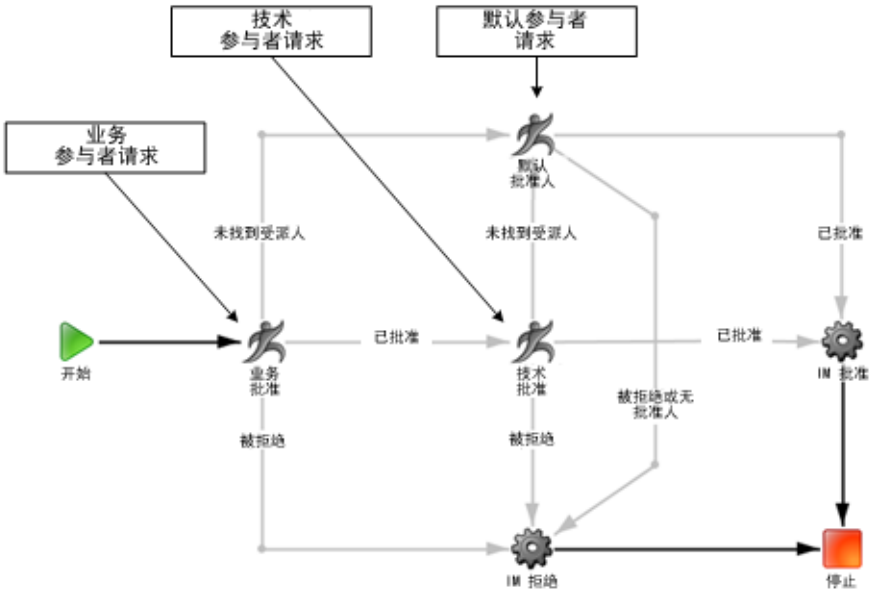


两个阶段模板图

下图说明了在 WorkPoint Designer 中显示的“两个阶段批准”流程模板。 “两个阶段批准”流程模板包括三个手工活动：

- 用于业务参与人的批准节点。 如果该用户批准或拒绝请求，则流程将继续运行至技术批准人。

- 用于技术参与人的批准节点。 如果该用户批准或拒绝请求，则流程将完成运行。
- 用于默认参与人的批准节点。 如果业务参与人或技术参与人未找到或未响应，则该用户可以批准或拒绝任务。

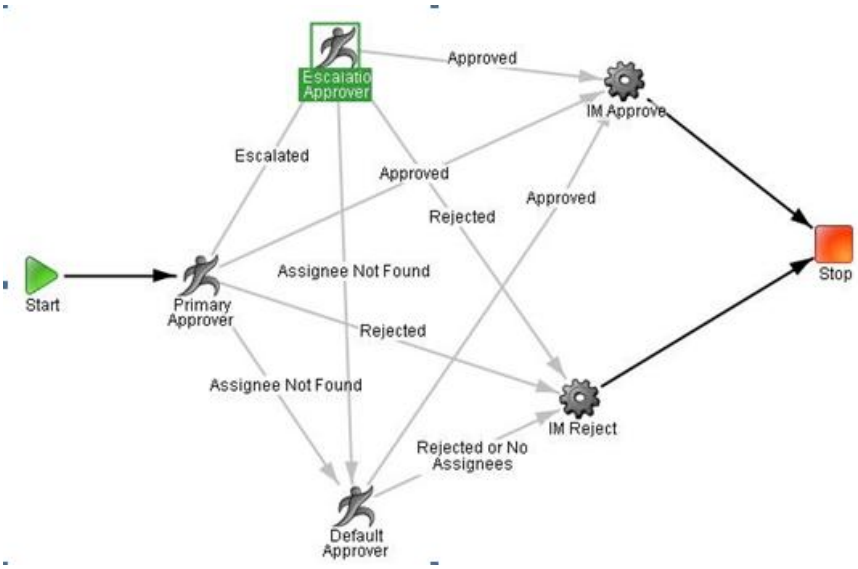


升级批准模板图表

下图说明了在 WorkPoint Designer 中显示的 EscalationApproval 流程模板。 该流程模板包括以下手工活动：

- 用于主参与人的批准节点。 如果该用户批准或拒绝请求，则流程将完成运行。
- 用于默认参与人的批准节点。 如果找不到主要参与人，则该用户可以批准或拒绝该请求。

- 从主要批准人到升级批准人的定时转换批准节点。 如果找到主要参与人，但在配置的超时期内未响应，那么该用户可以批准或拒绝请求。



注意：要将超时选项添加到现有过程中，请将用户数据字段 PARTICIPANT_TIMEOUT 添加到活动节点，并将“升级”转换到需要升级工作项的节点中。

使用升级批准模板

要使用升级批准模板，必须在从 r12.5 升级到 r12.5 SP1 时，手动导入以下 ZIP 文件：

Workflow 12.5 to 12.5 SP1 upgrade.zip

该 ZIP 文件位于管理工具下的 workflowScripts 文件夹。

。 管理工具安装在以下默认位置：

- Windows：<安装路径>\tools
- UNIX：<安装路径 2>/tools

参与人确定程序的类型

对于模板方法，有七种类型的参与人确定程序：

批准任务角色成员

指定参与人是授予批准任务访问权限的角色的成员。

用户列表

指定参与人是指定的用户列表。

组成员

指定参与人是指定组列表的成员。

管理角色成员

指定参与人是指定管理角色列表的成员。

管理任务成员

指定参与人是与指定管理任务列表关联的管理角色成员。

动态确定程序

指定根据正在批准的任务或事件，动态地选择参与人。

空确定程序

解析至不包含用户的空列表。

自定义

指定参与人由自定义参与人确定程序确定。

业务所有者确定程序

指定“编录规则”中配置的参与人列表作为某实体的业务所有者。

管理所有者确定程序

指定“编录规则”中配置的参与人列表作为某实体的管理所有者。

经理确定程序

指定设置为用户对象的经理的参与人。

批准任务角色成员

该确定程序将活动分配给授予批准任务访问权限的所有 CA Identity Manager 角色的所有成员。 该确定程序无需进一步配置。

用户列表

该确定程序向指定的用户列表分配工作项。

不强制执行范围确定。 由对工作流配置屏幕具有访问权限的任何人将任何用户添加到列表或从列表中删除。

该确定程序具有以下验证规则：

- 必须至少提供一个用户名。
- 用户名必须为当前现有用户的名称。

组成员

该确定程序向组列表中指定的所有组中的所有成员分配工作项。

执行组成员评估是在创建工作项时，而不是在指定参与人确定程序时。

不强制执行范围确定。 由对工作流配置屏幕具有访问权限的任何人将任何组添加到列表或从列表中删除。

该确定程序具有以下验证规则：

- 必须至少指定一个组。
- 组名必须为当前现有组的名称

管理角色成员

该确定程序向在管理角色列表中指定的管理角色的所有成员分配工作项。

创建工作项时，角色成员执行评估，而不是在指定参与人确定程序时。

不强制执行范围确定。 由对工作流配置屏幕具有访问权限的任何人将任何角色添加到列表或从列表中删除。

该确定程序具有以下验证规则：

- 必须至少指定一个管理角色。
- 管理角色名必须为当前现有管理角色的名称。

管理任务成员

此确定程序将工作项分配给与在管理任务列表中指定的管理任务相关联的所有管理角色的所有成员。

不强制执行范围确定。 由对工作流配置屏幕具有访问权限的任何人将任何任务添加到列表或从列表中删除。

执行角色成员和出现在任务中的角色评估是在创建工作项时，而不是在指定参与人确定程序时。

该确定程序具有以下验证规则：

- 必须至少指定一个管理任务。
- 管理任务名必须为当前现有管理任务的名称。

动态确定程序

该确定程序将根据运行时解析的动态规则返回用户列表。 使用以下选择设置动态规则限制：

批准人

指定批准该任务的用户类型。

注意：仅显示可能包含用户（或批准人）的对象。

用户或对象

指定可以从中找到批准人的用户或对象。

- 与事件关联的对象 - 工作流控制下的事件。
- 该任务的启动人 - 启动管理任务的用户。
- 该任务的主要对象 - 任务正在创建/修改的对象。
- 该任务的先前批准人 - 该任务以前的批准人。

与此帐户关联的用户

更新用户或对象属性字段，以便列出 CA Identity Manager 用户属性，而不是端点帐户属性。确定程序在 CA Identity Manager 用户级别清除属性。 在您选择端点帐户对象（如 Active Directory 帐户）时，此复选框应用。

属性

指定包含批准人的属性。

注意：属性列表按字母顺序排序并包含唯一显示名称列表。 扩展属性排除在列表之外。

事件对象类型

指定事件中对象的类型。

注意：仅在选中“与事件相关联的对象”时才显示。

注意：创建组的动态确定程序需要对象。组成员身份/管理员信息仅可与现有组的动态/匹配属性确定程序一起使用。

动态确定程序已得到增强，将上一批准人添加到所支持的对象列表中。 如果选择了承载经理信息的物理属性，该配置则会将批准路由给经理。

要为经理批准确定程序配置确定程序：

- 将批准人设置为用户
- 从“用户”或“对象”下拉列表中选择“该任务的前一个批准人”
- 将“属性”设置为包含经理信息的物理属性

匹配属性确定程序

该确定程序仅针对“用户”类型的对象。 来自任何可用对象的值与用户对象中的字段匹配。 使用以下选项设置匹配属性规则的限制：

批准人

指定批准该任务的用户类型。

用户或对象

指定批准人将在以下选定属性中具有的值。

注意：从用户或对象检索到的值应该是在用户上搜索选定属性的可接受值。

- 与事件关联的对象 - 工作流控制下的事件。
- 该任务的启动人 - 启动管理任务的用户。
- 该任务的主要对象 - 由任务正在创建/修改的对象（仅可用于任务级别的事件映射）。
- 该任务的先前批准人 - 该任务以前的批准人。

与此帐户关联的用户

更新用户或对象属性字段，以便列出 CA Identity Manager 用户属性，而不是端点帐户属性。确定程序在 CA Identity Manager 用户级别清除属性。 在您选择端点帐户对象（如 Active Directory 帐户）时，此复选框应用。

使用或对象属性

指定包含值的属性以便在批准人搜索中使用。

批准人搜索属性

指定在搜索中用于匹配以上识别的值的属性。

注意：在您将“批准创建用户”任务设置为在“用户”上工作的“匹配属性确定程序”、“参与人确定程序”时，您必须更改 WorkPoint Designer 上 imApprovers 脚本的方法签名以便指向 TwoStageProcessDefinition 的唯一名称。

空确定程序

空确定程序不返回用户。 根据工作流流程的设计方式，它可能导致流程完全跳过批准。 空确定程序无需进一步配置。

自定义参与人确定程序

自定义参与人确定程序是一个 Java 对象，可确定工作流活动参与人并将一个列表返回 CA Identity Manager，然后将该列表传递到工作流引擎。通常，仅当标准参与人策略无法提供活动所需的参与人列表时，您才可以编写自定义参与人确定程序。

注意：使用参与人确定程序 API 创建自定义参与人确定程序。 有关详细信息，请参阅 *《Programming Guide for Java》*。

设置工作流流程的电子邮件策略

您可以指定工作流流程每个步骤的电子邮件策略。 基于定义的电子邮件策略，在进程到达相应的步骤或活动时就会发送电子邮件。 对于工作流流程相关电子邮件通知，您只可以选择*"发送时间"*类型*"工作流未决电子邮件"*。

注意：有关电子邮件策略的更多信息，请参阅"如何创建电子邮件通知策略"。

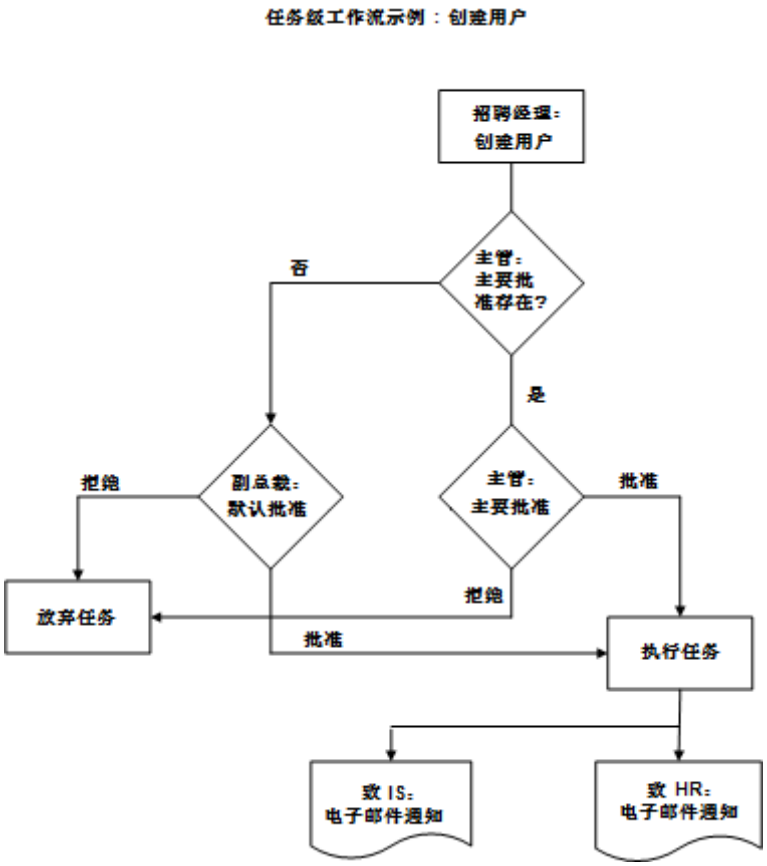
工作流示例：创建用户

公司的 CA Identity Manager 管理员需要定义工作流和用户角色以处理以下情况：

- 公司销售经理聘请了一名新销售代表。 销售经理必须能够为新雇员创建 CA Identity Manager 用户。
- 为了简化聘请流程，参与人仅想要执行一个工作项就能批准（或拒绝）任务。
- 销售主管应为所有新雇员的主要批准人。 如果销售主管出于某种原因而无法做到，则销售副总裁应为默认批准人。
- 如果新雇员被批准录用，则 CA Identity Manager 应通过电子邮件向人力资源 (HR) 和信息服务 (IS) 部门发送新用户通知。

创建用户控制图

下图说明了创建用户方案的逻辑流程：



工作流示例实施

要实施该示例方案，管理员需要执行以下任务：

- 确保任务启动人是所需的管理角色的成员。

  销售经理必须是“用户经理”管理角色的成员。 该角色赋予销售经理一些必需的权限，用以对新雇用的销售代表启动“创建用户”管理任务。

- 启用“创建用户”管理任务的任务级工作流。

  任务级工作流保证仅生成一个用以完成“创建用户”任务的工作项。 由于存在若干个与“创建用户”任务相关联的个别事件，因此，事件级工作流可能会生成若干个工作项，并且还可能更难进行配置。

- 配置参与人确定程序。

  可能的参与人确定程序数量由选定的工作流流程模板确定。SingleStageApproval 模板包括主要和默认批准人，其他模板可以包括更多批准人。

  由于该情况仅需要两个单独的批准人，因此“用户列表”参与人确定程序提供最简单的解决方案。 该确定程序允许按姓名逐个选择批准人，而不是按角色或组选择多个用户。

- 配置电子邮件通知。

  管理控制台允许为特定任务和事件发送电子邮件通知。 对于该方案，将启用任务电子邮件，并在“创建用户”任务完成时发送电子邮件通知。

  自定义电子邮件模板用于使用适当的主题行和邮件文本，将电子邮件发送给 HR 和 IS 部门。

更多信息

电子邮件通知 (p. 301)
将管理任务放置在工作流控制下 - 模板方法 (p. 223)
如何配置任务级工作流 (p. 225)

如何使用 WorkPoint 方法

WorkPoint 方法适用于 r12 之前的 CA Identity Manager 版本。默认情况下，有 14 个预定义的 WorkPoint 工作流流程映射到特定的 CA Identity Manager 事件。 必须使用 WorkPoint Designer 配置参与人确定程序，否则只能修改工作流流程。

WorkPoint 方法还要求使用管理控制台以将工作流流程映射到批准事件，从而在环境中以全局级别将相应的任务置于工作流控制之下。

本部分列出了使用 WorkPoint 方法将管理任务置于工作流控制之下所涉及的高级步骤。

注意：为了提高灵活性和易用性，CA 建议尽可能使用模板方法。

使用 WorkPoint 方法

1. 配置 WorkPoint 管理工具。 (p. 239)
2. 在管理控制台中：
   a. 确保通过在“高级设置”、“工作流”中选择“已启用”复选框，为您的环境启用工作流。

      注意：仅当您使用 WorkPoint 方法配置工作流时，才会应用该屏幕上的“事件映射”。 如果您使用模板方法（推荐），请勿使用该管理控制台将事件映射至流程。

b. （可选）对于全局事件映射，请将一个或多个事件关联到相应的预定义工作流流程。

c. 如果需要，重新启动 CA Identity Manager 环境。

3. 在用户控制台中：

a. 对于特定于任务的事件映射，请将一个或多个事件与相应的预定义工作流流程关联。（可选）

4. 在 WorkPoint Designer 中：

a. 将批准任务与工作流流程相关联（可选）。

b. 按照工作流流程配置参与人确定程序（可选）。

5. 在用户控制台中：

a. 配置工作流控制后，具有相应角色的用户可执行管理任务。

b. 指定的工作流参与人可批准或拒绝事件。

更多信息：

将流程映射到事件 (p. 244)
将工作流活动与批准任务相关联 (p. 249)
参与人确定程序：WorkPoint 方法 (p. 250)

配置 WorkPoint 管理工具

WorkPoint Designer 是 Workpoint LLC 公司（Planet Group, Inc. 的子公司）的软件，与 CA Identity Manager 集成。 通过 WorkPoint Designer，可以管理工作流流程和工作流作业。WorkPoint 管理工具包括 WorkPoint Designer 和 WorkPoint Archive。要配置 WorkPoint 管理工具，请安装 CA Identity Manager 管理工具。 如果尚未安装 CA Identity Manager 管理工具，则可以运行安装程序并选择“CA Identity Manager 管理工具”选项。

注意：要使用工作流的管理工具，必须在安装了管理工具的系统中安装支持的 JDK。 有关支持平台和版本的完整列表，请参阅 CA CA Identity Manager 支持网站中的“CA CA Identity Manager Support Matrix”。

工作流客户端工具位于 CA Identity Manager 管理工具中的 WorkPoint 目录。 管理工具安装在以下默认位置：

- **Windows：**<安装路径>\tools
- **UNIX：**<安装路径 2>/tools

通过该目录中的工具可以执行以下操作：

- 创建工作流数据库架构
- 加载默认的工作流脚本
- 设计并监控工作流进程和作业

在 JBoss 上配置 WorkPoint 管理工具

要在 JBoss 上配置 WorkPoint 管理工具，请编辑 init.bat/sh 和 workpoint-client.properties 文件。

编辑 init.bat/init.sh

编辑 init.bat/init.sh

1. 在文本编辑器中，编辑以下文件之一：
   - **Windows：**

     管理工具\Workpoint\bin\init.bat
   - **UNIX：**

     管理工具/Workpoint/bin/init.sh
2. 取消文件 JBoss 部分中 EJB_CLASSPATH 行的注释。

   注意：要确保针对其他应用程序服务器的所有部分都已加注释。
3. 将 jbossall-client.jar 从 *jboss_home*\client\ 复制到：

   管理工具\Workpoint\lib

编辑 workpoint-client.properties

根据 CA CA Identity Manager 安装过程中所选的应用程序服务器类型来编辑 workpoint-client.properties 文件。

配置 workpoint-client.properties 文件

1. 打开*管理工具*\Workpoint\conf\ workpoint-client.properties。

   *管理工具*是管理工具的安装位置。 管理工具安装在以下默认位置：
   - **Windows：** <安装路径>\tools
   - **UNIX：**<安装路径 2>/tools
2. 查找标题为“JBOSS SETTINGS”部分。

3. 取消该部分中所有属性值的注释。

   例如：

   ```
   java.naming.provider.url=localhost
   java.naming.factory.initial=org.jnp.interfaces.NamingContextFactory
   java.naming.factory.url.pkgs=org.jboss.naming
   ```

   注意：可能需要编辑 java.naming.provider.url 属性值。 例如，将 localhost 替换为 jnp://*server_name or ip*:*port*。 确保您使用 jnp 端口号 1099。

4. 保存该文件。

在 WebLogic 上配置 WorkPoint 管理工具

要在 WebLogic 上配置 WorkPoint 管理工具，请编辑 init.bat/sh 和 workpoint-client.properties 文件。

编辑 init.bat/init.sh

编辑 init.bat/init.sh

1. 在文本编辑器中，编辑以下文件之一：

   - **Windows：**

     管理工具\Workpoint\bin\init.bat

   - **UNIX：**

     管理工具/Workpoint/bin/init.sh

2. 取消文件 WebLogic 部分中 EJB_CLASSPATH 的注释：

   注意：要确保针对其他应用程序服务器的所有部分都已加注释。

3. 将 wlclient.jar 文件从 *weblogic_home*\server\lib 复制到以下位置：

   管理工具\Workpoint\lib\

编辑 workpoint-client.properties

根据 CA CA Identity Manager 安装过程中所选的应用程序服务器类型来编辑 workpoint-client.properties 文件。

配置 workpoint-client.properties 文件

1. 打开*管理工具*\Workpoint\conf\ workpoint-client.properties。
2. 查找该文件的 WebLogic 部分。
3. 取消该部分中所有属性值的注释。
4. 保存文件。

   注意：java.naming.provider.url 属性必须指向完全限定的域名和已经安装 CA Identity Manager 服务器的系统的 WebLogic 端口号。

在 WebSphere 上配置 WorkPoint 管理工具

要在 WebSphere 上配置 WorkPoint 管理工具，请编辑 init.bat/sh 和 workpoint-client.properties 文件。

编辑 init.bat/init.sh

编辑 init.bat/init.sh

1. 在文本编辑器中，编辑以下文件之一：
   - **Windows：**

     管理工具\Workpoint\bin\init.bat
   - **UNIX：**

     管理工具/Workpoint/bin/init.sh
2. 取消 IBM WebSphere 部分的注释。

   注意：不要注释 COMMON WP_CLASSPATH 部分中的 WP_CLASSPATH 条目。
3. 要确保针对其他应用程序服务器的所有部分都已加注释。
4. 如果需要，请将 JAVA_HOME 和 WAS_HOME 的值替换为针对您的环境的合适路径。

编辑 workpoint-client.properties

根据 CA CA Identity Manager 安装过程中所选的应用程序服务器类型来编辑 workpoint-client.properties 文件。

配置 workpoint-client.properties 文件

1. 打开*管理工具*\Workpoint\conf\workpoint-client.properties。

   *管理工具*是管理工具的安装位置。 管理工具安装在以下默认位置：
   - **Windows：**<安装路径>\tools
   - **UNIX：**<安装路径 2>/tools
2. 查找标题为“IBM WEBSPHERE SETTINGS”部分。
3. 取消该部分中所有属性值的注释。

   例如：

   ```
   java.naming.factory.initial=com.ibm.websphere.naming.WsnInitialContextFac
   tory
   java.naming.provider.url=iiop://localhost:bootstrap_port
   ```

   注意：bootstrap 端口号必须与在 WebSphere 管理控制台中指定的端口号匹配。 要找到正确的端口号，请依次进入“Server”、“Endpoints”、“Bootstrap server address”。

4. 按照如下方式更新 WebSphere 配置文件的 BOOTSTRAP_ADDRESS 端口：
   a. 在 WebSphere 管理控制台，浏览到“Application Servers”、“server_name”、“Communications”。
   b. 展开“Ports”。
   c. 编辑 iam_im.ear/config 下的 workpoint-client.properties 文件。
   d. 将 WebSphere 部分中的 默认端口 2809 更改为配置文件中 BOOTSTRAP_ADDRESS 的端口。
5. 保存文件。

启动 WorkPoint Designer

要启动 WorkPoint Designer，请运行以下文件：

- **Windows：** *管理工具*\WorkPoint\bin\Designer.bat
- **UNIX：** *管理工具*/WorkPoint/bin/Designer.sh

其中*管理工具*是 CA Identity Manager 管理工具的安装目录。 管理工具安装在以下默认位置：

- **Windows：**<安装路径>\tools
- **UNIX：**<安装路径 2>/tools

注意：您必须配置所安装的工作流组件才能运行 WorkPoint Designer。有关说明，请参阅应用程序服务器的“配置 WorkPoint 管理工具”一节。

更多信息：

在 JBoss 上配置 WorkPoint 管理工具 (p. 240)
在 WebLogic 上配置 WorkPoint 管理工具 (p. 241)
在 WebSphere 上配置 WorkPoint 管理工具 (p. 242)

WorkPoint 流程

CA CA Identity Manager 包括一些工作流流程，这些流程均在 WorkPoint Designer 中进行预定义。 可以使用预定义的流程及其默认事件映射，将工作流流程映射到其他事件、通过添加或删除活动修改工作流流程以及创建新的工作流流程。

全局流程到事件的映射

工作流流程映射到全局级别的事件可以是不基于策略或基于策略。

有关如何将事件映射到使用基于策略工作流的工作流流程的更多信息，请参阅“全局事件基于策略的工作流映射”。

该表显示了在管理控制台中指定的默认全局工作流流程与事件的映射。

重要说明：这些都是全局映射。 只要环境中某项任务生成了相应的事件，映射的工作流流程就会执行。

工作流流程	映射的事件
认证角色批准流程	认证角色事件
创建组批准流程	创建组事件
创建组织批准流程	创建组织事件
创建用户批准流程	创建用户事件
删除组批准流程	删除组事件
删除组织批准流程	删除组织事件
删除用户批准流程	删除用户事件
修改访问角色成员资格批准流程	分配访问角色事件 吊销访问角色事件
修改管理角色成员资格批准流程*	
修改组员资格批准流程*	
修改组织批准流程	修改组织事件
自行注册批准流程	自行注册用户事件

注意：默认情况下，标有星号 (*) 的工作流流程不映射到事件。

更多信息：

将流程全局映射到事件 (p. 245)
将流程映射到特定任务中的事件 (p. 246)

将流程映射到事件

可以在 WorkPoint Designer 中创建和修改工作流流程。 创建 CA Identity Manager 的工作流流程时，要牢记这是一项特定的 CA Identity Manager 任务。 该任务的执行由工作流流程控制。

除创建工作流流程外，还必须：

- 识别由 CA Identity Manager 任务生成的事件，该事件在“管理任务和事件”中进行了说明。 您可以创建适用于任何生成事件的 CA Identity Manager 任务的工作流流程。
- 通过执行以下操作之一，将工作流流程映射到事件：
  - 将工作流流程全局分配给事件。

    通过此全局映射操作，只要在环境中生成事件，工作流流程就会执行，而不必考虑生成事件的任务。
  - 将工作流流程分配给由特定任务生成的事件。

    通过此特定于任务的映射操作，仅在指定的任务生成事件时，工作流流程才会执行。

  注意：如果将事件全局映射到工作流流程，同时映射到某个特定任务，则将优先发生与该特定任务相关联的工作流流程。
- 为工作流流程中的工作流活动指定参与人确定程序。
- 将工作流活动与批准任务相关联。

更多信息：

将流程全局映射到事件 (p. 245)
将流程映射到特定任务中的事件 (p. 246)
工作流活动 (p. 247)
参与人确定程序：WorkPoint 方法 (p. 250)

将流程全局映射到事件

将工作流流程全局映射到事件，这样，当环境中的任意任务生成事件时，工作流流程就会执行。

将工作流流程全局映射到事件

1. 通过在浏览器中输入以下 URL 打开管理控制台：

   `http://hostname/iam/immanage`

   hostname

   定义安装了 CA CA Identity Manager 的服务器的完全限定域名。 例如 myserver.mycompany.com:port。
2. 单击“环境”，然后选择相应 CA CA Identity Manager 环境的名称。
3. 单击“高级设置”，然后单击“工作流”。

4. 执行以下操作以将事件映射到工作流流程：
   a. 从“事件”列表框中选择一个事件。
   b. 从“批准流程”列表框中选择一个工作流流程。
   c. 单击“添加”。
5. 将事件映射到工作流流程后，单击“保存”。
6. 重新启动 CA Identity Manager 环境以使更改生效。

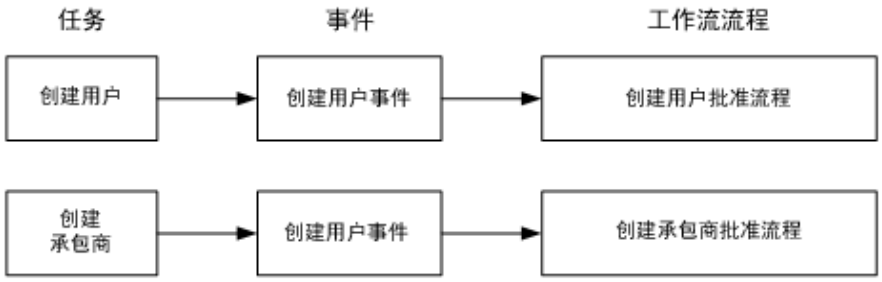
更多信息：

全局流程到事件的映射 (p. 244)

将流程映射到特定任务中的事件

您可以将工作流流程分配给由特定任务生成的事件。 在这种情况下，仅在指定的任务生成映射的事件时，工作流流程才会执行。

特定于任务的映射可提供对针对同一事件执行的工作流流程的多种控制。例如，下图显示了生成同一事件但触发两个不同工作流流程的两项不同任务：



在该图中，每项任务使用不同的工作流流程。

创建用户

指定触发 CreateUserEvent 的默认管理任务，该任务映射到默认工作流程 CreateUserApproveProcess。

创建合同工

基于创建用户指定自定义任务。 在这种情况下，CreateUserEvent 将映射到 CreateContractorApproveProcess，这是为批准新的合同工帐户而创建的自定义工作流流程。

将工作流流程映射到现有任务中的事件

1. 在用户控制台中，依次选择“角色和任务”、“管理任务”、“修改管理任务”。
2. 搜索管理员任务。
3. 选择一项任务（例如，“修改用户”或“创建用户”任务），然后单击“选择”。

4. 在“事件”选项卡中，为任务中的事件选择一个工作流流程。

   注意：必须启用工作流，以使事件名称和“工作流流程”下拉菜单显示在此选项卡中。

5. 使用“工作流流程”下拉菜单，将工作流流程分配到事件名称，然后单击“确定”。

6. 单击“提交”。

7. 打开管理控制台并重新启动 CA Identity Manager 环境，以使更改生效。

将工作流流程映射到新任务中的事件

1. 在用户控制台中，依次选择“角色和任务”、“管理任务”、“创建管理任务”。

   注意：请确保您选择了一个现有工作流批准任务（例如，“批准创建组”或“批准创建用户”）作为新工作流批准任务的模板。

2. 在“配置文件”选项卡的相应字段中输入信息。

3. 在“事件”选项卡中，为任务中的事件选择一个工作流流程。

   注意：必须启用工作流，以使事件名称和“工作流流程”下拉菜单显示在此选项卡中。

4. 使用“工作流流程”下拉菜单，将工作流流程分配到事件名称，然后单击“确定”。

5. 单击“提交”。

6. 打开管理控制台并重新启动 CA Identity Manager 环境，以使更改生效。

注意：“工作流流程”列表包括与模板方法和 WorkPoint 方法配合使用的流程：

- 当选择模板方法流程（“一步批准”或“两个阶段批准流程”）时，页面将展开以启用参与人确定程序配置。
- 当选择 WorkPoint 方法流程时，页面将不展开。 在 WorkPoint Designer 中配置参与人确定程序。

更多信息：

全局流程到事件的映射 (p. 244)

工作流活动

CA Identity Manager 包括一些工作流活动，这些活动均在 WorkPoint Designer 中进行预定义。 这些活动将分配给预定义的工作流流程。

预定义的工作流流程为一步流程，即每个流程包含一个预定义的活动。

每个预定义活动均与在 CA Identity Manager 中预定义的同名工作流批准任务对应。 可以使用在其他工作流流程中预定义的活动，也可以创建新的活动。

无需修改即可使用预定义的工作流流程，或向其中添加更多活动。 有关向工作流流程添加活动的信息，请参阅 WorkPoint 文档。

流程、任务和活动

下表列出了预定义的工作流活动，以及默认情况下分配了每个活动的预定义工作流流程。

注意：预定义的工作流活动及其相应的工作流批准任务具有相同名称。

工作流流程	工作流任务/活动
认证角色批准流程**	批准认证角色
咨询流程*	
创建组批准流程	批准创建组
创建组织批准流程	批准创建组织
创建用户批准流程	批准创建用户
删除组批准流程	批准删除组
删除组织批准流程	批准删除组织
删除用户批准流程	批准删除用户
修改访问角色成员资格批准流程	批准修改访问角色成员资格
修改管理角色成员资格批准流程	批准修改管理角色成员资格
修改组员资格批准流程	批准修改组员资格
修改身份策略集批准流程	批准修改身份策略集
修改组织批准流程	批准修改组织
修改用户批准流程	批准修改用户
自行注册批准流程	批准自行注册
一步批准*	
两个阶段批准流程*	

注意：标有一个星号 (*) 的工作流流程专用于与模板方法一起使用。这些工作流流程是在用户控制台中置的，因此没有任何默认的相关联任务或活动。 认证角色批准流程 (**) 是演示自定义参与人确定程序的样例流程。

将工作流活动与批准任务相关联

要将工作流活动与工作流批准任务相关联，您可以在 WorkPoint Designer 中定义一个名称/值对。

注意：如果没有为工作流活动定义名称/值对，则默认情况下，CA Identity Manager 将使用名称与批准任务相匹配的任务。

将工作流活动与批准任务相关联

1. 启动 WorkPoint Designer。
2. 依次单击“文件”、“打开”、“流程”。
3. 选择一个工作流流程，然后单击“打开”。
4. 在流程中的活动节点上单击右键，然后单击“属性”。
5. 从“类型”下拉菜单中选择“文本”。
6. 在“用户数据”选项卡中输入以下内容：
   - **名称** - TASK_TAG。
   - **值** - 批准任务标签名称。
7. 单击“添加”。
8. 单击“确定”保存更改。

为端点创建批准任务

您可以为帐户管理屏幕创建批准任务。 对于批准帐户修改的任务，批准屏幕必须为端点类型所特有，以便批准人可以查看更改的值。 要为创建或修改任务创建批准任务，请按照以下过程操作：

为端点创建批准任务

1. 在用户控制台中，依次单击“角色和任务”、“管理任务”、“创建管理任务”。
2. 选择用于在端点上管理帐户的“创建管理任务副本”。

   名称将始于创建和指定端点类型的名称。 创建 Active Directory 帐户是一个示例。
3. 在“配置文件”选项卡中进行以下更改。
4. 更改新任务的名称。
   - 更改任务标签。
   - 将操作更改为“批准事件”。
5. 在“选项卡”选项卡中做以下更改：
   a. 删除所有“关系”选项卡。
   b. 复制选项卡上的批准屏幕，然后根据需要进行编辑。

      注意：在批准任务中使用帐户屏幕时您可能会遇到问题，并可能需要更改默认帐户屏幕以使它们在批准任务中工作。
6. 单击“提交”。

参与人确定程序：WorkPoint 方法

要使用 WorkPoint 方法指定参与人，请在 WorkPoint Designer 中定义以下活动属性：

- 预定义 CA Identity Manager 脚本的名称，该脚本可实现 CA Identity Manager 和工作流服务器之间的通信。 该脚本向 CA Identity Manager 发出活动参与人请求，然后将该列表提供给工作流服务器。
- 对一个或多个参与人确定程序的引用。

参与人确定程序的类型

参与人由映射到*参与人确定程序*的任意名称引用，而不是在工作流活动属性中输入特定参与人列表。

对于预定义流程模型，有四种类型的参与人确定程序：

角色参与人确定程序

指定参与人是特定角色的成员。

组参与人确定程序

指定参与人是特定组的成员。

自定义参与人确定程序

指定参与人由自定义参与人确定程序确定。

筛选参与人确定程序

指定通过搜索筛选选择参与人。

角色参与人确定程序

通过角色类型参与人确定程序，CA Identity Manager 将检索该角色的所有成员，并将这些成员返回为参与人。

如果未在“活动”对话框的 UserData 参数中指定任何确定程序类型，则默认情况下，将使用角色类型确定程序。

如果在“WorkPoint 活动属性”对话框的“用户数据”选项卡中没有指定任何参与人确定程序，则默认情况下，CA Identity Manager 将查找包含此批准任务的所有可用角色，并将这些角色成员返回为参与人。

配置角色参与人确定程序

1. 启动 WorkPoint Designer。
2. 依次单击“文件”、“打开”、“流程”。
3. 选择一个工作流流程，然后单击“打开”。
4. 在流程中的活动节点上单击右键，然后单击“属性”。
5. 从“类型”下拉菜单中选择“文本”。
6. 在“用户数据”选项卡中输入以下内容：
   - **名称** - APPROVER_ROLE_NAME
   - **值** - CA Identity Manager 角色的名称（例如，安全经理）
7. 单击“添加”。

   注意：该角色无需承担任何批准任务。
8. 从“类型”下拉菜单中选择“文本”。
9. 在“用户数据”选项卡中，输入以下名称/值对（可选）：

   名称 - APPROVERS_REQUIRED

   值 - YES。
10. 单击“添加”。

注意：默认的批准设置是 APPROVERS_REQUIRED=NO。在这种情况下，如果没有找到参与人则自动批准活动。

如果 APPROVERS_REQUIRED=YES 且 CA Identity Manager 没有找到参与人，则该活动不会成功完成。

11. 单击“确定”保存更改。

组参与人确定程序

通过组类型参与人确定程序，CA Identity Manager 将检索该组的所有成员，并将这些成员返回为参与人。

要配置组参与人确定程序

1. 启动 WorkPoint Designer。
2. 依次单击“文件”、“打开”、“流程”。
3. 选择一个工作流流程，然后单击“打开”。
4. 在流程中的活动节点上单击右键，然后单击“属性”。
5. 从“类型”下拉菜单中选择“文本”。
6. 在“用户数据”选项卡中输入以下内容：
   - **名称** - APPROVER_GROUP_UNIQUENAME
   - **值** - CA Identity Manager 组的名称
7. 单击“添加”。
8. 从“类型”下拉菜单中选择“文本”。
9. 在“用户数据”选项卡中，输入以下名称/值对（可选）：
   - **名称** - APPROVERS_REQUIRED
   - **值** - YES。
10. 单击“添加”。

    注意：默认的批准设置是 APPROVERS_REQUIRED=NO。在这种情况下，如果没有找到参与人则自动批准活动。

    如果 APPROVERS_REQUIRED=YES 且 CA Identity Manager 没有找到参与人，则该活动不会成功完成。
11. 单击“确定”保存更改。

自定义参与人确定程序

自定义参与人确定程序是一个 Java 对象，可确定工作流活动参与人并将一个列表返回 CA Identity Manager，然后将该列表传递到工作流引擎。通常，仅当标准参与人策略无法提供活动所需的参与人列表时，您才可以编写自定义参与人确定程序。

注意：使用参与人确定程序 API 创建自定义参与人确定程序。 有关信息，请参阅 *《Programming Guide for Java》*。

配置自定义参与人确定程序

1. 通过在浏览器中输入以下 URL 打开管理控制台：

   `http://hostname/iam/immanage`

   hostname

   定义安装了 CA CA Identity Manager 的服务器的完全限定域名。 例如 myserver.mycompany.com:port。

2. 单击“环境”，然后选择相应 CA CA Identity Manager 环境的名称。
3. 依次单击“高级设置”、“Workflow 参与人确定程序”。
4. 在“工作流参与人确定程序”屏幕上，单击“新建”，然后输入以下内容：

   名称

   指定自定义参与人确定程序名称，如 APPROVER_CUSTOMRESOLVER_NAME

   说明

   对自定义参与人确定程序的说明。

   类

   指定 Java 类名，如 com.netegrity.samples.GroupFinder

5. 单击“保存”。
6. 启动 WorkPoint Designer。
7. 依次单击“文件”、“打开”、“流程”。
8. 选择一个工作流流程，然后单击“打开”。
9. 在流程中的活动节点上单击右键，然后单击“属性”。
10. 从“类型”下拉菜单中选择“文本”。
11. 在“用户数据”选项卡中输入以下内容：

    名称

    指定自定义参与人确定程序名称。 该名称必须与您在 CA Identity Manager 管理控制台中的“自定义类型参与人确定程序”屏幕上输入的名称相匹配，例如：

    APPROVER_CUSTOMRESOLVER_NAME

    值

    指定自定义确定程序的唯一名称，如 GroupFinder。

12. 单击“添加”。

注意：默认的批准设置是 APPROVERS_REQUIRED=NO。在这种情况下，如果没有找到参与人则自动批准活动。

如果 APPROVERS_REQUIRED=YES 且 CA Identity Manager 没有找到参与人，则该活动不会成功完成。

13. 单击“确定”保存更改。

筛选参与人确定程序

通过筛选参与人确定程序，CA Identity Manager 可以搜索符合筛选标准的用户或组。 可以在 WorkPoint Designer 中指定搜索筛选，CA Identity Manager 将返回与相应工作流活动匹配的批准人。

您可以在“WorkPoint 活动属性”对话框的“用户数据”选项卡上创建筛选参与人确定程序。

参与人确定程序筛选语法

需结合以下三个必需属性进行搜索筛选：

- 批准人属性，如职位
- 批准人属性操作，如等于
- 批准人属性值，如经理

必需的搜索筛选属性按以下顺序组合在一起：

属性 运算符 值

例如：

*“职位等于经理”*或*“部门包含劳资”*

必需的参与人确定程序筛选属性

以下为*必需*的参与人确定程序筛选属性：

注意：对于每个筛选，n 是表示搜索筛选数目的正整数。 默认值为 1。

APPROVER_FILTER_n_ATTRIBUTE

指定批准人属性。 例如，职位、部门、用户 ID。 （批准人属性名称字符串必须与 CA Identity Manager 用户属性名称字符串相匹配。）

APPROVER_FILTER_n_OP

指定与批准人属性相关联的运算符。例如，等于、不等于或包含。（运算符关键字不区分大小写。）

以下项为该筛选的有效条目：

- EQUALS
- STARTSWITH
- NOT_EQUALS
- CONTAINS
- ENDS_WITH
- GREATER_THAN
- LESS_THAN
- GREATER_THAN_EQUALS
- LESS_THAN_EQUALS

APPROVER_FILTER_n_VALUE

指定与批准人相关联的值。 例如，经理、劳资、工程。

可选的参与人确定程序筛选属性

以下是*可选的*参与人确定程序筛选属性。

APPROVER_OBJECTTYPE

USER 或 GROUP（不区分大小写）

默认值为 USER。

APPROVER_ORG_UNIQUENAME

批准人所在组织的唯一名称。 （组织名称字符串必须与 Identity Manager 组织名称字符串相匹配。）

默认值为 root。

APPROVER_ORG_AND_LOWER

批准人所在组织或分支组织：

- 0 表示在批准人所在组织中进行搜索。
- 1 表示在批准人所在组织的所有分支组织中进行搜索。

默认值为 1。

APPROVER_FILTER_NO

要使用的搜索筛选的数目。 如果您使用两个筛选，则该数值为 2。

默认值为 1。

注意：如果筛选数大于 1，则该筛选必填。

APPROVER_FILTER_n_CONJ_TYPE

您可以使用 OR 或 AND 联合类型组合使用搜索筛选。

注意：由 OR 联合隔开的筛选的优先级高于由 AND 隔开的筛选。

例如，如果您要搜索“职位等于经理”及“部门等于开发”，则可以指定 AND 联合类型。

注意：n 是大于 1 的正整数，表示搜索筛选数目。

添加参与人确定程序筛选

要添加参与人确定程序筛选

1. 启动 WorkPoint Designer。
2. 依次单击“文件”、“打开”、“流程”。
3. 选择一个工作流流程，然后单击“打开”。
4. 在流程中的活动节点上单击右键，然后单击“属性”。
5. 从“类型”下拉菜单中选择“文本”。
6. 在“用户数据”选项卡中输入以下内容：
   - **名称** - APPROVER_FILTER_1_ATTRIBUTE
   - **值** - 唯一的角色标识符（例如，职位）。
7. 单击“添加”。
8. 对搜索筛选中的每个属性重复执行步骤 6 和 7。

   注意：默认的批准设置是 APPROVERS_REQUIRED=NO。在这种情况下，如果没有找到参与人则自动批准活动。

   如果 APPROVERS_REQUIRED=YES 且 CA Identity Manager 没有找到参与人，则该活动不会成功完成。
9. 单击“确定”保存更改。

示例：筛选参与人确定程序

下表中的用户存储包含四个用户 - Holly、Sarah、John 和 Dave，及其用户 ID、职位名称和部门属性。

User	ID	标题	部门
Holly	admin1	系统管理员	管理
Sarah	test1	系统管理员	开发
John	admin2	经理	开发
Dave	admin3	系统管理员	财务

CA Identity Manager 针对上述用户存储应用下表中定义的三个筛选：

名称	值
APPROVER_FILTER_NO	3
APPROVER_FILTER_1_ATTRIBUTE	uid
APPROVER_FILTER_1_OP	等于
APPROVER_FILTER_1_VALUE	admin*
APPROVER_FILTER_2_CONJ_TYPE	AND
APPROVER_FILTER_2_ATTRIBUTE	部门
APPROVER_FILTER_2_OP	等于
APPROVER_FILTER_2_VALUE	管理
APPROVER_FILTER_3_CONJ_TYPE	OR
APPROVER_FILTER_3_ATTRIBUTE	title
APPROVER_FILTER_3_OP	等于
APPROVER_FILTER_3_VALUE	系统管理员

CA Identity Manager 按以下顺序应用筛选：

1. 评估由 OR 联合连接的第二个和第三个筛选。

   “部门等于管理”OR“职位等于系统管理员”

   这就排除了 John，返回 Holly、Sarah 和 Dave。

2. 评估由 AND 联合连接的第一个和第二个筛选（其中 * 为通配符）。

   “uid 等于 admin*”AND“部门等于管理”

   这就排除了 Sarah，返回 Holly 和 Dave。

从用户存储返回的最终用户是 Holly 和 Dave。

参与人确定程序的优先顺序

如果您未指定任何参与人确定程序，则默认情况下，Identity Manager 将识别包含批准任务的所有可用角色，并将这些角色成员返回为参与人。

如果指定了多个参与人确定程序，则 Identity Manager 将使用以下优先级顺序对其进行评估：

1. 自定义
2. 角色

3. Filter
4. Group

Identity Manager 按此优先级顺序识别和应用第一个确定程序，并忽略随后的任何其他确定程序。

一次只能对一个确定程序进行操作。 同时，请确保正确配置了确定程序，以便 Identity Manager 可正确识别参与人。

指定工作流资源脚本

Identity Manager 附带了名为 IM Approvers 脚本，该脚本在 Identity Manager 和工作流服务器之间传递信息。

当工作流活动需要参与人列表时，该脚本会将活动名称、“WorkPoint 活动属性”对话框的“用户数据”选项卡上提供的参与人标识符，以及“用户数据”选项卡上提供的其他所有信息传递给 Identity Manager。Identity Manager 将搜索参与人并将列表传回脚本。 然后，脚本将列表提供给工作流服务器。

当您具有新的工作流流程定义且工作流流程活动是一项 Identity Manager 工作流批准任务时，则必须在“WorkPoint 活动属性”对话框的“资源”选项卡中指定 IM Approvers 脚本。

在 WorkPoint Designer 中指定 IM Approvers 脚本

1. 在“资源”选项卡中，单击“选择”。
2. 在“选择资源”对话框中，从下拉列表中选择“规则”。此操作将列出可以与活动相关联的规则（脚本）。
3. 选择脚本名称 IM Approvers，然后单击“添加”。
4. 单击“确定”，然后单击“应用于活动属性”对话框。

注意：请勿修改 IM Approvers 脚本。

指定用于认证用户任务的参与人

认证用户任务可生成事件“认证角色事件”。 该事件通过预定义流程“认证角色批准流程”遵循工作流批准。

Identity Manager 还包括预定义的参与人确定程序“认证角色参与人确定程序”，默认情况下，该程序显示在您的环境中。 “认证角色批准流程”中活动的参与人通过“认证角色参与人确定程序”指定。

提供参与人配置信息

1. 通过在浏览器中输入以下 URL 打开管理控制台：

   `http://hostname/iam/immanage`

   hostname

   定义安装了 CA CA Identity Manager 的服务器的完全限定域名。 例如 myserver.mycompany.com:port。

2. 单击“环境”，然后选择相应 CA CA Identity Manager 环境的名称。
3. 单击“高级设置”，然后单击“杂项”。
4. 定义用于为要认证的每个角色指定批准人的名称/值对：
   - 在“属性”字段中，使用以下格式：*角色类型.角色名称*

     *角色类型*必须为以下类型之一：管理、访问、配给。

     *角色名称*为任一现有角色的名称。

     角色名称和角色类型必须用句点隔开 (.)。
   - 在“值”字段中，指定批准人的 ID，并用分号 (;) 隔开。

在下例中，以下参与人可为以下角色批准用户认证：

- jsmith01 和 ajones19 可为“用户经理”角色批准认证
- plewis12 只能做“系统经理”角色的批准人
- rtrevor8 和 pkitt3 可为“我的访问”角色批准认证

属性	值
admin.User Manager	jsmith01;ajones19
admin.System Manager	plewis12
access.My Access Role	rtrevor8;pkitt3

注意：任何未指定的角色均不具有“认证角色事件”的批准人。

WorkPoint Designer 中的流程

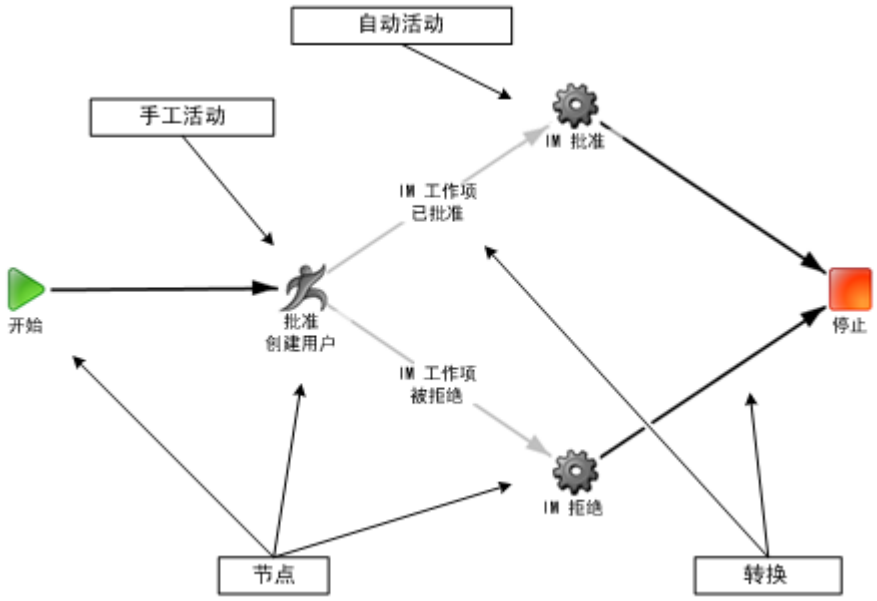
在 WorkPoint Designer 中，您可以自定义 Identity Manager 附带的默认工作流流程和活动，也可以新建工作流流程和活动。

该文档介绍了特定于 Identity Manager 的 WorkPoint 工作流信息。 有关完整信息，请参阅 WorkPoint Designer 文档。

注意：创建工作流流程时，请考虑按以下步骤执行：备份现有 Identity Manager 流程，然后修改新流程，使其满足您的需求。 以这种方式创建的工作流流程包括默认的 Identity Manager 特定元素和节点，例如转换脚本和自动活动。

WorkPoint 流程图

下图显示了用于控制 Identity Manager 任务的典型工作流流程，其中包含流程所需的最基本组成部分。该图显示了控制“创建用户”任务的执行的预定义流程“创建用户批准流程”。



WorkPoint 流程组成部分

工作流流程包括以下节点和转换：

开始

每个工作流流程均从该节点开始。

停止

每个工作流流程均以该节点结束。

手工活动

手工活动需要由参与人批准或拒绝 Identity Manager 任务，且必须与 Identity Manager 工作流批准任务具有相同的名称。

控制 Identity Manager 任务的工作流流程必须至少包括一个需要批准该任务的手工活动。

自动活动

将给自动活动分配以下两个脚本之一：

- 通知 IM 批准 - 通知 Identity Manager 执行工作流控制之下的 Identity Manager 任务。
- 通知 IM 拒绝 - 通知 Identity Manager 取消执行 Identity Manager 任务。

通常，如果所有手工活动均被批准，则激活通知 IM 批准脚本；如果任一手工活动被拒绝，则激活通知 IM 拒绝脚本。

无条件转换

无条件转换是从工作流流程的一个节点到另一个节点的路径，且不与条件脚本相关联。

条件转换

条件转换表示是从工作流流程的一个节点到另一个节点的可选路径，并与条件脚本相关联。

条件脚本通过评估相关联活动的结果确定是否执行转换。 如果脚本返回 True，将执行转换，并且流程转到下一个指定的节点。

可能两个或多个条件脚本均返回 True。 这将允许并行执行活动，因为每个脚本均与不同的转换相关联。

注意：您可以在条件转换中使用自定义脚本。有关说明，请参阅*《Java 编程指南》*。

手工活动属性

下表列出了特定于 Identity Manager 的属性设置。 这些设置在“WorkPoint Designer 活动属性”对话框的指定选项卡中进行定义。

属性选项卡	属性说明
资源	IM 批准人 - 在“包含”列表中指定。 该脚本在 Identity Manager 和工作流服务器之间传递信息。
代理	无人自动完成 - 在“异步”列表中指定，并与“可用”状态相关联。该脚本用于确定在不存在活动参与人的情况下是否应将活动视为已批准。
用户数据	定义 Identity Manager 用于检索活动参与人的名称/值对。另外，还可以定义要传递给自定义参与人确定程序的数据。

条件转换属性

以下默认脚本将显示在“转换属性”对话框的“条件”选项卡中：

批准的 IM 工作项

如果相关联的活动被批准，则返回 True。 工作流流程转到由转换指定的下一节点。

拒绝的 IM 工作项

如果相关联的活动被拒绝，则返回 True。 工作流流程转到由转换指定的下一节点。

作业和流程实例

*工作流流程*定义了在 Identity Manager 完成特定任务之前必须执行的步骤。*作业*是工作流流程的运行时实例。

例如，默认工作流流程“创建用户批准流程”定义了批准新用户必须执行的步骤。在 Identity Manager 中实际创建新用户且将任务提交以获得批准后，将在 WorkPoint Designer 中创建“创建用户批准流程”的作业实例。

您可以使用与用于编辑工作流流程的界面十分类似的界面，在 WorkPoint Designer 中打开、查看和修改作业。

基于同一流程的多个作业可同时存在。

筛选作业

WorkPoint Designer 包括筛选，使您可以根据各种标准搜索作业。 例如，您可以搜索以下作业：

- 基于一个或多个选定的工作流流程的作业
- 具有用户定义的作业参考或唯一作业 ID 的作业
- 处于特定状态（例如，活动、完成或挂起）的作业
- 在指定日期范围内创建或开始的作业

注意：有关作业筛选的说明和参考信息，请参阅 WorkPoint Designer 文档。

作业状态和属性

打开作业后，将显示作业的工作流图。 工作流活动节点和转换通过着色表明是否已执行。

您可以查看，某些情况下还可以修改以下内容：

- 作业属性，包括参与人和作业历史记录信息
- 开放作业的状态，例如是否已完成
- 作业中各个节点和转换的属性

活动和工作项属性

您可以查看，某些情况下还可以修改作业活动属性和流程活动属性，包括以下内容：

- 活动状态信息
- 活动批准信息
- 批准任务（在 WorkPoint Designer 中称为*工作项*）信息，例如：
  - 如果没有任何参与人保留了工作项（已从其他批准人的工作列表中删除），则状态为“可用”，且不显示任何参与人用户 ID。
  - 如果参与人已保留但尚未完成工作项，则状态为“未完成”，且显示参与人的用户 ID 和保留时间。
  - 如果工作项已完成，则状态为“完成”。将显示批准或拒绝工作流控制之下任务的参与人的用户 ID，并显示完成时间。

特定工作项属性包括：

- 工作项名称和当前状态
- 状态历史记录信息，包括负责设定状态的参与人的用户 ID
- 经授权的工作项参与人信息

注意：有关作业、活动和工作项属性的详细信息，请参阅 WorkPoint Designer 文档。

执行工作流活动

在工作流流程中，手工活动由被指定为活动参与人的人员执行，该人员可批准或拒绝与批准任务相关联的事件。 参与人在 Identity Manager 中执行此活动。

执行与 Identity Manager 批准任务相关联的活动时，将发生以下操作：

1. Identity Manager 通知参与人。
2. 参与人批准或拒绝该任务。
3. 工作流服务器完成该活动。

查找并通知参与人

与 Identity Manager 批准任务相关联的工作流活动开始时，工作流服务器会将关于活动参与人的信息传递给 Identity Manager。 在活动属性中定义此信息。 Identity Manager 使用此信息检索活动参与人，并提醒他们一个批准任务正处于未决状态。

识别参与人后，Identity Manager 会将一个新的工作项（批准任务）添加至每个参与人的工作列表。 或者，Identity Manager 也可向每个参与人发送关于新工作项的电子邮件通知。

注意：如果 APPROVERS_REQUIRED 活动属性设置为 False，且未找到任何参与人，则默认情况下该任务将被视为已批准。

注意：“状态”列中的圆圈表示批准任务可供任何批准人申请进行处理。 复选标记表示工作列表所有者已接受批准任务但尚未完成。

接受和执行批准任务

找到参与人后，直到一个参与人接受批准任务并批准或拒绝工作流控制下的任务后，才能完成活动。

参与人通过单击工作流活动控制台中的工作项名称，然后单击“保留项目”来接受批准任务。 （保留一个项目会将其从其他批准人的工作列表中删除。）

参与人接受批准任务后，他即负责决定是批准还是拒绝工作流控制下的任务。而由于多个参与人不能接受同一批准任务，因此会从其他参与人的工作列表中删除该批准任务。

参与人接受批准任务后，将显示批准屏幕，参与人可在其中执行以下操作之一：

- 立即批准或拒绝工作流控制下的任务。
- 释放批准任务，以使其他参与人可使用该任务。
- 关闭对话框，稍后再完成该活动。 要重新打开之前显示的“批准创建用户”对话框，参与人可在其工作列表中单击批准任务的名称。

此外，参与人可在批准屏幕上更新一个或多个可修改的字段（如果有）。 创建任务时可将此屏幕上的字段设为可修改。

参与人批准或拒绝工作流控制下的任务后，活动即完成，工作流流程即可按照由该活动的结果确定的路径继续进行，如下一部分中所述。

工作流服务器完成活动

Designer 窗口中将显示一个手工活动，并随之引发两个或多个条件转换。

每个条件转换均与脚本相关联。 参与人完成活动后，脚本将评估活动结果。 这些评估的结果将确定流程流的方向。

下图显示了 Designer 中的“批准创建用户”活动，以及 Identity Manager 中相应的同名批准任务。

当活动参与人（或批准人）在 Identity Manager 中单击“批准”或“拒绝”按钮时：

1. 流程作业实例中的“批准创建用户”活动将终止。 与条件转换相关联的脚本将评估活动的结果。

2. 作业实例将继续进行，这取决于哪些条件转换评估为 True：
   - 如果活动已批准，则 IM WorkItem Approved 脚本将返回 True。 工作流将 IM WorkItem Approved 转换转移至下一节点。 此自动活动 IM Approve 将通知 Identity Manager 执行“创建用户”任务。
   - 如果活动被拒绝，IM WorkItem Rejected 脚本将返回 True。工作流将 IM WorkItem Rejected 转换转移至下一工作流节点。 此自动活动 IM Reject 将通知 Identity Manager 取消“创建用户”任务。

Workpoint 作业视图

您可以在用户控制台的以下任务中查看 Workpoint 作业的运行时状态。

- 批准任务
- 查看提交的任务。

在新的环境中，所有的批准任务会默认包括“查看作业”选项卡。 仅有此版本中创建的事件支持在“查看提交的任务”中查看为所选事件或任务调用的所有流程定义的作业图像。 在较早版本中创建的事件不支持“工作流作业视图”功能。

将查看作业选项卡添加到现有批准选项卡

对于“批准”任务，您必须将新的“查看作业”选项卡添加到所有的现有任务中，才能查看该工作项的作业图像。

注意：新环境中的所有批准任务都包含该选项卡。

将作业视图选项卡添加到现有任务

1. 在“管理任务和角色”类别中，通过依次选择“管理任务”、“修改管理任务”来执行 ModifyAdminTask
2. 单击“搜索”，选择一个批准任务（如“批准创建用户”），然后单击“选择”。

   此时会出现“修改管理任务: 批准创建用户”对话框。
3. 单击“选项卡”选项卡，从下拉菜单中选择“查看作业(JobView)”，然后单击“提交”。

   “查看作业”选项卡已添加到该批准作业。

   对所有现有的批准任务重复该步骤。

配置查看作业选项卡

配置该选项卡的以下几个方面：

名称

您分配给选项卡的名称。

标签

任务中唯一的选项卡标识符。 它必须以字母或下划线开头，并且仅包含字母、数字或下划线。 该标签主要用于通过 XML 文档或 HTTP 参数设置数据值。

隐藏选项卡

使选项卡在任务中不可见。 该选项对于需要隐藏选项卡但仍可访问选项卡上属性的应用程序很有用。

作业视图

该选项卡为指定的工作项显示作业映像。

查看批准任务中的查看作业选项卡

要查看批准任务中的“查看作业”选项卡，请遵循下列步骤。

查看“查看作业”选项卡

1. 在“工作列表”对话框中，选择要查看的批准任务。
2. 单击“查看作业”选项卡查看任务的运行时状态。

   您可以从中进行“批准”、“拒绝”、“保留”，或关闭该选项卡。

您也可以单击“主页”选项卡，然后单击“查看我的工作列表”来转到“工作列表”对话框。

查看 EventLevel 工作流的工作流作业

要在“查看提交的任务”中查看 EventLevel 工作流的工作流作业，请遵循下列步骤。

查看工作流作业

1. 在“系统”选项卡中选择“查看提交的任务”，输入搜索条件，然后选择“搜索”。
2. 选择该事件，然后单击铅笔图标查看事件详细信息。
3. 在“事件工作流作业视图”中选择流程，然后单击铅笔图标查看该事件的作业图像。

查看 TaskLevel 工作流的工作流作业

要在“查看提交的任务”中查看 TaskLevel 工作流的工作流作业，请遵循下列步骤。

查看工作流作业

1. 在“系统”选项卡中选择“查看提交的任务”，输入搜索条件，然后选择“搜索”。
2. 选择该任务，然后单击铅笔图标查看任务详细信息。

在“任务工作流作业视图”中选择流程，然后单击铅笔图标查看该任务的作业图像。

基于策略的工作流

通过基于策略的工作流可以根据规则评估将事件或管理任务置于工作流控制之下。 这意味着，与之前事件或管理任务总是启动工作流流程不同，仅当规则与该事件或管理任务相关联的规则为真时，工作流流程才会运行并生成工作项。

*批准规则*是一个条件，决定是否启动工作流流程。 如果启动，该工作流流程则会通过向批准人工作列表中添加一个工作项的方式，将事件或管理任务置于工作流控制之下。

*批准策略*是批准规则、规则评估类型、策略顺序、策略说明以及工作流流程的组合。

例如，创建新组时，您可以定义一种批准策略，该策略会将 CreateGroupEvent 置于工作流控制之下，并且仅当新组属于指定的父组织时才创建工作项。 如果新组不属于该组织，工作流流程则不会运行，也不会创建任何工作项。

如果事件有多个规则，那么与事件关联的所有工作流流程需要为要批准的事件获取批准。 同样，对于管理任务，您可以定义批准策略，这些策略会将 CreateGroupTask 置于工作流控制下，并仅当新建组的名称始于“销售”时才创建工作项。 如果新建组的名称不始于“销售”，工作流流程不会运行，也不会创建工作项。

您创建的策略规则可以总是进行评估，也可以只有当某个受管理对象的指定属性发生更改时（例如，员工的工资值有所更改时）才进行评估。

注意：在基于策略的工作流早期版本中，如果任何批准人对属性做出任何更改，都将被发送用于重新批准。 使用属性级别的批准和拒绝，在任何阶段的更改仅被批准一次。 即使包含在规则内的属性已修改，工作项也从未被提交进行重新批准。 一旦批准人批准更改，他们将不会看到工作项，直到提交新的更改或重新提交任务。

更多信息：

事件级工作流 (p. 226)
任务级工作流 (p. 224)
策略顺序 (p. 271)
规则评估 (p. 269)

默认工作流流程

所有默认工作流模板和预定义的工作流流程都支持如下工作流规则：

- **流程模板** – 通过这些模板，您可以在用户控制台中配置批准人（或参与人确定程序）。
- **预定义的工作流流程** – 这些流程要求您使用 WorkPoint Designer 配置参与人确定程序。

另外，还可以创建自定义工作流流程以便与工作流规则一起使用。

更多信息：

WorkPoint 流程 (p. 243)

规则的对象

CA Identity Manager 管理员可以根据以下对象为事件或管理任务创建批准策略。如果对象应用于给定事件且在事件执行期间出现，则是事件的对象：

- **任务的发起者** – 执行该任务的 CA Identity Manager 管理员。
- **事件的主要对象** – 与事件相关联的主要对象。
- **事件的次要对象** – 与事件相关联且与主要对象相关的次要对象

以下内容是管理任务的对象：

- **任务的主要对象** – 与任务关联的主要对象。
- **任务的发起者** – 执行该任务的 Identity Manager 管理员。
- **身份策略违规** - 针对身份策略违规，规则会基于导致违规的身份策略的策略名称，例如，“Policy Name EQUALS TitlePolicy”。 违规消息显示在批准屏幕的“任务详细信息”选项卡中，与“查看提交的任务”的“任务详细信息”相同。SOD 违规消息显示在名为“身份策略违规”的新标题下。 批准人可以查看这些消息并且可以决定批准或拒绝任务。

规则评估

可以通过下列两种方式对事件的策略规则进行评估：

- Always

  无论策略中包含的任何属性是否更改，只要策略评估为“真”，评估类型为“Always”的策略就被调用。 在批准屏幕上针对由于策略评估类型为“Always”而生成的工作项，批准人可以更改批准屏幕上的任何可编辑属性。

  注意：如果批准人单击“拒绝”按钮，那么就会象以前一样拒绝该事件。

- 仅当批准条件中指定的属性有所更改时

  仅在策略评估为“真”且包含在策略中的属性更改时，评估类型为“OnChange”的策略才被调用。 在批准屏幕上针对由于策略评估类型为“Onchange”而生成的工作项，批准人仅可以更改那些包含在策略中的属性值（如果那些属性在该批准屏幕中有读写权限）。 存在于批准屏幕上的所有其他属性有只读权限。

  注意：如果批准人单击“拒绝”按钮，只拒绝那些对包含在批准策略中的属性所做的更改，然后对下一个批准策略进行评估。

  该选项仅应用于事件的主要对象或任务的主要对象。

以下列策略为例，所有策略都属于“修改用户”管理任务中的 ModifyUserEvent：

策略	规则	评估
Policy1	用户，其中（用户 ID = Smith01）	始终
Policy2	用户，其中（职位 = 经理）	当“职位”属性更改时
Policy3	用户，其中（工资 >= 80000）	当“工资”属性更改时

管理员每次为用户 Smith01 调用“修改用户”任务时即会评估 Policy1，无论更改哪个属性都会如此。

当管理员为任意用户对象调用“修改用户”任务以更改“职位”属性时即会评估 Policy2。 如果“职位”更改为“经理”，Policy2 为真。

当管理员为任意用户对象调用“修改用户”任务以更改“工资”属性时即会评估 Policy3。 如果工资更改为 80000 或更多，Policy3 为真。

在该示例中，如果管理员使用“修改用户”任务为用户 Smith01 将“职位”属性更改为“经理”，那么 Policy1 和 Policy2 都会评估为真，而其相应的工作流流程也会启动。 在这种情况下，即会应用标准排序优先级。

通过条件规则评估，某工作项的批准人可以更改对同一事件的其他工作项产生影响的属性（此时该事件仍处于未决状态）。 这对于评估类型为“Always”的批准策略是可能的。 在上面的示例中，如果管理员为用户 Smith01 更改属性，Policy1 则为真并生成工作项。 当批准 Policy1 生成的工作项时，该批准人可能会在同一批准屏幕上为 Smith01 更改“工资”属性。在这种情况下，Smith01 的新“工资”值将确定 Policy3 是否会为相同的 ModifyUserEvent 实例生成工作项。 如果批准人将工资更改为 90000，Policy3 即会生成新的工作项，该工作项必须获得批准后事件本身才会获得批准。 此时即应用标准排序优先级。

更多信息：

策略顺序 (p. 271)
规则的对象 (p. 268)

规则评估示例

请考虑以下策略，所有策略都适用于“修改用户”管理任务中的 ModifyUserEvent：

策略	规则	评估
Policy1	用户，其中（用户 ID = Smith01）	始终
Policy2	用户，其中（职位 = 经理）	当“职位”属性更改时
Policy3	用户，其中（工资 >= 80000）	当“工资”属性更改时

管理员每次为用户 Smith01 调用“修改用户”任务时即会评估 Policy1，无论更改哪个属性都会如此。

当管理员为任意用户对象调用“修改用户”任务以更改“职位”属性时即会评估 Policy2。 如果“职位”更改为“经理”，Policy2 为真。

当管理员为任意用户对象调用“修改用户”任务以更改“工资”属性时即会评估 Policy3。 如果工资更改为 80000 或更多，Policy3 为真。

在该示例中，如果管理员使用“修改用户”任务为用户 Smith01 将“职位”属性更改为“经理”，那么 Policy1 和 Policy2 都会评估为真，而其相应的工作流流程也会启动。 在这种情况下，即会应用标准排序优先级。

通过条件规则评估，某工作项的批准人可以更改对同一事件的其他工作项产生影响的属性（此时该事件仍处于未决状态）。 这对于评估类型为“Always”的批准策略是可能的。 在上面的示例中，如果管理员为用户 Smith01 更改属性，Policy1 则为真并生成工作项。 当批准 Policy1 生成的工作项时，该批准人可能会在同一批准屏幕上为 Smith01 更改“工资”属性。在这种情况下，Smith01 的新“工资”值将确定 Policy3 是否会为相同的 ModifyUserEvent 实例生成工作项。 如果批准人将工资更改为 90000，Policy3 即会生成新的工作项，该工作项必须获得批准后事件本身才会获得批准。 此时即应用标准排序优先级。

策略顺序

所有的批准策略都包含“策略顺序”字段，该字段中会有一个按从最低到最高排列的正整数值来指定优先级。 每个策略的优先级确定下列事项：

- 批准规则的评估顺序
- 工作流流程的启动顺序（对于值为真的规则）

具有较低整数值的策略具有较高优先级，其规则会在具有较高整数值的策略之前进行评估。 对于某事件或管理任务的值为真时的所有策略，具有最高优先级的策略会最先启动其工作流流程。

策略顺序示例

该简单示例演示如何进行策略排序。 在该示例中，假设策略规则始终被评估。

如果某事件具有多个始终被评估的策略，那么要使得该事件本身被批准，必须批准所有策略。 然而，如果与事件（策略评估类型为“ALWAYS”）关联的策略被拒绝，那么就会拒绝事件本身。

注意：如果与事件关联的策略的评估类型为 Onchange，则与包含在该策略内的属性关联的更改被拒绝。 事件本身不会被拒绝且评估行中的下一策略。

在该示例中，Policy1 、 Policy2 和 Policy3 都有 ALWAYS 的策略评估类型。 Policy1 评估为假，则名为 Process1 的工作流流程不会执行，且不会为 User1 生成任何工作项。 事件控制立即传递给 Policy2。 Policy2 和 Policy3 都评估为真。 由于工作流 Process2 具有较高优先级，所以首先运行并为 User2 生成工作项。

如果 User2 批准该工作项，工作流 Process3 即会运行并为 User3 生成工作项，而 User3 随后必须批准该工作项，才能使得该事件本身获得批准。 这些操作如下表所示：

优先级	策略	结果	工作流	批准人	操作
1	Policy1	假	Process1	User1	—
2	Policy2	真	Process2	User2	已批准
3	Policy3	真	Process3	User3	已批准

但是，如果 User2 拒绝工作项，事件本身将被拒绝且不会为 User3 生成任何工作项，如下表所示：

优先级	策略	结果	工作流	批准人	操作
1	Policy1	假	Process1	User1	—

优先级	策略	结果	工作流	批准人	操作
2	Policy2	真	Process2	User2	已拒绝
3	Policy3	真	Process3	User3	—

下一步，Policy1,Policy2，以及 Policy3 都有 ONCHANGE 的策略评估类型。 如果 User2 拒绝工作项，仅与包含在 Policy2 内的属性关联的更改会被拒绝。 之后评估 Policy3，并且工作流 Process3 运行并为 User3 生成工作项。 如果 User3 拒绝工作项，由于对该事件的所有更改被拒绝所以也拒绝该事件。 如果 User3 批准工作项，会批准事件且包含在 Policy3 内的属性更改会持续。

优先级	策略	结果	工作流	批准人	操作
1	Policy1	假	Process1	User1	—
2	Policy2	真	Process2	User2	已拒绝
3	Policy3	真	Process3	User3	已批准

策略说明

一个可选的不可搜索字符串说明属性已添加到批准策略管理的对象，并出现在结果工作项上。

支持的最大字符数：255 个字符

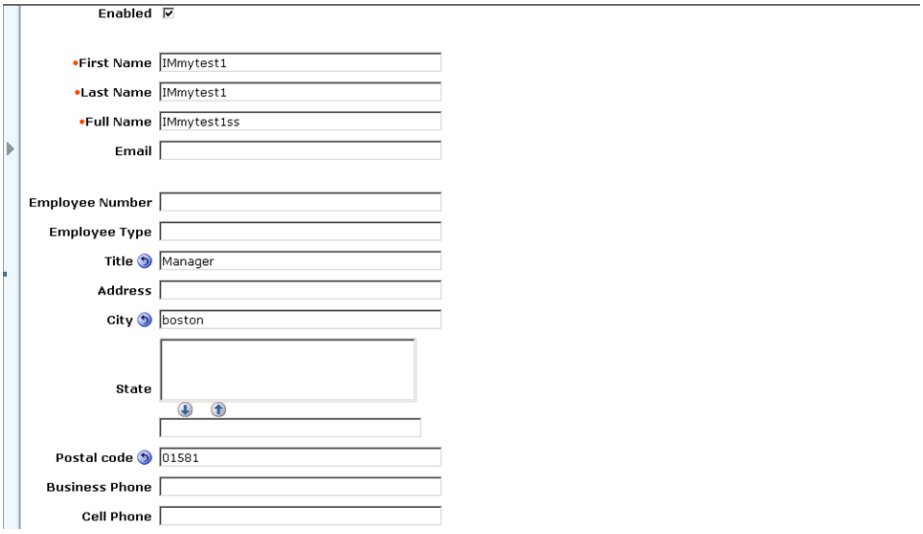
您可以使用以下格式输入 bundle、key 的信息进行说明：

```
$ (bundle=<fully qualified resource bundles name> : key=<key>)
```

在批准屏幕中突出显示更改的属性

为了让批准人了解已经修改哪些属性或让批准人在必要时撤销对那些属性的更改，已经在批准人配置文件屏幕中添加了撤销图标，通过它批准人可以了解已经更改了该属性。

批准人可以通过单击撤销按钮查看可编辑属性的原始值，也可以将属性值更改为任何其他值。



批准策略和多值属性

先前如果已为多值属性设置了规则，则无法将此规则设置为仅适用于为多值属性新添加或删除的值。 通过查看基于多值属性的规则的规则评估类型，现在可以实现。 如果规则评估类型是 Onchange，那么该规则仅可应用于多值属性的新添加或删除的值，而不是多值属性的所有值。 如果规则必须基于多值属性的所有值，不管他们是否是新添加还是删除的值，该规则的评估类型必须是“Always”。

对多值属性所做的更改突出显示在配置文件屏幕中并带有撤销图标。 如果评估的规则为真，是因为将新值添加到多值属性或从多值属性删除，批准该更改的批准人会查看包含在多值属性内的所有值。 单击撤销图标将该属性值恢复其原始值。 如果批准人要查看已删除的值，则单击撤销图标可以显示原始的值。 单击重做图标显示新值，通过它批准人可以区分哪些是已删除的值，哪些是已添加的值。 单击“批准”按钮批准对该多值属性的所有更改。 单击“拒绝”按钮拒绝对该多值属性的所有更改。 除非针对该多值属性有新的增量值，否则不会评估属于该多值属性的所有后续规则。

注意：对于基于多值属性的规则，包含在多值属性中的值是实际的值，而不是显示的值。 例如，MA 州的显示值是马萨诸塞州。 创建基于状态属性的批准策略时，该规则应为 state=MA。

以下列策略为例，所有策略都属于“修改用户”管理任务中的 ModifyUserEvent：

策略	规则	评估
Policy1	User where (State = MA)	OnChange
Policy2	User where (state = DC)	始终

管理员每次调用修改用户任务来更改状态属性时，都会对 Policy1 进行评估，如果值 MA 是从该状态属性新增或新删除的，则该策略评估为真。

管理员每次为其状态包含值 DC 的用户调用修改用户任务时，都会对 Policy2 进行评估。

在工作流批准屏幕上突出显示为已更改的属性

在批准屏幕上，即使管理员没有在原始任务中更改其他属性，他们也可能突出显示为已更改。 这是因为屏幕可以包含脚本，这些脚本可以更改包含在该屏幕中的各种属性值，针对某些其他属性的更改作为屏幕初始化或屏幕验证的一部分。

策略示例

下列业务案例说明如何为事件应用工作流批准策略：

示例 1：

使用案例 – 管理员修改某员工的关系数据库帐户。

管理任务 - ModifyMSSQLAccount

事件 – ModifyMSSQLAccountEvent

批准规则 – 用户，其中（职位 = RDBAcctManager）

工作流流程 – ModAcctApproval（自定义工作流流程）

对象 – 任务的发起者

评估 – 始终评估该规则

示例 2：

使用案例 – 管理员修改某员工的工资以便反映新的加薪情况。

管理任务 – 修改用户

事件 – ModifyUserEvent

批准规则 – 用户，其中（工资 >= 100000）

工作流流程 – SalaryChangeApproval（自定义工作流流程）

对象 – 事件的主要对象（用户）

评估 – 仅当“工资”属性更改时进行评估

示例 3：

使用案例 – 管理员将某用户添加到“合同工”组，此时该用户的职位更改为“合同工”。 该示例可以划分成下列两个批准策略：

策略 1：

管理任务 – 修改用户

事件 – ModifyUserEvent

批准规则 – 用户，其中（职位 = 合同工）

工作流流程 – SingleStepApproval（默认流程模板）

对象 – 事件的主要对象（用户）

评估 – 仅当“职位”属性更改时进行评估

策略 2：

管理任务 – 修改组（或修改组成员）

事件 – AddToGroup

批准规则 – 组，其中（组名称 = 合同工）

工作流流程 – SingleStepApproval（默认流程模板）

对象 – 事件的次要对象（组）

评估 – 始终评估该规则

下列业务案例说明如何为任务应用工作流批准策略：

示例 1：

使用案例 – 管理员修改属于某员工的 Active Directory 帐户。

管理任务 - ModifyActiveDirectoryAccount

对象 – 任务的发起者

批准规则 – 用户，其中（职位 = ActiveDirectoryManager）

工作流流程 - 单步批准

评估 – 始终评估该规则

示例 2：

使用安案 - 管理员修改员工代码是 HighSecurity 的用户。

管理任务 – 修改用户

对象 – 任务的主要对象

批准规则 - 用户，其中（职位 = HighSecurity）

工作流流程 - 单步批准

评估 – 始终评估该规则

示例 3：

使用安案 - 管理员修改用户以分配管理角色 CheckApprover 和 CheckSigner。

管理任务 – 修改用户

对象 - 身份策略违规

批准规则 – 身份策略，其中（名称 = CheckRoles）

工作流流程 - 单步批准

评估 – 总是评估为真

如何配置基于策略的工作流

配置基于策略的工作流的过程类似于配置事件级工作流的过程，额外的步骤就是定义确定是否执行工作流的批准策略。

配置基于策略的工作流

1. 在用户控制台中，依次选择“角色和任务”、“管理任务”、“修改 (或创建) 管理任务”。

   将显示“选择管理任务”屏幕。

2. 搜索您要将其置于工作流控制下的任务，然后单击“选择”。

   将显示“修改 (或创建) 管理任务”屏幕。

3. 在“配置文件”选项卡中，确认已选中“启用工作流”。

4. 在“事件”选项卡上，选择要映射至流程模板的事件。

   将显示工作流映射屏幕。

5. 选择“基于策略”单选按钮，然后单击“添加”。

   此时会出现“批准策略”屏幕。

6. 配置一个批准策略 (p. 278)。

7. 按照选定工作流流程所要求的那样配置参与人确定程序。

   参与人请求将添加至该流程。

8. 单击“确定”。

   CA Identity Manager 将保存事件级工作流配置。

9. 单击“提交”。

   CA Identity Manager 将处理任务修改。

注意：“工作流流程”列表包括与模板方法和 WorkPoint 方法配合使用的流程：

- 当选择模板方法流程（“一步批准”或“两个阶段批准流程”）时，页面将展开以启用参与人确定程序配置。
- 当选择 WorkPoint 方法流程时，页面将不展开。 在 WorkPoint Designer 中配置参与人确定程序。

更多信息：

参与人确定程序：WorkPoint 方法 (p. 250)
如何配置批准策略 (p. 278)

如何为任务配置基于策略的工作流

配置基于策略的工作流的过程类似于配置任务级工作流的过程，额外的步骤就是定义确定是否执行工作流的批准策略。

配置基于策略的工作流

1. 在用户控制台中，依次选择“角色和任务”、“管理任务”、“修改 (或创建) 管理任务”。

   将显示“选择管理任务”屏幕。

2. 搜索您要将其置于工作流控制下的任务，然后单击“选择”。

   将显示“修改 (或创建) 管理任务”屏幕。

3. 在“配置文件”选项卡中，确认已选中“启用工作流”。

4. 在“配置文件”选项卡上，单击“工作流流程”字段旁边的铅笔图标

   将显示工作流映射屏幕。

5. 选择“基于策略”单选按钮，然后单击“添加”。

   此时会出现“批准策略”屏幕。

6. 配置一个批准策略 (p. 278)。

7. 按照选定工作流流程所要求的那样配置参与人确定程序。

   参与人请求将添加至该流程。

8. 单击“确定”。

   CA Identity Manager 将保存任务级工作流配置。

9. 单击“提交”。

   CA Identity Manager 将处理任务修改。

注意：工作流流程列表包括用于任务级基于策略的工作流的模板方法的流程：

- 当选择模板方法流程（“一步批准”或“两个阶段批准流程”）时，页面将展开以启用参与人确定程序配置。

更多信息

如何配置批准策略 (p. 278)

如何配置批准策略

为事件或任务配置批准策略涉及以下步骤。

1. 选择要测试的对象。
2. 为该对象定义批准规则。
3. 对于主要对象，确定是否为条件评估。

4. 输入策略评估的顺序。
5. 配置当规则为真时要运行的工作流流程。

配置批准策略

1. 在“批准策略”屏幕上，从下拉列表中为要测试的规则选择一个对象。

   屏幕会随着您的选择有所变化。
2. 从对象名称旁边的新下拉列表中选择一个条件表达式模板。

   屏幕会随着您的选择有所变化。
3. 根据需要创建和编辑条件表达式。
4. 选择“规则评估”选项按钮以便指明是始终评估该规则，还是仅当批准条件中的属性更改时才进行评估。
5. 输入一个正整数值来指定策略评估顺序（如果该事件有多个策略）。
6. 选择并配置当规则评估为真时执行的工作流流程。
7. 单击“确定”保存批准策略。

更多信息：

如何配置事件级工作流 (p. 227)
如何配置基于策略的工作流 (p. 277)
如何为任务配置基于策略的工作流 (p. 278)

基于策略的工作流状态

CA Identity Manager 管理员可以使用下列标准系统工具来显示包含工作流批准策略的任务的状态：

- “查看提交的任务”选项卡
- “用户历史记录”选项卡
- 报表和日志

已提交的任务和任务历史记录信息包括：

- 任务和事件信息
- 工作流和批准规则信息
- 批准规则评估结果

有关已提交任务历史记录的说明，请参阅“系统”选项卡文档。

更多信息：

事件状态说明 (p. 478)
CA Identity Manager 中的任务状态 (p. 472)

全局事件级别基于策略的工作流映射

事件可以被映射到管理控制台的工作流流程，或与特定任务中的基于策略的工作流批准策略关联。 通过新的“为事件配置基于全局策略的工作流”任务，管理员可以在环境级别为事件设置基于策略的工作流映射。 不同于为管理任务中的事件设置基于策略工作流，所配置的基于策略工作流映射应用于生成该事件的所有任务。

注意：只有在启用工作流时，“为事件配置全局基于策略工作流”任务才可用。在禁用工作流时执行该任务会抛出错误。

此任务已添加到“系统”选项卡。 提交任务时，会以下列方式检索该任务中每个事件的工作流流程：

为该管理任务的事件配置的任何工作流具有优先权。 针对基于策略或不基于策略的工作流可以配置事件。 如果针对该管理任务的事件配置了基于策略的工作流，那么会调用与该策略关联的工作流流程。 如果没有规则匹配，则该事件不调用工作流。 同样，如果针对该管理任务的事件配置了不基于策略的工作流，那么会调用与该策略关联的工作流流程。 如果针对该管理任务的事件没有配置工作流，那么该事件的全局工作流配置具有优先权。

为事件配置全局基于策略工作流的任务屏幕

通过“为事件配置全局基于策略工作流”的任务，管理员可以为当前环境中的所有事件配置基于策略或不基于策略的工作流。 单击任务显示映射到工作流流程定义的默认事件。 可以修改或删除每个事件映射，也可以为尚未配置的事件添加新的事件映射。

该屏幕上的字段如下所示：

与该环境中的事件关联的工作流流程。

指定与批准策略关联的工作流流程。

添加新映射

指定映射到工作流流程的批准策略。

添加按钮

添加新映射。

添加或修改映射会打开工作流映射屏幕，在屏幕中可以选择流程映射和批准策略。 行为与事件级别工作流配置相同。 单击工作流映射页上的“添加”按钮会出现其他的页面，在页面中可以配置批准策略。

更多信息

如何配置基于策略的工作流 (p. 277)
如何配置批准策略 (p. 278)

为事件配置全局基于策略工作流

针对事件的全局基于策略工作流配置该选项卡。

名称

您分配给选项卡的名称。

标记

任务中唯一的选项卡标识符。 它必须以字母或下划线开头，并且仅包含字母、数字或下划线。该标签主要用于通过 XML 文档或 HTTP 参数设置数据值。

隐藏选项卡

使选项卡在任务中不可见。 该选项对于需要隐藏选项卡但仍可访问选项卡上属性的应用程序很有用。

用户搜索屏幕

定义要用于显示用户的搜索屏幕。

用户列表屏幕

定义确定该选项卡上的列和排序的屏幕。

组搜索屏幕

定义要用于显示组的搜索屏幕。

组列表屏幕

定义确定该选项卡上的列和排序的屏幕。

管理角色搜索屏幕

定义要用于显示管理角色的搜索屏幕。

管理角色列表屏幕

定义确定该选项卡上的列和排序的屏幕。

管理任务搜索屏幕

定义要用于显示管理任务的搜索屏幕。

管理任务列表屏幕

定义确定该选项卡上的列和排序的屏幕。

在线请求

通过 CA Identity Manager 可以创建通用的在线请求任务。 默认在线请求实施由一系列自行修改请求和管理员用户修改请求的相关任务组成。 不过，可轻松地为其他 CA Identity Manager 请求任务实现在线请求功能。

用户修改请求会触发生成工作项的工作流流程。 工作流参与人可以批准并实施该工作项，也可以拒绝该工作项。 用户在历史记录编辑器（CA Identity Manager 用于保留请求历史记录的文本区域）中输入请求的说明，启动该任务。 可将此历史记录编辑器配置为允许参与人保留有关其对工作项所执行的操作的注释。 这些注释会成为累积工作项历史记录的一部分。

同样可进行标准批准和拒绝操作之外（或直接代替）的新操作。 例如，业务参与人可以阐明请求或为其添加注释，而技术参与人可以实施该请求。 这些新活动可由新工作流操作按钮表示，如“阐明”和“实施”，您可以将这些按钮添加至批准任务上的标准“批准”和“拒绝”按钮。

在线请求任务

需配合执行五个任务才能实施默认的在线请求。 这些任务演示了自定义请求、历史记录和工作流操作按钮的使用：

注意：默认情况下，为使用“咨询流程”模板的事件级工作流配置管理任务（“更改我的帐户”和“创建在线请求”）。

更改我的帐户

这是一个自行修改管理任务，可创建一个用户帐户更改请求。 该任务包含带有用于对请求进行说明的历史记录编辑器的“请求”选项卡，以及具有只读用户详细信息的“配置文件”选项卡。

创建在线请求

这是一个用户修改管理任务，可为特定用户创建一个帐户更改请求。该任务包含带有用于对请求进行说明的历史记录编辑器的“请求”选项卡，以及具有只读用户详细信息的“主题配置文件”选项卡。

批准在线请求

这是一个批准任务，允许业务参与人批准或拒绝任务，或请求该任务的详细阐明信息。 此任务包含带有历史记录显示和用于查询或添加注释的历史记录编辑器的“请求”选项卡，以及只读的“主题配置文件”选项卡和“受派人”选项卡。

阐明在线请求

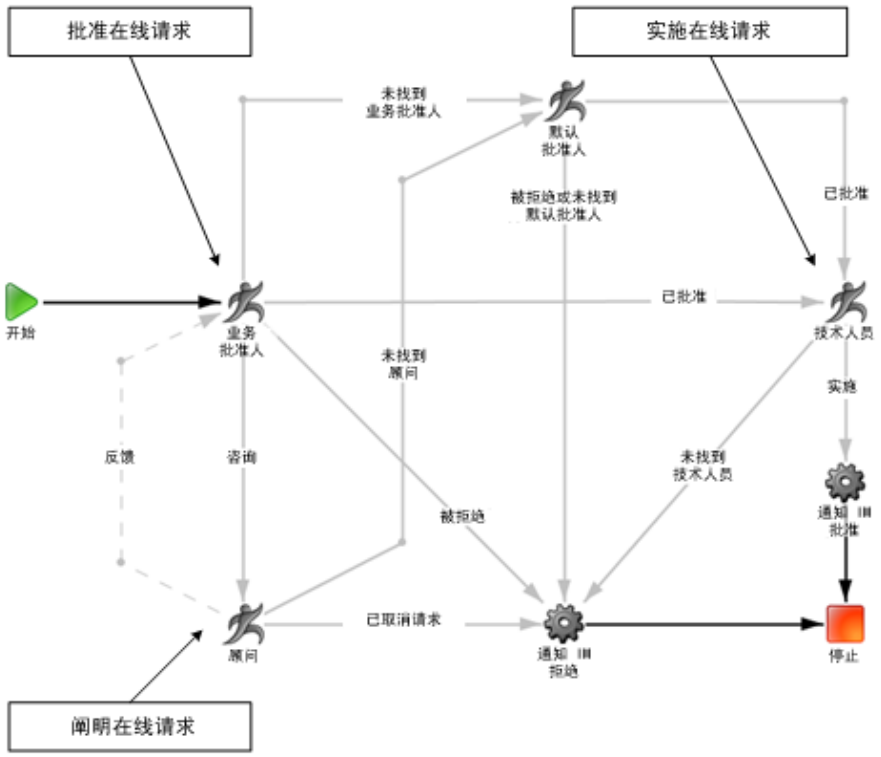
这是一个批准任务，允许阐明参与人响应阐明请求，并将任务发送回业务参与人进行批准。 此任务包含带有历史记录显示和用于添加注释的历史记录编辑器的“请求”选项卡，以及只读的“主题配置文件”选项卡。

实施在线请求

这是一个批准任务，允许技术参与人实施任务并为任务历史记录添加注释。 此任务包含带有历史记录显示和用于添加注释的历史记录编辑器的“实施请求”选项卡，以及只读的“主题配置文件”选项卡和“受派人”选项卡。

在线请求流程

在线请求任务由称为“咨询流程”的工作流流程模板控制，与在 WorkPoint Designer 中的显示方式一致：



“咨询流程”包括四个手工活动，这些活动与在线请求实施中的批准任务相对应：

- 适用于业务批准人（可拒绝工作项、批准工作项并将其传递给技术人员，或向顾问请求该任务的详细阐明信息）的活动。
- 适用于顾问（可阐明工作项并将其发送回业务批准人）的活动。
- 适用于默认批准人（在无法与业务批准人或顾问取得联系时，由默认批准人负责）的活动。
- 适用于技术人员（可实施请求并完成工作项）的活动。

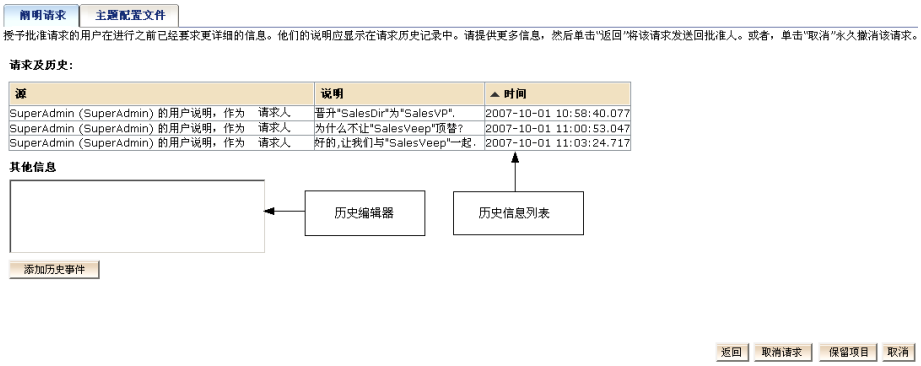
在线请求历史记录

通过在线请求历史记录功能，参与人可创建工作项操作的记录。 当工作项的职责从一个参与人转至另一参与人时，新的参与人可以在执行操作前查看工作项历史记录。

有两种控制方式用于实施在线请求历史记录：

- 历史记录显示为只读表格，包含之前的历史记录条目的详细信息，按时间顺序显示。
- 历史记录编辑器是用于创建新历史记录条目的文本框。 还包括一个可选按钮，用于添加多个条目而无需提交工作项。

默认情况下，历史记录编辑器和历史记录显示将显示在所有与在线请求实施相关联的任务的“请求”选项卡上。 以下屏幕说明了“阐明在线请求”任务中的历史记录控制：



使用在线请求

以下步骤介绍了在线请求工作流流程。对于每个步骤，生成的 IM 任务显示在括号中。 在流程中的每个步骤，参与人均可在历史记录编辑器中添加注释。 此注释显示在历史记录显示中，供该工作流流程的下一参与人查看。

1. 任务启动人请求修改 IM 用户（创建在线请求）。
2. 业务批准人接收工作项，并执行以下操作之一：
   - 批准工作项（批准在线请求）。
   - 拒绝工作项并终止工作流流程。 无新任务生成。
   - 向顾问请求阐明信息（阐明在线请求）。
3. 顾问接收工作项，并执行以下操作之一：
   - 添加阐明信息并将工作项返回给业务批准人。 无新任务生成。
   - 取消工作项并终止工作流流程。 无新任务生成。
4. 技术人员接收工作项并实施请求（实施在线请求）。

工作流操作按钮

从历史记录角度来说，CA Identity Manager 中的批准任务在相应的工作项屏幕上有批准和拒绝操作按钮。 工作流操作按钮允许管理员通过将操作按钮添加到批准任务中并删除或修改现有按钮，来扩展 CA Identity Manager 任务和工作流的功能。 （标准“批准”和“拒绝”按钮和自定义工作流操作按钮以同样的方法实施。）

例如，工作流流程可能需要允许中层参与者将某种特定情况升级到最后批准或拒绝的更高级参与者的操作。 这些中层参与者可能使用历史编辑器添加注释或建议，然后将工作项发送到高级参与者，以便审核及批准或拒绝。

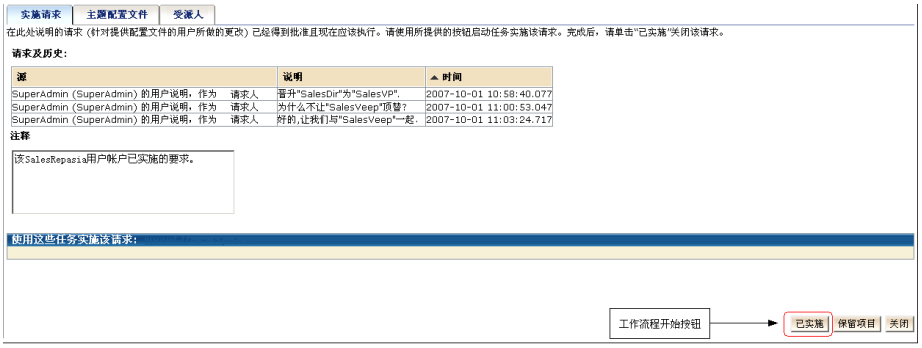
添加或删除工作流操作按钮需要对 WorkPoint 工作流流程做适当的更改，这为处理这些新的操作提供业务逻辑。

更多信息：

CA Identity Manager 中的按钮配置 (p. 287)
批准任务中的工作流按钮 (p. 286)
WorkPoint Designer 中的按钮配置 (p. 289)

批准任务中的工作流按钮

工作流操作按钮与 WorkPoint 流程图中从手工活动节点指向的转换节点相对应。例如，在“咨询流程”中，技术人员活动节点具有称为“已实施”的单个转换。 这与“实施在线请求”批准任务上的“已实施”按钮相对应，如下图所示：



注意：“保留项目”和“关闭”按钮由 CA Identity Manager 编程逻辑控制，而不受工作流控制。

更多信息：

工作流操作按钮 (p. 286)
CA Identity Manager 中的按钮配置 (p. 287)

CA Identity Manager 中的按钮配置

要配置工作流操作按钮，单击批准任务的“配置文件”选项卡上名为“工作流操作按钮”的按钮。

按钮“配置文件”选项卡具有一个表格，其中包含一行每个工作流操作按钮。 每个按钮行具有以下四个属性，与表中的列相对应：

显示名称

显示在批准屏幕的按钮上的名称。该名称是一个条件式本地化的值，可以是字符串，也可以是资源文件中本地化字符串的关键字。

Action

选中该选项时传回到工作流流程的值。此值为 WorkPoint 流程图中相应转换节点的属性。 该值是非本地化字符串。 默认设置为“已批准”和“已拒绝”。

工具提示

用户将鼠标光标悬停在按钮上方时，将显示该按钮操作的简短说明（或工具提示）。 该工具提示是一个条件式本地化的值，可以是字符串，也可以是资源文件中本地化字符串的关键字。

详细说明

按钮操作的较详细说明，添加了一条描述“查看已提交任务”屏幕上操作的消息。如果说明为空，在“查看提交的任务”屏幕上显示的消息将是按钮名称。 该名称是一个条件式本地化的值，可以是字符串，也可以是资源文件中本地化字符串的关键字。

更多信息：

WorkPoint Designer 中的按钮配置 (p. 289)

添加工作流操作按钮

要为现有的工作流流程添加新按钮，请执行以下高级步骤：

1. 在 Identity Manager 中添加工作流按钮。

   有关说明，请参阅“如何添加工作流操作按钮” (p. 288)。

2. 如有必要，添加本地化关键字。

   有关说明，请参阅 *《配置指南》*。

3. 在 WorkPoint Designer 中添加任何所需的新节点。

   有关说明，请参阅 WorkPoint Designer 在线帮助。

4. 在 WorkPoint Designer 转换节点中定义脚本。

   有关说明，请参阅“WorkPoint Designer 中的按钮配置” (p. 289)。

详细信息：

WorkPoint Designer 中的按钮配置 (p. 289)
如何添加工作流操作按钮 (p. 288)

如何添加工作流操作按钮

可以向 CA Identity Manager 中的批准任务添加工作流操作按钮。

向管理任务添加工作流操作按钮

1. 在用户控制台中，依次选择“角色和任务”、“管理任务”、“修改管理任务”。

   将显示“选择管理任务”屏幕。

2. 搜索批准任务，然后单击“选择”。

   将显示“修改管理任务”屏幕。

3. 在“配置文件”选项卡上，单击名为“工作流操作按钮”的按钮。

   将显示“工作流操作按钮配置文件”选项卡。

4. 单击“添加按钮”向批准任务添加新按钮。

5. 输入按钮属性信息。

6. 单击“确定”。

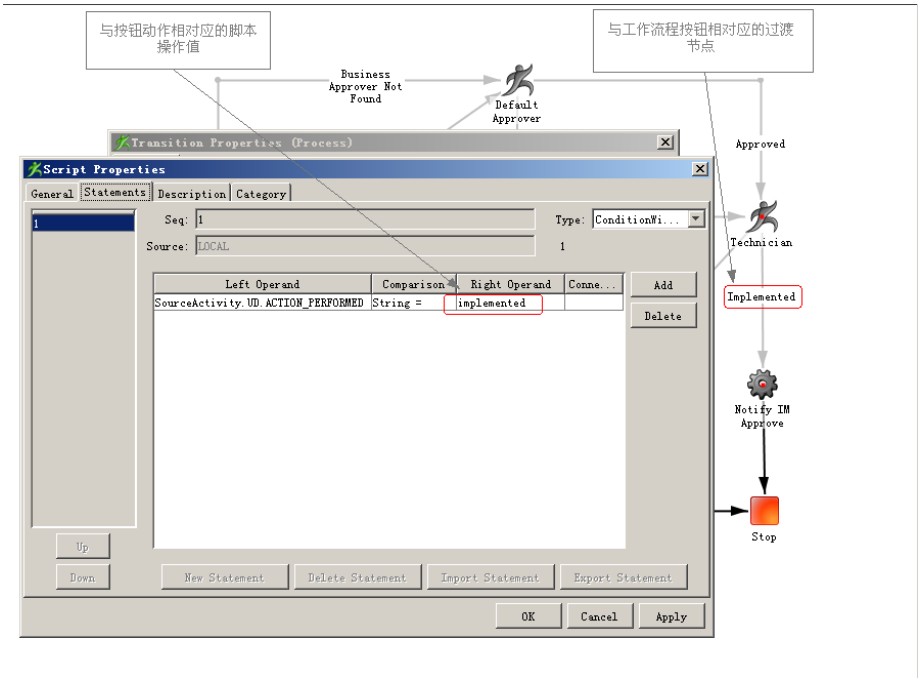
   CA Identity Manager 将保存新按钮信息。

7. 单击“提交”。

   CA Identity Manager 将处理任务修改。

WorkPoint Designer 中的按钮配置

在 WorkPoint Designer 中，可使用转换节点脚本属性配置工作流操作按钮，如下图所示：



默认情况下，工作流操作按钮使用以下脚本属性执行字符串比较：

- 左操作元 - ACTION_PEFORMED，在前述手工活动节点的“用户数据”属性中定义。
- 右操作元 - 按钮的“操作”值，在用户控制台的按钮配置文件选项卡中定义。

注意：请参阅 WorkPoint Designer 在线帮助，以获取有关活动节点以及转换节点脚本和属性的信息。

更多信息：

CA Identity Manager 中的按钮配置 (p. 287)

工作列表和工作项

*工作列表*是工作项（或批准任务）的列表，显示在授权批准任务的参与人的用户控制台中。 工作项与工作流流程中的手工活动相对应。 工作项表示为工作列表中的行。

可通过以下方式将工作项添加至工作列表：

- 参与人确定程序确定批准人列表。
- 接收另一用户的指派工作项。
- 将其重新分配给另一用户。

可通过以下方式从工作列表中删除工作项：

- 完成（批准或拒绝）工作项。
- 将其重新分配给另一用户。
- 保留该项目。 这会将从其他所有参与人的工作列表中删除。

注意：在您接受或拒绝工作项时，更改不是即时的。 例如，如果拒绝了一个工作项，该项仍然出现在您的工作列表，直到工作流流程记录信息并将进程进行到下一节点。

显示在工作项上的信息选项卡取决于该工作项是由任务级控制下的工作流生成的，还是由事件级控制下的工作流生成的：

- **配置文件 —** 提供关于受事件（仅限事件级）影响的对象的信息。
- **任务详细信息 —** 提供任务（仅限任务级）中所有事件的详细信息。
- **批准人 —** 列出任务或事件（任务级和事件级）各自所有的批准人和指派人

显示工作列表

如果您已被指定为参与人来批准由其他用户启动的任务（或工作项），则当您登录用户控制台时，将自动显示工作列表。

手工显示您的工作列表

1. 在用户控制台中，依次选择“主页”、“查看我的工作列表”。

   将显示您的工作列表。

2. 单击某一工作项的名称以进行显示。

   将显示所选的工作项。

管理员可管理其范围内用户的工作项。

注意：通过管理用户的工作项，管理员可以保留工作项。 查看用户的工作列表时，不允许对工作项进行任何形式的更改。

查看另一用户的工作列表

1. 在用户控制台中，依次选择“用户”、“管理工作项”、“查看用户的工作列表”。

   将显示选择用户屏幕。
2. 搜索您要查看其工作列表的用户，然后单击“选择”。

   将显示该用户的工作列表屏幕。

管理另一用户的工作项

1. 在用户控制台中，依次选择“用户”、“管理工作项”、“查看用户的工作项”。

   将显示选择用户屏幕。
2. 搜索您要管理其工作项的用户，然后单击“选择”。

   将显示该用户的工作列表屏幕。
3. 单击某一工作项的名称以进行显示。

   将显示所选的工作项。

保留工作项

可以保留工作项以“将其检出”并从其他参与人的工作列表中删除。 保留工作项会使执行保留的用户保有对该项的使用权。

如果执行保留的用户释放了工作项，该工作项便会再次出现在其他参与人的工作列表上。如果执行保留的用户批准或拒绝了该工作项，则该工作项即已完成，其他用户无法再使用。

详细信息：

指派和保留的工作项 (p. 292)
重新分配和保留的工作项 (p. 291)

重新分配和保留的工作项

如果用户保留了一个工作项，而该项又被重新分配，则该工作项保持其处于保留状态。 但如果用户之后释放了此工作项，他便无法访问该项。

管理员可以重新分配、保留或释放另一用户的工作项，但不能批准或拒绝另一用户的工作项。 只有分配的工作项参与人才能这样做。

详细信息：

重新分配工作项 (p. 297)

指派和保留的工作项

指派处于活动状态时，委托人或指派人均可保留工作项。 由一个用户保留的工作项无法显示在另一用户的工作列表上。

例如，如果撤销指派时委托人保留了工作项，则委托人将保持该工作项处于保留状态。 但如果委托人之后释放了此工作项，他便无法访问该项。

如果委托人用户已被删除，而保留了一个工作项，则该委托人仍将保留此工作项。如果委托人之后批准了该工作项，则审核便无法再确定谁指派了该工作项。

例如，如果撤销指派时委托人保留了工作项，则委托人将保留访问权，直到该工作项完成或被释放。

详细信息：

指派工作项 (p. 292)
保留工作项 (p. 291)

如何保留或释放工作项

可以保留工作项以“将其检出”并从其他参与人的工作列表中删除。

可以释放保留的工作项，使其出现在其他参与人的工作列表上。

注意：释放保留的工作项唯一方式是对其进行显式释放。

保留或释放工作项

1. 在用户控制台中，依次选择“主页”、“查看我的工作列表”。

   将显示您的工作列表。
2. 选择您要保留或释放的工作项。

   将显示扩展的工作项屏幕。
3. 单击“保留项目”或“释放项目”。

   CA Identity Manager 确认您的操作。

指派工作项

通过工作项*指派*，用户（指派人）可指定另一个用户（委托人）批准指派人工作列表中的任务。 当指派人“不在办公室”期间，他可以将工作项分配给另一批准者。在指派期间，指派人完全保留对其工作项的访问权。

不能以任何方式对指派的工作项进行更改。 记录指明某一工作项是否被指派。

通过授权委托人“模拟”指派人并查看该指派人工作列表中的项目来指派工作。查看工作列表时，委托人可看到自己的工作项以及指派人的工作项。

指派不可传递。委托人只能看到指派人直接分配的工作项。例如，如果用户 A 将工作项指派给了用户 B，而用户 B 将工作项指派给了用户 C，则用户 C 只能看到属于用户 B 的工作项，而看不到用户 A 可能已指派给用户 B 的任何工作项。

详细信息：

指派和保留的工作项 (p. 292)

指派已知属性

指派使用以下已知属性：

%DELEGATORS%

此已知属性将存储通过该属性对该用户进行指派的用户名称，以及创建指派的时间。

如何启用指派

必须启用工作流批准指派，才能将工作项指派给另一用户。 默认情况下，禁用指派。

启用工作流批准指派

1. 通过在浏览器中输入以下 URL 打开管理控制台：

   `http://hostname/iam/immanage`

   hostname

   定义安装了 CA CA Identity Manager 的服务器的完全限定域名。 例如 myserver.mycompany.com:port。

2. 单击“环境”，然后选择相应 CA CA Identity Manager 环境的名称。
3. 单击“高级设置”，然后单击“工作流批准指派”。
4. 选中“启用”复选框，然后单击“保存”。

详细信息：

如何为自己指派 (p. 294)
如何为另一用户指派 (p. 295)

如何为自己指派

当您“不在办公室”期间，可以将工作项指派给另一批准者。在指派期间，指派人完全保留对其工作项的访问权。

为自己指派工作项

1. 在用户控制台中，依次选择“主页”、“不在办公室协助”。

   将显示“不在办公室协助”屏幕。

2. 单击“添加用户”。

   将显示选择用户屏幕。

3. 搜索并选择一个或多个用户作为委托人。

   这些用户将被添加到委托人列表。

4. 单击“提交”。

   将提交任务并保存指派。

注意：添加委托人时，已经是委托人的用户不会显示在搜索结果中。

更多信息：

如何启用指派 (p. 293)

基于时间的工作项指派

在以前版本中，您可以指定指派的开始时间，但不能指定结束时间。 新创建的指派则将其指派日期均设置为真，其中默认开始日期设置为现在。

修改时，开始和结束日期均可更改。 默认结束时间是从开始日期起一周。

要更改开始或结束日期，请执行以下操作：

1. 在用户控制台的“主页”选项卡，选择“外出时助理”。
2. 单击要更改其指派信息的用户 ID 旁边的铅笔图标。

   此时将显示“编辑指派详细信息”屏幕。

3. 单击“开始日期”旁边的日历来更改指派开始日期。

   注意：如果选定的指派开始日期在当前日期之前，则会显示一条错误消息。

4. 如果您想选择结束日期，则选中“有结束日期”复选框。

   现在“结束日期”机会出现，以便设置结束日期。

5. 单击“结束日期”旁边的日历来设置指派的结束日期。
6. 一旦日期设置完毕，单击“确定”。

另外，您还可以在创建或修改用户时，从“指派工作项”选项卡执行同样操作。

启用基于时间的工作项指派

要在升级时在现有环境中启用基于时间的工作项指派，请执行以下操作：

在管理控制台中

1. 导航到“环境”页。
2. 向下浏览到选定的环境，“高级设置”，“工作项指派”。
3. 取消选中“已启用”复选框。
4. 保存更改并重新启动环境。
5. 向下浏览到“高级设置”，“工作项指派”。
6. 选中“已启用”复选框。
7. 保存更改并重新启动环境。

注意：该过程仅用于现有环境。 新环境已启用基于时间的工作流项指派。

外出时助理屏幕

可以使用以下“外出时助理”屏幕为自己添加及删除指派：

“外出时助理”屏幕将显示您当前的指派列表。 除识别指派的列外，列表中还包括另外三列：

开始日期

显示创建指派的日期。

结束日期

显示指派将结束的日期。

具有指派

表示指派是否已将工作项指派给另一用户。

在您单击选定用户 ID 旁边的铅笔图标时，“编辑指派详细信息”屏幕会出现在可以更改开始日期和指定指派结束日期的地方。

如何为另一用户指派

管理员可以将一个用户（指派人）的工作项指派给另一用户。 例如，一个用户可能因意外情况需要离开办公室，或者管理员需要将大量工作分配给多个用户。

管理员仅可为其范围内的用户分配工作项。 同样地，他们也仅可在委托人列表上添加或删除他们所管理的用户。

为另一用户指派工作项

1. 在用户控制台中，依次选择“用户”、“管理工作项”、“指派工作项”。

   将显示选择用户屏幕。

2. 搜索您要指派其工作项的用户（指派人），然后单击“选择”。

   将显示指派工作项屏幕。

3. 单击“添加用户”。

   将显示选择用户屏幕。

4. 搜索并选择一个或多个用户作为委托人。

   这些用户将被添加到委托人列表。

5. 单击“提交”。

   将提交任务并保存指派。

注意：添加委托人时，已经是委托人的用户不会显示在搜索结果中。

更多信息：

如何启用指派 (p. 293)

如何删除指派

如果用户登录 CA Identity Manager 时具有有效指派，则 CA Identity Manager 将显示以下提醒：

“您具有有效指派。 请确认是否还需要这些指派。”

为自己删除指派

1. 在用户控制台中，依次选择“主页”、“不在办公室协助”。

   将显示“不在办公室协助”屏幕。

2. 单击您要删除的委托人旁边的减号 (-)。

   委托人即从列表中消失。

3. 单击“提交”。

   将提交任务并删除指派。

为另一用户删除指派

1. 在用户控制台中，依次选择“用户”、“管理工作项”、“指派工作项”。

   将显示用户搜索屏幕。

2. 搜索并选择您要删除其指派的用户。

   将显示委托人列表。

3. 单击您要删除的委托人旁边的减号 (-)。

   委托人即从列表中消失。

4. 单击“提交”。

   将提交任务并删除指派。

注意：您仅可删除您范围内用户的委托人。

重新分配工作项

通过重新分配，用户和管理员可以在创建工作项后更改其受派人。管理员可以：

- 查看其他用户的工作列表
- 添加和删除工作项受派人
- 更改工作项的保留状态

例如，管理员可以重新分配工作项，或从没有操作该工作项的用户释放保留的工作项。

如果用户在重新分配工作项时保留了工作项，那么该用户保持其保留状态。 但是如果该用户释放该工作项，那么用户则无法访问它。

如果收回指派权限时指派保留了工作项，那么指派则保留访问权限，直到工作项完成或被释放。

更多信息：

重新分配和保留的工作项 (p. 291)

“批准人”选项卡

您在显示当前工作项批准人（或受派人）列表的“工作项批准人”选项卡上执行重新分配。 当您执行重新分配时，将未完成的工作项分配给列表中的所有批准人。 因此，要向新受派人重新分配工作项，您还必须删除当前受派人。

如何重新分配工作项

将一个用户的工作项重新分配给另一用户需要以下两个步骤：

- 选择一个新的批准人。
- 删除当前批准人。

注意：您必须对要重新分配的用户有作用域。

重新分配自己的工作项

1. 依次选择“主页”、“查看我的工作列表”。

   将显示您的工作列表。

2. 选择要展开的工作项。

3. 选择“批准人”选项卡。

   将显示所有当前批准人的列表，包括您正在管理的工作列表的用户。

4. 单击“添加受派人”。

   将显示选择用户屏幕。

5. 搜索并选择一个或多个要重新分配给的用户。

   注意：对于 ALL 和 SUBSET 批准模式，您只能对一名用户重新分配工作项。

6. 单击减号按钮 (-) 以便删除作为受派人的您自己。

7. 单击“执行重新分配”。

   工作项将显示在已重新分配用户的工作列表上。

注意：管理员可以重新分配、保留或释放其他用户的工作项，但无法批准或拒绝其他用户的工作项。 只有该工作项的所有者才能执行此操作。

重新分配其他用户的工作项

1. 依次选择“用户”、“管理工作项”、“管理用户的工作项”。

   将显示选择用户屏幕。

2. 搜索要重新分配其工作项的用户，然后单击“选择”。

   此时显示“管理用户的工作项”屏幕。

3. 选择要展开的工作项。

4. 选择“批准人”选项卡。

   将显示所有当前批准人的列表，包括您正在管理的工作列表的用户。

5. 单击“添加受派人”。

   将显示选择用户屏幕。

6. 搜索并选择一个或多个要重新分配给的用户。

7. 单击减号按钮 (-) 以删除当前的指派人。

8. 单击“执行重新分配”。

   工作项将显示在已重新分配用户的工作列表上。

针对工作项的批量操作

对于该版本的 CA Identity Manager，可以针对选定的工作项执行下列批量操作：

- 批准
- 拒绝
- 保留
- 释放

在用户控制台中，“配置工作列表”选项卡得以增强，现在包括一个新的支持批量工作流操作复选框。 如果启用该复选框，用户则可以批量批准、拒绝、释放和保留他们拥有的工作项，或任何指派人的工作项。 管理员仅可以使用管理用户的工作项任务，对工作项执行这些批量操作。

注意：无法为任何视图类型任务启用批量操作，如“查看我的工作列表”。

为批量操作配置工作列表选项卡

要对“工作列表”选项卡进行配置以便支持工作项的批量操作，请按照以下过程执行操作。

在用户控制台中的“角色和任务”选项卡

1. 选择以下任一选项：
   - 角色和任务
   - 任务、角色和任务
2. 依次选择“管理任务”、“管理管理任务”。
3. 单击“搜索”。
4. 选择“管理用户的工作项”。
5. 在“选项卡”选项卡，单击“工作列表”旁边的铅笔图标。

   此时将显示“配置工作列表”屏幕。
6. 选择“支持批量工作流操作”。
7. 保存更改并提交任务。

   此时工作项批量操作即可用。

第 13 章： 电子邮件通知

此部分包含以下主题：

CA CA Identity Manager 中的电子邮件通知

电子邮件通知会通知系统中任务和事件的 CA CA Identity Manager 用户。 例如，CA CA Identity Manager 在事件或任务需要批准时，可以给批准人发送邮件。

CA CA Identity Manager 为配置电子邮件通知提供以下方法：

- **电子邮件通知策略**

  通过电子邮件通知策略，业务管理员可以使用用户控制台中的任务创建、查看、修改和删除电子邮件通知。 创建电子邮件通知不需要代码。

  管理员可以定义电子邮件的内容、何时发送、何人接收。 电子邮件的内容（在 HTML 编辑器中定义）可以包含动态信息，如当前日期或事件信息，在发送电子邮件时，CA CA Identity Manager 将进行填充。 例如，您可以配置在创建新用户时发送给批准人的电子邮件通知。 电子邮件可以包含用户的登录信息、雇用日期以及管理者。

  注意：电子邮件通知策略是 Policy Xpress 策略 (p. 407)（由特定一组任务创建和管理）。

- **电子邮件模板**

  在该方式中，电子邮件通知来自于电子邮件模板。CA CA Identity Manager 提供默认电子邮件模板，这些模板可以按照安装时的状态使用，也可以由系统管理员自定义。这些管理员使用电子邮件模板 API 来指定动态内容（如收件人列表）以及有关触发电子邮件事件的信息。

在以下情况发生时 CA CA Identity Manager 可以生成电子邮件通知：

- 需要由工作流批准人批准或拒绝的事件处于未决状态

  注意：如果您有一个有多个批准活动的 Workpoint 批准流程，那么在用户控制台任务中配置的电子邮件通知会为每个活动发送通知。 如果使用电子邮件模板进行同样的通知，仅将一个电子邮件发送给批准人（在事件达到挂起状态时）。

- 批准人批准事件或任务
- 批准人拒绝事件或任务

- 事件或任务启动、失败或完成
- 用户被创建或被修改

要使用 CA CA Identity Manager 电子邮件通知，请配置您的 SMTP 设置 (p. 303)。如果正在使用电子邮件模板的方法，也会启用 CA CA Identity Manager 中的电子邮件通知。

如何选择电子邮件通知方法

下表概述电子邮件通知策略和电子邮件模板之间的差异：

活动	电子邮件管理任务	电子邮件模板
配置电子邮件通知	管理员可在用户控制台中使用管理员任务，来创建、修改、查看和删除电子邮件通知。	管理员可在 CA Identity Manager 管理工具中修改默认模板。
在发送电子邮件时进行配置	特定事件或者任务发生时，CA CA Identity Manager 可以生成电子邮件通知。 电子邮件管理任务和电子邮件模板支持相同的事件和任务，然而电子邮件管理任务在某些情况下可提供更多粒度。 针对下列任务和事件支持电子邮件通知： ■ 需要由工作流批准人批准或拒绝的事件处于未决状态 ■ **注意：**如果您有一个具有多个批准活动的 Workpoint 批准流程，那么使用电子邮件管理任务配置的电子邮件通知会为每个活动发送通知。 如果使用电子邮件模板进行同样的通知，仅将一个电子邮件发送给批准人（在事件达到挂起状态时）。 ■ 批准人批准事件或任务 ■ 批准人拒绝事件或任务 ■ 事件或任务启动、失败或完成 ■ 用户被创建或被修改	

活动	电子邮件管理任务	电子邮件模板
将动态内容添加到电子邮件	管理员可以从“创建电子邮件”或“修改电子邮件”任务的“内容”选项卡的选项列表中选择，从而将动态内容添加到电子邮件消息的正文中。 CA CA Identity Manager 根据触发通知的事件或任务中的信息自动填充动态内容。	管理员可使用电子邮件模板 API 来自定义默认电子邮件模板，该模板可用于生成电子邮件通知。
支持现有的电子邮件通知	使用电子邮件管理任务配置的电子邮件通知基于 Policy Xpress 策略。 如果您从 CA CA Identity Manager Option Pack 1 升级到 CA CA Identity Manager 12.6.4，您在 Policy Xpress 中配置的电子邮件通知仍然有效。 然而，您可使用电子邮件管理任务（而不是策略 Xpress）管理电子邮件通知。	您在 CA CA Identity Manager 的先前版本中使用电子邮件模板方法创建的电子邮件通知在 CA CA Identity Manager 12.6.4 中仍然有效。

配置 SMTP 设置

在启用电子邮件通知之前，配置 SMTP 设置。 参阅以下部分为您的应用程序服务器配置 SMTP 设置。

在 JBoss 上配置 SMTP 设置

1. 使用以下方法，在文本编辑器中，打开邮件服务部署描述符：

   单个节点：*jboss_home*\server\default\deploy\mail-service.xml

   群集：*jboss_home*\server\all\deploy\mail-service.xml

2. 使用以下方法，修改使用您的 SMTP 服务器名的 mail.smtp.host 属性：

   ```
   <-- Change to the SMTP gateway server -->
   <property name="mail.smtp.host" value="your_smtp_server "/>
   ```

   例如：

   ```
   <property name="mail.smtp.host" value="smtp.mailserver.company.com"/>
   ```

3. 保存 mail-service.xml 文件。

4. 在文本编辑器中，打开以下电子邮件属性文件：

   单个节点：
   jboss_home\server\default\deploy\iam_im.ear\config\com\netegrity\config\email.properties

   群集：
   jboss_home\server\all\farm\iam_im.ear\config\com\netegrity\config\email.properties

5. 要设置工作流生成的电子邮件使用的电子邮件返回地址，找到 admin.email.address 属性，且将值设置为适当的电子邮件地址。 例如：
   `admin.email.address=admin@company.com`

6. 如果使用的是电子邮件模板方法，在管理控制台中启用电子邮件通知。

   如果使用的是电子邮件通知策略，则不需要在管理控制台中启用电子邮件通知。

在 WebLogic 上配置 SMTP 设置

在 WebLogic 服务器管理控制台和 email.properties 文件中，配置电子邮件设置。

为 WebLogic 配置电子邮件设置

1. 在 WebLogic 服务器管理控制台中，使用以下属性创建邮件会话：
   - **mail.smtp.host** 属性：将此值设置为您的 SMTP 服务器。 例如，mail.smtp.host=mymailserver.company.com
   - **mail.transport.protocol** 属性：将此值设置为 SMTP。 例如，mail.transport.protocol=smtp
   - **JNDI 名称**：nete/Mail
   - **目标**：WebLogic 服务器名称

2. 在文本编辑器中，打开 CA CA Identity Manager 的以下电子邮件属性文件：

   weblogic_domain\applications\iam.ear\config\com\netegrity\config\email.properties

3. 通过找到 admin.email.address 属性，并且将值设置为适当的电子邮件地址，来设置工作流生成的电子邮件使用的电子邮件返回地址。 例如：
   `admin.email.address=admin@company.com`

4. 在管理控制台中启用电子邮件通知。

   注意：如果使用的是电子邮件通知策略，则不需要在管理控制台中启用电子邮件通知。

在 WebSphere 上配置 SMTP 设置

在安装 CA CA Identity Manager 组件后运行的 imsSetup 实用工具配置名为 mailMail 的新邮件会话对象。

要使电子邮件通知功能正确工作，在 mailMail 会话的“Mail Transport Host”（电子邮件传输主机）字段中指定发送电子邮件时 WebSphere 连接的服务器。

mailMail 会话位于 WebSphere 管理控制台的“Resources”（资源）-“Mail Providers”（邮件提供程序）-“Built-in Mail Provider”（内置邮件提供程序）-“Mail Sessions”（邮件会话）-“mailMail”。

注意：要查看 mailMail 对象，请在“Mail Session”（邮件会话）屏幕中将“Scope”（作用域）更改为“Server”（服务器）。如果您没有将作用域更改为“Server”（服务器），则不显示 mailMail 对象。

有关配置 WebSphere 邮件提供程序的详细信息，请参阅 WebSphere 文档。

如果您使用的是电子邮件模板方法，在您配置 SMTP 设置之后，在管理控制台中启用电子邮件通知。

注意：如果使用的是电子邮件通知策略，则不需要在管理控制台中启用电子邮件通知。

如何创建电子邮件通知策略

您可以使用用户控制台来创建在某些操作发生时发送电子邮件的电子邮件通知策略。 例如，您可以创建在新用户创建时发送电子邮件通知批准人的电子邮件通知策略。

遵循这些步骤:

1. 依次选择“系统”、“电子邮件”、“创建电子邮件”。
2. 选择下列选项之一：
   - 创建类型为“管理的电子邮件”的新对象
   - 创建类型为“管理的电子邮件”的对象副本

     使用现有电子邮件通知策略作为模板创建策略。
3. 提供“配置文件”选项卡下有关电子邮件通知策略的基本信息。

4. 在“发送时间”选项卡中指定 CA Identity Manager 发送电子邮件的时间。

   “发送时间”选项卡提供几个选项，通过他们您可以指定触发电子邮件通知的操作。

5. 在“收件人”选项卡中指定电子邮件的接收者。
6. 在“内容”选项卡中定义电子邮件的主题和内容。

   您可以指定动态内容，如电子邮件内容的日期、任务或事件名称以及用户属性。

更多信息：

发送时间选项卡 (p. 307)
收件人选项卡 (p. 309)
内容 (p. 310)
电子邮件通知“配置文件”选项卡 (p. 306)

电子邮件通知“配置文件”选项卡

通过电子邮件管理任务的“配置文件”选项卡您可以指定有关电子邮件通知策略的基本信息。 此选项卡包含以下字段：

电子邮件名称

识别用户控制台中的电子邮件通知策略。

注意：在发送电子邮件时，不显示电子邮件名称。 名称仅用于管理用户控制台中的电子邮件通知策略。

类别

将电子邮件通知策略分组便于管理。

通过从下拉列表中选择来指定现有类别，或选择第二个选项按钮并输入新类别的名称。

说明

向管理员说明电子邮件通知策略。

发送电子邮件时，不显示说明。

已启用

指定 CA CA Identity Manager 在满足“发送时间”选项卡中定义的条件时发送电子邮件。

自定义数据

在可用于配置自定义收件人或自定义内容的 Policy Xpress 中创建自定义数据元素。

自定义数据元素也可用作其他数据元素中的参数。

注意：此部分数据 (p. 412)提供有关数据元素的更多信息。

单击“自定义数据”时，CA CA Identity Manager 会打开屏幕，在屏幕中您可以添加新数据元素。

条目规则

在“发送时间”选项卡中的默认规则不精确的情况下，定义 CA CA Identity Manager 发送电子邮件通知时间的规则。

例如，“发送时间”选项卡提供一个默认规则，即在修改用户配置文件的任何属性时发送电子邮件。 如果要 CA CA Identity Manager 仅在用户的部门发生更改时发送电子邮件，则可以创建自定义的条目规则。（在这种情况下，创建识别部门更改时间的自定义数据元素，然后创建使用您所创建的自定义数据元素的条目规则）。

注意：此部分条目规则 (p. 414)提供更多信息。

发送时间选项卡

CA Identity Manager 提供几个发送电子邮件时的默认选项。一些选项需要附加信息，如任务或事件名称。 例如，在任务开始的时候，发送电子邮件需要选择触发电子邮件的任务。

您可以选择一个或多个以下“发送时间”选项：

用户已创建

在已创建用户时发送电子邮件。 在 CreateUserEvent 完成时发送电子邮件。

用户已修改

在已修改用户时发送电子邮件。在 ModifyUserEvent 完成时发送电子邮件。

工作流挂起

在工作流流程分配批准人时发送电子邮件。 选择该选项时，请指定相应的工作流流程。 在选定工作流进程的每一步，使用此策略定义的电子邮件将单个电子邮件发送给批准人。

工作流未决电子邮件

在工作流进程到达指定的活动时，发送电子邮件。 选择该选项时，请指定相应的工作流流程。 使用此策略定义的电子邮件针对每个批准步骤发送单个电子邮件通知。

事件已启动

在事件到达“之前”状态时发送电子邮件。选择该选项时，请指定事件。

注意：如果指定“事件已启动”，且电子邮件无法发送，那么与此通知关联的事件将不会执行。

事件已结束

在事件到达“之后”状态时发送电子邮件。选择该选项时，请指定事件。

事件已批准

在事件到达“已批准”状态时发送电子邮件。选择该选项时，请指定事件。

事件已被拒绝

在事件到达“已拒绝”状态时发送电子邮件。选择该选项时，请指定事件。

事件失败

事件失败时发送电子邮件。 选择该选项时，请指定事件。

任务已提交

任务开始处理时发送电子邮件。 选择该选项时，请指定任务。

任务完成

任务完成时发送电子邮件。 选择该选项时，请指定任务。

任务失败

如果任务失败，发送电子邮件。 选择该选项时，请指定任务。

收件人选项卡

您可以在电子邮件的“收件人”、“抄送”或“密送”字段中配置多个收件人。收件人列表可为静态，或取决于触发电子邮件的操作类型以及涉及的用户。

要指定收件人，请在“收件人”选项卡中选择“收件人”、“抄送”或“密送”字段旁边的编辑图标。 然后，选择下列的选项之一，通过他们您可以配置收件人列表：

工作流批准人

把电子邮件发送给工作流流程中的所有批准人。 该选项仅在针对工作流挂起事件发送电子邮件时适用。

管理者

把电子邮件发送给已经执行任务的用户的管理者。

注意：要使用管理者收件人选项，请针对环境配置管理者属性。 要配置管理者属性，请转到“管理控制台”中的“环境”、*EnvironmentName*、“高级设置”、“杂项”。 将管理者属性设置为物理属性的名称（存储用户管理者的唯一名称）。

对于关系数据库，请使用下列格式指定属性：

tablename.attribute

组成员

将电子邮件发送给组中所有成员。 选择该选项可以打开带有可用组名称的下拉列表。

角色成员

将电子邮件发送给管理角色的所有成员。 选择该选项可以打开带有可用角色名称的下拉列表。

静态地址

将电子邮件发送给选定的电子邮件地址。 您可以在其他可用文本区域内指定电子邮件地址。

注意：不要在文本区域内指定一个以上的地址。

用户

将电子邮件发送给已执行任务的用户。

请求的发起者

将电子邮件发送给提出请求的人。

自定义

允许您选择定义接收人的自定义数据元素。

在选择自定义选项时，下拉列表出现并带有可用的自定义数据元素。

注意：此部分数据 (p. 412)提供有关数据元素的更多信息。

内容

您可以使用简单文本定义电子邮件的主题和正文，或使用在发送电子邮件时计算出的动态内容添加。

主题行是纯文本字段，在此您可以写消息。 该消息是电子邮件的主题。

正文显示在 HTML 编辑器中。 您可以插入和格式化任何文本来组成电子邮件正文。

要包括动态内容，请从下拉列表中选择选项。 编辑器添加光标所在的动态内容指示器，如下所示：

{*type*}

type 表示所支持的动态内容类型之一。

例如，在您选择属性动态内容类型并指定 FirstName 属性时，HTML 编辑器在“内容”选项卡中显示以下内容：

{'Attribute: FirstName'}

注意：要将动态内容添加到主题行中，请使用主题行下的下拉列表。 要将动态内容添加到电子邮件正文，请使用内容框下的下拉列表。

在发送电子邮件消息时，CA CA Identity Manager 会使用适当文本替换动态内容。文本保留 HTML 编辑器中指定的格式，如粗体字符。

动态内容类型包括以下内容：

日期

采用您指定的格式指定今天的日期。

任务

指定发送电子邮件的任务。

对象名称

指定触发电子邮件事件中的对象名称。 如果事件是用户事件，该字段则是用户登录名。

对象可能是除用户之外的内容。 例如，它可能是任何管理对象如组、管理角色等。

属性

指定用户属性之一的值。 用户是任务的主题。 该选项需要从下拉列表中选择属性。

管理者属性

指定用户管理者的属性之一的值。 用户是任务的主题。 该选项需要从下拉列表中选择属性。

注意：要使用管理者收件人选项，请针对环境配置管理者属性。 要配置管理者属性，请转到“管理控制台”中的“环境”、*EnvironmentName*、“高级设置”、“杂项”。 将管理者属性设置为物理属性的名称（存储用户管理者的唯一名称）。

对于关系数据库，请使用下列格式指定属性：

tablename.attribute

自定义

允许您选择定义接收人的自定义数据元素。

在选择自定义选项时，下拉列表出现并带有可用的自定义数据元素。

注意：此部分数据 (p. 412)提供有关数据元素的更多信息。

修改电子邮件通知策略

修改现有电子邮件通知策略来满足您的业务要求。

修改电子邮件通知策略

1. 依次选择“系统”、“电子邮件”、“创建电子邮件”。

   CA Identity Manager 将显示搜索屏幕。

2. 搜索并选择要修改的电子邮件通知策略。
3. 需要时更改“配置文件”中的设置，如“发送时间”、“收件人”以及“内容”选项卡。

禁用电子邮件通知策略

通过使用“配置文件”选项卡中的“已启用”复选框，在创建或修改电子邮件通知策略时，您可以启用或禁用电子邮件通知策略。 在禁用电子邮件通知策略时，选定的电子邮件为不活动状态且不发送任何电子邮件。

注意：默认情况下，电子邮件通知策略为启用状态。

使用案例：发送欢迎电子邮件

雇用新员工时，Forward 公司想给新员工发封欢迎他们到公司的邮件。 电子邮件必须为新员工提供重要信息（如员工主页的链接）以及有关其经理和部门的信息。

要创建电子邮件，人力资源管理员使用用户控制台中的“创建电子邮件”配置以下设置：

- 在“发送时间”选项卡上，选择“用户已创建”。
- 在“收件人”选项卡上，完成下列步骤：
  - 单击“收件人”字段旁边的编辑图标。

    选择“用户”，然后单击加号。 使用同样的方法选择“管理者”，然后单击“确定”。
  - 单击“抄送”字段旁边的编辑图标。

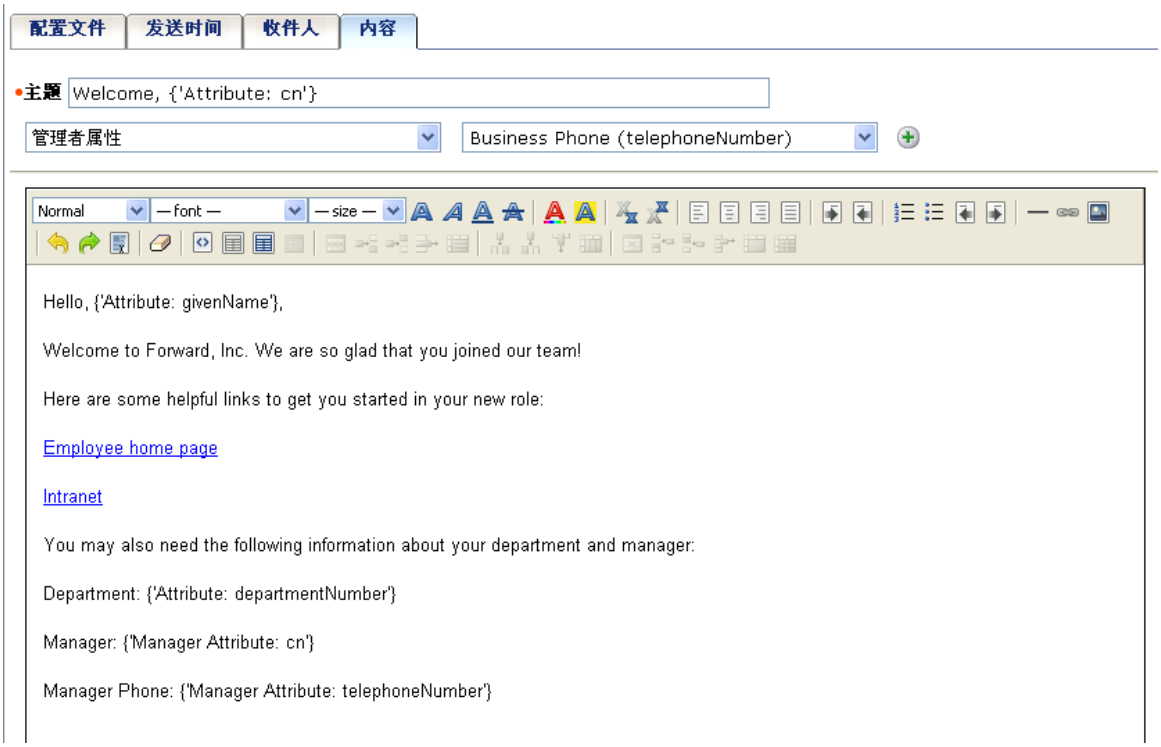
    选择“发起者”，单击加号，然后单击“确定”将电子邮件的副本发送给在 CA CA Identity Manager 中创建员工的用户。
- 在“内容”选项卡上，完成下列步骤：
  - 在“主题”字段中，输入以下文本：欢迎

    用光标在输入文本的结尾处，从下拉列表中选择“属性”。 然后，从第二个下拉列表中选择“全名”，然后单击加号。

    主题行类似以下内容：

    欢迎，{'Attribute: eTFullName'}

    注意：属性名称取决于用户存储以及正在使用的属性。
  - 在“内容”框中，添加任何欢迎的文本。 包括员工门户的链接，并使用内容框下的动态内容选项来显示用户的部门、经理和经理的电话号码，如下所示：



如何使用电子邮件模板

CA Identity Manager 包括您可以用来生成电子邮件消息的默认电子邮件模板。您可以依安装时的原样使用这些默认模板，也可以根据自己的业务需求对其进行自定义。

使用电子邮件模板

1. 配置 SMTP 设置以启用 CA Identity Manager 发送电子邮件通知。
2. 在管理控制台中启用电子邮件通知 (p. 314)。
3. 配置事件或任务以发送电子邮件。 (p. 314)
4. （可选）根据需要自定义默认模板 (p. 318)。

启用电子邮件通知

您可以为 CA Identity Manager 环境启用或禁用电子邮件通知。 如果您启用了电子邮件通知，CA CA Identity Manager 会针对指定的事件和任务发送电子邮件通知。

注意：要使用“忘记密码”功能，请启用电子邮件通知。\

在 CA CA Identity Manager 中启用电子邮件通知之前，请先为应用程序服务器配置 SMTP 设置 (p. 303)。

启用电子邮件通知

1. 在管理控制台中单击“Environments”（环境）。

   此时显示 CA Identity Manager 环境列表。
2. 单击恰当的 Identity Manager 环境。
3. 依次转到“Advanced Settings”（高级设置）、“Email”（电子邮件）。
4. 选择“Enabled”（已启用）复选框。
5. 配置触发电子邮件的事件和任务 (p. 314)。
6. 单击“Save”（保存）。
7. 重新启动安装了 CA CA Identity Manager 的应用程序服务器实例。

配置事件或任务以发送电子邮件

如果启用了电子邮件通知，您可以指定一个触发电子邮件通知的事件和任务的列表。 例如，您可能想要在以下情形下发送电子邮件：

- 通知系统管理员已完成“重置用户密码”任务。
- 通知新员工的管理员已完成“创建用户”任务。此外，当“创建用户”任务内生成的 AddToGroupEvent 获批时，会有另外一封电子邮件发送给添加了新用户的组的所有成员。

指定触发电子邮件通知的事件和任务

1. 在管理控制台中单击“Environments”（环境）。

   此时显示 CA Identity Manager 环境列表。
2. 单击适用的 CA Identity Manager 环境。
3. 依次转到“Advanced Settings”（高级设置）、“Email”（电子邮件）。

   此时将打开“Email Properties”（电子邮件属性）屏幕。

4. 选择以下要应用的“Enable”（启用）复选框：
   - “Events E-mail Enabled”（启用事件电子邮件）

     为 CA Identity Manager 事件启用电子邮件通知
   - “Tasks Email Enabled”（启用任务电子邮件）

     为 CA Identity Manager 任务启用电子邮件通知
5. 输入 CA CA Identity Manager 用来创建电子邮件消息的电子邮件模板的位置。

   电子邮件模板位于以下位置的子目录：

   iam_im.ear\custom\emailTemplates

   注意：要使用其他语言作为文件名来创建电子邮件模板文件，请在支持该语言字符集的操作系统会话中进行操作。
6. 指定要为其发送电子邮件通知的事件，方法如下：
   - 要添加一个事件，请在“Event”（事件）列表框中选择该事件，然后单击“Add”（添加）。

     CA CA Identity Manager 将选中的事件添加到为其发送电子邮件通知的事件列表。

     注意：如果您选择不与工作流进程相关联的事件，CA CA Identity Manager 会在事件完成时发送电子邮件通知。
   - 要删除事件，请选中事件的复选框，然后单击“Delete”（删除）。
7. 指定要为其发送电子邮件通知的任务，方法如下：
   - 要添加任务，请在第一个字段中选择条件，并在第二个字段中输入任务名称以搜索该任务。 单击“Search”（搜索）。

     通过使用通配符 (*) 字符，您可以仅输入一部分任务名称。 例如，要搜索某个“Create”（创建）任务，请输入“Create*”（创建*）。

     从搜索结果中选择一项或多项任务。 单击“Add”（添加）。

     注意：操作类型为“查看”或“自行查看”的任务不能使用任务级别的电子邮件通知。 要查看任务的操作类型，请依次转到“修改管理任务”、“选择任务”，然后在任务配置文件中查看“操作”字段。
   - 要删除任务，请选中任务的复选框，然后单击“Delete”（删除）。

     删除任务操作将从“任务”表中删除任务。 此操作不会实际删除任务。
8. 完成对触发电子邮件通知的任务和事件的配置后，单击“Save”（保存）。
9. 重新启动安装了 CA CA Identity Manager 的应用程序服务器。

电子邮件内容

电子邮件通知包含一个通用模板以及通过电子邮件 API 添加到电子邮件的特定于任务的详细信息。 例如，针对“创建用户”任务，可以在电子邮件中插入下列信息：

- 正在执行此任务的管理员名称
- 新用户的名称
- 用户的电子邮件地址、部门名称和其他属性数据
- 即将创建的用户所属的组织
- 工作流审批状态和审批时间
- 任务的名称和任务中事件的名称

电子邮件模板

电子邮件通知通过电子邮件模板来生成。 Identity Manager 提供默认的电子邮件模板，您可以将其作为已安装的模板直接使用，或用它来创建自己的电子邮件模板。

每个电子邮件模板都包含以下信息：

- **递送信息**－电子邮件收件人的列表。 Identity Manager 根据任务中涉及到的用户，自动生成收件人列表。 例如，审批电子邮件会发送给任务的所有审批者。
- **主题**－消息主题行中的文本。
- **内容**－消息正文。 正文通常包含静态文本和变量，Identity Manager 可根据触发电子邮件的任务或事件来解析这些内容。

默认电子邮件模板位于同样也安装了 Identity Manager 管理工具的 emailTemplates 目录中。 管理工具的默认安装位置是：

- 对于 Windows 系统－C:\Program Files\CA\CA Identity Manager\
- 对于 UNIX 系统－<home_directory>/CA/CA Identity Manager

emailTemplates 目录包含四个文件夹。 每个文件夹都与一个任务或事件状态相关联：

目录	内容
Approved	defaultEvent.tmpl－通知收件人事件已审批

目录	内容
Completed	■ CertificationNonCertifiedActionCompletedNotification.tmpl－通知管理员，已对员工应用了不合规定的操作。 ■ CertificationNonCertifiedActionPendingNotification.tmpl－通知管理员，将对员工应用不合规定的操作。 ■ CertificationRequiredFinalNotification.tmpl－对管理员的最终提醒：必须对员工完成“认证用户”任务。 ■ CertificationRequiredNotification.tmpl－通知管理员已开始对员工进行认证处理。 管理员必须完成对此员工的“认证用户”任务。 ■ CertificationRequiredReminderNotification.tmpl－提醒管理员必须完成对员工的“认证用户”任务。 ■ Certify Employee.tmpl－通知管理员已完成对员工的认证处理。 ■ CreateProvisioningUserNotificationEvent.tmpl－在配置目录中创建用户的帐户后，将临时密码发送给该用户。 ■ defaultTask.tmpl－通知收件人 Identity Manager 已完成某项任务。 ■ ForgottenPassword.tmpl－将临时密码发送给使用了“忘记密码”功能的用户。 ■ ForgottenUserID.tmpl－将用户 ID 发送给使用了“忘记用户 ID”功能的用户。 ■ Self Registration.tmpl－通知用户已成功完成“自行注册”任务。
Pending	■ defaultEvent.tmpl－通知审批者，工作列表中所列的项目需要予以注意 ■ ModifyUserEvent.tmpl－与默认模板相同，但包含用于检索“用户”管理对象属性的方法
Rejected	defaultEvent.tmpl－通知收件人事件已被拒绝

使用 安装在 *<im_admin_tools_dir>*\Identity Manager\emailTemplates 中的 Identity Manager 模板和模板目录结构为基础，创建自定义的电子邮件模板。

模板目录

“电子邮件模板” (p. 316)中所述的每个模板目录都与特定的任务或事件状态相关联。 例如，如果要为在工作流进程中已被拒绝的事件发送电子邮件，则 Identity Manager 会在部署的“rejected”目录中查找可供使用的模板。Identity Manager 接着会使用该目录中恰当的电子邮件模板来生成电子邮件。

目录中的电子邮件模板

每个部署的模板目录包含一个或多个电子邮件模板。 当为其启用了电子邮件的任务或事件发生时，Identity Manager 将在恰当的模板目录中搜索与任务或事件同名的模板。 如果无法找到此模板，Identity Manager 将使用该目录中的默认模板。 默认模板名列在“电子邮件模板” (p. 316)中。 例如，Identity Manager 可使用 Pending 目录中的 defaultEvent.tmpl，通知审批者存在新的工作列表项。

模板目录集合

模板目录集合包含“approved”、“completed”、“pending”和“rejected”目录。 您可以部署多个模板目录集合，并且为给定的 Identity Manager 环境指定其中一个集合。

“电子邮件模板部署” (p. 335)提供有关部署模板目录集合的信息。

有关配置电子邮件模板目录，以便 Identity Manager 能将恰当的集合应用于给定环境的信息，请参阅 *《CA Identity Manager 配置指南》*。

创建电子邮件模板

创建自定义电子邮件消息

1. 打开您要修改的模板。

   例如，如果您要为未决的“创建用户”事件创建电子邮件消息，请在 Pending 目录中打开 defaultEvent.tmpl。

2. 使用新的文件名将此模板保存在同一目录中。 此名称必须与对其应用了电子邮件的事件名称相匹配，并且以 .tmpl 作为扩展名。

   例如，将与未决的“创建用户”事件对应的消息命名为：

   CreateUserEvent.tmpl

   请参阅“Identity Manager 事件”以获取事件的列表。

   注意：要使用其他语言作为文件名来创建电子邮件模板文件，请在支持该语言字符集的操作系统会话中进行操作。

3. 按照下一部分“自定义电子邮件模板” (p. 319)中所述，按需修改消息模板。

自定义电子邮件模板

电子邮件模板是一个支持 HTML 和嵌入式服务器端 JavaScript 的动态文件。模板使您能够将变量值插入到静态文本，允许您根据单个模板生成特定情形的消息。

可使用同一模板打印静态文本样本（如已审批的短语）以及与给定上下文相关的可变文本（如正在审批的事件的名称），并且其使用次数不受限制。

例如，以下是一个用于报告事件审批的模板：

```
<!-- Define the E-mail Properties --->
<%
   _to = _util.getNotifiers("ADMIN");
   _cc = "" ;
   _bcc = "";
   _subject = _eventContextInformation.getEventName() + " approved";
%>
<!--- Start of Body --->
<html>
<body text="Navy">

Event: <b> <%=_eventContextInformation.getEventName()%> </b><br>
<%=_eventContextInformation.getPrimaryObjectTypeName()%>:
<b><%=_eventContextInformation.getPrimaryObjectName()%></b><br>
In <%=_eventContextInformation.getSecondaryObjectTypeName()%>:
<b><%=_eventContextInformation.getSecondaryObjectName()%></b><br>
Status: <b>Approved</b>
</body>
</html>
```

注意：以上示例中用到的 Identity Manager 对象 _util 和 _eventContextInformation 将在“电子邮件模板 API”中说明。

假设针对事件 CreateUesrEvent 生成了一项审批，并且在组织 HR 中创建了用户 John Jones，那么根据审批模板生成的电子邮件通知的正本大概如下：

Event: **CreateUserEvent**
USER: **John Jones**
In ORGANIZATION: **HR**
Status: **Approved**

以下部分阐述了用于生成动态电子邮件消息的语法和 Identity Manager 对象。

模板元素

Identity Manager 电子邮件模板支持：

- 标准 HTML 标记。
- 服务器端 JavaScript。
- Identity Manager 可用于模板实例（即电子邮件消息）的一个或多个隐式对象。
- Identity Manager 标记，这些标记使您能够在模板中嵌入 JavaScript，调用隐式的 Identity Manager 对象中的方法，以及在模板的静态文本中插入变量。

Identity Manager 标记扩展

电子邮件模板支持以下标记：

<% %>

在电子邮件模板中嵌入 JavaScript。

<%= %>

在静态文本中插入变量值。

这些标记将在下一部分中说明。

<% %>

此标记使您能够将并列执行的 JavaScript 嵌入到电子邮件模板。

您可以在嵌入的 JavaScript 中使用任何 JavaScript 对象。 您也可以在嵌入的 JavaScript 中调用 Identity Manager 隐式对象方法。

例如，下列代码对“自定义电子邮件模板” (p. 319)中所示的审批模板正文作出了修改。 JavaScript 可用于判断事件是否涉及到次要对象（如添加用户主要对象后产生的组织对象）。 如果没有次要对象，与次要对象相关的文本将从消息中删除：

```
Event: <b> <%=_eventContextInformation.getEventName()%> </b><br>
<%=_eventContextInformation.getPrimaryObjectTypeName()%>:
<b><%=_eventContextInformation.getPrimaryObjectName()%></b><br>
<%
var secondaryType
=       _eventContextInformation.getSecondaryObjectTypeName();
if (secondaryType != "") {
   template.add("In " + secondaryType + ": ");
   template.add("<b> "+_eventContextInformation.getSecondary
                                    ObjectName()+" </b><br>");
   }
%>
Status: <b>Approved</b>
```

<%= %>

此标记使您能够将变量值插入静态文本。 值可以是：

- 由模板中之前执行的 JavaScript 定义的变量，例如：

```
<%
var secondaryType
=      _eventContextInformation.getSecondaryObjectTypeName();
...           // More JavaScript processing
%>
...           // More HTML
The primary object was created in <%=secondaryType%>.
```

- 由 Identity Manager 隐式对象中的方法返回的值，例如：

```
Event <%=_eventContextInformation.getEventName()%> is approved.
```

电子邮件模板 API

当使用模板来生成消息时，Identity Manager 提供以下可在消息中使用的隐式对象。 这些对象使您能够通过调用电子邮件模板 API 中的方法，将实例特定的信息插入消息。

模板可以调用以下所有对象的方法：

- _contentType。 指定电子邮件的 contentType。
- _priority。 指定电子邮件的优先级。
- _to。 将收件人添加到消息的“To”（收件人）字段。
- _cc。 将收件人添加到消息的“cc”（抄送到）字段中。
- _bcc。 将收件人添加到消息的“bcc”（密送到）字段中。
- _subject。 指定电子邮件的主题。
- _encoding。 指定电子邮件的编码。
- template。 允许您将表示多行 JavaScript 代码的文本串添加到消息中。
- _util。 实用工具对象。
- _eventContextInformation。 包含与当前任务生成的事件相关的信息，如事件名和审批状态。
- _taskContextInformation。包含一系列与当前任务相关的信息，如任务名称、组织名称和组成事件。

这些对象将在下一部分中说明。

_contentType

指定电子邮件的 contentType。

如果没有通过变量 _contentType 指定 contentType，则使用默认的 contentType“text/html”。

方法：无。

示例：

```
<% _contentType = "text/html"; %>
```

_priority

指定电子邮件的优先级。 指定 0 为没有优先级（默认），1 为重要优先级。

方法：无。

示例：

```
<% _priority = "1"; %>
```

_to

将收件人添加到消息的“To”（收件人）字段。

_to 变量的值是 JavaScript 字符串。 允许存在多个收件人，但是字符串必须符合 JavaScript 语法，如下列示例所示。

方法：无。

示例：

```
<%
_to =
_util.getNotifiers("USER") + ',' +
_util.getNotifiers("USER_MANAGER","ManagerLookup=managerattribute");
_cc = "" ;
_bcc = "" ;
_subject = "Your new password ";
%>
```

注意：如果电子邮件警告参与人任务处于未决状态且由工作流控制，则会使用参与人的地址预先填充 _to 对象。 您不得在未决模板中使用 _to 对象。

_cc

将收件人添加到消息的“cc”（抄送到）字段中。

_to 变量的值是 JavaScript 字符串。 允许存在多个收件人，但是字符串必须符合 JavaScript 语法，如下列示例所示。

方法：无。

示例：

```
<%
_cc =
_util.getNotifiers("USER") + ',' +
_util.getNotifiers("USER_MANAGER","ManagerLookup=managerattribute");
%>
```

_bcc

将收件人添加到消息的“bcc”（密送到）字段中。

此字段指定的电子邮件地址不在电子邮件中显示。

_to 变量的值是 JavaScript 字符串。 允许存在多个收件人，但是字符串必须符合 JavaScript 语法，如下列示例所示。

方法：无。

示例：

```
<%
_bcc =
_util.getNotifiers("USER") + ',' +
_util.getNotifiers("USER_MANAGER","ManagerLookup=managerattribute");
%>
```

_subject

指定电子邮件的主题。

方法：无。

示例：

```
<% _subject=_eventContextInformation.getEventName()+" approved";%>
```

_encoding

指定电子邮件的编码。

如果没有通过 _encoding 或 LANG 变量指定编码，可能无法正确显示电子邮件中的字符。 确保将 _encoding 或 LANG 设置为适当的区域。

方法：无。

示例：

```
<% _encoding = "UTF-8"; %>
```

_additionalHeaders

_additionalHeaders

在电子邮件模板中指定额外电子邮件标题属性。

您必须将 HashMap() 分配给此属性。 存储在 HashMap 中的名称和值必须是字符串。

示例：添加自定义标题属性

以下示例显示如何添加两个自定义标题属性，即“X-TCCCSWD”和“myheader”：

```
<!-- Define the E-mail Properties --->
<%
_to = "siteadmin@ca.com";
_cc = "" ;
_bcc = "" ;
_subject = _eventContextInformation.getEventName() +" completed";
var additionalHeaders = new java.util.HashMap();
additionalHeaders.put("header_a","1");
additionalHeaders.put("header_b","foo");
_additionalHeaders = additionalHeaders;
%>
```

template

允许您通过几行 JavaScript 代码（指 <% %> 标记之内的行）将文本字符串添加到消息中。 字符串可以包含 Identity Manager 隐含对象中的方法返回的 HTML 标记、静态文本和/或变量值。

注意：模板对象不以下划线 (_) 字符开始。

方法：

- add(String)

  参数求值必须为字符串，包括对 Identity Manager 隐含对象中的方法的任何调用。 在下面的示例中，请参阅 _eventContextInformation.getSecondaryObjectName()。

示例：

```
<%
var secondaryType
=       _eventContextInformation.getSecondaryObjectTypeName();
if (secondaryType != "") {
   template.add("In " + secondaryType + ": ");
   template.add("<b> "+_eventContextInformation.getSecondary
                                    ObjectName()+" </b><br>");
   }
%>
```

_util

实用工具对象。

方法：

- getNotifiers(String [,String])

  基于通知规则返回电子邮件 ID。

  第一个参数支持以下预定义的通知规则（括在引号中）：

  - “ADMIN”。 将电子邮件发送给启动任务的管理员。
  - “USER”。 将电子邮件发送到当前上下文的用户。
  - “USER_MANAGER”。 将电子邮件发送到当前上下文的用户的管理员。

  您也能引用使用通知规则 API 创建的自定义通知规则。 有关信息，请参阅 *《Programming Guide for Java》*。

  第二个参数是可选的。 您可以使用它来将一个或多个用户定义的名称/值对传递到自定义通知规则中。 使用逗号分开每个名称/值对，格式如下：
  `"name1=value1,name2=value2,..."`

示例：

```
<%
_to = _util.getNotifiers("ADMIN");
_cc = "";
%>
<%
_to = _util.getNotifiers("MYRULE","type=loan,district=3");
_cc = "";
%>
```

通知用户的管理员

您可以使用 USER_MANAGER 通知规则来向任何用户的管理员发送电子邮件。Identity Manager 在支持用户授权认证的电子邮件模板中使用此规则。

注意：USER_MANAGER 通知规则仅仅适用于创建或管理单一用户的事件或任务。

因为在用户目录中有多种不同方法可以指定用户－管理员关系，默认用户管理者通知适配器通过在 getNotifiers() 方法的第二个参数中指定一个属性表达式解析此关系。

示例：

```
<%
_to = _util.getNotifiers("USER_MANAGER","ManagerLookup=managerattribute");
_cc = "";
%>
```

用户管理者通知适配器支持两个查找选项：

- managerattribute = <*Manager AttributeName*>－其中用户对象保留表示该用户的管理员的 DN 或 UserID 的属性
- commonattribute = <*AttributeName*>－其中用户和用户的管理员共享通用属性值，如“department”

在 Identity Manager 管理控制台环境的“Miscellaneous Properties”（杂项属性）中，可以配置这些查找选项。

要配置 USER_MANAGER 通知规则，请按以下步骤操作：

1. 在 Identity Manager 管理控制台中，选择“Identity Manager Environments”（Identity Manager 环境）。 然后，选择您要配置电子邮件通知的环境。
2. 依次选择“Advanced Settings”（高级设置）、“Miscellaneous Properties”（杂项属性）。

3. 在“Miscellaneous Properties”（杂项属性）页面中，完成希望使用的查找选项的配置步骤：
   - 要使用 managerattribute=<Manager AttributeName> 查找选项：
     a. 在“Property”（属性）字段中，输入“managerattribute”。
     b. 在“Value”（值）字段中，输入存储管理员 DN 或用户 ID 的属性。
     c. 单击“Add”（添加）。
     d. 单击“Save”（保存）。
   - 要使用 commonattribute=<AttributeName> 查找选项：
     a. 在“Property”（属性）字段中，输入“commonattribute”。
     b. 在“Value”（值）字段中，输入用户和用户管理员共有的属性。
     c. 单击“Add”（添加）。
     d. 在“Property”（属性）字段中，输入：ismanagerfilter。
     e. 在“Value”（值）字段中，使用下列语法输入搜索表达式：

        <attribute> <operator> <filter>

        例如，标题 EQUALS 管理员
     f. 单击“Add”（添加）。
     g. 单击“Save”（保存）。

您也可以编写自定义适配器，并且创建自己的用户管理员通知规则。 请参阅《*Programming Guide for Java*》。

_eventContextInformation

包含与当前任务生成的事件相关的信息，如事件名和审批状态。 此信息叫做事件的*上下文*信息。

_eventContextInformation 对象是通过包 com.netegrity.imapi 的 ExposedEventContextInformation 类创建的。

此对象可用于已批准、未决和已拒绝模板的电子邮件。 有关这些模板的信息，请参阅“电子邮件模板” (p. 316)。

方法：以下所有方法都返回一个字符串。

方法	说明
getAdminName()	返回提交生成事件的任务的人的名称。 在 CA CA Identity Manager 5.6 中启用。 使用下列继承的方法之一： ■ getAdministrator() ■ getAdminFriendlyName()
getApprovalStatus()	返回事件的批准状态。这些值之一： APPROVAL_STATUS_APPROVED APPROVAL_STATUS_REJECTED
getApprovalTime()	返回事件被批准的时间。
getEventName()	返回事件的名称。 有关事件名的列表，请参阅“CA Identity Manager 事件”。
getOrgName()	返回任务正在执行的组织的友好名称。 在 CA CA Identity Manager 5.6 中启用。 使用继承的方法 getObjectOrganizationFriendlyName()。
getPassword()	如果主要对象是类型 USER，返回该用户的密码。
getPrimaryObjectTypeName()	返回主要对象的类型。 返回的主要对象类型： ACCESSROLE ACCESSTASK ADMINROLE ADMINTASK GROUP ORGANIZATION USER

方法	说明
getPrimaryObjectName()	返回受事件影响的主要对象的名称。 *主要对象*是直接受事件影响的对象。如果有的话，*次要对象*是主要对象绑定的对象。 例如： ■ CreateUserEvent 的主要对象类型是 USER。 次要对象是创建该用户的对象－也就是 ORGANIZATION。 ■ CreateAdminRoleEvent 的主要对象类型是 ADMINROLE。 此对象没有绑定到其他对象，因此不存在次要对象。 如果主要对象的类型是 USER，getPrimaryObjectName() 可能返回 John Jones。
getSecondaryObjectTypeName()	如果次要对象受到事件的影响，返回对象类型。 返回的次要对象类型： ACCESSROLE ACCESSTASK ADMINROLE ADMINTASK GROUP ORGANIZATION USER
getSecondaryObjectName()	如果次要对象受到事件的影响，返回该对象名。 有关主要和次要对象的详细信息，请参阅 getPrimaryObjectName()。 如果次要对象的类型为 ORGANIZATION， 方法 getSecondaryObjectName() 可能返回 HR。

注意： _eventContextInformation 中的方法是通过接口 ExposedEventContextInformation 提供的。 因为 ExposedEventContextInformation 继承了核心 CA CA Identity Manager API 中的方法，_eventContextInformation 也能调用来自电子邮件模板的这些方法以及上面的表中的方法。 有关这些继承的方法的详细信息，请参阅"其他方法" (p. 333)。

示例一关于未决事件的电子邮件通知：

```
<%
_cc = "" ;
_bcc = "";
_subject = _eventContextInformation.getEventName() +
                                                " Approval Request";
%>
<!--- Start of Body --->
<html>
<body text="Navy">

The following item has been added to your work list for approval:
<br><br><br>
Event: <b><%=_eventContextInformation.getEventName()%></b> <br>
<%=_eventContextInformation.getPrimaryObjectTypeName()%>:
<b><%=_eventContextInformation.getPrimaryObjectName()%></b><br>
In <%=_eventContextInformation.getSecondaryObjectTypeName()%>:
<b><%=_eventContextInformation.getSecondaryObjectName()%></b><br>
</body>
</html>
```

可能的电子邮件正文：

From: lsmith@security.com [mailto:lsmith@security.com]
To: vimperioso@security.com
Subject: CreateUserEvent Approval Request

The following item has been added to your work list for approval:

Event: **CreateUserEvent**
USER: **Richard Ferrigamo**
In ORGANIZATION: **Mortgages & Loans**

注意：“From”字段的值是从 email.properties 文件获得的。 要更改值，请编辑以下文件：

<*iam_im.ear*>\config\com\netegrity\config\email.properties

其中，<*iam_im.ear*> 是应用程序服务器域的 CA CA Identity Manager 的安装位置，例如：

对于 WebLogic：

<*WebLogic_home*>\user_projects\<domain>\applications\iam_im.ear

对于 JBoss：

<*Identity Manager_home*>\jboss-3.2.2\server\default\deploy\iam_im.ear

对于 WebSphere：

<*im_admin_tools_dir* >\WebSphere-ear\iam_im.ear

要将受该事件影响的用户的附加信息添加到前一个示例的电子邮件中，请添加类似以下内容的文本：

```
<% user = _eventContextInformation.getEvent().getUser(); %>
<b>User information:</b><br>
Last Name: <b><%=user.getAttribute("%LAST_NAME%")%></b><br>
First Name: <b><%=user.getAttribute("%FIRST_NAME%")%></b><br>
Full Name: <b><%=user.getAttribute("%FULL_NAME%")%></b><br>
Email: <b><%=user.getAttribute("%EMAIL%")%></b><br>
Organization Membership: <b><%=user.getAttribute("%ORG_MEMBERSHIP%")%></b><br>
```

可能的电子邮件正文：

From: lsmith@security.com [mailto:lsmith@security.com]
To: vimperioso@security.com
Subject: CreateUserEvent Approval Request

The following item has been added to your work list for approval:

Event: **CreateUserEvent**
USER: **Richard Ferrigamo**
In ORGANIZATION: **Mortgages & Loans**
User information:
Last Name: Ferrigamo
First Name: Richard
Full Name: Richard Ferrigamo
Email: rferrigamo@mybank.org
Organization Membership: **Mortgages & Loans**

_taskContextInformation

包含一系列与当前任务相关的信息，如任务名称、组织名称和组成事件。 此信息称为任务的*上下文*信息。

此对象适用于根据已完成模板创建电子邮件消息。 有关此模板的信息，请参阅“电子邮件模板” (p. 316)。

方法：所有下列方法都会返回一个字符串，除了返回 Java Vector 的方法 getExposedEventContexts() 之外。

方法	说明
getAdminName()	返回提交任务的人的名称。 在 Identity Manager 5.6 中弃用。 使用下列继承的方法之一： ■ getAdministrator() ■ getAdminFriendlyName()

方法	说明
getExposedEventContexts()	返回与该任务有关的所有事件的 Java Vector。 Vector 中的每个对象是事件的上下文对象。 您可以使用在 _eventContextInformation 中列出的方法来检索给定事件对象的上下文信息。 返回对象是标准 Java Vector 对象。 您可以使用任何 Vector 对象的方法（例如 get() 和 size()）管理 Vector 中的元素。
getOrgName()	返回正在执行任务的组织的名称。 在 Identity Manager 5.6 中弃用。 使用继承的方法 getObjectOrganizationFriendlyName()。
getTaskName()	返回被执行的任务的名称。 在 Identity Manager 5.6 中弃用。 使用下列继承的方法之一： ■ getAdminTask() ■ getTaskFriendlyName()

注意：_taskContextInformation 中的方法是通过接口 ExposedTaskContextInformation 提供的。 因为 ExposedTaskContextInformation 继承了核心 Identity Manager API 中的方法，_taskContextInformation 也能调用来自电子邮件模板的这些方法以及上面的表中的方法。 有关这些继承的方法的详细信息，请参阅"其他方法" (p. 333)。

示例－针对密码更改的电子邮件通知模板的正文：

```
<%
var imsEventContexts
=              _taskContextInformation.getExposedEventContexts();
if(imsEventContexts != null)
   {
   for(var i=0;i<imsEventContexts.size();i++)
      {
      var eventContext = imsEventContexts.get(i);
      template.add("Hi "+
eventContext.getPrimaryObjectName()
                + ",");
      template.add("<br>Your new password is: <b>"+
                              eventContext.getPassword());</br>
      template.add("<hr>");
      }
   }
%>
```

可能的电子邮件正文：

Hi Victor Imperioso,
Your new password is: LFH7F1226

其他方法

_taskContextInformation 和 _eventContextInformation 中的方法是通过 Identity Manager 对象 ExposedTaskContextInformation 和 ExposedEventContextInformation 分别提供的。

这些对象继承核心 Identity Manager API 中的方法。 因此，继承的方法也可以用于 _taskContextInformation 和 _eventContextInformation。

从 TaskInfo 对象继承的下列方法对电子邮件模板特别有用：

- getAdministrator()。 为正在执行当前任务的管理员检索用户对象。
- getAdminTask()。 为当前任务检索 AdminTask 对象。

这些检索的对象允许您将针对管理员和针对任务的信息插入电子邮件。 例如：

```
<!-- Define the E-mail Properties --->

<%
   _cc = "" ;
   _bcc = "" ;
   _subject = _eventContextInformation.getEventName() +
                                                 " Approval Request";
%>
<!--- Start of Body --->
<html>
<body text="Navy">

The following item has been added to your work list for approval:<br>
<br>
User <b><%= _eventContextInformation.getAdministrator().
               getAttribute(Packages.com.netegrity.llsdk6.imsapi.
                managedobject.User.PROPERTY_FRIENDLY_NAME)%> </b>
               from department <b><%= _eventContextInformation.
               getAdministrator().getOrg(null).getFriendlyName()
               %></b> initiated task <b><%= _eventContextInformation.
               getAdminTask().getFriendlyName() %></b>at
<b><%=                 _eventContextInformation.getSessionCreateTime() %></b>
<br><br>
<font color="green">Details: </font><b><%=_eventContextInformation.
                                          getEventName()%></b><br>
<font color="green"><%=_eventContextInformation.
                               getPrimaryObjectTypeName()%>:</font>
<b><%=_eventContextInformation.getPrimaryObjectName()%></b>
                                                    was modified
<br>
```

```
<font color="green">Updated Attributes:</font>
<table border="1">
<tr>
<td><b>Name</b></td>
<td><b>Value</b></td>
</tr>
<%
   var event = _eventContextInformation.getEvent();
   if(event instanceof Packages.com.netegrity.imapi.UserEvent) {
      var user = event.getUser();
      var attributes = user.getAttributes().keys();
      while(attributes.hasMoreElements()) {
         var attr = attributes.nextElement();
         var value = user.getAttribute(attr);
         if(user.hasAttributeChanged(attr)) {
            template.add("<tr><td>" + attr +"</td>");
            template.add("<td>" + value +"</td></tr>");
         }
      }
   }
%>
</table>
<br>
</body>
</html>
```

可能的电子邮件正文：

The following item has been added to your work list for approval:

User **Robert Jenkins** from department **HR** initiated task **Modify User** at **3:17 pm**

Details: **ModifyUserEvent**
User: **John Jones** was modified
Updated Attributes:

Name	Value
email	jjones@mycorp.com
phone	781 555 1234

有关电子邮件模板 API 可用的继承的方法的详细信息，请参阅“Identity Manager Javadoc”中的 ExposedTaskContextInformation 和 ExposedEventContextInformation 对象。

Java 标准输出流

电子邮件消息也能从在 JavaScript 标记 (<% %>) 中调用 Java 标准输出流。例如，下面的调用会将消息“Done”发送到服务器控制台：

```
<%
...       // JavaScript processing
out.println("Done.");
%>
```

Javadoc 参考

有关 ExposedTaskContextInformation 和 ExposedEventContextInformation 对象以及它们从核心 Identity Manager API 继承的方法的信息，请参阅“Identity Manager Javadoc”。

Javadoc 页面已整合到《Programming Guide for Java》的 HTML 版本（可以在 Identity Manager 总目录中找到）。

电子邮件模板部署

CA CA Identity Manager 准备发送电子邮件时，会在应用程序服务器中的下列根位置搜索用于生成电子邮件的模板：

iam_im.ear\custom\emailTemplates

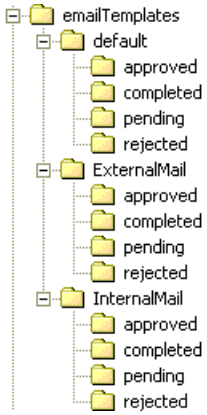
部署在此根的电子邮件模板位于有同样目录结构的模板集内－也就是说，在每个集中有已批准、已完成、未决和已拒绝的目录。

模板集

您可以在 emailTemplates 下面部署几组电子邮件模板。 例如，在安装期间，下列电子邮件模板集会在 iam_im.ear\custom\emailTemplates 下创建：

default\approved
default\completed
default\pending
default\rejected

默认电子邮件模板集包含在“电子邮件模板” (p. 316)中描述的已安装模板。 您可以在默认模板集中添加自定义模板。 在您在与默认模板集相同的级别中定义的目录结构中，您也能部署其他的电子邮件模板集。 例如，iam_im.ear\custom 可能包含以下部署的电子邮件模板：



注意：有关 CA CA Identity Manager 在模板集中选择特定电子邮件模板的方法的信息，请参阅“模板目录” (p. 318)。

如何为环境指定模板集

在为 Identity Manager 环境配置电子邮件时，指定想要用于该环境的电子邮件模板集。 有关为 Identity Manager 环境配置电子邮件的信息，请参阅 *《CA Identity Manager 配置指南》*。

模板名

自定义模板集的目录应当包含与安装在默认模板集中的那些模板名称相同的默认模板。"电子邮件模板" (p. 316)列出了这些默认名称。如果 Identity Manager 找不到名称与执行的任务或事件匹配的其他模板时，就使用默认模板。

（可选）如果想要通过特定模板生成某一电子邮件，您可以将其他模板添加到模板集的一个或多个目录中。 为此，请执行以下步骤：

- 为模板分配与将为其生成电子邮件的任务或事件相同的名称。
- 将模板放置在与将为其生成电子邮件的任务或事件相关联的目录中。

例如，如果 CreateUserEvent 被拒绝，要通过特定模板生成电子邮件，则将名为 "CreateUserEvent.tmpl"的模板放置在该环境模板集的已拒绝目录中。

第 14 章： 报告

此部分包含以下主题：

配置概述

在 CA Identity Manager 中，您可以运行两种不同类型的报告：

快照报告

包括来自快照数据库的数据，其中包含来自 CA Identity Manager 对象存储和 CA Identity Manager 用户存储的信息。 快照报告的一个示例就是“用户配置文件”报告。 您可以通过使用指定所包含信息的“快照定义”来定义要添加到快照数据库中的数据。

非快照报告

包括来自其他数据源（如审核数据库）的数据。 例如，CA Identity Manager 包括默认的审核报告。 （在用户控制台中，这些报告的名称中具有前缀 "审核 - "）。 默认情况下，CA Identity Manager 仅包括审核报告，但您可以创建自定义报告，以包括来自任何数据源（如工作流数据库或任务持久性数据库）的数据。

CA Identity Manager 中的每个报告都需要进行初始配置，然后才能运行。配置步骤取决于要运行的报告类型。

下列步骤概述了本章包含的过程。

对于快照报告：

1. 创建快照定义文件以定义添加到快照数据库中的数据。
2. 捕获报告的快照数据。
3. 修改用户控制台中的报告任务，然后执行以下操作：
   a. 将快照定义与任务相关联。
   b. 将 rptParamConn 连接对象添加到任务。

4. 使用以下方法之一请求报告：
   - 立即运行报告
   - 排定报告
5. 在用户控制台中查看报告。

对于非快照报告：

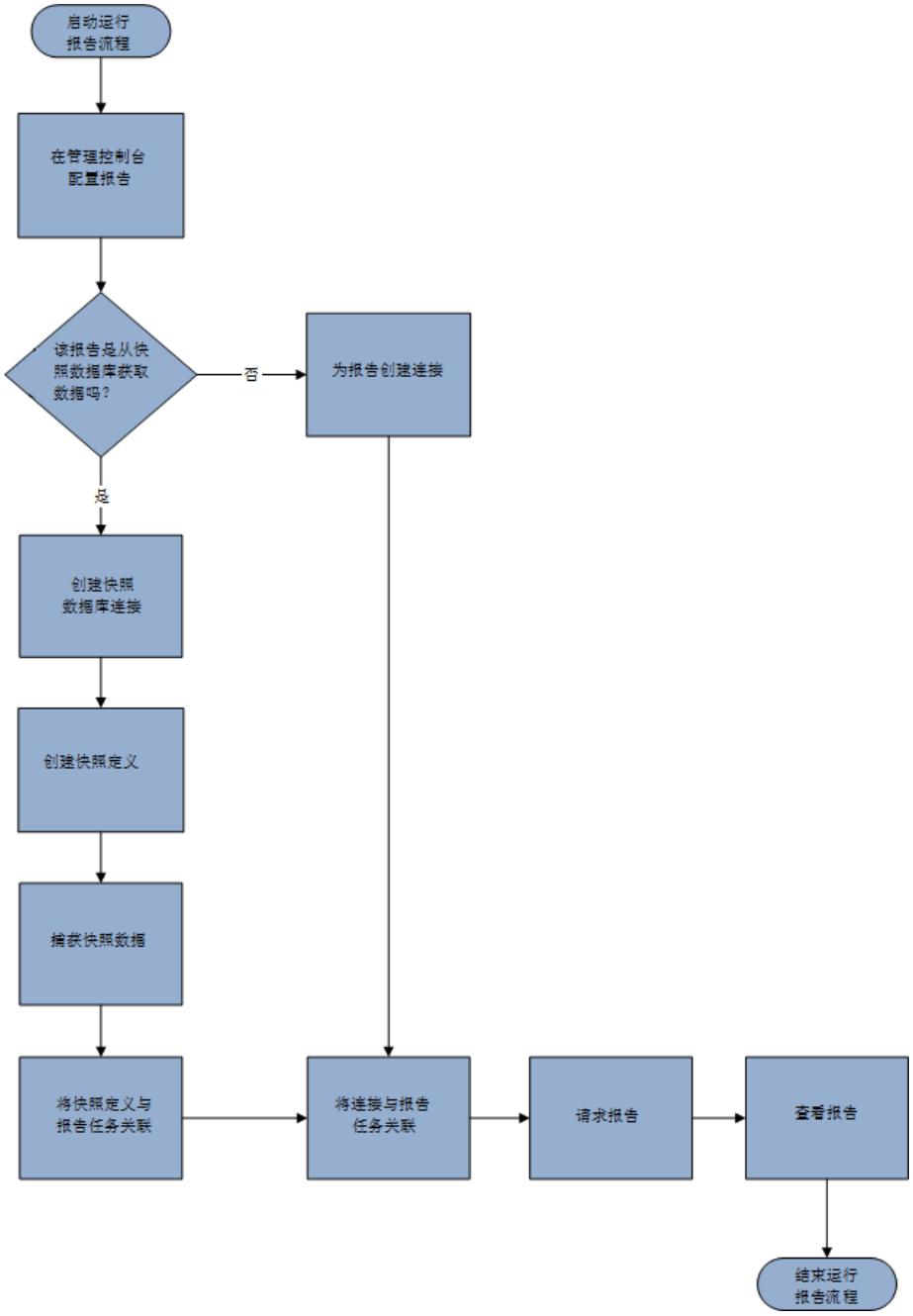
1. 为报告创建带有数据源信息的连接对象。
2. 修改 CA Identity Manager 中的报告任务，然后将连接对象添加到该任务。
3. 使用以下方法之一请求报告：
   - 立即运行报告
   - 排定报告
4. 在用户控制台中查看报告。

完成报告的初始配置后，您可以在 CA Identity Manager 中请求报告。 您可以立即运行报告，或者排定报告在稍后的时间运行。您还可以为 CA Identity Manager 中的报告创建周期排定。

最后一点，您可以在用户控制台中查看报告，或者将报告导出为各种格式。

报告过程

下图详细介绍了运行和查看报告所需的过程：



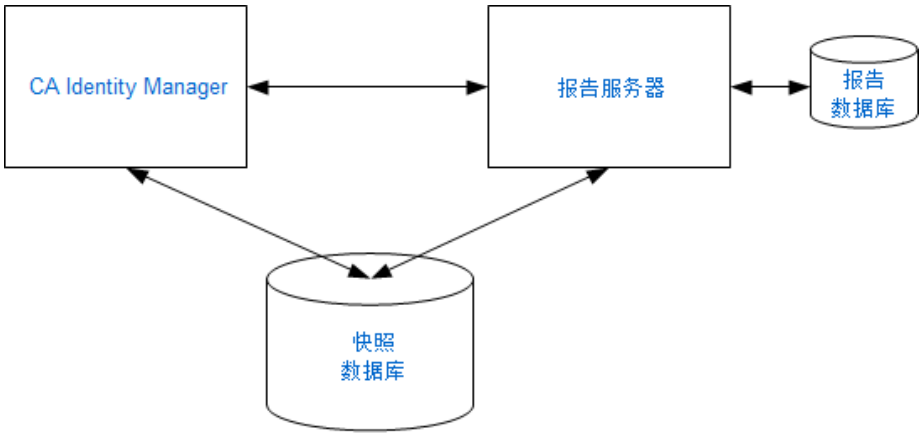
如何运行快照报告

通过 CA Identity Manager 报告，您可以查看 CA Identity Manager 环境的当前状态。 您可以使用此信息以确保遵从内部业务政策或外部法规。

可以从描述 CA Identity Manager 环境中对象之间关系的管理数据中生成 CA Identity Manager 报告。 管理数据的示例包括：

- 用户的配置文件属性
- 包含特定任务的角色列表
- 一个角色或组的成员
- 构成一个角色的规则

在 CA Identity Manager 中，报告设置需要以下三个主要组件：



注意：此图形中的快照数据库也可为审核数据库或工作流数据库。

报告服务器

也称为 CA Business Intelligence，此服务器生成报告，直接与 CA Identity Manager 和快照数据库通讯。

报告数据库

CA 报告服务器（业务对象）存储其数据的数据库。

CA Identity Manager

CA Identity Manager 允许您将 CA Identity Manager 对象数据导出到报告数据库。

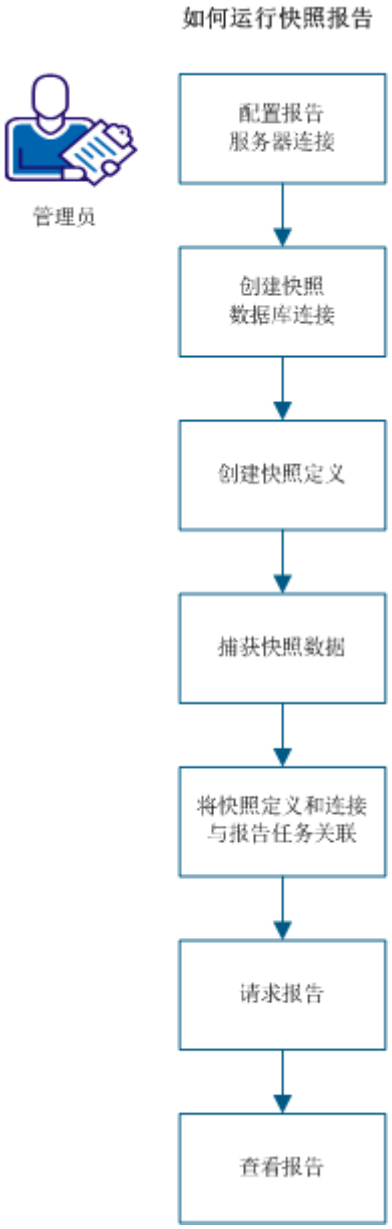
快照数据库

包含 CA Identity Manager 中对象的快照数据的单独数据库

重要说明！报告服务器使用业务对象企业。如果您已经在环境中有报告服务器，且想将它与 CA Identity Manager 结合使用，则由 CA Identity Manager 所需的最小版本是 CA Business Intelligence 3.2 SP5。

快照报告包括来自快照数据库的数据，其中包含来自 CA Identity Manager 对象存储和用户存储的信息。 快照报告的一个示例就是“用户配置文件”报告。 您可以定义要添加到快照数据库中的快照数据，并通过使用快照定义指定要包含的信息。

以下图表说明运行快照报告的过程：



要运行快照报告，请执行下列步骤：

1. 配置报告服务器连接 (p. 355)。
2. 创建快照数据库连接。
3. 创建快照定义。
4. 捕获快照数据。

5. 将快照定义和连接与报告任务相关联。
6. 请求报告。
7. 查看报告 (p. 358)。

配置报告服务器连接

配置 CA Identity Manager 和报告服务器之间的连接。

注意：建议将报告中涉及的所有系统均设置为相同的时区和时间。

配置报告

1. 在用户控制台中，依次单击“任务”、“系统”、“报告”、“报告服务器连接”。
2. 输入报告服务器设置。 请注意下列事项：
   - 主机名和端口 -- 安装报告服务器的系统的主机名和 HTTP URL 端口号。
   - 报告文件夹名称－默认 CA Identity Manager 报告的位置。
   - 用户 ID－为报告服务器创建的用户。
   - 密码－在报告服务器中创建的用户的密码。
   - 安全连接－选中该复选框，以便可在 CA Identity Manager 和报告服务器之间建立安全套接字层 (SSL) 连接。

     注意：在选中“安全连接”复选框之前，请确认您已从 BOServer 安装证书。有关如何配置 SSL 的更多信息，请参阅《*安装指南*》中“报告服务器安装”一章。
   - Web 服务器－对于 Tomcat，设置为非 IIS
3. 单击“测试连接”来验证连接。
4. 单击“提交”。

报告连接已建立。

创建快照数据库连接

CA Identity Manager 需要了解要将快照数据导出到什么位置。创建从 CA Identity Manager 到快照数据库的数据库连接。

创建快照数据库连接

1. 在用户控制台中，依次单击“任务”、“报告”、“快照任务”、“管理快照数据库连接”、“创建快照数据库连接”。
2. 通过完成所有必填字段可以创建一个新的快照数据库连接。
3. 单击“提交”。

   此时已创建新的快照数据库连接。

创建快照定义

快照反映 CA Identity Manager 中的对象在给定时间的状态。 可以使用此快照数据来构建报告。 要捕获 CA Identity Manager 对象数据，请创建将数据导出到快照数据库的快照定义。 使用快照定义，您可以定义加载用户、端点、管理角色、开通角色、组以及组织的规则。

遵循这些步骤:

1. 在用户控制台中，依次选择“任务”、“报告”、“快照任务”、“管理快照定义”、“创建快照定义”。
2. 选择创建或复制类型为“快照类型”的对象。
3. 单击“确定”。
4. 在“配置文件”选项卡上，完成以下字段以创建快照定义配置文件：

   快照定义名称

   标识指定给快照定义的唯一名称。

   快照定义说明

   显示要用于描述快照的任何附加信息。

   已启用

   指定 CA Identity Manager 将在排定的时间根据当前快照定义创建快照。

   注意：如果未选择该选项，则不会在排定的时间捕获快照定义。 此外，快照定义将不会在捕获快照数据屏幕中列出。

   保留的快照数

   指定保留在快照数据库中的成功快照的数量。

   注意：如果没有为该字段指定值，则 CA Identity Manager 存储快照的数量将不受限制。
5. 在“快照策略”选项卡中，选择与要导出的策略相关的对象。
6. 在“角色设置”选项卡中，为快照选择一个或多个要导出的角色组件和可用属性。

   注意：在“快照策略”选项卡中，如果您选择“访问角色”、“管理角色”或“开通角色”对象，请在“角色设置”选项卡中选择属性。
7. 在“用户属性详细信息”选项卡上，为快照选择一个或多个要导出的用户属性。

   注意：在“快照策略”选项卡中，默认情况下，如果仅选择用户对象，则导出与数据相关的所有用户属性。
8. 在“端点帐户属性”选项卡中，选择端点类型的一个或多个帐户属性。

注意：默认情况下，对于选定的端点类型，则导出与端点帐户属性相关的所有数据。 要捕获与特定属性相关的数据，请选择适当的属性。 有关选择需要为端点类型导出属性的更多信息，请参阅《*配置指南*》中的“默认报告”部分。

9. （可选）选中“导出孤立帐户”复选框，以便涵盖在开通服务器中没有全局用户的端点帐户。

   注意：要导出非标准、非标准趋势和孤立帐户报告的报告数据，请选择 exceptionAccount 属性和“导出孤立帐户”复选框。

10. 单击“提交”。

    将配置 CA Identity Manager 以创建在快照定义中提到的对象的快照。

现在您已经创建快照定义，您可以立即捕获快照数据或排定在日后导出快照数据。 有关详细信息，请参阅主题“捕获快照数据”。

更多信息：

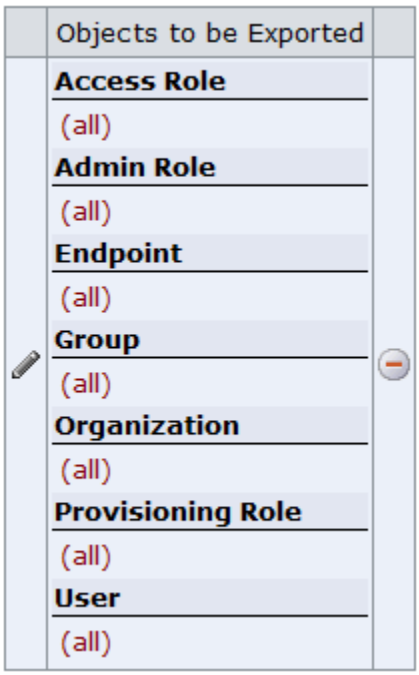
重现选项卡 (p. 347)

示例：为用户权限数据创建快照定义

下列示例将说明为用户权限报告创建快照定义的过程：

1. 在用户控制台中，依次选择“任务”、“报告”、“快照任务”、“管理快照定义”、“创建快照定义”。
2. 选择“创建类型为快照类型的新对象”。
3. 输入快照定义名称、说明和需要保留的快照数目。
4. 在“快照策略定义”选项卡中，单击“添加”。

   从下拉列表中选择“用户”并选择“所有”。同样地，按照下面屏幕所示添加端点、开通角色、管理角色、访问角色、组织以及组：



5. 在“角色设置”选项卡中，选中所有的用户角色复选框。
6. 在“用户属性”选项卡中，从“可用值”列表中选择必要的属性，并将其移至“当前值”列表。
7. 单击“提交”。

管理快照

通过 CA Identity Manager，您可以查看、修改和删除快照定义。当您查看或修改快照定义时，会显示“配置文件”和“维护”选项卡。仅在快照曾被捕获的情况下才会出现“维护”选项卡。在“维护”选项卡上，您可以删除快照（即使快照的状态为失败）。

要查看、修改或删除快照定义，请转至“报告”、“快照任务”、“管理快照定义”，然后单击您要执行的任务。

注意：如果正在使用快照定义将数据导出至快照数据库，则无法删除此快照定义。如果删除正在使用的快照定义，数据导出至快照数据库的操作会停止，但该快照定义仍可用。

捕获快照数据

如果要立即捕获快照数据或在稍后或按周期排定时间排定快照数据导出，请运行“捕获快照数据”任务。该任务立即向快照数据库导出数据（由快照定义定义）。

重要说明！如果要导出大量的数据，则导出快照数据可能花费大量的时间。我们建议您在导出大量数据时排定快照。

捕获快照数据

1. 在用户控制台中，依次选择“任务”、“报告”、“快照任务”、“捕获快照数据”。
2. 选择“立即执行”立即运行数据导出，或选择“排定新作业 (p. 347)”稍后或按周期排定运行数据导出。
3. 单击“下一步”。
4. 选择一个快照定义。
5. 单击“提交”。

   快照数据即被导出至快照数据库。

注意：如果“捕获快照数据”任务似乎需要较长时间，您可以通过单击“系统”选项卡上的“查看提交的任务”来检查该任务的进程。

重现选项卡

使用该选项卡可排定作业。 该选项卡上的字段如下所示：

立即执行

立即运行该作业。

排定新的作业

排定新的作业。

修改现有作业

指定您是否要修改一个已存在的作业。

注意：仅在已为该任务排定了作业时才会出现该字段。

作业名

指定想要创建或修改的作业的名称。

时区

指定服务器的时区。

注意：如果您的时区与服务器的时区不同，则会显示一个下拉框以便您可以在排定新作业时选择您的时区或者服务器的时区。 修改现有作业时不能更改时区。

按日排定

指定作业在每几天运行。

每（天数）

定义作业运行之间的天数。

按周排定

指定作业在一星期内的特定某天或某几天和特定时间运行。

周内某日

指定作业在一星期内的某天或某几天运行。

按月排定

指定作业在周内某日或月内某日运行（以月为基础）。

按年排定

指定作业在周内某日或月内某日运行（以年为基础）。

高级排定

指定其他排定信息。

Cron 表达式

有关填充该字段的信息，请参阅以下页面：

http://quartz-scheduler.org/api/2.1.0/org/quartz/CronExpression.html

执行时间

指定作业运行当天的时间（ 24 小时格式）。 例如，14:15。

将快照定义与报告任务相关联

将快照定义分配到报告任务，CA Identity Manager 即可得知在运行该报告时使用哪个快照定义。此外，CA Identity Manager 报告的信息可能有多个来源，而根据您想要在报告中查看的信息，每个报告都应该与一个特定数据源相关联。

将快照定义和连接与报告任务相关联

1. 在用户控制台中，依次选择“任务”、“角色和任务”、“管理任务”、“修改管理任务”。
2. 搜索您想要与某个快照定义相关联的报告任务
3. 转至“选项卡”选项卡，然后单击“关联快照定义”选项卡旁边的“编辑”按钮。
4. 单击“添加”。
5. 搜索要与报告任务相关联的快照定义，然后单击“选择”。

   在将快照定义与报告任务相关联时，请注意下列事项：

   - 一个报告可以和一个或多个快照定义相关联。
   - 一个快照定义可以和多个报告相关联。
   - 与单个报告任务相关联的多个快照不能使用相同的重现时间。
6. 单击“确定”。
7. 转至“搜索”选项卡，然后单击“浏览”找到搜索屏幕。
8. 编辑报告任务的搜索屏幕，然后选择“报告的连接对象”下面的 rptParamConn。
9. 单击“确定”。
10. 单击“选择”。
11. 单击“提交”。

将端点帐户与帐户模板同步

此任务可在关联帐户模板修改后同步端点帐户。 例如，Active Directory 帐户或许没有组，但是关联帐户模板被定义为包括组。

遵循这些步骤:

1. 登录到用户控制台。
2. 依次选择“任务”、“端点”、“管理端点”、“检查端点帐户同步”。
3. 选择端点。

   系统将显示一个页面，其中列出了该端点上的帐户、关联帐户模板以及不同步的属性。
4. 单击“同步”使这些帐户的属性与帐户模板中定义的属性匹配。

   对帐户模板所做的更改将影响现有的帐户，如下所述：

   - 如果更改功能属性的值，则会更新相应的帐户属性以与该帐户模板属性值同步。 请参阅弱同步和强同步的说明。
   - 某些帐户属性由连接器指定为在帐户模板发生变化时不进行更新。示例中列出的是端点类型仅允许在帐户创建过程中设置的某些属性以及密码属性。

管理任务示例

创建管理任务时，可以定义任务中屏幕的内容和布局，包括：

- 任务的名称
- 显示任务的类别
- 任务中要使用的选项卡和字段，以及字段显示属性
- 管理员可在搜索查询中使用的字段，以及搜索结果中显示的字段

要了解任务的元素，请参见“修改用户”任务。 在此情况下，“用户”是类别，“管理用户”是子类别，“修改用户”是任务。 创建任务时您会创建类别及任务名称。

选择“修改用户”后，将显示一个搜索屏幕。 *搜索屏幕*提供了用于查找要查看或修改的对象的选项。每个选项都称为一项*筛选*，是对搜索查找到的对象的限制。

填写搜索屏幕后，将显示带有多个选项卡的屏幕。例如，下图显示了“修改用户”任务的选项卡。 首先显示的是“配置文件”选项卡，该选项卡显示了用户属性；其他选项卡显示了该用户的角色和组权限。

对于您创建的任务，您可以确定要包括的选项卡及其顺序和内容。

例如，将“修改用户”任务用作模板，您可以创建“修改承包商”任务，该任务对以下方面进行了更改：

- “配置文件”选项卡上的字段
- 任务中要包括的选项卡及其内容
- 在其中显示任务的类别

  您可以在新类别“承包商”下创建此任务。

“修改承包商”任务包括“修改用户”任务中“配置文件”选项卡上的某些字段以及其他一些字段，例如合同的生效日期和承包商所在的公司。 管理员可以通过搜索承包商的姓名、公司及生效日期来搜索承包商。

新任务还包括一个“承包商角色”选项卡，可从中为承包商添加角色。

请求报告

要查看该报告，为用户请求具有报告管理权限的报告。 需要批准的原因是，一些报告的运行可能需要很长时间或重要的系统资源。 如果您的报告请求需要批准，系统会向您发送电子邮件报警。

遵循这些步骤:

1. 登录到具有报告任务用户权限的用户控制台。
2. 依次选择“任务”、“报告”、“报告任务”和“请求报告”。

   随即将显示报告列表。
3. 选择您要请求的报告。

   此时将显示参数屏幕。

   提供所需的参数信息。

   注意：如果您要运行快照报告，但没有可用于该报告的快照，则必须首先捕捉快照。

   - 一些报告显示特定时间点的系统状态。当请求这种报告时，您要选择希望查看的报告数据所对应的时间点。 此时间点称为 *快照*。

     注意：您可以选择的快照日期和时间是预先确定的。通常，由系统管理员或具有报告管理权限的其他用户配置快照。如果您要请求的报告没有快照可用，请与系统管理员联系。
   - 一些报告显示一段时间内的活动。 这些报告的标题通常以“*审核*”开头。当请求这种报告时，您要指定要查看报告数据的所对应的时间段。例如，您可以运行过去 30 天的“审核-重置密码报告”。
4. 单击“排定报告”，并为您的报告选择日程。

   立即

   指定立即运行报告。

   一次

   指定报告在特定时间段内运行一次。 选择想要生成报告的开始日期、结束日期、开始时间和结束时间。

   注意：如果您正在请求的报告需要大量数据，请考虑选择此选项。 为了节省系统资源，请选择系统活动较少的时间。
5. 单击“提交”。

   报告请求即会提交。 根据您的环境配置，请求会立即运行，或在管理员批准后运行。

   通常，报告请求必须先由系统管理员或具有报告管理权限的其他用户批准，然后系统才能完成该请求。 需要批准的原因是，一些报告的运行可能需要很长时间或重要的系统资源。 如果您的报告请求需要批准，系统会向您发送电子邮件报警。

查看报告

根据您的环境配置，在管理员批准报告请求后，报告将可用于查看。 如果您的报告请求正在等待批准，系统会向您发送电子邮件报警。 在获得批准前，您要查看的报告不会显示在搜索列表中。

注意：要使用“查看我的报告”任务查看 CA Identity Manager 中的报告，请在您的浏览器中启用第三方会话 cookie。

遵循这些步骤:

1. 在用户控制台中，依次选择“任务”、“报告”、“报告任务”，然后单击“查看我的报告”。
2. 搜索要查看的生成报告。

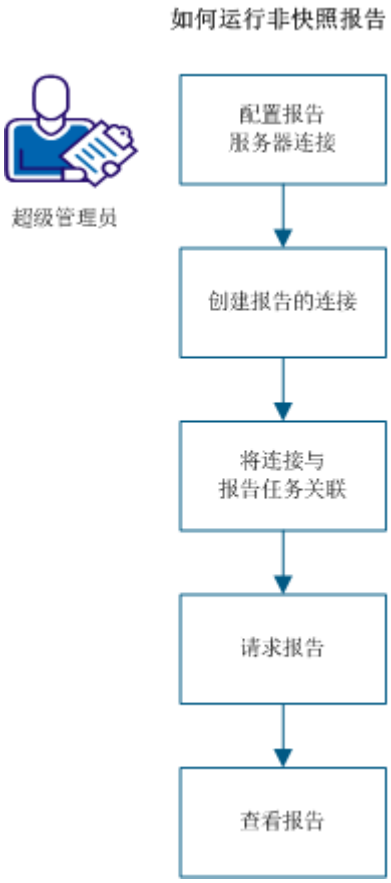
   重现生成报告和即时报告实例都会显示出来。

   注意：如果该报告的状态为未决/周期，则不会生成报告，且可能需要花费时间完成。
3. 选择您想要查看的报告。
4. （可选）单击“导出此报告”（左上角）将该报告导出为以下格式：
   - Crystal Reports
   - PDF
   - Microsoft Excel (97-2003)
   - Microsoft Excel (97-2003) 仅数据
   - Microsoft Excel (97-2003) - 可编辑
   - RTF 文本格式
   - 分隔值 (CSV)
   - XML

如何运行非快照报告

非快照报告包括来自其他数据源（如审核、工作流或任务永久数据库）的数据。CA Identity Manager 在用户控制台中包括其名称带有前缀“Audit-”的默认审核报告。默认情况下，CA Identity Manager 仅包括审核报告，但您可以创建可以包括来自任何数据源数据的自己的自定义报告。

此方案说明超级管理员如何配置报告数据库连接，并运行非快照报告。



以下图表说明运行快照报告的过程：

要运行非快照报告，请执行下列步骤：

1. 配置报告服务器连接。 (p. 355)
2. 为报告创建连接。
3. 将连接与报告任务相关联。
4. 请求报告。
5. 查看报告。 (p. 358)

配置报告服务器连接

要从报告服务器收集数据，您必须配置与报告服务器的连接。在开始程序之前，请收集以下报告服务器的有关信息：

名称	说明
主机名	安装报告服务器的计算机的主机名
端口	安装报告服务器的计算机的端口名
报告文件夹名称	默认 CA Identity Manager 报告的位置。
用户 ID	指定为报告服务器创建的用户。
密码	指定在报告服务器中创建的用户的密码。
安全连接	指定报告服务器的安全连接。选中复选框以启用 CA Identity Manager 和报告服务器之间的安全套接字层 (SSL) 连接。 **注意：**在选中“安全连接”复选框之前，请确认您已从 BOServer 安装证书。有关如何配置 SSL 的更多信息，请参阅《*Installation Guide*》（《安装指南》）中“Report Server Installation”（报告服务器安装）一章。
Web 服务器	指定 Web 服务器。 设置为 Tomcat 的非 IIS。

注意：建议将报告中涉及的所有系统均设置为相同的时区和时间。

遵循这些步骤:

1. 在用户控制台中，依次单击“系统”、“报告”、“报告服务器连接”。
2. 输入报告服务器设置。
3. 单击“测试连接”来验证连接。
4. 单击“提交”。

报告连接已建立。

为报告创建连接

CA Identity Manager 报告的信息可能有多个来源。要指定报告的其他数据源的连接详细信息，请在 CA Identity Manager 内创建 JDBC 连接。

遵循这些步骤:

1. 在用户控制台中，依次选择“任务”、“系统”、“JDBC 连接管理”、“创建 JDBC 连接”。
2. 创建新的连接对象，或根据特定的 JNDI 数据源选择一个连接对象。
3. 填写所有必需的字段，然后单击“提交”。

   此时就创建了一个新的 JDBC 连接。

重要说明！ 建议您 *不要*使用 CA Identity Manager 对象存储数据库来生成报告。

将连接与报告任务相关联

CA Identity Manager 报告的信息从多个来源捕获，而根据您想要在报告中查看的信息，每个报告必须与一个特定数据源相关联。

将连接与报告任务相关联

1. 在用户控制台中，依次选择“任务”、“角色和任务”、“管理任务”、“修改管理任务”。
2. 搜索您想要与某个连接相关联的报告任务。
3. 转至“搜索”选项卡，然后单击“浏览”找到搜索屏幕。
4. 编辑报告任务的搜索屏幕，然后选择“报告的连接对象”下面的连接。
5. 单击“确定”。
6. 单击“选择”。
7. 单击“提交”。

请求报告

要查看该报告，为用户请求具有报告管理权限的报告。 需要批准的原因是，一些报告的运行可能需要很长时间或重要的系统资源。 如果您的报告请求需要批准，系统会向您发送电子邮件报警。

遵循这些步骤:

1. 登录到具有报告任务用户权限的用户控制台。
2. 依次选择“任务”、“报告”、“报告任务”和“请求报告”。

   随即将显示报告列表。

3. 选择您要请求的报告。

   此时将显示参数屏幕。

   提供所需的参数信息。

   注意：如果您要运行快照报告，但没有可用于该报告的快照，则必须首先捕捉快照。

   - 一些报告显示特定时间点的系统状态。当请求这种报告时，您要选择希望查看的报告数据所对应的时间点。 此时间点称为*快照*。

     注意：您可以选择的快照日期和时间是预先确定的。通常，由系统管理员或具有报告管理权限的其他用户配置快照。如果您要请求的报告没有快照可用，请与系统管理员联系。

   - 一些报告显示一段时间内的活动。 这些报告的标题通常以*"审核"*开头。当请求这种报告时，您要指定要查看报告数据的所对应的时间段。例如，您可以运行过去 30 天的"审核-重置密码报告"。

4. 单击"排定报告"，并为您的报告选择日程。

   立即

   指定立即运行报告。

   一次

   指定报告在特定时间段内运行一次。 选择想要生成报告的开始日期、结束日期、开始时间和结束时间。

   注意：如果您正在请求的报告需要大量数据，请考虑选择此选项。 为了节省系统资源，请选择系统活动较少的时间。

5. 单击"提交"。

   报告请求即会提交。 根据您的环境配置，请求会立即运行，或在管理员批准后运行。

   通常，报告请求必须先由系统管理员或具有报告管理权限的其他用户批准，然后系统才能完成该请求。 需要批准的原因是，一些报告的运行可能需要很长时间或重要的系统资源。 如果您的报告请求需要批准，系统会向您发送电子邮件报警。

查看报告

根据您的环境配置，在管理员批准报告请求后，报告将可用于查看。 如果您的报告请求正在等待批准，系统会向您发送电子邮件报警。 在获得批准前，您要查看的报告不会显示在搜索列表中。

注意：要使用“查看我的报告”任务查看 CA Identity Manager 中的报告，请在您的浏览器中启用第三方会话 cookie。

遵循这些步骤:

1. 在用户控制台中，依次选择“报告”、“报告任务”，然后单击“查看我的报告”。
2. 搜索要查看的生成报告。

   重现生成报告和即时报告实例都会显示出来。

   注意：如果该报告的状态为未决/周期，则不会生成报告，且可能需要花费时间完成。
3. 选择您想要查看的报告。
4. （可选）单击“导出此报告”（左上角）将该报告导出为以下格式：
   - Crystal Reports
   - PDF
   - Microsoft Excel (97-2003)
   - Microsoft Excel (97-2003) 仅数据
   - Microsoft Excel (97-2003) - 可编辑
   - RTF 文本格式
   - 分隔值 (CSV)
   - XML

设置报告选项

配置用户可以为特定报告生成的报告实例数。

修改报告选项

1. 依次选择“任务”、“报告”、“报告任务”、“设置报告选项”。

   CA Identity Manager 将连接至 IAM 报告服务器，然后检索所有报告的列表。
2. 选择一个报告，然后单击“修改”。

   将显示该报告的属性窗格。
3. 编辑以下字段：

   名称

   为所选报告指定显示名称。

   实例数

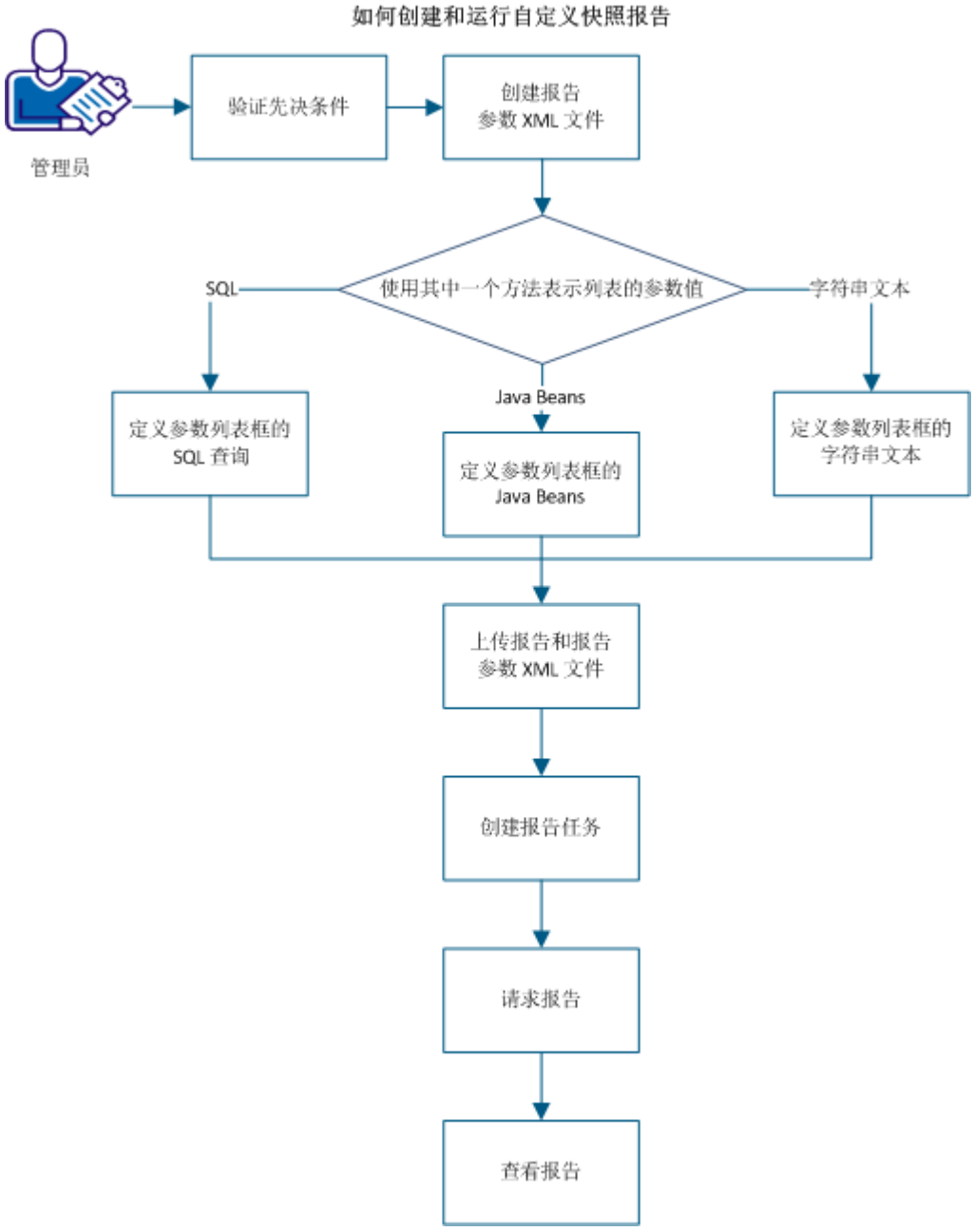
   指定用户可为此报告生成的实例数。
4. 单击“确定”。

   报告属性即被更改。

如何创建和运行自定义快照报告

CA Identity Manager 允许您创建和自定义报告，以满足自己的业务需求。 CA Identity Manager 提供报告参数 XML 文件，其包括与报告属性有关的所有参数。根据您的业务需求，您可以选择必要的属性，以便填充来自快照数据源的报告数据。

以下图表说明创建并运行自定义快照报告的过程：



作为系统管理员，完成以下步骤：

1. 验证先决条件 (p. 361)

2. 创建报告参数 XML 文件 (p. 361)
3. 使用以下其中一个方法为列表表示参数值：
   - 定义参数列表框的 SQL 查询 (p. 364)
   - 定义参数列表框的 Java Bean (p. 364)
   - 定义参数列表框的字符串文本 (p. 365)
4. 上传报告和报告参数 XML 文件 (p. 365)
5. 创建报告任务
6. 请求报告
7. 查看报告 (p. 358)

在 Crystal Reports 中创建报告

要在 CA Identity Manager 中使用自定义报告，请在 Crystal Reports Developer 中创建报告（RPT 文件）。 有关如何在 Crystal Reports 中创建报告的详细信息，请参阅 Crystal Reports 文档。

注意：如果要参考 CA Identity Manager 架构，以便创建自定义报告，请在以下位置查找 CA Identity Manager 数据库架构：

```
C:\Program Files\CA\Identity Manager\IAM Suite\Identity Manager\db\objectstore
```

创建报告参数 XML 文件

参数是报告中的一个字段，可以用来筛选报告。 您可以通过使用参数筛选数据来生成报告。 要允许自定义报告搜索屏幕，每个报告（RPT 文件）都要与报告参数 XML 文件关联。 在 CA Identity Manager 中，您可以创建报告任务并创建搜索屏幕，以便用户在报告生成期间可以输入或选择所需的数据。

注意：如果报告查询对象上的属性，您只需一个报告参数 XML 文件即可。

报告参数 XML 文件必须与报告（RPT 文件）同名，并使用 .xml 扩展名。 例如，如果您将名为 test1.rpt 的报告上传至报告服务器，则应将 XML 文件命名为 test1.xml。

报告参数 XML 文件包含以下元素：

<product>

指明使用参数的产品。 您可以使用同一参数 XML 文件为多个产品创建不同的参数。

<screen>

定义在屏幕上显示的参数。 您可以使用屏幕元素来将参数绑定到指定屏幕。 屏幕 ID 由字母数字组成，并且是唯一的，用于指明屏幕及其参数。

<parameters>

指定屏幕的参数集合。

<param>

定义将指定数据传递到报告的参数元素。 <param> 元素中使用以下属性：

id

定义报告中要关联的参数。

注意：ID 必须有与 Crystal Reports 中的参数相同的名称。

name

此字段当前未用于 CA Identity Manager。 将此属性设置为与 id 同样的值。

displaytext

为该参数指定要在屏幕中显示的用户友好的文本。

type

定义参数的类型。 屏幕根据此属性显示相应更改。 支持的参数类型如下所示：

- **文本框**

  示例：<param id="param1" displaytext="First Name" name="param1" type="string"/>

- **日期和时间**

  示例：<param id="dateVal" displaytext="Date" name="dateVal" type="date_str"/>

  <param id="timeVal" displaytext="Time" name="timeVal" type="time_str"/>

  <param id="datetimeVal" displaytext="Date & Time" name="datetimeVal" type="date_time_str"/>

- **下拉列表**

  示例：<param id="lastname1" displaytext="Name" name="lastname1" type="dropdown" default="key1%1FMy Value1%1Ekey2%1FMy Value2" selected_value="My Value2"/>

- **列表框**

  示例：<param id="lstlastname1" displaytext="Name" name="lstlastname1" type="listbox" rows="10" default="key1%1FSuper%1Ekey2%1Fsql2kSuser01%1E key1F%Super"/>

- **单选框**

  示例：<param id="optionslist" displaytext="Option 1" name="optionslist" type="radiobox" value="option1"/>

  <param id="optionslist" displaytext="Option 2" name="optionslist" type="radiobox" value="option2"/>

  <param id="optionslist" displaytext="Option 3" name="optionslist" type="radiobox" value="option3"/>

- **复选框**

  示例：<param id="enabled" displaytext="Enabled" name="enabled" type="checkbox"/>

row

定义列表框中显示的行数。

默认值：5

default

定义屏幕上显示的给定参数的默认值。此属性可以与字符串、列表框和下拉列表类型一起使用。

定义参数列表框的 SQL 查询

您可以在报告参数 XML 文件中将 SQL 查询定义为列表框或下拉框的一部分。在您将参数与该报告关联并创建报告任务时，参数为用户显示在列表框或下拉框中。要在下拉框或列表框参数中使用 SQL，请在 sql 属性中提供有效的 SQL 语句。

示例：

```
<param id="lstlastname2" displaytext="Name" name="lstlastname2" type="sqlstr"
multiselect="true" sql="select lastname, lastname from tblusers where firstname
like 'S%/>
```

在上例中，会将名字以“*S*”开始的所有用户的姓氏提供给报告。

不过，名字以“*S*”开始的这一条件是静态的。对于根据在以前的某一屏幕（用于同一报告参数组中）中输入的参数值来加载值的用户来说，这一条件不够灵活。为了使用以前在其他屏幕中输入的值，可以利用“*##<parameter id>##*”扩展 SQL 语句。

例如，如果您使用了包含 id=User 的类型为字符串的参数：

```
<param id="User" displaytext="First Name" name="firstname" type="string"/>,
```

您想在 SQL 中使用该参数的输入值，SQL 语句可以如下所示：

```
<param id="lstlastname2" displaytext="Name" name="lstlastname2" type="sqlstr"
multiselect="true" sql="select lastname, lastname from tblusers where firstname
like '##User##' />
```

CA Identity Manager 将会使用为包含 id=User 的参数输入的值替换 ##User##。

注意：要替代的参数值不能和 SQL 参数位于同一屏幕上。例如，如果“*lstlastname2*”在屏幕 3 中，则“User”参数应位于前面的某一屏幕中。

定义参数列表框的 Java Bean

如果使用 SQL 不理想，您可以使用 Java Bean 来计算值并向 CA Identity Manager 提供 <键、值> 对的列表。Java Bean 应位于 CA Identity Manager 的 classpath 中。

示例：

```
<param id="lastname2" displaytext="Name using Javabean" name="lastname2"
type="dropdown" class="com.ca.ims.reporting.unittests.TestDataCollector"/>
```

在上例中，TestDataCollector 以自己的方式检索值，并且将下拉列表的数据发送到该报告。<键、值> 对以 %1F 分开。

确保 Java Bean 位于 iam_im.ear\custom 目录中。

注意：有关实施 Java Bean 的详细信息，请参阅“业务对象文档”。

定义参数列表框的字符串文本

表示列表或下拉框的参数值的最简单方式是使用字符串文本。 键值以 %1F 分割，而每个 <键、值> 对都以 %1E 分开。

示例：

```
<param id="lastname1" displaytext="Name" name="lastname" type="dropdown"
default="key1%1FMy Value1%1Ekey2%1FMy Value2" selected_value="My Value2"/>
```

上传报告和报告参数 XML 文件

在您创建报告 (RPT) 和相应的报告参数 XML 文件之后，将两个文件上传至报告服务器 (BusinessObjects)。

遵循这些步骤:

1. 登录到业务对象中央管理控制台。
2. 单击“文件夹”。
3. 选择“IM Reports”（IM 报告）文件夹。
4. 创建对象程序包。
5. 在新的对象程序包中，浏览以添加 Crystal Report。
6. 浏览至您创建的新报告 (RPT)。

   注意：确保您已选择“IM Reports”（IM 报告）文件夹作为保存该报告的文件夹。
7. 单击“确定”。

   Crystal Report 文件已添加。
8. 在新的对象程序包中，添加新的本地文档，并浏览新的报告参数 XML 文件。
9. 选择“文件类型”作为*文本*。
10. 单击“确定”。

报告和报告参数 xml 文件现在被上传。 为了验证，请转到“IM 报告”文件夹，并确认两个新文件都可用。

创建报告任务

报告任务用来创建、管理、查看和删除用户控制台中生成的报告的模板。

遵循这些步骤:

1. 在用户控制台中，依次选择“任务”、“角色和任务”、“管理任务”、“创建管理任务”。
2. 选择“新建管理任务”，然后单击“确定”。
3. 在“配置文件”选项卡上，填写下列字段：

   名称

   定义报告的名称。 每个报告任务的名称必须唯一。

   标记

   定义任务的唯一标识符。 该字段用于 URL、Web 服务或属性文件中。 只能包含字母、数字和/或下划线，并以字母或下划线开始。

   类别

   指定当前任务所属的类别。

   注意：选择报告类别。

   类别 2

   指定当前任务所属的子类。 此字段中可输入任何字符串。

   主要对象

   指定任务的操作对象。

   注意：选择“报告实例”作为主要对象。

   操作

   指定在主要对象上执行的操作。

   注意：选择“创建”作为操作。
4. 要创建报告任务的新搜索屏幕，请执行下列步骤：
   a. 转至“搜索”选项卡，然后单击“浏览”找到搜索屏幕。

      将显示可用搜索屏幕列表。
   b. 单击“新建”。

      此时显示“创建属性”窗格。
   c. 从列表中选择“报告模板选择屏幕”，然后单击“确定”。

      CA Identity Manager 连接到报告服务器并显示所有报告。
   d. 填写以下字段：

      名称

      定义报告的名称。 每个报告任务的名称都应是唯一的。

标记

充当任务中的唯一标识符。 可以包含 ASCII 字符（a-z，A-Z）、数字 (0-9) 或下划线字符，以字母或下划线开头。

标题

定义新搜索屏幕的标题。 该标题必须唯一。

报告模板

标识要与搜索屏幕相关联的报告。

注意：选择您已添加到报告服务器的报告之一。

报告的连接对象

定义要用于该报告的数据源的连接详细信息。

5. 单击“确定”。

   现在创建报告的新搜索屏幕。

6. 在创建报告任务的“选项卡”选项卡时，请执行下列操作：

   a. 单击“选项卡”。

      对用户可见的选项卡显示。

   b. 选择“标准选项卡控制器”。

   c. 如果您的报告使用快照定义，请执行下列操作：

      a. 从“哪些选项卡应出现在该任务中?”中选择“关联快照定义”。

         “关联快照定义”选项卡会被添加到选项卡列表中。

      b. 单击  来编辑“关联快照定义”选项卡。

      c. 单击“添加”，将报告任务与快照定义关联。

         然后会显示可用的“快照定义”列表。

      d. 选择“快照定义”，并单击“确定”。

         报告任务与快照定义关联。

   d. 单击“提交”。

      报告任务即会创建。

   e. 将新建的报告任务分配给管理角色。

      CA Identity Manager 管理角色用户可以使用新的报告任务。

报告任务现在准备好，可由管理员使用。

注意：一个报告（RPT 文件）只能与一个报告任务关联。

请求报告

要查看该报告，为用户请求具有报告管理权限的报告。 通常，报告请求必须先由系统管理员或具有报告管理权限的其他用户批准，然后系统才能完成该请求。需要批准的原因是，一些报告的运行可能需要很长时间或重要的系统资源。 如果您的报告请求需要批准，系统会向您发送电子邮件报警。

遵循这些步骤:

1. 以对报告任务有访问权限的用户身份登录到用户控制台。
2. 从导航菜单中，依次选择“任务”、“报告”、“报告任务”、“请求报告”。

   随即将显示报告列表。
3. 选择您要请求的报告。

   此时将显示参数屏幕。
4. 提供所需的参数信息。

   注意：如果您要运行快照报告，但没有可用于该报告的快照，则必须首先捕捉快照。

   - 一些报告显示特定时间点的系统状态。当请求这种报告时，您要选择希望查看的报告数据所对应的时间点。 此时间点称为 *快照*。

     注意：您可以选择的快照日期和时间是预先确定的。通常，由系统管理员或具有报告管理权限的其他用户配置快照。如果您要请求的报告没有快照可用，请与系统管理员联系。
   - 一些报告显示一段时间内的活动。 这些报告的标题通常以“*审核*”开头。当请求这种报告时，您要指定要查看报告数据的所对应的时间段。例如，您可以运行过去 30 天的“审核-重置密码报告”。
5. 单击“排定报告”，并为您的报告选择日程。

   立即

   指定立即运行报告。

   一次

   指定报告在特定时间段内运行一次。 选择想要生成报告的开始日期、结束日期、开始时间和结束时间。

   注意：如果您正在请求的报告需要大量数据，请考虑选择此选项。 为了节省系统资源，请选择系统活动较少的时间。
6. 单击“提交”。

   报告请求即会提交。 根据您的环境配置，请求会立即运行，或在管理员批准后运行。

查看报告

根据您的环境配置，在管理员批准报告请求后，报告将可用于查看。 如果您的报告请求正在等待批准，系统会向您发送电子邮件报警。 在获得批准前，您要查看的报告不会显示在搜索列表中。

注意：要使用“查看我的报告”任务查看 CA Identity Manager 中的报告，请在您的浏览器中启用第三方会话 cookie。

遵循这些步骤:

1. 在用户控制台中，依次选择“任务”、“报告”、“报告任务”，然后单击“查看我的报告”。
2. 搜索要查看的生成报告。

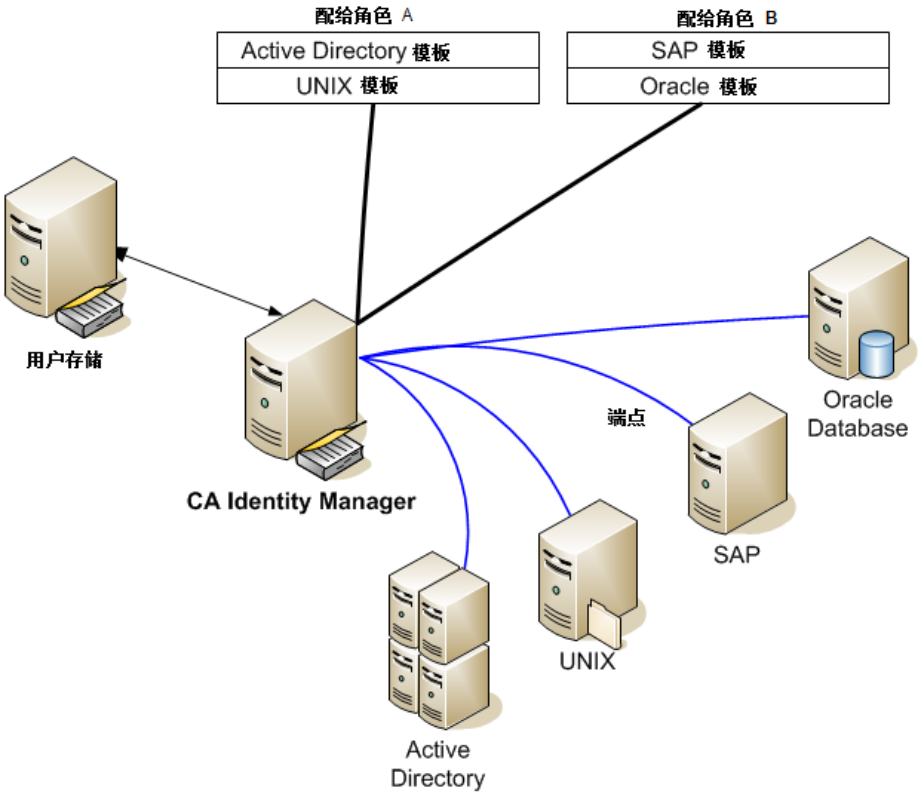
   重现生成报告和即时报告实例都会显示出来。

   注意：如果该报告的状态为未决/周期，则不会生成报告，且可能需要花费时间完成。
3. 选择您想要查看的报告。
4. （可选）单击“导出此报告”（左上角）将该报告导出为以下格式：
   - Crystal Reports
   - PDF
   - Microsoft Excel (97-2003)
   - Microsoft Excel (97-2003) 仅数据
   - Microsoft Excel (97-2003) - 可编辑
   - RTF 文本格式
   - 分隔值 (CSV)
   - XML

同步用户、帐户和角色

将多个端点和帐户集成到一个用户管理系统会导致同步丢失。 分配给用户的配给角色或帐户模板可能与该用户的实际帐户不同。

例如，设想一个包含两个配给角色的情况，其中一个角色拥有 Active Directory 和 UNIX 帐户模板，另一个拥有 SAP 和 Oracle 模板。 用户 john_smith 拥有包含 Active Directory 和 UNIX 帐户模板的配给角色 A，但该用户仅拥有 Active Directory 帐户。 UNIX 帐户模板可能是在分配给该用户之后才添加到角色中的。 因此，管理员需要同步该用户和当前的角色定义。



以下情况是用户与配给角色或帐户模板同步丢失的其他原因：

- 由于网络中的硬件或软件问题，创建必要帐户的之前尝试失败，导致帐户缺失。
- 配给角色和帐户模板出现变化，从而创建了额外帐户或导致帐户缺失。
- 帐户创建后被分配给帐户模板，因此存在帐户，但是与其帐户模板不同步。
- 因为被指定稍后创建帐户，因此新帐户创建推迟。
- 获得了新端点。 在浏览和关联过程中，配给服务器未自动将配给角色分配给用户。 您需要更新角色以指明端点上需要帐户的用户。 在用户同步时，与用户关联的任何帐户均被列为额外帐户。

- 通过将帐户复制到用户的方式，将现有帐户分配给用户。
- 通过将用户分配给角色之外的其他方式为用户创建帐户。 例如，将用户复制到该用户配给角色中不包含的帐户模板。 帐户被列为额外帐户或具有额外帐户模板的帐户。如果将用户复制到端点以使用默认帐户模板创建帐户，则该帐户可能成为额外帐户。

以下章节将介绍如何执行三种类型的同步操作：

1. 将用户与角色同步 (p. 147)。
2. 将用户与帐户模板同步 (p. 147)。
3. 将端点帐户与帐户模板同步 (p. 148)。

将用户与角色同步

此任务可创建、更新或删除帐户，以便帐户与分配给用户的开通角色保持一致。例如，管理员使用端点上的内置工具添加或删除帐户，但是您尚未重新浏览该端点以更新开通目录。 因此，用户具有额外或缺失的帐户。 另外，此任务还可确保每个帐户都属于正确的帐户模板。

遵循这些步骤:

1. 登录到用户控制台。
2. 依次选择“用户”、“同步”、“检查角色同步”。
3. 选择用户。

   系统将显示一个页面，其中列出了预期帐户、额外帐户和缺失帐户。
4. 单击“同步”使帐户与此角色中的模板匹配。
   a. 您可以选中复选框在端点上创建帐户。如果用户有多个帐户模板限定的都是同一个帐户，则该帐户是通过合并所有相关帐户模板创建的。

      此帐户会分配给当前与该帐户不同步的那些帐户模板。
   b. 您可以选中复选框删除额外帐户。不过，用户可能有拥有这些帐户的正当理由。 如果是这种情况，请不要选中此选项。

      在某些端点上，帐户删除功能被禁用；因此，无法删除帐户。

将用户与帐户模板同步

此任务可将端点帐户的属性与用户的关联帐户模板同步。 不过，完全同步取决于以下因素：

- 帐户完全同步出现在两种情况下。 帐户模板使用强同步 (p. 149)，或者两个或更多帐户模板被添加到帐户。
- 如果帐户模板使用弱同步 (p. 149)，则此任务将启动仅涉及此模板的帐户同步。 如果在此更新前，帐户之前没有与其他帐户模板保持帐户同步，更新后将仍然如此。

遵循这些步骤:

1. 登录到用户控制台。
2. 依次选择“用户”、“同步”、“检查帐户模板同步”。
3. 选择用户。

   系统将显示一个页面，其中列出了预期帐户、额外帐户和缺失帐户。
4. 单击“同步”使帐户与模板匹配。

   a. 您可以选中复选框在端点上创建帐户。如果用户有多个帐户模板限定的都是同一个帐户，则该帐户是通过合并相关帐户模板创建的。

   此帐户会分配给与该帐户不同步的帐户模板。新创建的帐户不需要执行帐户同步。

   b. 您可以选中复选框删除额外帐户。不过，用户可能有拥有这些帐户的正当理由。 如果是这种情况，请不要选中此选项。

   在某些端点上，帐户删除功能被禁用；因此，无法删除帐户。

将端点帐户与帐户模板同步

此任务可在关联帐户模板修改后同步端点帐户。 例如，Active Directory 帐户或许没有组，但是关联帐户模板被定义为包括组。

遵循这些步骤:

1. 登录到用户控制台。
2. 依次选择“端点”、“管理端点”、“检查端点帐户同步”。
3. 选择端点。

   系统将显示一个页面，其中列出了该端点上的帐户、关联帐户模板以及不同步的属性。
4. 单击“同步”使这些帐户的属性与帐户模板中定义的属性匹配。

   对帐户模板所做的更改将影响现有的帐户，如下所述：

   - 如果更改功能属性的值，则会更新相应的帐户属性以与该帐户模板属性值同步。 请参阅弱同步和强同步的说明。
   - 某些帐户属性由连接器指定为在帐户模板发生变化时不进行更新。示例中列出的是端点类型仅允许在帐户创建过程中设置的某些属性以及密码属性。

更新哪些属性

当您更改帐户模板中的功能属性时，帐户的相应属性也会发生更改。 此更改会对帐户的属性产生影响。 产生的影响基于以下因素：

- 该帐户模板定义为使用弱同步还是强同步。
- 该帐户是否属于多个帐户模板。

弱同步

*弱同步*可确保用户具有其帐户的最少功能属性。 在多数端点类型中弱同步是默认值。如果更新使用弱同步的模板，CA Identity Manager 将更新功能属性，如下所述：

- 如果在帐户模板中更新了数字字段，且该新数字大于该帐户中的数字，CA Identity Manager 则会更改帐户中的值以与新数字匹配。
- 如果之前在帐户模板中没有选中，但您在之后选中了该复选框，CA Identity Manager 则会在未选中复选框的任何帐户中更新该复选框。
- 如果在帐户模板中更改了列表，CA Identity Manager 则会更新所有帐户以包括未包括在该帐户列表值中的新列表中的任何值。

如果帐户属于其他帐户模板（无论这些模板使用弱同步还是强同步），CA Identity Manager 则仅会参考正在更改的模板。 此操作比检查每个帐户模板更有效。 因为弱同步仅将功能添加到帐户，所以通常不需参考那些其他帐户模板。

注意：从弱同步帐户模板传播时，将要删除或降低功能的更改会保持某些帐户的状态，而不同步。 请记住，使用弱同步，从不会删除或降低功能。 在不参考帐户的其他模板的情况下，传播不会考虑弱同步是否充分。

在这种情况下，请使用“将用户与帐户模板同步”让帐户与其帐户模板保持同步。

强同步

强同步可确保帐户具有与在帐户模板中指定的那些帐户属性完全相同的帐户属性。

例如，假设您将一个组添加到现有 UNIX 帐户模板中。最初，帐户模板使帐户成为“人员”组的成员。 现在，您希望帐户同时成为“人员”和“系统”两个组的成员。当每个帐户都是“人员”组和“系统”组（且没有其他组）的成员时，与帐户模板关联的所有帐户即被视为同步。任何不在“人员”组中的帐户会被添加到两个组中。

要考虑的一些其他因素包括以下内容：

- 如果帐户模板使用强同步，则属于除“人员”组和“系统”组之外的其他组的任何帐户会被从这些额外组中删除。
- 如果帐户模板使用弱同步，则帐户会被添加到“人员”组和“系统”组中。已定义其他组的任何帐户仍然是这些组的成员。

注意：定期同步帐户和其模板，以便确保帐户保持与其帐户模板同步。

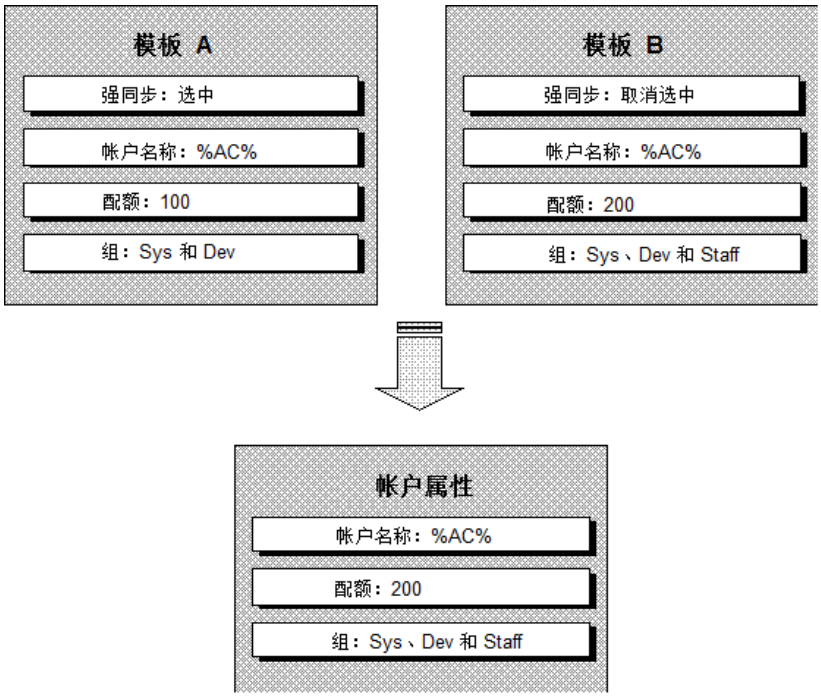
带有多个模板的帐户

同步还取决于帐户是否属于多个帐户模板。 如果帐户只有一个帐户模板，并且该模板使用强同步，则每个属性均会更新，以精确匹配帐户模板属性值所求得的结果。 结果与属性是初始属性时的结果一样。

一个帐户可能属于多个帐户模板，就像一个用户属于多个开通角色，每个角色都规定了在同一管理端点上的某一访问级别。 在这种情况下，CA Identity Manager 会将这些帐户模板合并为一个有效的帐户模板，其规定来自单个帐户模板的功能超集。 如果所有单个帐户模板均为弱同步，则此帐户模板本身被视为使用弱同步；如果任何单个帐户模板为强同步，则此帐户模板本身被视为使用强同步。

注意：通常，对于控制一个帐户的帐户模板，将仅使用弱同步或仅使用强同步，具体取决于您公司的角色是否完全定义了用户所需的访问权限。 如果用户不适合定位明确的角色，您需要一定的灵活性，以便向用户帐户授予其他能力，则使用弱同步。如果您可以定义角色以精确指定用户需要的访问，则使用强同步。

下列示例说明如何将多个帐户模板合并为一个有效的帐户模板。 在本例中，一个帐户模板被标记为弱同步，另一个为强同步。 因此，通过合并两个帐户模板而创建的有效帐户模板被视为强同步帐户模板。 整数“配额”属性取两个帐户模板中较大的值，多值“组”属性取两者的联合值。



仅针对新帐户的属性

在帐户模板中，某些属性仅在创建帐户时适用。 例如，密码属性是定义新帐户密码的规则表达式。 该规则表达式从不更新帐户的密码。对密码规则表达式的更改仅影响在设置规则表达式之后创建的帐户。

与之相似，只读帐户属性的模板规则表达式也只影响在设置规则表达式之后创建的帐户。 更改这种规则表达式对现有帐户没有任何影响。

疑难解答

以下部分针对有关报告的故障排除主题提供了详细信息。

查看报告时会重定向到 Infoview 登录页

在 CA Identity Manager 中查看报告时，您可能会被重定向到业务对象 Infoview 登录页。

重定向后查看报告

1. 请确保使用 CA 报告服务器（业务对象）的完全限定域名。
2. 右键单击 Infoview 登录网页并且选择“查看源文件”。
3. 查找该报告的 URL。
4. 将该 URL 复制并粘贴到新的浏览器窗口。
5. 如果看不到该报告，则使用 HTTP 跟踪工具来提供更多信息。
6. 如果能看到该报告，则尝试以下操作来修复浏览器设置：
   - 接受第三方 Cookie。
   - 允许会话 Cookie。
   - 删除高安全性设置。

生成 20,000 多条记录的用户帐户

如果有超过 20,000 条记录，则需要执行其他一些步骤来生成用户帐户报告。

生成 20,000 多条记录的用户帐户报告

1. 打开 Business Objects Central Management 控制台。
2. 单击“Servers”（服务器），然后选择 *servername*.pageserver。
3. 对于条目“Database Records To Read When Previewing Or Refreshing a Report”（预览或刷新报告时读取的数据库记录数），选择“Unlimited”（无限制）记录数。
4. 使用 Crystal Reports 设计器，打开用户帐户报告。
5. 依次选择“Database”（数据库）、“Set Datasource Location”（设置数据源位置），将数据库位置设置为您的快照数据库。
6. 保存该更改。
7. 依次选择“Database”（数据库）、“Datasource Expert”（数据源专家），右键单击右侧窗口中的“Command”（命令）。

   此时将在左侧显示 SQL 语法，还将显示参数列表。

8. 输入报告模板“Parameters”（参数）字段中的参数名。
9. 更改左侧的查询，并在查询中添加该参数。

   例如，如果您有 reportid 参数，该查询将为：

   ```
   Select *  from endPointAttributes, endpointview, imreport6
   where endPointAttributes.imr_endpointid = endpointview.imr_endpointid and
   endPointAttributes.imr_reportid = endpointview.imr_reportid
    endpointview.imr_reportid = imreport6.imr_reportid and
   imreport6.imr_reportid = {?reportid}
   ```

10. 保存该报告。

第 15 章： 身份策略

此部分包含以下主题：

身份策略

身份策略是指在用户符合某一条件或规则时，所发生的一组业务更改。 您可以使用身份策略集执行以下操作：

- 自动执行某些身份管理任务，例如分配角色和组员资格、分配资源或修改用户配置文件属性。
- 强制执行职责划分。 例如，您可以创建一个身份策略集，用于禁止支票签署人角色的成员拥有支票批准人角色，并将公司每个人可签署支票的金额限定在 10000 美元以内。
- 强制遵从。例如，您可以审核担任某一职务且酬劳超过 100000 美元的用户。

  强制遵从的身份策略称为*遵从策略*。

与身份策略相关联的业务更改包括：

- 分配或吊销角色，包括配给角色（如果仅使用配给目录）
- 分配或吊销组员资格
- 更新用户配置文件中的属性

例如，某家公司可能会创建一个身份策略，规定所有副总裁均属于乡村俱乐部成员组，且均具有工资批准人角色。 当用户的职称变为副总裁，且该用户与该身份策略同步时，CA Identity Manager 会将该用户添加到相应的组和角色。如果副总裁晋升为 CEO，她将不再满足副总裁身份策略中的条件，因此将吊销该策略所应用的更改，并且将应用基于 CEO 策略的新更改。

基于身份策略的更改操作包含可置于工作流控制下且能进行审核的事件。 在上一示例中，工资批准人角色向其成员授予了重要权限。为保护工资批准人角色，公司可以创建一个工作流流程，要求在分配此角色之前经过一系列批准，并且可配置 CA Identity Manager 对角色分配进行审核。

为简化身份策略管理，身份策略将组成一个身份策略集。 例如，副总裁策略和 CEO 策略可能属于行政权限身份策略集。

注意：CA Identity Manager 包括身份策略的其他类型，名为 *预防性身份策略* (p. 396)。 通过在提交任务之前执行的这些策略，管理员可以在分配权限或更改配置文件属性之前检查策略违规。 如果违规存在，在提交任务之前，管理员可以清除违规。

身份策略集计划工作表

身份策略集包含一个或多个身份策略。 创建身份策略集之前，请使用以下工作表计划该集中每个身份策略。

问题	您的答案
您要将该身份策略命名为什么？	
该身份策略适用于哪些用户？	
身份策略应用到用户后，CA CA Identity Manager 应执行哪些操作？	
如果不再继续应用曾经应用到用户的身份策略，CA CA Identity Manager 应执行哪些操作？	
CA CA Identity Manager 应当多次应用身份策略的更改，还是只应该在首次用户满足策略条件时应用身份策略更改？	

针对策略集中的每个身份策略完成此工作表后，验证这些策略与其他策略不相冲突。 例如，确保某一策略不会授予另一策略吊销的权限。

创建身份策略集

要创建身份策略集，您必须具有系统管理员角色，或具有承担创建身份策略集任务的角色。

要创建身份策略集，请完成以下步骤：

1. 为身份策略集定义配置文件 (p. 379)
2. 创建策略集成员规则 (p. 380)
3. 创建身份策略 (p. 380)
4. 指定身份策略集的所有者 (p. 388)

注意：要对 CA Identity Manager 环境使用策略，请在 CA Identity Manager 管理控制台中启用身份策略。 有关详细信息，请参阅 *《配置指南》*。

为身份策略集定义配置文件

通过“配置文件”选项卡您可以为身份策略集定义基本属性。

定义身份策略集配置文件

1. 从用户控制台中依次选择“策略”、“管理身份策略”、“创建身份策略集”。

   您必须作为具有管理身份策略权限的用户登录 CA CA Identity Manager。 默认系统器角色包括这些权限。
2. 选择创建新的身份策略集，或创建现有身份策略集的副本。
3. 输入身份策略集的名称。
4. 输入身份策略集的类别。

   类别将把具有类似用途的身份策略集组合在一起以便进行报告。 “类别”字段为必填字段。
5. （可选）输入身份策略集的说明。
6. 如果您不希望身份策略集可用，请清除“已启用”复选框。
7. 当您完成“配置文件”选项卡时，选择“策略”选项卡来创建身份策略集的身份策略。

更多信息：

创建身份策略 (p. 380)
创建策略集成员规则 (p. 380)

创建策略集成员规则

您可以为策略集创建成员规则，以便策略集仅适用于某些用户。 在评估集中的身份策略之前评估该规则，这可以节省不少时间。 例如，如果某个成员规则限制的身份策略评估为用户的 10%，那么该规则将会节省 90% 的评估时间。

创建策略集成员规则

1. 选择“策略”选项卡。
2. 单击“策略集成员规则”下的“编辑”符号。
3. 输入将策略仅应用于某些用户的规则。
4. 单击“确定”。

更多信息：

创建身份策略 (p. 380)

创建身份策略

为身份策略集定义配置文件和成员规则后，可以定义该策略集中的身份策略。

注意：在大型实施中，可能需要花费大量的时间来评估身份策略规则。 要缩短包括用户属性的规则的评估时间，您可以启用内存中的评估选项。 有关详细信息，请参阅《*Configuration Guide*》。

创建身份策略

1. 选择“策略”选项卡。
2. 单击“添加”。
3. 输入身份策略的名称。
4. 如果希望仅在用户第一次满足策略时应用该策略，请选中“应用一次”复选框。
5. 选中“遵从”复选框将此策略标记为遵从策略。

   选中此复选框后：

   - CA CA Identity Manager 可以为与遵从策略不同步的用户生成报告。
   - 在“应用/删除策略时的操作”列表框中可以看到“遵从违规”操作。
6. 在“策略条件”区域中，标识策略应用到的用户。
7. 在“应用策略时的操作”区域中，定义将身份策略应用到用户时 CA CA Identity Manager 执行的操作。

8. 在“删除策略时的操作”区域中，定义当用户不再满足身份策略的条件时 CA CA Identity Manager 执行的操作。
9. 单击“确定”。

注意：首先要在管理控制台中启用身份策略，才能使用创建的身份策略集。 有关详细信息，请参阅*《配置指南》*。

“应用一次”设置

CA CA Identity Manager 基于“应用一次”设置以不同的方式应用身份策略。

启用“应用一次”设置

启用“应用一次”设置后，CA CA Identity Manager 将在用户*第一次*满足身份策略中定义的条件时应用与该策略相关联的更改。 仅执行一次与该策略相关联的更改操作。 因此，如果之前已应用过该策略，CA CA Identity Manager 将不对用户应用策略更新。

用户不再满足该策略中定义的条件时，CA CA Identity Manager 将执行策略的删除操作。

“应用一次”设置通常在配给资源时使用。 例如，您可以制定一个将手机分配给经理的策略。 用户首次成为经理时，会分配给该用户一部手机。 CA CA Identity Manager 仅发放手机一次，而非每次评估策略时均发放。 如果手机策略更新为包括较新的手机型号，则 CA CA Identity Manager 将不向现有经理发放新手机。

注意：当 CA CA Identity Manager 与配给服务器集成时，资源配给可用。

禁用“应用一次”设置

如果未启用“应用一次”设置，则在每次评估身份策略时均会应用与身份策略相关联的更改操作。 这意味着 CA CA Identity Manager 会为符合策略条件的每个用户应用更改操作，无论先前是否应用过这些更改操作。

通常，在强制遵从的身份策略中会禁用“应用一次”设置。 例如，可以创建身份策略，将经理的财务开支授权限制为 5000 美元。如果 CA CA Identity Manager 遇到财务开支授权设置为 10000 美元的经理，则会将其财务开支授权重置为 5000 美元。 每次同步经理与身份策略时，CA CA Identity Manager 均会执行检查以确保财务开支授权设置正确。

如果对用户配置文件进行了与更改操作相冲突的手工更改，则 CA CA Identity Manager 将在同步用户与策略时覆盖此更改。

在上面的示例中，如果有人将经理的财务开支授权手工增加为 10000 美元，则 CA CA Identity Manager 会在同步经理与策略时，将财务开支授权重置为 5000 美元。

下表总结了启用或禁用“应用一次”设置的效果。

如果“应用一次”为……	那么……
已启用	■ 与身份策略相关联的更改操作仅应用一次 ■ 保留在应用身份策略后进行的手工更改 ■ 如果 CA CA Identity Manager 先前应用了身份策略，则更新将不应用到符合该身份策略条件的用户 ■ 如果某一用户不再符合身份策略条件，则 CA CA Identity Manager 将执行删除操作
禁用	■ 每次同步用户与策略时，均应用与身份策略相关联的更改操作 ■ 应用身份策略时将覆盖手工更改 ■ 在同步用户时应用对策略的更新 ■ 如果某一用户不再符合身份策略条件，则 CA CA Identity Manager 将执行删除操作

策略条件

策略条件是用于确定应用身份策略的用户组的规则。

下表介绍了一些可用选项。

语法	条件	示例
(所有)	身份策略应用于所有用户。	
其中 <用户筛选>	用户必须与一个或多个属性值相匹配。	职位=经理且位置=东部的用户

语法	条件	示例
在 <组织规则>	用户必须属于指定的组织。 **注意：**选中此选项后，CA CA Identity Manager 将显示一个新的列表框，您可以从中选择以下选项： ■ 组织 <组织> [及下级部门] - 使用组织搜索屏幕选择一个组织，并可选择包括该组织的下级组织。 ■ 组织，其中 <组织筛选> [及下级部门] - 指定选择一个或多个组织的筛选。	销售部门及下级组织中的用户
其中 <用户筛选>，谁在 <组织规则>	用户必须与特定的用户属性相匹配并属于特定组织。	职位=经理且组织=销售部门*
谁是 <组员规则> 的成员	用户必须属于满足组属性指定条件的组。 **注意：**选中此选项后，CA CA Identity Manager 将显示一个新的列表框，您可以从中选择以下选项： ■ 组 <组> - 使用组搜索屏幕来选择组。 ■ 组，其中 <组筛选> - 指定选择一个或多个组的筛选。	属于所有者=CIO 的组成员的用户

语法	条件	示例
谁是 <角色规则> 的成员	用户必须是某个角色的成员。 角色可以是： ■ 访问角色 ■ 管理角色 ■ 配给角色 **注意：**要使用配给角色，CA CA Identity Manager 必须与配给服务器集成。 有关详细信息，请参阅 *《Installation Guide》*（《安装指南》）。	属于“帮助中心”角色成员的用户
谁是 <角色规则> 的管理员	用户必须是某个角色的管理员。 角色可以是： ■ 访问角色 ■ 管理角色 ■ 配给角色 **注意：**要使用配给角色，CA CA Identity Manager 必须与配给服务器集成。 有关详细信息，请参阅 *《Installation Guide》*（《安装指南》）。	属于“销售经理”角色管理员的用户
谁是 <角色规则> 的所有者	用户必须是某个角色的所有者。 角色可以是： ■ 访问角色 ■ 管理角色 ■ 配给角色 **注意：**要使用配给角色，CA CA Identity Manager 必须与配给服务器集成。 有关详细信息，请参阅 *《Installation Guide》*（《安装指南》）。	属于“用户经理”角色所有者的用户
由查询 <LDAP 查询> 返回	用户必须满足 LDAP 查询的条件。	符合 LDAP 查询条件的用户。 例如：(departmentNumber=Accounts)

语法	条件	示例
在 <管理并集限制>	用户必须至少符合条件列表中的一个条件。可以将以下类型的筛选包括在管理交集限制中： ■ 访问/管理/配给角色的成员 ■ 访问/管理/配给角色的管理员 ■ 访问/管理/配给角色的所有者 ■ 组员	属于“认证经理”角色成员*或*“认证经理”角色所有者的用户。
在 <管理交集限制>	用户必须符合条件列表中的所有条件。可以将以下类型的筛选包括在管理交集限制中： ■ 访问/管理/配给角色的成员 ■ 访问/管理/配给角色的管理员 ■ 访问/管理/配给角色的所有者 ■ 组员	属于“合约发起人”角色*及*“合约批准人”角色成员的用户。

针对应用/删除策略的操作

您可以定义在 CA CA Identity Manager 评估身份策略时执行的更改操作。 包括以下操作：

应用策略时的操作

当用户满足策略条件中的条件时 CA CA Identity Manager 执行的一套操作。

删除策略时的操作

当用户不再满足策略条件中的条件时 CA CA Identity Manager 执行的一套操作。

应用或删除身份策略时 CA CA Identity Manager 可执行的操作是相同的。 有关详细信息，请参见下表。

更改操作	说明
添加到组 <组名> [...]	将用户添加到一个组。 选中此选项后，CA CA Identity Manager 将显示一个屏幕，您可以从中搜索所需的组。
添加到用户所在组织中的 <组名>	将用户添加到一个本地组。 选中此选项后，CA CA Identity Manager 将显示一个文本框，您可以从中输入所需组的名称。
将 <单个值用户属性> 设置为 <值>	设置用户配置文件中属性的值。 如果已存在一个值，则 CA CA Identity Manager 将用在更改操作中指定的值将其覆盖。
将 <值> 添加到 <多值用户属性>	将值添加到多值用户属性。 该选项不会覆盖现有值。
成为访问角色的成员	将用户分配到访问角色。
成为访问角色的管理员	使用户成为访问角色的管理员
成为管理角色的成员	使用户成为管理角色的成员
成为管理角色的管理员	使用户成为管理角色的管理员
成为配给角色的成员	使用户成为配给角色的成员，配给角色可创建相关联的端点帐户。 **注意：**要使用配给角色，CA CA Identity Manager 必须与配给服务器集成。有关应用程序服务器的信息，请参阅*《Installation Guide》*（《安装指南》）。
成为配给角色的管理员	使用户成为配给角色的管理员。 **注意：**要使用配给角色，CA CA Identity Manager 必须与配给服务器集成。有关应用程序服务器的信息，请参阅*《Installation Guide》*（《安装指南》）。
从组 <组名> 中删除 [...]	从组中删除用户。 选中此选项后，CA CA Identity Manager 将显示一个屏幕，您可以从中搜索所需的组。

更改操作	说明
从用户所在组织中的 <组名> 中删除	从本地组中删除用户。 选中此选项后，CA CA Identity Manager 将显示一个文本框，您可以从中输入所需组的名称。
从 <多值用户属性> 中删除 <值>	从多值用户属性中删除值。
从访问角色中删除成员	吊销访问角色。
从访问角色中删除管理员	吊销特定访问角色的管理员权限
从管理角色中删除成员	吊销管理角色。
从管理角色中删除管理员	吊销特定管理角色的管理员权限
从配给角色中删除成员	吊销配给角色。
从配给角色中删除管理员	吊销特定配给角色的管理员权限。
发送审核消息	将您创建的消息发送到审核数据库。 此消息可能会显示在您创建的报告中。
遵从违规	将您创建的消息发送到审核数据库。 如果创建了遵从报告，则此消息将在每次从用户中应用/删除身份策略时显示。 有关审核的详细信息，请参阅*《Configuration Guide》*（《配置指南》）。 **注意：**必须启用“身份策略集”的“配置文件”选项卡上的“遵从”复选框，才能使用“遵从违规”选项。
接受 （仅针对应用策略的操作）	当出现预防性身份策略违规时，允许任务提交。 在选择该操作时，提供一个消息，即 CA CA Identity Manager 在审核数据库中写入，并在违规发生时，显示在“查看提交的任务”中。

更改操作	说明
拒绝 （仅针对应用策略的操作）	在身份策略违规发生时，阻止任务提交。 该操作与预防性身份策略一起用于防止用户接收一些可能导致利益冲突或欺骗的权限。 在选择该操作时，也提供一个消息，即在违规发生时 CA CA Identity Manager 会显示。消息存储在审核数据库中并且显示在用户控制台中。
警告 （仅针对应用策略的操作）	如果您把该违规与工作流批准策略关联，那么在预防性身份策略违规发生时会触发工作流流程。 CA CA Identity Manager 允许任务提交，不管工作流是否已配置。 **注意：**有关将工作流流程与预防性身份策略关联的更多信息，请参阅“工作流和预防性身份策略 (p. 401)”。 在选择该操作时，也提供一个消息，即在违规发生时 CA CA Identity Manager 会显示。 消息存储在审核数据库中并且显示在“查看提交的任务”中。

更多信息：

预防性身份策略 (p. 396)
工作流和预防性身份策略 (p. 401)

指定身份策略集的所有者

在“所有者”选项卡上，可以定义关于谁可以成为身份策略集的所有者的规则。身份策略集的所有者可以修改关于策略集的基本信息，并可以添加、更改或删除策略集中的身份策略。

填写“所有者”选项卡：

1. 定义所有者规则，这些规则将确定哪些用户可以修改身份策略集。
2. 单击“提交”。

管理身份策略集

CA CA Identity Manager 包括以下用于管理身份策略集的任务：

- 查看身份策略集
- 修改身份策略集
- 删除身份策略集

默认情况下，当管理员使用其中一个任务时，CA CA Identity Manager 将显示其所有者为该管理员的所有身份策略集的列表。 然后，管理员可以从该列表中选择其所需的策略集。

在包括多个身份策略集的 Identity Manager 环境中，您可能希望自定义查看、修改及删除身份策略集任务，以允许管理员可以搜索身份策略集，而非将其显示在列表中。

自定义这些任务：

1. 在用户控制台中，依次选择“角色和任务”、“管理任务”、“修改管理任务”。

   此时将打开“修改管理任务”屏幕。
2. 搜索并选择您要自定义的任务。
3. 在“作用域”选项卡上，选择“所有身份策略集”。

   在您选择该选项时，CA CA Identity Manager 使用默认身份策略集搜索屏幕定义。
4. 单击“提交”。

用户和身份策略如何同步

使用身份策略时，了解 CA CA Identity Manager 如何评估策略及将策略应用到用户很重要。 如果对用户同步过程了解得不够透彻，则在配置身份策略集时可能会出现意外结果。

以下步骤说明了 CA CA Identity Manager 如何评估和应用身份策略：

1. 用户同步过程开始：
   - **自动** - 可以将 CA CA Identity Manager 任务配置为自动触发用户同步。
   - **手工** - 使用用户控制台中的“同步用户”任务来同步用户。
2. CA CA Identity Manager 确定应用到用户的身份策略集。

3. CA CA Identity Manager 将要应用到用户的身份策略集和已应用到该用户的策略列表进行比较。

   注意：已应用到用户的策略列表存储在用户配置文件中的已知属性 %IDENTITY_POLICY% 中。 有关配置此属性的信息，请参阅《*Configuration Guide*》。

   - 如果某一身份策略位于适用策略列表中，*且*该策略先前*未*应用到用户，则 CA CA Identity Manager 会将该策略添加到分配列表中。
   - 如果某一身份策略位于适用策略列表中，该策略先前已应用到用户，且该策略的“应用一次”设置处于禁用状态，则 CA CA Identity Manager 会将该策略添加到重新分配列表中。
   - 如果某一身份策略未在适用策略列表中，且该策略已应用到用户，则此用户将不再匹配策略条件。CA CA Identity Manager 会将这些策略添加到取消分配列表中。

4. CA CA Identity Manager 为用户评估所有策略后，将按以下顺序应用策略：
   a. 取消分配列表中的身份策略
   b. 分配列表中的身份策略
   c. 重新分配列表中的身份策略
5. 应用身份策略后，CA CA Identity Manager 将重新评估这些策略，以确定是否需要根据在第一次同步过程（步骤 2 至 4）中发生的更改进行任何其他更改。

   这有助于确保应用身份策略时所做的更改不会触发其他身份策略。
6. CA CA Identity Manager 会继续重新评估和应用身份策略，直到用户与所有适用策略同步，或者直到 CA CA Identity Manager 达到在管理控制台中定义的最大递归级别。

   例如，为用户分配角色时，某个身份策略可能会更改用户所在的部门。 新部门会触发另一个身份策略。 不过，如果递归级别设置为 1，则只有再次同步用户时，才会进行随后的更改。

   有关设置递归级别的详细信息，请参阅管理控制台在线帮助。

配置自动用户同步

CA CA Identity Manager 可以在任务周期内的不同时刻自动同步用户帐户和身份策略。

CA CA Identity Manager 任务可生成*事件*，即任务处理过程中出现的可检测到的活动。 例如，默认的“创建用户”任务可生成“创建用户事件”、“将用户添加到组事件”以及“分配访问角色事件”。可以将 CA CA Identity Manager 配置为在任务完成后或每个事件完成时同步用户。

注意：“同步用户与身份策略” (p. 389)一节提供了有关用户同步进程的详细信息。

配置任务以触发用户同步

1. 以可以修改管理任务的用户身份登录到 CA CA Identity Manager。
2. 依次选择“角色和任务”、“管理任务”、“修改管理任务”。

   CA CA Identity Manager 显示搜索屏幕。
3. 搜索并选择将触发用户同步的管理任务。
4. 为该任务选择“配置文件”选项卡的“用户同步”字段中的以下选项之一：
   - **关闭** — 此任务将不触发用户同步。
   - **任务完成时** - CA CA Identity Manager 在所有事件完成后开始用户同步过程。 此设置是“创建用户”、“修改用户”和“删除用户”任务的默认同步选项。 所有其他任务的默认设置为“关闭”。

     注意：如果为包括多个事件的任务选择了“任务完成时”选项，则 CA CA Identity Manager 在完成任务中的所有事件之后才同步用户。 如果其中一个或多个事件需要工作流批准，则可能需要几天时间。如果不想让 CA CA Identity Manager 等到所有事件完成才应用身份策略，请选择“每个事件时”选项。
   - **每个事件时** - CA CA Identity Manager 在任务中的每个事件完成之后开始用户同步过程。

     对于具有同一用户的主要事件和次要事件的任务，将用户同步设置为“每个事件时”所导致的对应用到用户的策略进行的评估，比选中“任务完成时”时进行的评估要多。

手工同步用户

您可能希望手工将用户与身份策略集同步，以确保用户帐户具有适当的权限或符合遵从策略。

可以通过使用 CA CA Identity Manager 用户控制台中的“同步用户”任务手工同步用户。

注意：为使“同步用户”任务正常运行，必须将“用户同步”选项设置为“关闭”且必须将“帐户同步”选项设置为“任务完成时”或“每个事件时”。为提高性能，请选择“任务完成时”选项。 在“同步用户”任务的“配置文件”选项卡上设置这些选项。

“同步用户”任务包括以下选项卡：

- **当前匹配的策略** - 显示身份策略列表，提交“同步用户”任务后，CA CA Identity Manager 会将这些策略应用到用户。

  注意：“当前匹配的策略”选项卡仅显示在访问“同步用户”任务时应用到用户的身份策略。 同步用户与这些策略后，可能会发生触发其他身份策略的更改。 为防止 CA CA Identity Manager 在您查看新策略之前应用这些策略，请在 CA CA Identity Manager 管理控制台中将身份策略的递归级别设置为 1。 提交“同步用户”任务后，再次访问该任务以查看策略。

- **策略已经应用** - 显示已应用到用户的身份策略列表。
- **同步摘要** - 显示所有应用到用户的身份策略以及对这些策略进行的更改操作。

同步用户帐户

1. 以可以使用“同步用户”任务的用户身份登录到 Identity Manager。（默认情况下，具有“系统管理员”角色的用户可以使用此任务。）
2. 依次选择“策略”、“同步用户”。

   将打开“同步用户”任务。
3. 选择“同步摘要”选项卡。
4. 查看 CA CA Identity Manager 将应用到用户的策略及相关联的操作，然后单击“提交”。

验证用户同步

要验证同步用户与身份策略后是否进行了相应的更改，请查看“同步用户”任务中的“策略已经应用”选项卡。

1. 以可以使用“同步用户”任务的用户身份登录到 CA CA Identity Manager。（默认情况下，具有“系统管理员”角色的用户可以使用此任务。）
2. 依次选择“策略”、“同步用户”。

   将打开“同步用户”任务。
3. 选择“策略已经应用”选项卡。
4. 查看 CA CA Identity Manager 已应用到用户的策略及相关联的操作。

Identity Manager 环境中的身份策略集

以下各节介绍了几种使用身份策略的不同方法：

- 示例：自动填充用户属性 (p. 392)
- 示例：分配资源和权利 (p. 393)
- 示例：强制遵从 (p. 394)
- 示例：强制职责隔离 (p. 395)

示例：自动填充用户属性

可以使用一个身份策略集，根据另一属性值或用户权限自动分配用户属性值。例如，您可以创建一个身份策略集，根据用户在家办公地点自动填写用户邮件地址。

要配置员工地址的身份策略集，请使用以下设置为每个办公室地点创建身份策略：

设置	值
策略条件	办公室 = <办公室位置>
应用策略时的操作	设置街道地址 = <某街道地址> 设置城市 = <某城市> 设置省/自治区/直辖市 = <某省/自治区/直辖市> 设置邮政编码 = <某邮政编码>

下图显示了“员工地址”身份策略集的策略示例。

身份策略

策略集

	策略名称	策略成员规则	应用策略时的操作
	Boston	其中 (Office = "Boston")	将 “Address” 设置为 “201路” 将 “City” 设置为 “Boston” 将 “State” 设置为 “MA” 将 “Postal code” 设置为 “02451”
	NY	其中 (Office = "NY")	将 “Address” 设置为 “601路” 将 “City” 设置为 “NY” 将 “State” 设置为 “NY” 将 “Postal code” 设置为 “10017”

示例：分配资源和权限

如果用户符合策略条件，则身份策略会自动分配资源（例如域帐户）或授予权限（例如使用户成为角色的成员）。 例如，您可以创建根据用户的职位分配资源和角色的身份策略集。

要创建分配资源和角色的身份策略集，请使用以下设置为您所在组织的每个职位创建身份策略：

设置	值
策略条件	职位 = <某职位>

设置	值
应用策略时的操作	向符合策略条件的用户分配资源或权限的任意操作，例如： ■ 成为 <某组> 的成员 ■ 成为管理角色 <某管理角色> 的成员 ■ 成为配给角色 <某配给角色> 的成员
针对删除策略的操作	当用户不再符合策略条件时，删除资源或权限的任意操作。例如，如果应用身份策略后，Identity Manager 使用户成为角色的成员，则您可能希望配置 Identity Manager 以在用户不再符合策略条件时吊销角色。

下图展示了“员工资源”身份策略集的策略示例：

身份策略

策略集

	策略名称	策略成员规则	应用策略时的操作	删除策略时的操作
	人力资源	其中（ Title = "人力资源" ）	成为管理角色 “UM ” 的成员 添加到组 “ UG ” 成为配给角色 “ UP” 的成员	从组 “UG ” 中删除 从管理角色 “UM ” 中删除成员 从配给角色 “UP ” 中删除成员
	管理者	其中（ Title = "管理者" ）	成为管理角色 “UM ” 的成员 成为配给角色 “ UP” 的成员	从管理角色 “UM ” 中删除成员

示例：强制遵从

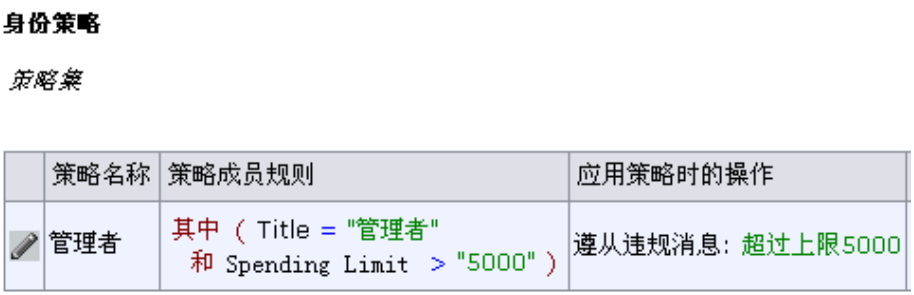
您可以配置身份策略以定义必须存在或必须不存在的条件，以及根据对这些条件的评估采取特定操作。例如，可以定义规定经理的财务开支限制为 5000 美元的遵从策略。如果经理的财务开支限制为 10000 美元，则 CA CA Identity Manager 可以重置经理的财务开支限制，并记录遵从违规以进行审核。

要创建强制财务开支限制的遵从策略，请使用以下设置创建身份策略：

设置	值
应用一次	未启用
遵从	已启用

设置	值
策略条件	定义遵从或遵从违规的任意条件，例如： 职位=<某职位> AND 财务开支限制 > <某财务开支限制>
应用策略时的操作	应用策略条件时 CA CA Identity Manager 应该执行的操作，例如： ■ 遵从违规消息：超出财务开支限制 ■ 将财务开支限制设置为 <某值>

下图显示了此例中介绍的遵从策略示例。



示例：强制职责隔离

身份策略可定义不能同时使用且不能同时授予同一用户的角色。 例如，可以防止有权加薪的用户经理同时成为工资批准人。

要创建强制职责隔离的身份策略集，请使用以下设置创建身份策略：

设置	值
应用一次	未启用
遵从	已启用
策略条件	使用“在 <管理交集限制>”选项定义违反业务策略的条件集合。 如果某一用户符合所有条件，则 Identity Manager 将执行“应用策略时的操作”字段中的操作。 例如，按如下所示设置策略条件： 交集（是 <某个角色> 的成员并且是 <某个其他角色> 的成员）

设置	值
应用策略时的操作	应用策略条件后，Identity Manager 应该执行的操作，例如： ■ 遵从违规消息：用户具有不可同时使用的角色 ■ 从 <某个角色> 删除成员

下图展示了此例中的身份策略。

预防性身份策略

*预防性身份策略*是一种身份策略，它会阻止用户接收可能会导致利益冲突或欺骗的权限。 这些策略支持公司的职责隔离 (SOD) 要求。

通过在提交任务之前执行的这些预防性身份策略，管理员可以在分配权限或更改配置文件属性之前检查策略违规。 如果违规存在，在提交任务之前，管理员可以清除违规。

例如，公司可以创建一个预防性身份策略，来阻止具有用户经理角色的用户同时具有用户批准人角色。 如果管理员使用修改用户任务为用户管理者提供用户批准人角色，CA Identity Manager 则会显示一条关于该违规的消息。管理员可以更改角色分配以便在提交任务之前清除该违规。

您可以针对下列更改创建预防性身份策略：

- **角色成员资格**

  防止用户同时拥有某些特定角色。

  例如，用户不能同时拥有用户经理和用户批准人角色。

- **角色管理员**

  如果某些用户是某些角色的管理员，防止这些用户成为其他角色的管理员。

  例如，用户不能同时是用户经理和用户批准人角色的管理员。

- **用户属性**

  防止用户同时拥有某些配置文件属性。

  例如，用户不能在具有高级客户职务的同时属于 IT 部门。

- **组织属性**

  防止在某个特定组织中创建用户配置文件。

  例如，管理员不能在供应商组织中创建员工配置文件。

- **组属性**

  防止用户成为某些组的成员。

  例如，用户不能同时是项目团队组和会计组的成员。

更多信息：

针对预防性身份策略违规的操作 (p. 397)

针对预防性身份策略违规的操作

当某个预防性身份策略应用于业务更改时，CA 将执行特定的操作以解决违规。

在身份策略中指定上述操作之一时，要指定一个描述违规的消息。 该消息将记录在审核数据库中。 根据操作类型的不同，该消息还可能在用户控制台中显示给用户，并记录到“查看提交的任务”中。

您可以为预防性身份策略配置以下操作：

接受

CA CA Identity Manager 在“查看提交的任务”中显示一条说明该违规的消息，但允许提交任务。

拒绝

CA CA Identity Manager 在用户控制台中显示一条消息并禁止任务提交。

警告

CA CA Identity Manager 在用户控制台和“查看提交的任务”中显示一条消息。 该操作可以触发一个工作流流程，要求获得相应用户的批准后，CA CA Identity Manager 才执行该任务。

要触发工作流流程，您要在可能导致违规的任务中将预防性身份策略与基于策略的工作流流程相关联 (p. 402)。

例如，如果在用户同时接收某些角色时发生违规，那么要为将那些角色分配给用户的所有任务配置工作流流程。

注意：当您为任务配置基于策略的工作流流程时，批准规则必须引用该预防性身份策略的名称。

预防性身份策略如何工作

下列示例演示了预防性身份策略的工作过程：

1. 身份策略管理员创建一个预防性身份策略，防止具有高级会计师职务的用户同时位于 IT 部门。

   定义该身份策略时，管理员指定 CA CA Identity Manager 应拒绝违反该策略的任何更改。

2. HR 管理员使用创建用户任务为一个新的高级会计师创建用户配置文件。 该 HR 管理员正确选择了该用户的职务，但错误选择了 IT 部门。

3. 该 HR 管理员在创建用户任务中完成剩余字段并单击“提交”。

4. CA CA Identity Manager 检测到该任务涉及在身份策略中定义的更改并将这些更改评估为违规。

5. CA CA Identity Manager 检测到违规，向 HR 管理员显示一条消息，并阻止任务提交。

   CA CA Identity Manager 还在审核数据库中记录该消息。

6. 该 HR 管理员在消息中查看违规的详细信息，并将用户的部门更改为财务。然后，该管理员重新提交该任务。

7. CA CA Identity Manager 针对所有合适的身份策略评估提请的更改，然后允许该创建用户任务提交。

关于预防性身份策略的重要说明

实施预防性身份策略之前，请注意以下内容：

- 预防性身份策略仅防止因为当前任务中的建议更改内容而将发生的违规。他们不防止现有的违规。

  例如，一个公司创建预防性身份策略，禁止用户同时拥有“用户管理者”和“用户批准人”角色。管理员将“组管理者”角色分配给已经有“用户管理者”和“用户批准人”角色的用户。 CA CA Identity Manager 允许新分配成功，因为该更改不直接引起策略的违规。

- 如果多个预防性身份策略应用于一套建议更改的内容，CA CA Identity Manager 首先会使用拒绝操作应用策略。

- 不要指定预防性身份策略条件中的动态组。（策略条件决定预防性身份策略应用于的用户集）。

  例如，公司有一个动态组，包括经理职位的所有用户。 该公司也创建了一个预防性身份策略，即禁止经理组的成员具有合同工角色。

  管理员将具有合同工角色的用户职位更改为经理。 任务成功提交*之后*，该更改将会使该用户成为经理组的成员。 然而，用户的职位在 CA CA Identity Manager 评估策略时不是经理，所以就不会检测出违规。
- 预防性身份策略的策略条件中不支持角色所有者筛选和 LDAP 查询筛选。

创建预防性身份策略

在您创建预防性身份策略之前，要创建身份策略集，即对身份策略集进行逻辑分组。

注意：开始之前，请参阅关于预防性身份策略的重要注意事项 (p. 398)。

创建预防性身份策略集

1. 在用户控制台中依次打开“策略”、“创建身份策略集”。

   新建一个身份策略集，或使用现有的身份策略集作为模板。
2. 为身份策略集定义配置文件 (p. 379)（位于“配置文件”选项卡）。
3. 创建策略集成员规则 (p. 380)（位于“策略”选项卡）。
4. 按照下列方式创建预防性身份策略：
   a. 单击“添加”。
   b. 输入身份策略的名称。

      注意：“应用一次”和“遵从性”设置不适用于预防性身份策略。
   c. 在“策略条件”区域中，标识策略应用到的用户。

      注意：角色所有者筛选和 LDAP 查询筛选不支持预防性身份策略。

d. 在“应用策略时的操作”字段中，定义 CA CA Identity Manager 在检测到策略违规时采取的操作：

接受

CA CA Identity Manager 在“查看提交的任务”中显示一条说明该违规的消息，但允许提交任务。

拒绝

CA CA Identity Manager 在用户控制台中显示一条消息并禁止任务提交。

警告

CA CA Identity Manager 在用户控制台和“查看提交的任务”中显示一条消息。 该操作可能会触发工作流流程 (p. 401)。

当您选择其中一个操作时，CA CA Identity Manager 会显示一个文本框，您可以在该框中指定发生违规时出现的消息。

e. 在文本框中指定消息。

注意：如果您正在用户控制台中进行本地化，则可以在该消息字段中指定资源键，来代替文本。有关资源键的详细信息，请参见《*User Console Design Guide*》。

f. 如果必要的话添加其他操作并单击“确定”。

5. 指定身份策略集的所有者 (p. 388)。

注意：必须首先在管理控制台中启用身份策略，才能使用创建的身份策略集。有关详细信息，请参阅《*Configuration Guide*》。

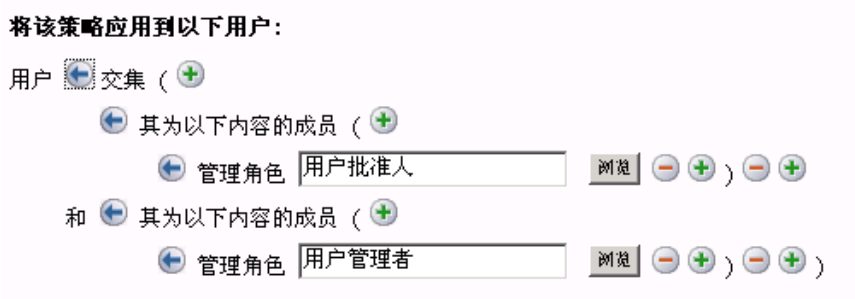
使用示例：防止用户拥有冲突角色

Forward, Inc. 想防止其员工同时拥有用户经理角色和用户批准人角色。同时具有这两个角色的员工会修改用户属性（如工资），并对其进行批准，而这都是不可取的。

为了防止这种情况，Forward, Inc. 创建了一个应用于具有用户经理和用户批准人角色的用户的预防性身份策略。 如果管理员为用户提供这两个角色，CA CA Identity Manager 则会拒绝任务提交并显示一个解释违规的消息。

您要按照下列方式对预防性身份策略进行配置以便支持该使用示例：

- 为要创建的策略创建一个身份策略集。
- 使用以下设置创建一个预防性身份策略：
  - 策略条件：



  - 应用策略时的操作：
    - 拒绝并显示消息：用户不能同时是用户批准人和用户经理角色的成员

工作流和预防性身份策略

如果预防性身份策略配置为发出警告，您则可以为可能触发违规的任务定义一个任务级基于策略的工作流流程，使其与该身份策略相关联。 例如，如果某个身份策略会阻止高级会计师成为 IT 部门成员，您则可以基于创建用户任务和修改用户任务定义一个任务级基于策略的工作流流程。

必须首先批准由于任务级基于策略的工作流生成的所有工作项，然后 CA CA Identity Manager 才能执行该任务。 批准人登录用户控制台后，会看到一个工作列表项。 批准人单击该工作列表项时，则会出现一个批准任务，其中包括说明该违规的警告消息。 批准人可以基于违规的情况选择批准或拒绝该任务。

基于策略的工作流流程按照策略名与预防性身份策略相关联。

更多信息：

基于策略的工作流 (p. 267)

批准任务中的身份策略违规

当任务的预防性身份策略与工作流流程关联时，CA CA Identity Manager 会为适当的批准人生成工作列表项。 这些批准人使用“批准任务”来批准或拒绝触发策略违规的更改。

默认的批准任务包括列出身份策略违规的部分。 如果建议更改的内容触发多个预防性身份策略，可能有一个以上的违规。

每个违规可以有下列状态：

- **未决评估**

  CA CA Identity Manager 还没开始评估任务的批准规则。 这是起始状态。

- **等待批准**

  CA CA Identity Manager 查找批准规则中定义的身份策略的匹配项目并触发关联的工作流流程。

- **已批准**

  批准人批准建议更改的内容。 CA CA Identity Manager 做出触发预防性身份策略违规的更改。

- **已拒绝**

  批准人拒绝建议更改的内容。 该任务被拒绝。

- **未配置工作流**

  没有为该违规配置工作流流程。该任务在没有任何所需批准的情况下执行。

如何为预防性身份策略配置工作流

您要在为包括可能触发身份策略违规的更改的管理任务中，为预防性身份策略配置工作流。

例如，如果预防性身份策略阻止用户同时具有某些特定管理角色，则将分配管理角色的任务配置为支持预防性身份策略的工作流。

注意：配置工作流之前，请使用下列设置创建预防性身份策略：

- 一个唯一的策略名称

  该策略名在所有身份策略集中都必须是唯一的，因为工作流流程按照策略名与预防性身份策略相关联。

  如果多个预防性身份策略具有相同的名称，则可能应用多个工作流流程。

- 应用策略时的操作字段中的警告

  警告是唯一能触发工作流流程的操作。

配置了预防性身份策略之后，您要确定可能触发策略违规的任务。 然后，为这些任务创建工作流批准策略 (p. 403)。

创建用于预防性身份策略的工作流批准策略

您可以为管理任务配置任务级的基于策略的工作流流程。 该工作流流程包括可以将预防性身份策略与工作流关联的一个或多个批准策略。 CA CA Identity Manager 在关联的预防性身份策略发生违规时执行该工作流。

注意：有关任务级别基于策略的工作流流程的详细信息，请参阅“基于策略工作流 (p. 267)”。

创建用于预防性身份策略的工作流批准策略

1. 修改管理任务，允许可能触发预防性身份策略违规的更改。

   例如，如果身份策略违规发生的原因是因为用户有“用户管理者”和“用户批准人”角色，则修改管理任务，允许管理员分配角色如“创建用户”、“修改用户”和“修改管理角色成员/管理员”。

2. 单击“配置文件”选项卡上“工作流流程”字段旁边的编辑图标，为任务添加工作流流程。

   CA CA Identity Manager 显示“任务级别工作流配置”屏幕。

3. 选择“基于策略”的，然后单击“添加”。

4. 在“批准规则”部分中，选择“身份策略违规”对象。

5. 在“身份策略”字段中，选择决定哪个身份策略触发与批准策略关联的工作流的筛选。

   在筛选中，包括身份策略名称，而*不*是身份策略集名称。

6. 需要时配置“规则评估”、“策略顺序”、“策略说明”字段。

7. 选择工作流流程，然后单击“确定”。

   当选择工作流流程时 CA CA Identity Manager 显示其他字段。

8. 指定所需的批准任务和批准人。

   CA CA Identity Manager 将工作流流程与预防性身份策略关联。

使用案例：批准职位

Forward, Inc 公司有这样一个公司策略，所有经理必须是全职员工。 然而，Forward, Inc 公司最近为特殊项目雇佣了许多合同工。要高效地运行这些特殊项目，就要给某些合同工“经理”的职位。Forward, Inc 公司要在允许管理员将“经理”职位分配给合同工之前，需要人力资源主管的批准。

为了将这些情况的批准流程自动化，Forward, Inc 公司创建名为“用于合同工的经理职位”的预防性身份策略，当用户职务为“经理”且组织为“合同工”时就会检测。Forward, Inc 公司也在“修改用户”任务上配置基于策略的批准流程。在违反“用于合同工的经理职位”的策略时，将触发该批准流程。

管理员将合同工的职位更改为“经理”时，CA CA Identity Manager 会显示警告消息并将工作项发送给人力资源主管进行批准。 CA CA Identity Manager 直到工作项被批准，才会更改合同工的职位。

要为这种情况配置支持，需要在 CA CA Identity Manager 中完成以下操作：

- 使用以下设置创建名为“用于合同工的经理职位”的预防性身份策略：
  - 策略条件：用户，其中（职位 = “经理”和组织 = “合同工”）
  - 应用策略的操作：出现“经理必须是全职员工”的警告消息
- 修改“修改用户”任务，以便在下列的设置中包括工作流流程：
  - 工作流流程：基于策略
  - 批准规则对象：身份策略违规
  - 身份策略：其中（名称 = “用于合同工的经理职位”)
  - 工作流流程：SingleStepApproval

组合身份策略和预防性身份策略

您可以将身份策略和预防性身份策略进行组合，以满足职责隔离 (SOD) 要求。这种情况下，身份策略解决现有的 SOD 违规，预防性身份策略则防止新的违规。

要支持这种使用情况，要对身份策略集配置两种类型的操作：

- 在用户同步期间发生的操作

  这些操作会导致用户属性、组和角色成员、管理员或所有者的更改。 例如，在检测到违规时，该类型的操作可能会从角色删除用户。

  这些操作不同于预防性操作，因为它们在提交任务后将不再适用。 它们仅在用户同步期 (p. 389)适用。

- 预防性操作

  这些操作决定在任务被提交*之前*，发生预防性身份策略违规时 CA CA Identity Manager 应执行的操作。CA CA Identity Manager 可以允许任务提交、发出警告并触发工作流流程，或阻止任务提交。

  在上述每种情况下，都会在审核数据库中记录该违规。

以一个公司为例，该公司想防止用户同时具有 HR 管理员和工资批准人角色。该公司创建了一个具有两个“应用策略时的操作”的身份策略：

- 从角色“工资批准人”中删除用户

  当 CA CA Identity Manager 将用户与身份策略进行同步时发生该操作。

  在这里，该公司为修改用户任配置了用户同步。当管理员修改用户时，CA CA Identity Manager 会评估所有合适的身份策略并应用操作。 在该示例中，CA CA Identity Manager 会从工资批准人角色中删除同时具有 HR 管理员角色和工资批准人角色的用户。

- 拒绝该任务

  该预防性操作会通过不允许管理员提交该任务，来阻止管理员为一个人分配两个角色。

注意：当您配置具有上述两种操作类型的身份策略时，请确认这两种操作不冲突。例如，您可以配置一个身份策略，来防止用户同时具有经理和临时工角色。在策略中，您指定两个操作：

- 一个是触发工作流流程的警告，该警告说明在分配角色之前需要批准，以及
- 一个从经理角色删除用户的操作

批准人批准经理和临时工角色的角色分配，但当发生用户同步时，第二个操作会将该用户从经理角色删除。

第 16 章： Policy Xpress

此部分包含以下主题：

Policy Xpress 概述

通过 Policy Xpress，您可以在 CA Identity Manager 中创建复杂的业务逻辑（策略），而无需开发自定义代码。 然而，创建 Policy Xpress 策略所涉及的概念却是复杂的，需要认真考虑和规划。 使用 CA Identity Manager 门户屏幕的管理员可以在 Policy Xpress 内配置要实施的策略，即使需要最复杂的业务逻辑也可实现。 当业务策略变更时，管理员可以在 CA Identity Manager 内使用配置屏幕来修改策略，而无需麻烦开发人员进行基础代码变更，更重要的是，通过适当的变更管理程序，无需重新启动 CA Identity Manager 服务。

注意：有关 Policy Xpress 的更多详细信息，请参见 Policy Xpress Wiki。

如何创建策略

要使用 Policy Xpress 创建策略，请定义策略的以下基本元素。

配置文件

定义策略类型和优先级，可以将相似策略分组，便于管理。

事件

定义策略运行的时间。

注意： 一定要小心设置事件的参数。 为防止数据损坏和性能增加，业务逻辑必须在特定时间运行。 例如，在创建用户时，应发生将用户设置成已启用的情况。 在所有时间运行此逻辑很可能会导致本应当禁用的用户帐户再次变成已启用。 另外一个示例，授予用户一个可以访问某个系统的配给角色。 仅将该角色在分配和批准其他角色之后分配给该用户。 在事件和业务逻辑任务处理程序处理的过程中，通过 Policy Xpress 可以激活其业务逻辑，此情况与自定义适配器十分类似。 因此，与身份策略不同，可以在任何时候触发该逻辑，不仅是在任务的开始。

数据（数据元素）

指定策略使用的数据。 每个类型的业务逻辑需要与某些数据共同使用。该数据可用于判定或者用于构建更复杂的数据。Policy Xpress 提供许多单个组件来收集数据。 这些组件被看作*数据元素*。 数据元素的示例，如用户的属性值。 例如，Policy Xpress 可以收集用户的名字并将其存储为数据元素供以后使用。

条目规则

定义在执行之前必须满足的要求。 通过定义条目规则您可以指定 Policy Xpress 评估策略的时间，这可以简化策略并能提高性能。 条目规则的示例，如*仅*在名字或姓氏已经更改时才运行“设置全名”的策略。

操作规则

根据所收集的信息定义采取的操作。 例如，根据用户的部门名称，Policy Xpress 可以将用户分配给不同的角色或指定不同的帐户值。

操作

指定要执行的操作。 在过程结束时，Policy Xpress 执行业务逻辑所需要的操作。 Policy Xpress 通过附加多个操作的一个操作规则来工作，因此当满足该规则时，就会执行操作。 操作可以包括将属性值分配给用户或帐户、执行命令行、运行 SQL 命令或生成新事件。

配置文件

Policy Xpress 策略的“配置文件”选项卡包含管理策略和优化策略功能的字段。

注意：策略仅应用于创建策略时所在的环境。 例如，如果当您登录 neteauto 环境时创建了一个策略，那么此策略仅针对 neteauto 环境运行。

在创建策略时提供下列配置文件信息：

策略名称

定义策略的唯一友好名称。

策略类型

定义触发策略的侦听程序 (p. 409)。 每个策略类型有不同的配置。

注意：您一旦保存了此策略就不得更改该字段。

类别

定义一组相关策略。 通过该字段您可以将策略分组便于管理。

说明

指定策略的说明。

优先级

如果多个策略在单一的事件中运行，那么该字段指定运行策略的时间。 根据优先级执行策略。 数字越小，优先级越高（优先级为 1 的首先运行，优先级为 10 的第二个运行，优先级为 50 的第三个运行，以此类推）。
设置优先级对于彼此有依存关系的策略或将一个复杂的策略拆分为两个简单的策略，运行完一个接着一个运行的情况时十分有用。
例如，有这样三个策略，在数据库中有特定值时才运行。 您可以创建一个在其他三个策略之前运行并检查值的策略，而不是让每个策略验证数据库中的值。 如果新策略匹配所需要的值，那么 Policy Xpress 可以设置变量。 只有设置了该变量，其他三个策略才运行，这可以防止多次访问数据库。

已启用

指定策略是否在 CA CA Identity Manager 中为活动状态。 如果想禁用策略而不删除它，您可以清除该复选框。

运行一次

指定策略是否仅运行一次。 某些策略可能需要在每次满足条件时就运行，而另外一些策略仅需要运行一次。 该值确定过去已经执行的操作规则是否应当再次执行。

例如，将 SAP 角色根据部门添加到用户就是这样一个操作，仅在该用户第一次匹配该部门时发生。 另外，*不*会将根据职称设置用户工资级别的策略设置为运行一次，这样可以确保不会发生未授权的更改。

注意： “运行一次”选项应用于对象，不会全局应用。

侦听程序

Policy Xpress 策略由系统中发生的情况来触发。为了实施该功能，与系统集成的侦听程序在事件发生时通知 Policy Xpress，并提供有关发生事件的详细信息。

存在以下侦听程序：

事件

侦听系统中每个事件和与该事件关联的所有状态（之前、已批准、已拒绝等等）。该侦听程序也把事件的名称报告给 Policy Xpress。 下列状态可用于事件侦听程序：

- 之前
- 已拒绝
- 已批准

- 之后
- 失败

UI

侦听同步状态过程中系统中运行的不同任务，即用户针对打开的任务仍然有用户界面。 下列状态可用于 UI 侦听程序：

- 启动 - 在任务开始时
- 设置主题 - 发现主要对象时
- 更改时验证 (p. 410) - 在属性（以“更改时验证”标志设置）更改时
- 提交时验证 - 在单击“提交”按钮时
- 提交 - 在提交任务时

工作流

侦听已经发现批准人的工作流进程。 侦听程序在基于批准人执行逻辑时十分有用，如给批准人发送电子邮件。

已提交任务

侦听未在后台运行的已提交任务。 然而，侦听程序与事件侦听程序相似，它将任务作为一个整体考虑，而不是任务的事件。 下列状态可用于已提交任务侦听程序：

- 任务已启动
- 任务已完成
- 任务失败

反向同步

侦听与 CA CA Identity Manager 浏览功能相关的系统中的通知。

屏幕上属性验证

除定义的触发器（策略类型）之外，Policy Xpress 也可以侦听属性的验证。 通过它您可以创建在已经标记为“更改时验证”的屏幕上属性更新时可以运行的策略。

该功能可用于创建依存下拉列表。 例如，如果在屏幕上有两个下拉列表，在选择第一个下拉选项时，Policy Xpress 会运行，然后会根据在第一个中所选的选项为第二个下拉列表设置值。 可以完成无限个下拉列表和其他屏幕的刷新。 这不同于选择框数据，它允许使用任何逻辑来填充下拉选项，而不是导入静态选项的 XML 文件。

其他用户根据一个属性值填充其他属性。 例如，当管理员选择部门时，Policy Xpress 可以自动填充其他属性，如部门经理、部门编号以及 HR 部门代码。 这取代了写入逻辑属性处理程序自定义代码的需求。

使用 Policy Xpress 策略配置验证

1. 在用户控制台中，修改任务的配置文件屏幕并选择要侦听的字段。
2. 访问字段的属性并针对“更改时验证”在下拉列表中选择“是”。
3. 在 Policy Xpress 中，创建类型为“UI (p. 409)”的策略。
4. 在“发生事件时运行”选项卡下，选择状态为“更改时验证”和您在第 1 步中修改的任务。

使用情况：检查冒犯性名称

在创建新用户时，您可能想检查用户名是否带有冒犯性。 以下过程说明如何使用 Policy Xpress 策略检查冒犯性名称。

1. 确保“创建用户任务的配置文件”屏幕上的相应字段已设置为“更改时验证 = 是”。
2. 在 Policy Xpress 中，创建类型为“UI”的策略。
3. 在“发生事件时运行”选项卡下，选择“更改时验证”状态和“创建用户”任务。
4. 创建以下数据元素来检查名字：
   - 获取名字属性（属性、用户属性、获取）
   - 将名字解析为所有小写字母（一般、字符串解析程序、到小写）
   - 在数据库表中检查名字是否有冒犯性（数据源、SQL 查询数据）
5. 如第 4 步的操作，创建相似数据元素来检查姓氏。
6. 创建操作规则如下：
   - 条件 - 名字不等于 ""（如果查询返回消息称名字具有冒犯性，则会发生）
   - 操作 - 显示的消息（消息、在屏幕上消息），表示冒犯性名字。

   该规则将强制用户在再次提交“创建用户”任务之前更改名字。
7. 如第 6 步的操作，创建姓氏的相似操作规则。

事件

根据“配置文件”选项卡上选择的策略类型，您可以在评估策略时配置要建立的激活时间。 例如，可以设置“事件”类型的策略在 CreateUserEvent 之前评估。 可以设置“任务”类型的策略在 DisableUserEvent 的设置主题时评估。

要配置激活时间，请选择以下字段：

省/自治区/直辖市

指定与激活策略的事件相关的时限或操作。 例如，可以将策略设置为在发生事件“之前”运行。

事件名称

指定激活策略的事件，如 CreateUserEvent。

策略可以有多个激活时间。 每当指定的激活时间（状态和事件）在系统发生时，Policy Xpress 就会搜索带有该激活时间的所有策略，并按照其顺序评估各个策略。

注意：如果策略与发生在系统中的激活时间匹配，这并不说明会自动运行该策略。 在过程中稍后评估的规则条件确定策略是否完成。

数据元素

数据元素用于创建策略数据。 策略可以包含表示策略使用的信息的多个数据元素。

Policy Xpress 使用灵活插件来收集数据元素信息。每个插件可以执行小的专门任务。 然而，一起使用几个插件可以建立更复杂的策略。 数据元素插件的示例如用户属性元素。 元素的目标是收集有关为用户配置文件一部分的某个属性的信息。

调用数据元素时会对数据元素进行计算，意味着规则正在使用数据元素或者需要计算的其他元素正在将数据元素用作参数。
例如，SQL 查询数据元素可以从表中检索值，但是它需要用户的部门来建立查询。在这种情况下，部门数据元素必须在 SQL 查询数据元素之前运行，然后值可用作参数 (p. 413)。

以下字段定义数据元素：

名称

定义说明数据元素的友好名称。 某些数据元素是复杂的（如获得变量或从数据库检索信息）。 一定要选择有意义的名称以简化数据元素管理。

类别

提供一组数据元素。 该字段对数据元素进行排序并便于选择。

类型

指定数据元素类型，每一个都是自身专用。 该字段是根据选定的类别而定。

函数

定义相同数据的可能变化。 多数数据元素仅支持“获取”函数。

例如，用户属性数据元素有以下函数：

- 获取 - 返回属性值
- 是多值 - 如果值为多值，则返回真
- 是逻辑属性 - 如果值为逻辑属性，则返回真

函数说明

提供函数的预填充说明。 选定的每个函数提供不同的说明以帮助理解其使用方法以及所期望的值。

参数

定义传递到数据元素的参数。 数据元素为动态且可以根据参数执行各种操作。 用户属性数据元素根据所选属性返回不同结果。 子类型选项也定义参数的数量、名称及可用的可选值。

如果必要的话，您可以添加其他参数。SQL 查询示例接受两个必需的参数，即数据源和查询本身。 查询可以使用“?”被替换成值（很象预定义语句）。 通过添加其他参数您可以设置那些值。

注意：在查看 Policy Xpress 中的数据元素时，有一名为“使用中”’的列。 选中该列意味着，数据元素由规则、操作参数或作为其他数据元素的参数使用。

使用数据或操作元素中的动态值

动态值是计算数据元素的结果，其值仅在运行时确定。 之后这些值可用作其他数据元素的参数（根据优先级随后算出）。

使用动态值作为数据元素的参数

1. 在“策略数据”选项卡中，找到要设置动态值的参数。
2. 在空文本字段中，输入任何常规的文本或从右边的下拉列表中选择动态值。
3. 单击“确定”。

变量

Policy Xpress 具有与操作一起设置并保存为数据元素（变量类别）的变量。变量在同一时间运行的所有策略中共享，因此可以通过较低优先级的其他策略使用已经设置的变量。

例如，变量可以包含由策略计算一次的值，然后与不再需要重新计算值的其他策略共享。 初始策略将值设置为变量，稍后运行的策略通过使用与参数相同的变量名的数据元素来读取该值。

变量对于其他策略而言也可为触发器。 在这种情况下，这些策略仅在他们之前的策略已经运行时才运行。

条目规则

条目规则为策略应运行的时间定义条件。 这些条件使用由策略中的数据元素收集的值。

策略中可以有多个条目规则，而条目规则也可以有多个条件。 至少必须匹配一个条目规则，即必须满足针对策略的该条目规则中的*所有*条件才可进入到操作规则。

下列字段定义条目规则：

名称

提供条目规则的友好名称。

说明

定义条目规则的含义。

条件

指定要匹配的条件。

注意：条目规则中的条件总是在他们之间有“AND”操作符。

更多信息：

条件 (p. 414)

条件

条件用于条目规则和操作规则，并且包含以下组件：

- 策略数据
- 操作符
- 值

例如，要创建检查用户部门是否已更改的一个条件。 首先，定义“部门已更改”的数据元素，然后，在条件中选择“部门已更改”的数据元素，再将操作符设置为“等于”，并将值设置为“真”。

更多信息：

条目规则 (p. 414)
操作规则 (p. 415)

操作规则

操作规则在结构上类似于条目规则，但在功能方面却有所不同。 操作规则定义采取操作的时间。 例如，如果希望策略在用户的部门更改为销售时执行操作，则创建定义“部门 = 销售”时的操作规则。

此外，可能会匹配多个操作规则，而不是必须匹配一个条目规则。 带有最高优先级的单个规则（0 为最高优先级）是*唯*一一个被使用的。

操作规则也包含一个或多个操作，且操作分为“增加操作”和“删除操作”。

下列字段定义操作规则：

名称

提供操作规则的友好名称。 该名称必须唯一。

说明

定义操作规则的含义。

条件

指定要匹配的条件。

优先级

定义在多个操作规则匹配的情况下要执行哪个操作规则。 该字段在定义默认操作时十分有用。 例如，如果您有多个规则，每一个规则为一个部门名称，则可以通过添加没有条件但为较低优先级（如 10，而其他优先级是 5）的其他规则来设置默认值。如果不匹配任何部门的规则，那么将使用默认值。

添加操作

在匹配规则时定义采取的操作列表。 例如，您可以配置这样一个规则，如果用户的部门与条件中配置的规则匹配，则添加特定的 Active Directory 组。操作规则根据“运行一次”的设置，会有不同的行为。如果将策略设置为“运行一次”，那么在首次规则匹配时执行相关联的操作。 对于各后续的规则匹配，则不会再次执行这些操作。 在以上的示例中，仅将 Active Directory 组添加到该用户一次。 如果没有设置“运行一次”，那么只要匹配规则，操作就会再次运行。 该字段对于执行值十分重要。

删除操作

在规则不再匹配时，定义要执行的操作列表。 例如，在前面的示例中，根据部门将 Active Directory 组添加到用户中。 如果该部门更改，那么删除操作会删除 Active Directory 组。

更多信息：

条件 (p. 414)

操作

在所有决定操作完成后，操作会执行业务逻辑。 操作是以与数据元素相似的方式执行，只是在结尾时不同。 操作运行时，它执行任务，而不是返回值。

注意：运行操作的顺序是按照在用户控制台中出现的顺序执行。

以下字段定义操作：

操作名称

定义操作的目的。

类别

提供一组操作。 该字段对操作进行排序，便于选择。

类型和函数

定义采取操作的类型和函数。

注意：有关类型和函数的详细信息，请参阅“数据”。

函数说明

提供函数的预填充说明。 选定的每个函数提供不同的说明以帮助理解其使用方法以及所期望的值。

参数

定义传递到操作的参数。

流控制

默认情况下，策略按照优先级排序，然后逐个评估。 当该流通常总是应用时，必要时，您可以更改流。

此流更改功能由可以附加于任何操作规则的操作来表示。 流更改功能位于操作的“系统”类别下。

重要说明！ 更改流时，请小心使用。 使用这些操作可能导致无限循环。 例如，如果不带任何条件对操作规则设置了“重做当前策略”，那么该规则将总为真，且策略将总是重新启动，从不退出。

可以使用以下四个流更改功能：

停止处理

导致将忽略当前策略之后的所有策略，并导致 Policy Xpress 退出。
注意：仅 Policy Xpress 退出。 如果也想强制 CA CA Identity Manager 停止，则可以使用“异常”类型操作插件。

重新启动所有策略

停止处理剩下的策略并回到列表的开始。 在一个策略的操作导致其他策略（在其之前运行但并未执行）现在满足输入标准的情况下，该选项十分有用。 现在重新评估该策略。

重做当前策略

导致策略再次运行。 该选项对迭代十分有用。 例如，创建唯一用户名需要策略一次次运行，直到找到唯一名称。

转到特定策略

该操作需要选择现有策略。 如果该策略与当前策略同时运行（可在之前或之后），Policy Xpress 则会跳到选定的策略。 如果新策略优先级较低，会忽略当前策略和选定策略之间的所有策略。 如果新策略优先级较高，则回到该过程。

注意：因为操作可能导致 Policy Xpress 跳过某些策略，所以请小心使用该操作类型。

设置与帐户关联的对象

在创建添加操作设置与帐户关联的对象时，如“成员”，特定的关系格式将用于表示对象。 以下二种类型的格式可以表示 CA CA Identity Manager 中的对象：

- 要表示对象和帐户之间的简单关系，如 Active Directory 组：
  `NativeGroup=Administrators,Container=Builtin,EndPoint=LocalAD,Namespace=ActiveDirectory,Domain=im,Server=Server`
- 要表示对象和帐户之间的绑定关系，如 SAP 角色：
  `{"validFromDate":"2009\/12\/01","roleName":"SAPRole=SAP_AUDITOR_ADMIN,EndPoint=sap endpoint,Namespace=SAP R3,Domain=im,Server=Server","validToDate":"2009\/12\/31"}`

  绑定关系不同于简单的关系，因为对象和帐户之间的关联有其他数据。 在前一个示例中，参数 validFromDate 和 validToDate 仅包含与该关联（帐户和 SAP 角色之间）相关的数据。 validFromDate 和 validToDate 数据不存在于帐户或角色对象中。

要识别关系格式，请创建“获取”对象值的数据元素。 返回值的格式为设置该对象的“添加操作”中使用的格式。

示例：Active Directory 组

1. 使用以下设置创建 Policy Xpress 策略：
   - 策略类型：事件
   - 事件：之后 - 修改用户
2. 在操作规则中，配置以下添加操作：
   - 类别：属性
   - 类型：设置帐户数据
   - 函数：设置
   - 终端类型：Active Directory
   - 端点：*端点_名称*
   - 帐户名称：*帐户*
   - 属性：(groupMembership) 的成员
   - 值：
     NativeGroup=Administrators,Container=Builtin,Endpoint=*endpoint_name*,
     Namespace=ActiveDirectory,Domain=im,Server=Server

高级

Policy Xpress 可用于多种配置变化，还可与外部组件交互。 由于这种灵活性，错误可能会发生，但未必是缺陷，如错误配置了数据源，从动态数据元素返回一个缺少值，或是没响应的端点。

通常在错误发生时，系统将停止当前步骤的策略计算。 然而，您可以根据错误的类别来更改默认错误响应。 例如，如果您有非关键的策略，您可以定义为在错误事件中继续处理。

通过“高级”选项卡，您可以在必要时更改默认的错误响应。

注意：我们建议保持这些错误响应的默认值，但对于高级的使用情况，可以根据策略更改这些设置。 例如，如果您有非关键的策略，您可以定义为尽管策略失败也继续处理。

可以在选项卡中配置以下错误类别：

- 验证 - 通过向插件提供不正确信息引发。 在尝试操作之前报告这种错误类型。
- 环境 - 由环境中的问题引发，如用于 SQL 插件的失败数据库服务器。
- 允许 - 非严重错误。该错误类型的默认行为是继续处理请求，如在发送电子邮件失败时。

对于每个先前的错误，可以设置下列选项：

- 失败事件 - 停止当前操作。 这是多数错误类型的默认情况。
- 失败策略 - 停止当前和与其关联的所有操作。 剩余的策略继续。
- 忽略 - 记录失败，但不停止操作或策略。

第 17 章： CA Identity Manager 移动应用程序

CA Identity Manager 移动应用程序使您能够利用现有的 CA Identity Manager 基础架构，以便允许用户在移动设备（如智能手机或平板电脑）中完成以下任务：

- 重置已遗忘的密码
- 更改密码
- 通过接受或者拒绝批准请求对其进行响应。 使用用户控制台可以保留或发布请求。
- 查看用户信息

  此功能允许用户在该组织中查看其他用户的信息。 例如，工作项批准人在作出批准决定之前可以查看用户的经理（如姓名和地址）的基本信息。 如果需要更多信息，批准人可以单击链接以查看完整的配置文件。

此部分包含以下主题：

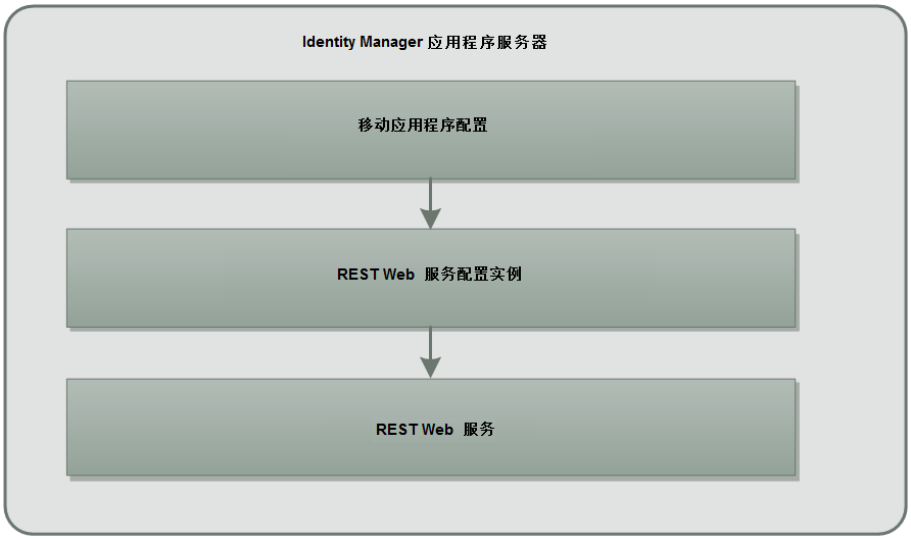
CA Identity Manager 移动应用程序体系结构

CA Identity Manager 移动应用程序体系结构旨在向各种移动设备（如智能手机和平板电脑）提供一组 CA Identity Manager 功能。 为移动应用程序选择的功能取决于关键业务需求以及用户交互适用于小型设备的移动设备。

体系结构中心是使用展示 CA Identity Manager 服务器功能的应用程序和 RESTful Web 服务所特有的配置组件。 CA Identity Manager 服务器能够管理给定环境的移动应用程序配置以及应用程序使用的 REST Web 服务配置。

注意： REST Web 服务是 CA Identity Manager 移动应用程序所特有的，与基于 SOAP 的任务执行 Web 服务 (TEWS) 不同，不计划将其用作公共 API。

REST Web 服务的每个 CA Identity Manager 环境 (IME) 可以支持多种配置，每种配置通常与特定 REST 客户端（如移动应用程序）相关联。 高级体系结构以及移动应用程序配置和 Web 服务配置之间的关系如下所示。



REST Web 服务配置需要选择一组特定选项，以便移动应用程序正常运行。 在创建移动应用程序配置之前，必须通过 Web 服务配置任务定义 Web 服务配置，也可以通过管理任务进行定义。

移动应用程序 Web 服务配置详细信息

REST Web 服务配置包括以下元素：

- 定义唯一配置名称、标识符和启用标志的配置文件。
- 定义使用 SSL、负载加密和加密密钥的安全配置。
- 一组管理对象类型以及每种类型通过 REST 支持的操作和属性。
- 支持的自助服务操作（如重置密码）和允许的一组用户自助服务属性。
- 用户有权对其调用已配置的 REST 操作的成员策略。

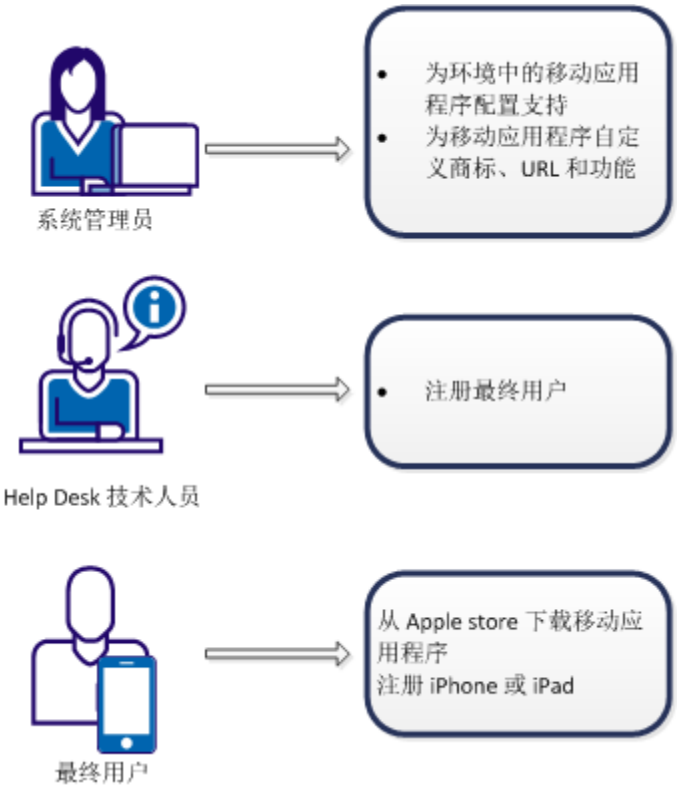
下表显示 Web 服务配置详细信息和移动应用程序所需的设置。

配置部分	项目	说明	移动应用程序设置
配置文件	名称	配置的名称	部署选项
	标识符	给定客户端必须在每个 CA Identity Manager 服务器请求的“配置 ID”http 头中设置的唯一标识符。	部署选项。移动应用程序配置服务返回必须用于所有后续 REST 请求的标识符。
	已启用	启用/禁用配置	True
安全	需要安全通信	是否需要 http	部署选项。移动应用程序配置服务下载的值。
	启用加密	用于为非 SSL 加密负载。需要客户端加密库、加密密钥知识和显式客户端加密/解密支持。	未使用。保持未选中。
	配置密钥	需要作为 REST 客户端到服务器信任模型一部分的共享密钥。	必须指定。 部署应在定义配置实例时生成密钥。
对象类型	对象类型	作为 REST 资源公开的对象类型。	用户对象类型

	方法和属性	选定对象类型支持的资源方法 (CRUD) 以及这些方法允许的一组属性。	可以查看访问部署特定用户架构中的下列属性的用户对象类型： ■ 办公电话 ■ 部门 ■ 电子邮件 ■ 名字 ■ 姓氏 ■ 管理者 ■ 办公室 ■ 标题
自我管理	成员规则	指出哪些用户可以执行自我管理的规则。	应该与移动应用程序配置上的成员规则匹配。 要修改的一组属性应为空。
	启用密码重置	支持用户重置其自己的密码	启用
	属性	用户可以自己管理的一组属性	空列表
成员	成员	定义用户有权调用为此配置定义的 REST 操作的规则	与一组移动应用程序用户匹配的成员规则

实施过程的工作方式

设置移动应用程序涉及到三类用户。 下列图形说明这些用户类型以及他们执行的任务。



要使最终用户能够将移动应用程序与 CA Identity Manager 结合使用，必须完成以下工作：

1. 系统管理员配置对环境中的移动应用程序的支持。

   配置涉及以下活动：

   - 配置激活和重置代码属性
   - 为注册移动用户添加任务、Policy Xpress 策略和电子邮件模板
   - 创建 Web 服务定义
   - 修改注册电子邮件。

   系统管理员还需要配置商标、URL 和移动用户能够访问的功能。

2. 管理员（如帮助台技术员）可在用户控制台中注册适当的最终用户。

   注册过程可为每个最终用户触发激活代码，并自动地将包含代码和注册说明的电子邮件发送给最终用户。

3. 最终用户可从 Apple 商店下载移动应用程序，并使用他们收到的电子邮件中的说明和代码来注册设备（如智能手机或平板电脑）。

   最终用户之后可以使用移动应用程序来访问 CA Identity Manager 功能。

   注意：如果在用户创建期间选择“密码必须更改”选项，那么移动应用程序用户则无法完成激活。

应用程序配置的工作原理

移动应用程序从 CA Identity Manager 服务器配置 API 检索其配置。 移动应用程序首次安装且没有下载任何配置时，系统将提示用户输入用户名和密码，并使用这些凭据通过用户注册电子邮件中提供的链接下载定义的配置。

下载初始配置之后，每次启动应用程序时，都会将其与 CA Identity Manager 服务器上提供的最新版本进行比较。 配置版本检查 API 用于检测是否存在可用的后期版本。

用户注册的工作原理

希望获得移动应用程序访问权限的每位用户必须在 CA Identity Manager 中请求访问权限。如果批准访问，用户将更新为具有激活代码（表示已授予访问权限）。移动应用程序配置成员策略和基础 Web 服务成员策略应满足为请求访问权限的移动用户定义的任何条件。 “注册”值至少需要定义为 %ACTCODE% 或大于 0。

如果删除用户的移动访问权限，CA Identity Manager 服务器将重置激活属性并阻止用户访问该移动应用程序。

如何配置 CA Identity Manager 以支持移动应用程序

移动应用程序通过与 CA Identity Manager 通讯（使用 REST Web 服务）可管理密码和审批。 要启用此通信，系统管理员应完成下列步骤：

1. 配置必要的属性 (p. 427)。
2. 导入管理任务。 (p. 430)
3. 创建 Web 服务 (p. 431)。
4. 修改注册电子邮件 (p. 432)。
5. （可选）为移动应用程序配置 SiteMinder 支持。

配置必要的属性

CA Identity Manager 用户存储必须包括以下已知属性，以实现用户注册以及通过移动应用程序访问：

- %ACTCODE%－识别存储随机生成的激活码的属性。 注册用户之后，此属性包含注册的词。
- %ACTCODEVAL%－识别存储客户端在注册期间设置的激活代码的属性。 CA Identity Manager 将此值与 %ACTCODE% 的值进行比较。
- %CURRENT_AUTH_QUESTIONS%－识别临时存储质询问题值的属性。用户正确回答后，系统将清除此值。
- %MOBILE_PIN%－识别存储个人标识号或字符串值的属性，其中提供用户和系统之间共享的字母数字密码，可用于对登录系统的用户进行身份验证。
- %PWRESETCODE%－识别存储加密代码的属性，在密码重置期间提供单因素身份验证

您将这些已知属性映射到目录配置文件 (directory.xml) 中可用的用户存储属性。如果没有可用的属性，请扩展用户存储架构。 有关扩展架构的更多信息，请参阅用户存储的文档。

在属性说明中包括以下数据分类：

<DataClassification name="sensitive"/>

将重置代码值替换为任务屏幕、审核记录和系统日志中的通配符。

重要说明！ 不要在 %ACTCODE% 属性定义中包括敏感数据分类。 如果包括敏感属性，移动应用程序则不会正常工作。

<DataClassification name=" AttributeLevelEncrypt "/>

使用定义的加密密钥，从用户存储被写入和读取时，会加密和解码重置代码值。

<DataClassification name=" ignore_on_copy "/>

使 CA Identity Manager 在管理员于用户控制台中创建对象的副本时忽略某属性。

注意：有关这些常用属性的示例，请参阅本主题的结尾部分。

遵循这些步骤:

1. 登录到管理控制台。
2. 选择“Directories”（目录），然后单击包含移动用户的目录。
3. 导出该目录。
4. 添加或修改属性说明以包括 %ACTCODE% 已知属性。

   您可以将任何可用属性映射到 %ACTCODE% 常用属性。
5. 重复第 4 步，以便定义 %ACTCODEVAL% 常用属性。 包括以下数据分类：
   `<DataClassification name="sensitive"/>`

```
<DataClassification name="ignore_on_copy"/>
<DataClassification name=" AttributeLevelEncrypt"/>
```

6. 添加 %CURRENT_AUTH_QUESTIONS% 常用属性的属性说明。包括以下数据分类：

```
<DataClassification name="ignore_on_copy"/>
```

7. 添加 %MOBILE_PIN% 常用属性的属性说明。 包括以下数据分类：

```
<DataClassification name="sensitive"/>
<DataClassification name="ignore_on_copy"/>
<DataClassification name=" AttributeLevelEncrypt"/>
```

8. 添加 %PWRESETCODE% 已知属性的属性描述。 包括以下数据分类：

```
<DataClassification name="sensitive"/>
<DataClassification name="ignore_on_copy"/>
<DataClassification name=" AttributeLevelEncrypt"/>
```

9. 保存 directory.xml 文件。
10. 在管理控制台的“Directory Properties”（目录属性）页面中，单击“Update”（更新）以加载之前保存的 directory.xml 文件。

示例

注意：您可以将任何可用属性映射到这些常用属性。

%ACTCODE%

```
<ImsManagedObjectAttr
physicalname="attribute_name"
displayname="your_attribute_display_name"
description="your_attribute_description"
valuetype="String"
required="false"
multivalued="false"
wellknown="%ACTCODE%"
maxlength="0"
hidden="true"
system="true">
    <DataClassification name="ignore_on_copy"/>
    <DataClassification name=" AttributeLevelEncrypt"/>
    </ImsManagedObjectAttr>
```

%ACTCODEVAL%

```
ImsManagedObjectAttr
physicalname="attribute_name"
displayname="your_attribute_display_name"
description="your_attribute_description"
valuetype="String"
required="false"
multivalued="false"
wellknown="%ACTCODEVAL%"
```

```
    maxlength="0"
    hidden="true"
    system="true">
        <DataClassification name="ignore_on_copy"/>
        <DataClassification name=" AttributeLevelEncrypt"/>
        </ImsManagedObjectAttr>
```

%CURRENT_AUTH_QUESTIONS%

```
    <ImsManagedObjectAttr
    physicalname="attribute_name"
    displayname="your_attribute_display_name"
    description="your_attribute_description"
    valuetype="String"
    required="false"
    multivalued="false"
    wellknown="%CURRENT_AUTH_QUESTIONS%"
    maxlength="0"
    hidden="true"
    system="true">
        <DataClassification name="ignore_on_copy"/>
```

%MOBILE_PIN%

```
    <ImsManagedObjectAttr
    physicalname="attribute_name"
    displayname="your_attribute_display_name"
    description="your_attribute_description"
    valuetype="String"
    required="false"
    multivalued="false"
    wellknown="%MOBILE_PIN%"
    maxlength="0"
    hidden="true"
    system="true">
        <DataClassification name="ignore_on_copy"/>
        <DataClassification name=" AttributeLevelEncrypt"/>
        </ImsManagedObjectAttr>
```

%PWRESETCODE%

```
    <ImsManagedObjectAttr
    physicalname="attribute_name"
    displayname="your_attribute_display_name"
    description="your_attribute_description"
    valuetype="String"
    required="false"
    multivalued="false"
    wellknown="%PWRESETCODE%"
    maxlength="0"
    hidden="true"
```

```
system="true">
    <DataClassification name="ignore_on_copy"/>
    <DataClassification name=" AttributeLevelEncrypt"/>
    </ImsManagedObjectAttr>
```

导入管理任务

管理员在“用户控制台”中注册移动用户后，移动用户才能登录到 CA Identity Manager。 注册过程生成一个激活代码并通过电子邮件发送给移动用户。

要支持这些活动，请将添加了以下功能的角色定义文件导入到环境中：

- 移动配置任务
- 注册移动应用程序用户以及从移动应用程序任务中删除用户
- 生成激活代码，并注销用户帐户的移动客户端的 Policy Xpress 策略。
- 用于将电子邮件发送到移动用户的电子邮件模板

遵循这些步骤:

1. 登录到管理控制台。
2. 选择“Environments”（环境），然后单击支持移动应用程序的环境。
3. 选择“Role and Task Settings”（角色和任务设置），然后在下一屏上单击“Import”（导入）。
4. 选择“MobileApp-RoleDefinitions”（移动应用程序-角色定义），然后单击“Finish”（完成）。
5. 重新启动环境。
6. 将以下任务添加到系统管理员角色中：
   - 创建移动配置
   - 修改移动配置
   - 查看移动配置
   - 删除移动配置
   - 注册移动应用程序的用户
   - 从移动应用程序中删除用户

   新的任务在“用户”和“系统”类别中。

创建 Web 服务配置

移动应用程序使用 REST Web 服务来与 CA Identity Manager 通讯。要支持移动应用程序，系统管理员应在用户控制台中创建 Web 服务定义。

注意：如果启用 Web 服务配置中的加密，REST 调用则不会起作用。

遵循这些步骤:

1. 以具有系统管理员权限的用户身份登录到“用户控制台”。
2. 按照以下所述创建 Web 服务定义：
   a. 依次导航到“系统”、“Web 服务”、“创建 Web 服务配置”。
   b. 在“配置文件”选项卡上，填写下列字段：
      - 名称：*任何名称*。例如：RestMobile
      - 标识符：*唯一的标识符*。默认值为“RestMobile”。

        “标识符”字段的值必须与移动应用程序配置的**“restid”**的值匹配。

        请考虑更改“标识符”和 restid 的值以增强安全性。
      - 启用属性：请选中此复选框。
   c. 在“安全”选项卡上，填写下列内容：
      - 确定是否需要选择“需要安全通信”选项：

   注意：请考虑加密所有移动应用程序 http 流量。 通常，可以通过两种方式配置此流量：

      - 使用代理服务器进行通信：在此用例中，CA Identity Manager 服务器将位于防火墙后面。 您可能决定不保护代理服务器到 CA Identity Manager 服务器的通信的安全。 但是，应确保移动应用程序与代理服务器之间的 http 通信的安全。 对于此用例，不选择“需要安全通信”。

   注意：如果不集成 CA Identity Manager 和 SiteMinder，请选择“需要安全通信”选项，以便为 Web 服务调用保留 SSL 通信。

      - 直接与 CA Identity Manager 服务器进行通信：在此用例中，移动客户端直接与 CA Identity Manager 服务器进行通信；应对此 http 通信进行加密。 要强制实施此要求，请选择“需要安全通信”选项。
      - 确认是否没有选择“启用加密”。

   注意：如果启用加密，用户详细信息则不会在移动应用程序中显示。

   d. 在“对象类型”选项卡上，浏览“用户”，选择“用户”，然后单击“编辑”按钮。
   e. 选择仅允许查看访问。

      通过清除“允许修改访问”、“允许创建访问”和“允许删除访问”选项来删除其他访问权限。

f. 在“自我管理”选项卡上，完成下列步骤：
   - 选择“成员规则”下面的“添加”按钮来创建成员角色并指定“全部”。

     注意：您只能创建一个成员规则。
   - “启用密码重置”在移动应用程序中支持“更改密码”功能

g. 在“成员”选项卡上，使用下列条件来构建成员规则：
   - Activation Code = Registered，或者
   - Activation Code >0

h. 提交并保存 Web 服务。

修改注册电子邮件

编辑默认注册电子邮件以包括移动配置对象的 URL。

遵循这些步骤:

1. 在用户控制台中，依次导航到“系统”、“电子邮件”、“修改电子邮件”。
2. 搜索并选择“Registered User for Mobile App”（已注册的移动应用程序用户）电子邮件。
3. 在“Content”（内容）选项卡上，单击“Toggle HTML Source”（切换 HTML 源）按钮。
4. 在 href 条目中为 mobileregservidm 指定移动配置对象的 URL，方法如下：

   ```
   <a
   href="mobileregservidm://{'Attribute:%ACTCODE%'}&amp;https://FQN/iam/im
   /ws/Alias/mobile/ConfigName">
   ```

   FQN

   指定 CA Identity Manager 服务器 的名称或 IP 地址。

   Alias

   指定环境名称。

   ConfigName

   指定配置对象的名称。
5. 单击“提交”。

如何为移动应用程序配置 SiteMinder 支持

移动应用程序所使用的 Web 服务可以使用移动应用程序通过 HTTP AUTHORIZATION 头或 SiteMinder 身份验证传递的用户名/密码凭据，支持本地身份验证。正如前面所讨论的，Web 服务配置定义每个 REST 资源和方法请求的授权策略。

IM REST Web 服务 URL

IM REST 服务依赖于以下基本 URL：

`http[s]://[FQN]/iam/im/ws/[别名]`

- FQN－CA Identity Manager 服务器访问点的完全限定名和端口。
- 别名－要连接到的 CA Identity Manager 环境的公共别名。

移动应用程序配置 URL

移动应用程序配置包含特定 URL，允许检索下载移动应用程序配置所需的 bootstrap 配置信息。 配置 URL 如下所示：

`http[s]://[FQN]/iam/im/ws/[别名]/mobile/[配置名称]`

配置名称－一组给定移动应用程序用户的 CA Identity Manager 环境的移动应用程序配置名称。 通过在批准用户访问移动应用程序的请求时发送的注册电子邮件中的配置 URL 链接，向应用程序公布配置名称。

未身份验证的 REST API

配置 API

下列配置 API 不需要身份验证。

`http[s]://[FQN]/iam/im/ws/[别名]/mobile/[配置名称]/image`
`http[s]://[FQN]/iam/im/ws/[别名]/mobile/[配置名称]/ver`

重置密码 API

`https://[FQN]/iam/im/ws/[别名]/myself/resetpasswordWithResetCodeAndToken`

注意：resetPasswordWithResetCodeAndToken API 包含通过 http 头传递的来自移动应用程序的安全令牌。 CA Identity Manager 服务器验证这些令牌是否存在及有效。

在与 SiteMinder 集成以保护 CA Identity Manager 访问权限时，可以使用不受保护或使用匿名身份验证方案保护的领域定义这些 URL。

已身份验证的 REST API

移动应用程序使用的下列 URL 需要使用 Web 服务配置授权策略进行身份验证。

配置

`http[s]://[FQN]/iam/im/ws/[别名]/mobile/[配置名称]/conf`

自助服务用户
`http[s]://[FQN]/iam/im/ws/[别名]/myself`

工作列表
`http[s]://[FQN]/iam/im/ws/[别名]/worklist`

用户
`http[s]://[FQN]/iam/im/ws/[别名]/mo/User`

配置移动应用程序

系统管理员在用户控制台中配置 CA Identity Manager 移动应用程序。

环境可以包括多个移动的应用程序配置。 创建不同配置允许您为不同类型的移动用户支持不同的商标或功能。 例如，您可以为员工密码更改创建一个配置，为经理批准工作项创建另外一个配置。

管理员可以为移动应用程序配置以下属性：

- 商标

  指定移动应用程序中的公司徽标。
- 功能

  启用下列功能：
  - 已遗忘密码支持
  - 更改密码支持
  - 工作流审批队列
  - 显示管理员链接
- 支持信息
- 属性映射

  将用户存储中的属性映射到在移动应用程序中可见的属性。

遵循这些步骤:

1. 作为可以使用移动配置任务的用户，登录用户控制台。
2. 依次单击“任务”、“系统”、“移动配置”、“创建移动配置”。
3. 接受默认的选项，“创建类型为“移动配置”的新对象”。
4. 在“一般”选项卡上，完成必填字段： 您可以为移动应用程序指定图像。

   基本 URL

   验证当前环境的基本 URL。 在您创建移动配置时，自动填充基本 URL。

   CA Identity Manager 使用基本 URL 来检索服务器名称、端口和协议，移动应用程序使用这些构建 REST 调用的 URL。

   配置

   浏览配置或输入唯一的配置名称。

   版本

   每次在您修改和保存配置时，增加版本号。

   移动应用程序使用版本号来决定何时下载配置的新版本。在移动应用程序启动时，它将服务器的版本号与加载的配置的版本进行比较。 如果新版本可用，那么移动应用程序则更新配置。

   注意：请不要在首次修改此文件时增加版本号。

   商标图像

   指定带有透明背景的 PNG 图像的完整 URL。该图像在移动应用程序中的屏幕顶端显示。

5. 在“功能”选项卡上，选择移动应用程序的功能。

   密码重置行为

   选择用于此行为的方法，在您配置必需属性时确定此方法：

   - 默认
   - PIN 质询
   - QnA 质询

   注意：如果您选择“QnA 质询”，您必须转到“任务”、“环境管理员”，然后选择“问题和答案配置”。 确保选中“启用”框，输入身份验证问题（1 到 5）的数字，然后单击“提交”。 您必须点击“提交”按钮使得配置设置生效，即使您没有对默认设置做任何的更改。

6. 在“支持”选项卡上，指定移动用户的支持信息。

7. 在“属性映射”选项卡上，将移动应用程序映射到 CA Identity Manager 用户存储中的属性。 您可以将这些属性映射到物理属性或已知属性。
8. 在“其他属性”选项卡上，指定其他属性值对，以便在移动应用程序中支持新的功能或字段。

   使用以下格式：

   键 1=值 1

   键 2=值 2

   键 3=值 3

   注意：在管理员需要添加其他属性时，CA Technologies 将提供说明。 在此版本中，您不需要指定任何其他属性。
9. 在“成员”选项卡上，指定规则，这些规则确定在移动应用程序上查看此配置的用户集。
10. 单击“提交”。

配置其他属性

配置移动应用程序之后，可以选择指定其他属性键值对，以便在移动应用程序中支持新功能。 使用“其他属性”选项卡执行此操作。

使用以下格式：

- demoMode="Disable/Enable"
- maxPinRetries=<任意正数值>
- multiAccount="Disable/Enable"
- managerTraversal="Disable/Enable"
- startupWithBrandLogo="true/false"

注意：在管理员需要添加其他属性时，CA Technologies 将提供说明。

但是，默认情况下移动配置启用这五项功能：

- DemoMode：允许您查看移动应用程序的演示版。 移动应用程序的“设置”部分提供此选项。
- maxPinRetries：允许管理员为移动用户配置错误或失败的 PIN 条目尝试次数。 失败尝试次数的默认值为 5。
- MultiAccount：允许您添加多个帐户，主要是通过添加多个已注册的移动用户及其激活代码。
- ManagerTraversal：在工作项详细信息中显示批准人和请求人的管理员详细信息。
- startupWithBrandLogo：允许用户指定要显示的自定义帐户徽标（帐户的商标图像），而非默认的 CA 徽标。 如果此键值设为 true，但出于某些原因，品牌徽标字段为空或包含无效 url，则启动时启动屏幕将保留为空白。 应用程序在安装后首次启动时，都会显示 CA 徽标。该属性是帐户数据的一部分，首次启动时没有可用的帐户数据。
  注意：仅在成功与 CA Identity Manager 服务器进行通信之后，在后续启动中才反映这些更改。

您必须在 CA Identity Manager 移动配置的“其他属性”选项卡中添加以下键值对，以便在移动客户端禁用这些功能。

- 启用或禁用 DemoMode 功能

  将 DemoMode 设置为“启用”或“禁用”

  - demoMode="Disable/Enable"
- 启用或禁用 maxPinRetries 功能

  将 maxPinRetries 设置为任意正数值

  - maxPinRetries=<任意正数值> 注意：失败尝试次数的默认值为 5。
- 启用或禁用 MultiAccount 功能

将 MultiAccount 设置为“启用”或“禁用”

- multiAccount="Disable/Enable"

- 启用或禁用 ManagerTraversal 功能

  将 ManagerTraversal 设置为“启用”或“禁用”

  - managerTraversal="Disable/Enable"

- 启用或禁用 startupWithBrandLogo 功能

  将 startupWithBrandLogo 设置为 true 或 false

  - startupWithBrandLogo="true/false"

遵循这些步骤:

1. 以管理员（超级用户）身份登录到 CA Identity Manager 用户控制台。
2. 依次单击“任务”、“系统”、“移动配置”、“创建移动配置”。
3. 在“其他属性”选项卡上，指定其他属性键值对，以便在移动应用程序中支持新功能。
   - demoMode="Disable/Enable"
   - maxPinRetries=<任意正数值> 失败尝试次数的默认值为 5。
   - multiAccount="Disable/Enable"
   - managerTraversal="Disable/Enable"
   - startupWithBrandLogo="true/false"

下载移动应用程序

一旦配置移动应用程序，最终用户可以从 Apple 商店下载它。 要在 Apple 商店中找到移动应用程序，请搜索“CA Identity Manager”。

通过使用最终用户在电子邮件中接收到的说明和代码，最终用户可以注册他们的设备，如智能手机或平板电脑。

移动应用程序故障排除

允许支持人员请求日志文件

如果用户在使用移动应用程序时遇到问题，支持工程师可以请求获取日志文件以帮助排除故障。

移动用户需要在其 iPhone 或 iPad 中启用调试。一旦启用了调试，移动用户便能使用移动应用程序，将日志发送至提供支持的电子邮件地址。

要使移动应用程序能够生成日志，移动用户需要完成下列步骤。

1. 在 iPhone 或 iPad 上，依次导航到“设置”、“Identity Manager”、“调试”。
2. 点击“已启用”。
3. 重新启动应用程序，然后执行需要显示在日志中的操作。
4. 在 CA Identity Manager 移动应用程序的“设置”选项卡上，点击“电子邮件日志”。

   移动应用程序创建以日志文件作为附件的电子邮件。 该电子邮件可发送到在用户控制台中为提供支持配置的电子邮件地址。

在 Identity Manager 任务的环境管理员下，使用默认问答配置设置的 QnA“重置密码行为”失败。

症状

在选择使用默认的“问题和答案配置”设置的 QnA“重置密码行为”时，重置密码失败，并显示以下错误消息：

“错误 [im.webservices.QuestionAndAnswerResource] (http-/0.0.0.0:8443-1) 无法处理获取用户凭据问题。 消息: 服务器日志文件中出现 java.lang.NullPointerException”

解决方案：

执行下列步骤，通过 QnA“重置密码行为”重置密码：

遵循这些步骤:

1. 以 SuperAdmin 身份登录到 CA Identity Manager。
2. 导航到“任务”、“环境管理员”，然后选择“问答配置”。
3. 单击“提交”按钮。

   注意：即使是“启用”选项和“身份验证问题数”的默认值，也仅在执行此步骤之后应用。

第 18 章： CA 用户活动报告

此部分包含以下主题：

CA Enterprise Log Manager 功能

CA Enterprise Log Manager 与 CA Identity Manager 集成时，您可获得以下功能：

- CA Enterprise Log Manager 代理收集 CA Identity Manager 审核信息，并且将它发送至 CA Enterprise Log Manager，以转换为 CA Common Event Grammar (CEG)。
- 借助用来筛选返回信息的 CA Identity Manager 上下文信息，CA Identity Manager 用户控制台可以无缝检索 CA Enterprise Log Manager 报告和/或查询。
- CA Identity Manager 附带了大量默认报告和基础架构，可用来将 CA Enterprise Log Manager 报告和/或查询添加到现有的或新的任务中。
- CA Enterprise Log Manager 代理安装在 CA Identity Manager [审核数据库] 计算机上
- CA Identity Manager Connector 在 CA Enterprise Log Manager 代理上配置
- 已创建 Identity Manager 环境的 CA Enterprise Log Manager 产品注册
- 已为产品注册创建可选的 CA Enterprise Log Manager 数据访问筛选器

CA Enterprise Log Manager 组件

在 CA CA Identity Manager 与 CA Enterprise Log Manager 集成时，下列组件将添加到 CA Identity Manager 体系结构：

- “CA Elm Viewer”选项卡使您可以在任何新的或现有的任务中嵌入 CA Enterprise Log Manager 对象。

  注意：必须配置 CA Enterprise Log Manager 服务器连接。
- 能够导入的角色定义

集成限制

以下是与 CA Enterprise Log Managers 服务器的框架集成的已知的限制：

- 在运行时检索任务配置的查询和报告可能会降低运行速度。
- CA Enterprise Log Manager API 只能识别默认的 Java 命名的时区。
- 在用于复合筛选器时，EQUAL 运算是区分大小写的。
- CA Enterprise Log Manager 服务器的最低版本是 CA ELM 服务器 (45.10)，并按推出顺序应用了以下订阅更新：
  1. SP-1 订阅修补程序
  2. M5 内容修补程序
  3. Open API 更新
- 只支持同时与 CA Enterprise Log Manager 服务器建立一个连接。

如何将 CA Enterprise Log Manager 与 CA CA Identity Manager 集成

管理员执行以下操作后，您才可以查看和管理 CA Enterprise Log Manager 报告和查询：

1. 安装 CA Enterprise Log Manager 代理
2. 创建新的连接器。
3. 在 CA CA Identity Manager 中启用审核。
4. 配置 CA Enterprise Log Manager 服务器

CA Enterprise Log Manager 代理安装先决条件

完成以下操作后，才能安装 CA Enterprise Log Manager 代理：

- 确保运行 CA CA Identity Manager 或托管 CA Identity Manager 审核数据库的计算机可以访问 CA Enterprise Log Manager 服务器计算机。
- 确保服务器计算机可以访问代理计算机。
- 配置代理计算机上的数据源。 单击此处 (p. 443)可以获得相关说明。
- 确认 Adobe Flash Player 的版本为 9.0.28 或更高。 您可以从以下网址下载：

  http://www.adobe.com/go/getflash
- 下载代理二进制文件。 单击此处 (p. 443)可以获得相关说明。
- 获得代理身份验证密钥。 单击此处 (p. 444)可以获得相关说明。
- 使服务器名称/IP 易于访问
- 使帐户信息易于访问，但不危害安全。 这是代理作为服务 (Windows) 运行的身份帐户。
- 如果连接器已经存在，导出默认连接器信息并使其易于使用。
- 确保计算机有 4 GB RAM。

配置代理计算机上的数据源

按照此过程配置代理计算机上的数据源。

配置数据源

1. 依次导航到“控制面板”、“管理工具”、“数据源 (ODBC)”
2. 从“系统 DSN”选项卡上，添加以下内容：

   指向审核数据库的 imsauditevent12 数据源 (ODBC)。
3. 单击“应用”或“确定”。

   数据源配置完成。

下载代理二进制文件

按照此过程下载代理二进制文件。

下载代理二进制文件

1. 使用以下 URL 登录到 CA Enterprise Log Manager 服务器：

   https://<host>:5250/spin/calm/CALMSpindle.csp
2. 依次导航到“管理”、“日志收集”、“代理资源管理器”、“下载代理二进制文件”、<OS> <版本>
3. 保存到文件。

获取代理身份验证密钥

使用此过程来获取代理身份验证密钥。

获取代理身份验证密钥

1. 从 CA Enterprise Log Manager 服务器依次导航到“管理”、“日志收集”、“代理资源管理器”、“代理身份验证密钥”。
2. 使密钥易于访问，但不危害安全。

安装 CA Enterprise Log Manager 代理

CA Enterprise Log Manager 代理负责收集事件和将该信息分派到 CA Enterprise Log Manager 服务器。在 CA Identity Manager 数据库服务器或端点计算机上安装该代理，以启用记录功能。

注意：Windows 和 Linux 支持 CA Enterprise Log Manager 代理。

安装 CA Enterprise Log Manager 代理

1. 在数据库服务器上，运行 ca-elmagent-<版本>.exe 安装程序并指定以下内容：

   CA Enterprise Log Manager 服务器名称/IP 地址和身份验证代码。

   用来运行该代理（作为服务/后台进程）的代理服务器帐户信息。
2. 指定默认连接器列表文件（如果可用）。
3. 使用以下 URL 登录到 CA Enterprise Log Manager 服务器：

   https://<host> :5250/spin/calm/CALMSpindle.csp
4. 依次导航到“管理”、“日志收集”、“代理资源管理器”、“默认代理组”
5. 选择代理计算机，并启动“状态和命令”视图。

   此时，状态应在运行。

导入角色定义

您必须首先导入 CA Enterprise 角色定义，然后才能在用户控制台中配置企业日志管理器连接。

导入角色定义：

1. 使用以下 URL 登录到管理控制台：

   `http://host:port/iam/immanage`
2. 导航到“Environment”（环境）、“Role and Task Settings”（角色和任务设置），单击“Import”（导入）按钮，并选择“Enterprise Log Manager - Enterprise Log Manager Role Definitions.xml”。
3. 单击“Save and Close”（保存并关闭）。
4. 在用户控制台的“系统”选项卡中，单击“配置企业日志管理器连接”，然后填写必要的信息并单击“提交”。

创建新的连接器

按照此过程创建新的连接器。

创建新的连接器

1. 使用以下 URL 登录到 CA Enterprise Log Manager 服务器：

   `https://<host> :5250/spin/calm/CALMSpindle.csp`

2. 依次导航到“管理”、“日志收集”、“代理资源管理器”、“默认代理组”
3. 选择代理计算机。
4. 切换到“连接器”视图。
5. 单击“创建新的连接器”按钮并输入以下信息：

   连接器详细信息

   选择“集成类型 CAIdentityManager”，并根据需要更改连接器名称。

   连接器配置

   连接字符串

   - Driver={SQL Server} ; Server=<Auditing DB Server> ; Database=<Auditing DB>
   - Driver={Microsoft ODBC for Oracle} ; Dbq=<Auditing DB TNSname>

   用户名：<审核数据库用户>

   密码：<审核数据库用户密码>

6. 将以下连接配置更改应用到 CA Identity Manager 连接器，以与 12.6.4 一起使用。

   - SourceName：代理计算机上的数据源名称 - imsauditevent12
   - AnchorSQL：select max(id) from imsauditevent12
   - AnchorField：IMS_EVENTID
   - EventSQL：

```
select imsauditevent12.id as IMS_EVENtid ,imsauditevent12.audit_time as
IMS_AUDITTIME ,imsauditevent12.envname as ENVNAME
,imsauditevent12.admin_name as
ADMINUNIQUENAME ,imsauditevent12.admin_dn as
ADMINID ,imsauditevent12.tasksession_oid as TRANSACTIONID
,imsauditevent12.event_description as
EVENTINFO ,imsauditevent12.event_state as
EVENTSTATE ,imsauditevent12.tasksession_oid as TASKOID
,imsaudittasksession12.task_name as
TASKNAME ,imsauditeventobject12.object_type as OBJECTTYPE ,
imsauditeventobject12.object_name as
OBJECTUNIQUENAME ,imsauditobjectattributes12.attribute_name as
ATTRNAME ,imsauditobjectattributes12.attribute_oldvalue as ATTROLDVALUE
```

```
,imsauditobjectattributes12.attribute_newvalue as
ATTRNEWVALUE ,imsauditobjectattributes12.attribute_newvalue as
ATTRVALUE from
imsauditTasksession12, imsauditevent12, imsauditeventobject12,
imsauditobjectattributes12 where imsauditevent12.id >? and
imsauditevent12.tasksession_id = imsauditTasksession12.id and
imsauditevent12.tasksession_oid =
imsauditTasksession12.tasksession_oid and
imsauditeventobject12.parent_event_id = imsauditevent12.id and
imsauditobjectattributes12.parent_object_id = imsauditeventobject12.id
ORDER BY
imsauditevent12.id ASC;
```

7. 保存并关闭。

验证连接器是否正在工作

1. 依次导航到“管理”、“日志收集”、“代理资源管理器”、“默认代理组”
2. 选择代理计算机
3. 切换到“连接器”视图，然后单击“Launch Status and Command View”（启动状态和命令视图）按钮。

   此时，状态应在运行。

在 CA Identity Manager 中启用审核

在 CA Identity Manager 中启用审核

1. 打开管理控制台

   http://host:port//iam/immanage

2. 依次导航到“Environments”（环境）、“<Environment>”、“Advanced Setting”（高级设置）、“Auditing”（审核）。

3. 导出现有设置并保存文件。

4. 按照以下内容修改保存的文件并保存修改：

   - <Audit enabled="true" auditlevel="BOTH" datasource="auditDbDataSource"
   - 在已经定义的最后一个审核配置文件下为密码策略添加审核配置文件：

     <AuditProfile objecttype="FWPASSWORDPOLICY" auditlevel="BOTHCHANGED"/>

5. 将文件导回至管理控制台中，并执行以下任一任务来触发审核信息的汇总：

   - 在用户管理的对象上执行的任务
   - 在组管理的对象上执行的任务
   - 在密码策略管理的对象上执行的任务

6. 使用以下 URL 登录到 CA Enterprise Log Manager 服务器：

   https://<host> : 5250/spin/calm/CALMSpindle.csp

7. 要演练现有报告，请依次导航到“查询和报告”、“查询”、“CA Identity Manager”

   注意：您必须已经配置了 Enterprise Log Manager 服务器。

8. 根据您已经执行的任务，打开以下默认报告验证即将发生的事件：

   - 系统所有事件（按用户）任务调用按用户 ID 筛选的“CA Identity Manager－系统所有事件”
   - “帐户管理（按主机）”任务按原样调用“帐户管理（按主机）”
   - “帐户创建（按帐户）”任务按原样调用“帐户创建（按帐户）”
   - “帐户删除（按帐户）”任务按原样调用“帐户删除（按帐户）”
   - “帐户锁定（按帐户）”任务按原样调用“帐户锁定（按帐户）”
   - “认证过程活动（按主机）”任务按原样调用“CA Identity Manager－过程活动（按主机）”
   - “密码策略修改活动”任务按原样调用“CA Identity Manager－策略修改活动”

配置 CA Enterprise Log Manager 服务器

在配置要管理的 CA Enterprise Log Manager 服务器前，请确保满足以下条件：

- 您必须拥有 EiamAdmin 凭据
- 您必须安装了 Adobe Flash Play 版本 9.0.28 或更高版本。

配置 CA Enterprise Log Manager 服务器后，即可使用以下功能：

- 单个 CA Enterprise Log Manager 服务器或联合层级结构使用多个生成审核事件的环境。
- 通过 CA Enterprise Log Manager 的数据访问筛选器可以实施远程系统的数据授权。

配置 CA Enterprise Log Manager 服务器

1. 通过以下 URL 使用 CA Enterprise Log Manager 管理员凭据登录到 CA Enterprise Log Manager 服务器产品注册页：

   `https://host:port/spin/calmapi/products.csp`

2. 单击“注册”按钮，并提供证书名称和密码，注册您的 CA Identity Manager 环境。

   注意：每个环境都有单独的注册（证书名称/密码）对。

3. 依次导航到“管理”、“用户和访问管理”、“New Data Access Filter”（新数据访问筛选器），提供要创建的筛选器的名称。
4. 进入下一步。
5. 在“所有身份”下保留所选择的身份，然后进入下一步。
6. 单击“新事件筛选器”按钮，创建访问筛选器。

   配置“数据访问”筛选，将针对计算机/环境创建的证书限制为只用于从 CA CA Identity Manager 收集的日志。 您也可以将证书限制为仅访问管理端点的本地端点信息。

7. 保存并关闭。
8. 单击“Open Access Policies”（打开访问策略）按钮，打开访问策略。
9. 选择“Obligation Policies”（责任策略），然后单击可用的单个策略。
10. 删除“所有身份”并且添加证书名称。
11. 保存策略。
12. 登录 Identity Manager 用户控制台，并且配置“企业日志管理连接”。

配置 Enterprise Log Manager 连接

使用该屏幕可以管理新添加的 CA Enterprise Log Manager 连接任务。

该屏幕上的字段如下所列：

连接名称

指定用于单个 CA ELM 连接管理对象的唯一名称。

这是一个只读字段。

说明

对 CA ELM 连接作出说明。

主机名

指定 CA Enterprise Log Manager 服务器的主机名或 IP 地址。

这是必填字段。

端口号

指定 CA Enterprise Log Manager 服务器的连接端口。

默认值：52520

这是必填字段。

认证机构签署的 SSL 证书

选中后，指定了连接到 CA Enterprise Log Manager 服务器时要执行严格的 SSL 证书检查。

如果您有自签名的 SSL 证书（例如，默认情况下与 CA Enterprise Log Manager 一起安装的证书），则不能选中该复选框，这是因为根证书机构的信任路径不存在。

证书名称

指定 CA Enterprise Log Manager 进行身份验证的证书名称。

这是必填字段。

证书密码

指定 CA Enterprise Log Manager 密码。

这是必填字段。

属性

不支持。 尝试将连接信息保存为测试时会检索版本。

删除企业日志管理器连接

从列表中选择连接，然后单击“删除”。 CA Enterprise Log Manager 连接任务已删除。

将其他 CA Enterprise Log Manager 报告或查询与 CA Identity Manager 相集成

您可以使用“企业日志管理器查看器”选项卡，将其他 CA Enterprise Log Manager 报告或查询与 CA Identity Manager 相集成。 这些新报告或查询可以与现有的任务（包括向导）和新任务相结合。 需要时还可包含 CA Enterprise Log Manager 联合数据。 使用“企业日志管理器查看”选项卡，您可以将筛选应用于检索的信息。 这些筛选可以使用：

- 常数值
- 管理对象的属性
  - 例如，物理一::MyPhysicalAttribute::

    逻辑一::|MyLogicalAttribute|::
- 任何字段（如 CA Enterprise Log Manager Common Event Grammar (CEG) 所描述）
  - dest_username
  - dest_objectname
  - dest_uid
  - source_username
  - source_objectname
  - source_uid
  - ...

配置 Enterprise Log Manager 查看器选项卡

配置 CA Enterprise Log Manager 查看器选项卡上是否显示以下任何或全部字段：

名称

您分配给选项卡的名称。

标签

任务中唯一的选项卡标识符。 它必须以字母或下划线开头，并且仅包含字母、数字或下划线。 该标签主要用于通过 XML 文档或 HTTP 参数设置数据值。

隐藏选项卡

使选项卡在任务中不可见。 该选项对于需要隐藏选项卡但仍可访问选项卡上属性的应用程序很有用。

Enterprise Log Manager 查询

指定要显示 CA Enterprise Log Manager 查询。

注意：您可以指定 CA Enterprise Log Manager 查询或者 CA Enterprise Log Manager 报表，但不能两者都指定。

Enterprise Log Manager 报表

指定要显示 CA Enterprise Log Manager 报表。

注意：您可以指定 CA Enterprise Log Manager 查询或者 CA Enterprise Log Manager 报表，但不能两者都指定。

Enterprise Log Manager ID

指定查询或报表的 ID。

包括联合数据

在结果中包含还是排除 CA Enterprise Log Manager 联合数据。默认情况下，此字段是选中的。

显示提示符

指定仅显示 CA Enterprise Log Manager 提示查询。默认情况下，此字段是选中的。

筛选

指定用于缩小 CA Enterprise Log Manager 查询或报表返回结果范围的基于 SQL 的高级条件。 可以包括常量值和动态值。 下面是一个表达式示例：

```
((source_uid EQUAL ::logical.attribute.X:: ) AND (source_username
EQUAL ::logical.attribute.Y:: ))
```

支持的运算包括：

- equals (EQUAL)

- not equals (NEQ)
- less (LESS)
- greater (GREATER)
- less or equals (LEQ)
- greater or equals (GREATEQ)
- like (LIKE)
- not like (NOTLIKE)
- in set (INSET)
- not in set (NOTINSET)

支持的连接符包括：

- AND
- OR

圆括号是强制的。 如果条件表达式中左边的值两端没有“::”标记，则该值将被认为是常量，将原样发送到 CA Enterprise Log Manager。

参数/值表

指定将用于范围确定的字段和值。

只有匹配范围确定标记和标记逻辑的查询或报表会被选择。

参数

指定开始、结束和限制参数的值。 支持下列参数：

- 时间粒度 (仅趋势)
- 开始时间
- 结束时间
- 最早分组事件的日期晚于 (仅针对分组查询)
- 最新分组事件的日期晚于 (仅针对分组查询)
- 最新分组事件的日期早于 (仅针对分组查询)
- 分组中的事件最小数 (仅针对分组查询)
- 分组中的事件最大数 (仅针对分组查询)

第 19 章： 访问角色

访问角色提供另一种在 CA Identity Manager 或其他应用程序中提供权利的方式。例如，您可使用访问角色来完成下列任务：

- 提供对用户属性的间接访问
- 创建复杂的表达式
- 在用户配置文件中设置一个属性，另一个应用程序使用该属性来确定权利

访问角色与身份策略类似，也是将一组业务更改应用到用户或用户组。 然而，在使用访问角色来应用业务更改时，您可以通过查看访问角色的成员看到更改应用到哪些用户。

在大多数情况下，访问角色不与任务关联。

注意：当 CA Identity Manager 与 CA SiteMinder 集成时，访问角色还可提供对受 CA SiteMinder 保护的应用程序的访问。 在这种情况下，访问角色确实包括访问任务。 有关详细信息，请参阅《*Configuration Guide*》中有关 SiteMinder 集成的章节。

此部分包含以下主题：

访问角色如何管理权利

您可以使用访问角色通过指定更改操作来管理权利，作为角色的成员或管理员添加或删除用户时会发生。

要使用访问角色，要完成以下步骤：

1. 管理员创建访问角色。
2. 在“成员”选项卡上，管理员指定添加或删除操作，确定在将访问角色分配给用户时 CA Identity Manager 采取的操作。
3. 管理员根据需要指定管理员和所有者策略，然后提交任务以创建访问角色。
4. 访问角色管理员将访问角色分配给用户。
5. CA Identity Manager 完成角色中指定的添加操作。

示例：间接配置文件属性修改

您可以使用访问角色在用户的配置文件中间接更改属性。 例如，公司可能不允许任何用户直接更改其他用户的职位。 在管理员将该角色分配给用户之后，该公司可以创建更改职位的访问角色。

要间接更改属性，需要为访问角色设置更改操作。 管理员分配角色时，更改操作可使一个或多个更改成为用户配置文件的属性。

要使用访问角色间接修改属性，请执行以下操作：

1. 创建访问角色。
2. 在“成员”选项卡上，选择“管理员可添加或删除该角色的成员”复选框，然后单击箭头图标。

   CA Identity Manager 显示其他添加操作和删除操作字段。
3. 在“添加操作”或“删除操作”字段中，从列表框中选择一项操作。

   基于选定的选项，CA Identity Manager 显示其他字段。
4. 根据需要配置添加或删除操作。
5. 选择“管理员”选项卡，指定可以将成员添加到正在创建的访问角色的管理员。
6. 选择“所有者”选项卡，指定可以修改访问角色定义的管理员。
7. 单击“提交”完成访问角色的创建。
8. 根据需要将访问角色分配给用户。

创建访问角色

要创建访问角色，需执行以下步骤：

- 开始创建访问角色 (p. 454)
- 定义访问角色的配置文件 (p. 455)
- 为访问角色定义成员策略 (p. 455)
- 为访问角色定义管理员策略 (p. 455)
- 为访问角色定义所有者规则 (p. 456)

开始创建访问角色

1. 以承担创建访问角色任务的角色，登录到 Identity Manager 帐户。

2. 依次单击“访问角色”->“创建访问角色”。

   选择可创建新角色或角色副本的选项。 如果选择“复制”，将搜索角色。

3. 继续执行下一部分“定义访问角色的配置文件”。

定义访问角色的配置文件

定义访问角色的配置文件

1. 输入名称、说明并完成为角色定义的所有自定义属性。

   注意：可以在“配置文件”选项卡指定自定义属性，以便用于指定访问角色的有关附加信息。 可以使用这些附加信息帮助在含有很多角色的环境中进行角色搜索。

2. 如果想要在创建角色之后即使其可用，请选择“已启用”。

3. 继续执行下一部分“为访问角色定义成员策略” (p. 455)。

为访问角色定义成员策略

在“成员”选项卡上：

1. 选择“添加”以定义成员策略。

2. （可选）在“成员策略”页面中，有选择地为应该能够使用此角色的人员定义成员规则。

   此操作会自动将角色分配给符合成员策略标准的用户。

3. 验证“成员”选项卡上显示的成员策略。

   要编辑策略，请单击左侧的箭头符号。 要删除策略，请单击减号图标。

4. 在“成员”选项卡上，启用“管理员可以添加和删除该角色的成员”复选框。

   启用此功能后，定义“添加操作”和“删除操作”。这些操作将定义添加或删除角色成员用户时会出现的情况。

5. 继续执行下一部分“为访问角色定义管理员策略” (p. 455)。

为访问角色定义管理员策略

在“管理员”选项卡上：

1. 如果要使“管理管理员”选项可用，请启用“管理员可以添加和删除该角色的管理员”复选框。

   启用此功能后，定义添加或删除角色管理员用户时所执行的操作。

2. 在“管理员”选项卡上添加管理员策略，这些策略包含管理员规则、范围规则和管理员权限。 每种策略均至少需要一种权限（管理成员或管理管理员）。

   对于符合规则的管理员，您可以为其添加包含不同规则和不同权限的多个管理员策略。

3. 要编辑策略，请单击左侧的箭头符号。 要删除策略，请单击减号图标。
4. 继续执行下一部分“为访问角色定义所有者规则” (p. 456)。

为访问角色定义所有者规则

在“所有者”选项卡上：

1. 定义所有者规则，用于确定哪些用户可以修改角色。
2. 单击“提交”。

   将显示一条消息，指示该任务已提交。 可能会出现短暂的延迟，之后用户才能够使用角色。

第 20 章： 系统任务

此部分包含以下主题：

默认系统任务

CA CA Identity Manager 包括以下有助于管理员管理 CA Identity Manager 环境的任务：

- 查看提交的任务任务

  通过此任务，管理员可查看环境中的任务状态。 此外，请从“查看提交的任务”屏幕中删除过时的任务。

- 批加载程序任务

  上载用于同时处理大量受管理对象的 Feeder 文件。

- 批量任务

  根据对象的属性（如部门、城市、终止日期等等）运行对象（如用户）上的任务。 您可以定期（如每个星期六）运行此任务。

  您还可以使用此任务来进行批量用户更改。

- 选择框数据任务

  通过此任务，管理员可在管理任务中上载用于在字段（例如选择框）中填充选项的文件。

- 逻辑属性处理程序任务

  通过此任务，管理员可管理逻辑属性，这些属性用于在任务屏幕上以用户友好的格式显示用户存储属性（称为物理属性）。

- JDBC 连接管理任务

  在 CA CA Identity Manager 中配置数据库服务器连接详细信息。

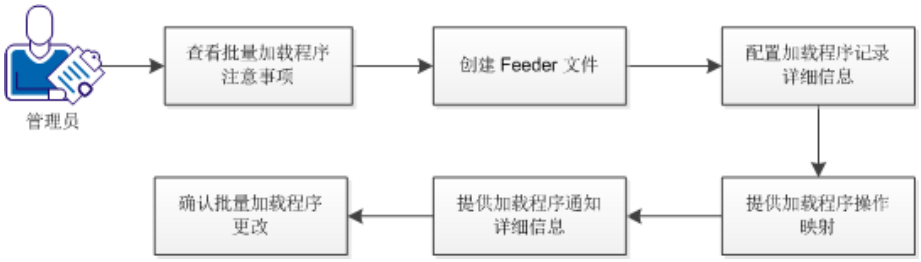
- 电子邮件任务

  管理电子邮件通知策略。

如何添加具有 Feeder 文件的用户

您可以使用“批量加载程序”选项卡上载 Feeder 文件，这些文件用于同时处理大量的受管理对象。 例如，您可以在系统中手动创建 1000 名用户，您也可以使用批量加载程序。 还可将“批加载程序”任务映射至工作流流程。

批量加载客户端是进行批处理的命令行实用程序。 如果您的环境为群集（用于负载平衡目的），我们建议使用批量加载客户端。 批量加载程序客户端位于配给组件介质上。



遵循这些步骤:

1. 查看批量加载程序注意事项 (p. 459)。
2. 创建 CSV 或 XLS feeder 文件 (p. 461)并上传。
3. 配置加载程序记录详细信息 (p. 462)。

   该选项卡允许您在 Feeder 文件中指定操作和标识符字段。

4. 提供加载程序操作映射 (p. 463)。

   该选项卡允许您选择主对象并指定为某对象的操作执行的任务。

5. 提供加载程序通知详细信息 (p. 463)。

   该选项卡允许您选择用于证明批量加载程序任务更改的用户。

6. 确认并修改批量加载程序任务更改的进度 (p. 464)。

批量加载程序注意事项

您可以使用“批量加载程序”选项卡上载 Feeder 文件，这些文件用于同时处理大量的受管理对象。 使用批量加载程序时注意以下注意事项：

- 考虑在非高峰时间排定大批量加载，如在夜间。大批量加载可影响性能。在某些情况下，包括许多子任务的批量加载可阻止用户提交的任务完成，直到批量加载完成。
- 如果在长时间运行任务（例如上传大量对象）期间服务器停机，可在“查看提交的任务”下重新启动该任务。 重新启动任务后，将从上次成功执行的记录开始。
- 如果将 LDAP 作为用户存储用于 Solaris，那么批量加载程序在导入期间可能会挂起。 要解决该问题，请参阅《*Configuration Guide*》（《配置指南》）中的“Specify LDAP Connection Settings”（指定 LDAP 连接设置）主题，并应用所叙述的设置。
- 如果使用批量加载程序来导入大量用户，您可能会看到内存用完异常。 要解决该问题，请调整以下堆大小内存参数：
  - -Xmx
  - -XX:maxPermSize

  注意：有关调整内存参数的更多信息，请参阅您的应用程序服务器文档。
- 使用批量加载程序来处理许多管理的对象（如创建许多用户）可能会影响性能。 为了提升性能，请考虑以下建议：
  - 在使用用户控制台进行批量加载时，把一个大 CSV 文件分成多个小文件。 例如，与进行 10 万名用户的一次批量加载相比，进行 1 万名用户的十次批量加载更快。

    注意：具有超过 5 万个条目的 CSV 文件可能在系统中引起问题。
  - 限制正在执行批量加载的用户所具有的任务数。例如，当启动批量加载的管理员只有很少任务时，性能会提升。 当管理员有许多任务时，CA Identity Manager 必须进行更广泛的权限检查，这可能会影响性能。
  - 限制 Policy Xpress 策略数，其与涉及配给的批量更改相关联。 此外，考虑创建简单的 Policy Xpress 策略，其不象复杂策略那样在批量加载操作期间对性能产生显著影响。
  - 确认您有足够的系统资源。

限制数据验证以提高批量加载性能

管理任务通常包括多个选项卡。 默认情况下，批量操作验证任务中每个选项卡上的数据。

验证会影响批量操作的性能。 要提高性能，您可以为任务选项卡禁用数据验证（如果不要求验证）。

遵循这些步骤:

1. 以具有修改管理任务的用户身份登录到用户控制台。
2. 依次选择“任务”、“角色和任务”、“管理任务”、“修改管理任务”。
3. 搜索并选择在批量操作中应用的任务。
4. 选择“选项卡”，然后选择要修改的选项卡。
5. 选择“不在批量操作中验证”，然后单击“确定”。
6. 针对不需要数据验证的每个选项卡，重复步骤 4 和 5。
7. 单击“提交”。

   您修改的选项卡的数据验证即被禁用。

限制自定义业务逻辑

包括自定义业务逻辑（如业务逻辑任务处理程序和事件侦听程序），在用于批量操作的任务中，可以影响性能。

要提高性能，请在批量加载操作中禁用自定义业务逻辑。

遵循这些步骤:

1. 打开管理控制台。
2. 选择包括事件侦听程序或业务逻辑任务处理程序的适合环境。
3. 选择“高级设置”、“业务逻辑任务处理程序”（如果适用）。
4. 将“UseInBulkOperation”属性值设置为 false，然后单击“保存”。
5. 重复事件侦听程序的第 4 步。
6. 一旦您已完成对业务逻辑任务处理程序和事件侦听程序的修改，请重新启动环境。

创建一个 Feeder 文件

批加载程序文件用于对大量受管理对象自动执行重复操作。 上传 feeder 文件时，系统会解析并读取 feeder 文件。

Feeder 文件必须为 CSV 或 XLS 扩展名，并应具有以下属性：

- 该文件必须包含一个标题行，用于指定受管理对象的物理属性、逻辑属性或常见属性的名称。
- 标题行必须包含一个列，指明要对记录执行的操作。
- Feeder 文件中的每一行被称为一条记录。 记录包含由标题行指定的每个属性的值。 以下选项是属性可接受的值：
  - 值－属性将设置为您指定的值。
  - 值;值;值;...－将该属性设置为指定的多值属性。
  - “”（空）－属性不会更改。
  - 空－属性已删除。 删除顺序在默认情况下被设置为空，但可在“批加载程序文件上载搜索”屏幕中进行编辑。

注意：要在 Feeder 文件中使用井字标记 (#)，请使用双引号引上井字标记，例如，将 user#1 指定为 "user#1"。

重要说明！ 必须以 UTF-8 编码保存 Feeder 文件。

用于创建用户的示例 Feeder 文件

此示例 Feeder 文件通过特定必需属性来创建用户。

```
action,%USER_ID%,%FIRST_NAME%,%LAST_NAME%,%FULL_NAME%,%PASSWORD%,%EMAIL%
create,JD,John,Doe,John Doe,mypassword,Johndoe@a.com
create,BD,Baby,Doe,Baby Doe,mypassword2,Babydoe@a.com
```

在上述代码中，Feeder 文件具有以下属性：

标题

代码的第一行是标题行。标题行具有受管理对象“用户”的物理属性或已知属性。

操作

操作列标识要对每个记录执行的任务。 例如，上述文件指定应对名字“John”执行一个“创建”操作。

用于启用用户的示例 Feeder 文件

此示例 Feeder 文件用于更改 |enabled| 逻辑属性的值。 您可在文件头指定逻辑属性，并在每个用户条目中指定值（在本例中，值为 true 或 false）。

```
action,%USER_ID%,|enable|

MODIFY,user1,false

MODIFY,user2,true
```

加载程序记录详细信息选项卡

“加载程序记录详细信息”选项卡显示 Feeder 文件中可用记录的简要预览。 预览表最多可显示 5 条记录。 预览表可帮助用户识别加载的文件是否正确。 另外，使用该选项卡还可以标识要对 Feeder 文件中指定的受管理对象执行的操作。 必须填写以下字段：

什么字段表示对对象执行的操作？

标识 Feeder 文件中涉及要对受管理对象执行的操作的字段。 例如，可以使用“操作”字段中包含“创建”、“修改”和“删除”值的 Feeder 文件。 您必须在加载程序操作映射 (p. 463)中将以下每个操作映射到管理任务。

什么字段将用于唯一地标识对象？

标识 Feeder 文件中可唯一标识主要对象的字段。

注意：如果 Feeder 文件的标题行无效，则 Feeder 文件记录不会显示在“加载程序记录详细信息”选项卡中。在标题无效的情况下，请选择其他 Feeder 文件。如果 Feeder 文件包含一些无效记录，则上载的详细状态将显示在“系统”选项卡下的“查看提交的任务”中。

加载程序操作映射选项卡

使用“加载程序操作映射”选项卡可以选择一个主要对象，在 Feeder 文件中指定的操作将针对该对象执行。还必须将 Feeder 文件中的操作映射到所选主要对象的管理任务。

什么是主要对象？

标识 CA Identity Manager 将使用 Feeder 文件处理的主要对象。 您可以选择以下任一主要对象：

- 用户
- 组
- 组织

选择一个任务来执行“操作”

标识对于 Feeder 文件指定的每个操作要执行的管理任务，如删除或修改任务。

注意：必须将 Feeder 文件中的所有操作映射到管理任务。 另外，显示在该字段中的管理任务取决于所选的主要对象。 例如，如果选择“用户”作为主要对象，则只显示与“用户”相关的管理任务。

选择“操作”的非存在对象的任务

标识受管理对象尚未存在于 CA Identity Manager 的情况下针对 Feeder 文件中指定的操作要执行的其他管理任务，如创建任务。

“加载程序通知详细信息”选项卡

重要说明！ 默认情况下，此选项卡不包括在批量加载程序向导中。 您必须通过修改批量加载程序任务并添加“加载程序通知详细信息”选项卡手工添加它。另外，此选项卡需要您在环境中启用工作流。

“加载程序通知详细信息”选项卡允许您为批量加载程序任务选择认证管理者。批量加载程序任务完成时，CA Identity Manager 针对为该任务配置的所有认证管理者创建批量加载程序通知。 此通知出现在批量加载程序通知下的“主页”选项卡中。 单击通知可显示由批量加载操作启动的任务的详细信息。 认证管理者然后可以查看和确认通知中详细说明的更改。

注意：要提供认证管理者的列表，请使用下拉列表中的任何可用的参与人确定程序。 有关参与人确定程序的详细信息，请参阅本指南的“工作流”部分。

确认批量加载程序任务更改

批量加载程序通知包含有关批量加载程序任务启动的所有更改的详细信息。 认证管理者可以查看和确认由批量加载程序任务启动的任何更改。

查看和确认批量加载程序任务更改

1. 以某个用户的身份登录到用户控制台，该用户已列为批量加载程序任务的认证管理者。
2. 转到“主页”，选择“查看我的批量加载程序通知”。
3. 选择要查看的批量加载程序通知。

   将出现“管理批量加载程序通知”屏幕，显示了一个列出已启动的所有批量加载程序任务更改的表。

   您可以在此屏幕上执行以下操作：

   - 要查看创建或修改对象的特定任务详细信息，请单击“说明”列下的超链接。
   - 如果存在遵从违规或者要删除添加到用户的角色，则可以通过单击用户 ID 旁边的“编辑”图标直接从通知屏幕编辑用户。
   - 要查看添加到用户的任何角色，请单击与用户 ID 相关联的“已请求角色分配”列下的超链接。
4. 在查看特定对象的所有更改后，选中该对象的“确认”复选框。
5. 在完成更改的确认后，单击“确认”从列表中删除所有选定的更改通知。

   注意：您可以选择“确认全部”来确认批量加载程序通知中的所有更改。 这会从“主页”选项卡中删除批量加载程序通知。另外，您可以选中“确认”列顶部的复选框来选择此时在屏幕上的所有更改通知，并逐个屏幕地确认更改。

   在确认与批量加载程序任务关联的所有用户更改时，批量加载程序通知会从“主页”选项卡中消失。

为批量加载程序任务配置电子邮件通知

在一些环境中，默认情况下，会配置批量操作电子邮件通知。 要检查批量操作电子邮件通知是否在您的系统中配置，请转到“系统”、“电子邮件”、“查看电子邮件”，并搜索“批量”。

如果没有在您的环境中配置电子邮件通知，则请配置在批量操作完成后发送的电子邮件。

遵循这些步骤:

1. 在用户控制台中，依次导航到“系统”、“电子邮件”、“创建电子邮件”。
2. 完成“配置文件”选项卡中的所需字段。

3. 在“发送时间”选项卡中，完全以下步骤：
   a. 在第一个字段中选择“任务已完成”。
   b. 在第二个字段中选择“批量加载程序”。
4. 完成“收件人”和“内容”选项卡，然后单击“提交”。

   为批量加载程序任务配置电子邮件通知。

排定批加载程序任务

可以在系统中排定批量加载程序任务。 要排定批量加载程序任务，请向任务添加“排定程序”选项卡 (p. 58)。

修改批加载程序的解析程序文件

要修改用于解析 Feeder 文件的解析程序，请配置对应的管理任务。

修改批加载程序管理任务

1. 依次导航到“角色和任务”、“管理任务”、“管理管理任务”。
2. 搜索批加载程序任务。
3. 选择批加载程序任务，然后单击“选择”。
4. 选择“批加载程序”任务的“搜索”选项卡。
5. 单击“浏览”以找到搜索屏幕。

   将显示可用搜索屏幕列表。
6. 选择一个搜索屏幕，然后单击“编辑”。

   将显示搜索屏幕详细信息。
7. （可选）编辑解析程序完全限定名称。

   解析程序完全合格名称必须与您的解析程序文件名称匹配。

   注意：有关创建自定义 CSV 解析程序的详细信息，请参阅适用于 FeederParser 类的 Javadoc。如果您使用 JBoss 作为应用程序服务器，且您创建了自定义解析程序，则自定义解析程序文件必须位于 iam_im.ear/user_console_war/WEB-INF/classes 目录中。
8. 单击“确定”。

适用于批加载程序的 Web 服务支持

批量加载程序具有 Web 服务 API，该 API 可使用 CA Identity Manager 任务执行 Web 服务 (TEWS) 接口进行调用。 通过 TEWS，客户端应用程序可以将远程任务提交给 CA Identity Manager 执行。 该接口实施 WSDL 和 SOAP 开放标准，从而提供对 CA Identity Manager 的远程访问。

CA Identity Manager 中包括 Java 客户端示例，用于演示将批量加载程序作为 Web 服务进行调用。 此类 Java 示例位于以下源文件中：

管理工具\samples\WebService\Axis\optional\ObjectsFeeder.java

用于演示将批加载程序作为 Web 服务进行调用的数据示例和文档位于以下目录：

管理工具\samples\Feeder\

注意：有关详细信息，请参阅《*Programming Guide for Java*》（《Java 编程指南》）。

JDBC 连接管理

CA CA Identity Manager 报告的信息可能有多个来源，而根据您想要在报告中查看的信息，每个报告都应该与一个特定数据源相关联。

要建立用于报告的不同数据源（例如审核数据库或任务持久性数据库），请在 CA CA Identity Manager 中创建连接管理对象。 创建连接后，可以通过修改报告任务并在报告任务的搜索选项卡下设置“报告的连接对象”将报告与特定连接管理对象相关联。

创建 JDBC 连接

使用以下步骤可在 CA Identity Manager 内提供连接详细信息。

创建 JDBC 连接

1. 依次单击“系统”、“JDBC 连接管理”、“创建 JDBC 连接”。
2. 创建新的连接对象，或根据特定的 JNDI 数据源选择一个连接对象。
3. 填写所有必需的字段，然后单击“提交”。

   此时就创建了一个新的 JDBC 连接。

逻辑属性处理程序

通过 CA Identity Manager 逻辑属性，您可在任务屏幕上以用户友好格式显示用户存储属性（称为物理属性）。 CA Identity Manager 管理员使用任务屏幕在 CA Identity Manager 中执行功能。用户存储中不存在逻辑属性。通常，逻辑属性表示一个或多个物理属性来简化演示。例如，逻辑属性日期可能表示物理属性月、日和年。

逻辑属性由逻辑属性处理程序处理，该程序是使用逻辑属性 API 编写的 Java 对象。（请参阅 *《Java 编程指南》*。）例如，显示任务屏幕时，逻辑属性处理程序可将用户存储中的物理属性数据转换为逻辑属性数据，该逻辑属性数据将显示在任务屏幕上。 您可以使用 CA Identity Manager 包含的预定义逻辑属性和逻辑属性处理程序，也可以使用逻辑属性 API 创建新的逻辑属性和逻辑属性处理程序。

注意：有关逻辑属性的详细信息，请参阅 *《Java 编程指南》*。

在用户控制台中，“环境”类别包含了用于管理逻辑属性处理程序的任务。 此列表包括 CA Identity Manager 附带的预定义处理程序和您站点上定义的任何自定义处理程序。

从“环境”任务类别中，您可以执行以下操作：

- 通过 CA Identity Manager 创建新的逻辑属性处理程序
- 复制处理程序
- 删除处理程序
- 修改现有的处理程序配置

注意：要更改逻辑属性处理程序的执行顺序，请使用管理控制台。

创建逻辑属性处理程序

创建逻辑属性处理程序

1. 依次导航到“系统”、“逻辑属性”、“创建逻辑属性处理程序”。
2. 在“创建逻辑属性处理程序”屏幕中，选择“创建标准逻辑属性处理程序”，然后单击“确定”。
3. 在“创建逻辑属性处理程序”屏幕中，配置逻辑属性处理程序的设置。

   有关每个字段的说明，请单击此屏幕上的“帮助”链接。
4. 单击“提交”。

   该处理程序即被添加至“逻辑属性处理程序”屏幕上的处理程序列表中。

注意：使用用户控制台配置逻辑属性处理程序后，无需重新启动应用程序服务器。

创建逻辑属性处理程序

创建逻辑属性处理程序

1. 依次导航到“系统”、“逻辑属性”、“创建逻辑属性处理程序”。
2. 在“创建逻辑属性处理程序”屏幕中，选择“创建逻辑属性处理程序定义的副本”，然后单击“搜索”。
3. 选择一个逻辑属性处理程序（例如 ConfirmPasswordHandler），然后单击“确定”。
4. 在“创建逻辑属性处理程序”屏幕中，配置逻辑属性处理程序的设置。

   有关每个字段的说明，请单击此屏幕上的“帮助”链接。
5. 单击“提交”。

   该处理程序即被添加至“逻辑属性处理程序”屏幕上的处理程序列表中。

注意：使用用户控制台配置逻辑属性处理程序后，无需重新启动应用程序服务器。

创建 ForgottenPasswordHandler 逻辑属性处理程序

ForgottenPasswordHandler 逻辑属性处理程序使用针对以下内容的独立逻辑属性：

- 配置
- 运行时问题和答案

创建 ForgottenPasswordHandler 逻辑属性处理程序

1. 依次导航到“系统”、“逻辑属性”、“创建逻辑属性处理程序”。
2. 在“创建逻辑属性处理程序”屏幕中，选择“创建标准逻辑属性处理程序”，然后单击“确定”。
3. 选择 ForgottenPasswordHandler，然后单击“确定”。
4. 在“创建逻辑属性处理程序中”：“ForgottenPasswordHandler”屏幕，配置逻辑属性处理程序的设置。

   有关每个字段的说明，请单击此屏幕上的“帮助”链接。
5. 单击“提交”。

   该处理程序即被添加至“逻辑属性处理程序”屏幕上的处理程序列表中。

注意：使用用户控制台配置逻辑属性处理程序后，无需重新启动应用程序服务器。

删除逻辑属性处理程序

删除逻辑属性处理程序

1. 依次导航到“系统”、“逻辑属性”、“创建逻辑属性处理程序”。
2. 在“删除逻辑属性处理程序”屏幕中，选中每个要删除的逻辑属性左侧的复选框。
3. 单击“选择”。

   CA Identity Manager 显示一条确认消息。
4. 单击“是”确认删除。

修改逻辑属性处理程序

修改逻辑属性处理程序

1. 依次导航到“系统”、“逻辑属性”、“创建逻辑属性处理程序”。
2. 在“修改逻辑属性处理程序”屏幕中，选择您要修改的处理程序，然后单击“选择”。
3. 选择一个逻辑属性处理程序（例如 ConfirmPasswordHandler），然后单击“确定”。
4. 在“创建逻辑属性处理程序”屏幕中，配置逻辑属性处理程序的设置。

   有关每个字段的说明，请单击此屏幕上的“帮助”链接。
5. 单击“提交”。

注意：使用用户控制台配置逻辑属性处理程序后，无需重新启动应用程序服务器。

查看逻辑属性处理程序

查看逻辑属性处理程序

1. 依次导航到“系统”、“逻辑属性”、“创建逻辑属性处理程序”。
2. 在“查看逻辑属性处理程序”屏幕中，选择您要查看的处理程序，然后单击“选择”。
3. 查看逻辑属性处理程序的属性，然后单击“关闭”。

选择框数据

可以填充以下字段中可用的选项：

- 复选框多项选择
- 下拉列表
- 下拉组合框
- 多项选择
- 选项选择器
- 选项选择器组合框
- 单选按钮单项选择
- 单项选择

这些选项存储在选择框数据 XML 文件中。 例如，对于“创建用户”任务，可以使用选择框数据 XML 文件填充“配置文件”选项卡上“城市”或“省/自治区/直辖市”下拉框的选项。

还可以使用选择框数据 XML 文件配置管理任务中两个字段之间的依赖性。 例如，“城市”字段中的可用选项可能取决于用户在“省/自治区/直辖市”字段中选择的选项。

注意：有关选择框数据的详细信息，请参阅*《User Console Design Guide》*（《用户控制台设计指南》）。

配置关联属性任务屏幕

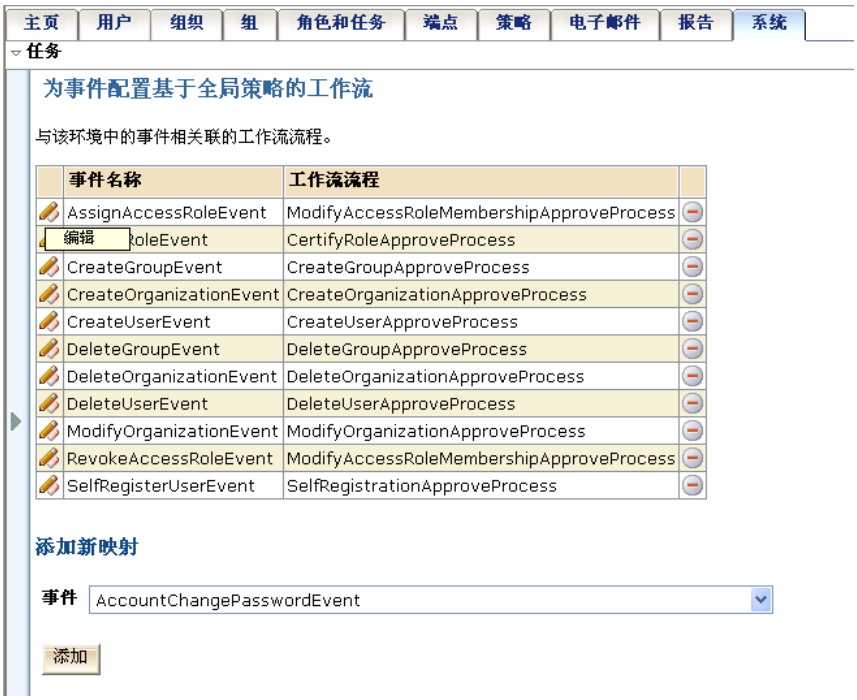
此主题仅适用于 CA CloudMinder。

使用配置关联属性任务屏幕，可为环境配置关联规则。

CA Identity Manager 将配置参数读到内存，并定期将内存版本与通用 DSA 的数据库版本进行同步。 由于关联属性是特定于承租方的，因此，配给服务器会在浏览和关联操作期间，从相应承租方 DSA 中读取关联属性。 更新的关联规则立即生效，无需等待参数更新时间。

为事件配置全局基于策略工作流的任务屏幕

通过“为事件配置全局基于策略工作流”的任务，管理员可以为当前环境中的所有事件配置基于策略或不基于策略的工作流。 单击任务显示映射到工作流流程定义的默认事件。 可以修改或删除每个事件映射，也可以为尚未配置的事件添加新的事件映射。



该屏幕上的字段如下所示：

与该环境中的事件关联的工作流流程。

指定与批准策略关联的工作流流程。

添加新映射

指定映射到工作流流程的批准策略。

添加按钮

添加新映射。

添加或修改映射会打开工作流映射屏幕，在屏幕中可以选择流程映射和批准策略。 行为与事件级别工作流配置相同。 单击工作流映射页上的“添加”按钮会出现其他的页面，在页面中可以配置批准策略。

更多信息

如何配置基于策略的工作流 (p. 277)
如何配置批准策略 (p. 278)

CA Identity Manager 中的任务状态

提交要进行处理的 CA Identity Manager 任务后，管理员可能希望跟踪这些任务的状态。 CA Identity Manager 提供了以下查看任务状态的方法：

- **“查看提交的任务”选项卡**

  通过此选项卡，您可以搜索并显示已提交进行处理的 CA Identity Manager 任务。

  管理员可以查看高级任务详细信息或查看其他级别的详细信息。

  “查看提交的任务”选项卡包括在两个默认任务中：

  - 查看我提交的任务

    通过此任务，管理员可搜索并显示已提交进行处理的任务的有关信息。

  - 查看提交的任务

    通过此任务，管理员可搜索并显示已由其他管理员提交进行处理的任务的有关信息。

- **“用户历史记录”选项卡**

  您可以将此选项卡添加到用户任务（例如“查看用户”或“修改用户”），通过该选项卡，管理员可以查看所选用户的以下信息：

  - 对用户执行的任务
  - 用户执行的任务
  - 用户批准的工作流

- **报告**

  通过 CA Identity Manager 报告，您可以查看 CA Identity Manager 环境的当前状态。 您可以使用此信息以确保遵从内部业务政策或外部法规。

  报告提供了关于设置和使用报告的其他信息。

- **日志**

  显示关于 CA Identity Manager 安装中所有组件的信息，并提供关于 CA Identity Manager 中所有操作的详细信息。

  有关 CA Identity Manager 日志的详细信息，请参阅《*Configuration Guide*》（《配置指南》）。

CA Identity Manager 确定任务状态的方式

*任务*是一项用户可在 CA CA Identity Manager 中执行的管理功能。 任务包括*事件*和 CA Identity Manager 为完成任务而执行的操作。一项任务可能包括多个事件。例如，“创建用户”任务可能包括创建用户的配置文件、将用户添加到组以及分配角色等事件。

可将 CA Identity Manager 任务和事件与工作流流程关联，工作流流程确定了 CA Identity Manager 如何执行所需操作和其他自定义业务逻辑。 还可将任务与其他任务关联，称为嵌套任务。在这种情况下，CA Identity Manager 将通过原始任务处理嵌套任务。

任务的状态取决于其关联事件、工作流流程、嵌套任务和自定义业务逻辑的状态。

查看提交的任务

CA Identity Manager 包括一个“查看提交的任务”功能，该功能提供了 CA Identity Manager 环境中任务的有关信息。您可以使用此功能搜索并查看关于 CA Identity Manager 所执行操作的高级详细信息， 各个详细信息屏幕提供每项任务和事件的其他相关信息。

根据任务的状态，您可以使用“查看提交的任务”来中止或重新提交任务。

通过“查看提交的任务”，您可以自始至终跟踪任务的处理。例如，如果 CA Identity Manager 任务包括配给角色分配，且该分配将触发其他系统中的帐户创建，那么“查看提交的任务”选项卡将显示原始任务和帐户创建的所有详细信息。

“查看提交的任务”包括系统中所执行操作的详细信息。 这些操作可能是某个 CA Identity Manager 事件的结果，如 EnableUserEvent。 系统发出的通知在该事件下分组。“查看提交的任务”会显示一条信息，指示通知为“进行中”，直到发出了“结束详细信息”通知。 然后，此条消息更改为“已完成”。

默认情况下，CA Identity Manager 将在以下两个任务中包括“查看提交的任务”选项卡。

- 查看提交的任务
- 查看我提交的任务

搜索已提交的任务

执行以下步骤搜索提交的任务。

要搜索已提交的任务

1. 依次单击“系统”、“查看提交的任务”。

   此时出现“查看提交的任务”页面。

2. 指定搜索条件，输入要显示的行数，然后单击“搜索”。

   将显示满足您搜索条件的任务。

   注意：有关在搜索条件中指定属性的更多信息，请参阅“查看提交的任务的搜索属性 (p. 474)”。

搜索查看提交的任务的属性

要查看已提交进行处理的任务，您可以使用“查看提交的任务”中的搜索功能。您可以根据以下条件搜索任务：

启动人

将启动任务的用户名标识为搜索条件。 根据用户名进行搜索。 要确保您输入了有效的用户名，请使用“验证”按钮。

批准任务执行者

将任务批准人姓名标识为搜索条件。 根据用户名进行搜索。 要确保您输入了有效的用户名，请使用“验证”按钮。

注意：如果您选择了“批准任务执行者”条件筛选任务，则默认情况下，也将启用“显示批准任务”条件。

任务名称

将任务名称标识为搜索条件。 可以通过指定条件（例如：等于、包含、始于或终于“任务名称”字段的值）来细化搜索。 例如：您可以选择等于条件，然后在文本字段中输入“创建用户”，以此指定搜索条件“任务名称等于‘创建用户’”。

任务状态

将任务状态标识为搜索条件。您可以启用“任务状态等于”，然后选择条件，以此选择任务状态。 您可以根据以下条件进一步细化搜索：

- 已完成
- 进行中
- 失败
- 已拒绝
- 部分完成

- 已中止
- 已排定

注意：有关详细信息，请参阅任务状态说明 (p. 476)。

任务优先级

将任务优先级标识为搜索条件。您可以启用“任务优先级等于”，然后选择条件，以此选择任务优先级。 您可以根据以下条件进一步细化搜索：

低

指定您可以搜索具有低优先级的任务。

中

指定您可以搜索具有中优先级的任务。

高

指定您可以搜索具有高优先级的任务。

执行对象

标识在所选对象实例上执行的任务。 如果您未选择一个对象实例，则将显示在该对象所有实例上执行的任务。

注意：仅当在“配置提交的任务”屏幕上填充“配置执行对象”字段时，才显示该字段。 您可以使用此屏幕配置“提交的任务”选项卡。 有关详细信息，请参阅适用于该屏幕的联机帮助。

日期范围

标识要搜索的提交的任务的日期范围。 您必须提供“起始”和“截止”日期。

显示未提交的任务

标识处于“审核”状态的任务。标识已启动其他任务的任务或还未提交的任务。 如果您选择了此选项卡，将审核并显示所有此类任务。

显示批准任务

标识必须在工作流流程中批准的任务。

搜索已提交任务的存档

标识已存档的提交任务。

更多信息：

任务状态说明 (p. 476)

任务状态说明

已提交的任务处于以下所说明的状态之一。 您可以根据任务的状态执行诸如取消或重新提交任务之类的操作。

注意：要取消或重新提交任务，您必须将“查看提交的任务”配置为根据任务状态显示取消和重新提交按钮。 有关取消和重新提交任务的详细信息，请参阅自定义“查看提交的任务”选项卡 (p. 479)。

进行中

发生以下任一情况时显示该状态：

- 工作流已启动但尚未完成
- 在当前任务之前启动的任务正在进行中
- 嵌套任务已启动但尚未完成
- 主要事件已启动但尚未完成
- 次要事件已启动但尚未完成

您可以取消处于此状态下的任务。

注意：取消任务会取消当前任务的所有未完成的嵌套任务和事件。

已取消

您取消任何进行中的任务或事件时，将显示该状态。

已拒绝

CA Identity Manager 拒绝工作流流程中的事件或任务时，将显示该状态。 您可以重新提交已拒绝的任务。

注意：重新提交任务时，CA Identity Manager 将重新提交所有已失败或已拒绝的嵌套任务和事件。

部分完成

您取消某些事件或嵌套任务时，将显示该状态。 您可以重新提交部分完成的事件或嵌套任务。

已完成

任务完成时，将显示该状态。 当前任务的嵌套任务和嵌套事件完成之后，该任务才算完成。

失败

任务、嵌套任务或嵌套在当前任务中的事件无效时将显示该状态。任务失败时将显示该状态。 您可以重新提交已失败的任务。

已排定

将该任务排定在稍后的日期执行时，将显示该状态。 您可以取消处于此状态下的任务。

已审核

当前任务已经过审核时，将显示该状态。

查看任务详细信息

CA CA Identity Manager 提供任务详细信息，例如已提交任务的状态、嵌套任务和与任务关联的事件。

查看提交的任务的详细信息

1. 单击“查看提交的任务”选项卡中选定任务旁边的右键头图标。

   将显示任务详细信息。

   注意：事件和嵌套任务（如果有）将显示在“任务详细信息”页面中。 您可以查看每个任务和事件的任务详细信息。

2. 单击“关闭”。

   此时“任务详细信息”选项卡将关闭，CA CA Identity Manager 将显示带有任务列表的“查看提交的任务”选项卡。

查看事件详细信息

CA CA Identity Manager 提供事件详细信息，例如已提交事件的状态、事件属性和事件的任何其他相关信息。

查看提交的事件的详细信息

1. 单击“查看任务详细信息”页面中某个事件旁边的右箭头图标。

   将显示事件详细信息。

2. 单击“关闭”。

   将关闭“事件详细信息”页面。

事件状态说明

CA Identity Manager 中的事件可处于以下描述的状态之一。可以根据事件状态取消事件或重新提交事件供执行。

注意：要允许管理员取消或重新提交事件，您必须将“查看提交的任务”配置为显示“取消”和“重新提交事件”按钮。 配置任务时，您可以指定哪些管理员可以取消和重新提交事件。有关取消和重新提交事件的详细信息，请参阅自定义“查看提交的任务”选项卡 (p. 479)。

进行中

发生以下任一情况时显示该状态：

- 工作流或前期事件已启动、正在进行或已批准。
- CA Identity Manager 正在执行事件
- CA Identity Manager 执行后期事件

您可以取消处于此状态下的事件。

已拒绝

CA Identity Manager 拒绝工作流中的事件时，将显示该状态。您可以重新提交已拒绝的任务。

已取消

取消任何进行中的事件时，将显示该状态。 您可以重新提交已拒绝的任务。

已完成

事件完成时，将显示该状态。

失败

如果执行事件时 CA Identity Manager 遇到异常，将显示该状态。您可以重新提交已拒绝的任务。

注意：主要事件处于已完成状态后，您才能重新提交次要事件。

已排定

将该事件排定在稍后的日期执行时，将显示该状态。 您可以取消处于此状态下的事件。

已审核

当前事件已经过审核时，将显示该状态。

自定义“查看提交的任务”选项卡

可以自定义“查看提交的任务”选项卡，如下所述：

- 指定不同的任务名称和标签。
- 更改默认的显示属性。 安装后，用户将看到一个搜索屏幕，在此屏幕中用户可以输入标准，以确定将显示在选项卡中的任务。 您可以将选项卡配置为自动显示当天提交的任务，用户便无需输入搜索条件。
- 确定审核事件是否显示在“任务详细信息”页面中。
- 在任务显示中另外添加一列。
- 指定用于取消或重新提交任务和事件的标准。

注意：某些任务和事件详细信息可能包括诸如薪金或密码等数据，这些数据不应该显示在“查看提交的任务”选项卡的明文中。 可以在 directory.xml 文件中定义这些属性时通过指定数据分类参数隐藏这些属性。 有关 directory.xml 文件的详细信息，请参阅 *《Configuration Guide》*（《配置指南》）。

您可以通过修改相应的管理任务来配置“查看提交的任务”选项卡。

配置“查看提交的任务”选项卡

1. 依次单击“角色和任务”、“管理任务”、“修改管理任务”。

   将显示“选择管理任务”页面。

2. 在“搜索管理任务”字段中选择“名称”或“类别”，输入要搜索的字符串，然后单击“搜索”。

   CA CA Identity Manager 将显示符合搜索标准的管理任务。

3. 选择“查看提交的任务”，然后单击“选择”。

   CA CA Identity Manager 将显示“查看提交的任务”管理任务的任务详细信息。

4. 单击“选项卡”选项卡。

   将显示用于“查看提交的任务”选项卡的选项卡。

5. 单击右箭头图标可编辑“提交的任务”选项卡。

   将显示选项卡详细信息。

6. 根据需要编辑字段，以对“查看提交的任务”选项卡进行自定义。 请参阅已提交的任务选项卡的配置设置 (p. 480)。

“查看提交的任务”选项卡的配置设置

使用以下字段更改“查看提交的任务”选项卡的外观和功能。

名称

定义任务的名称。

标签

定义任务的唯一标识符。 它用于 URL、Web 服务或属性文件中。 必须由字母、数字或下划线组成，且以字母或下划线开头。

隐藏选项卡

标识选项卡向用户显示，但不会被执行。 如果您选择了此选项，CA Identity Manager 将向用户显示一个错误。

显示加载的任务列表

显示当天已提交的任务。

注意：如果您已启用此选项，用户单击“查看提交的任务”便可直接看到当天提交的任务。

显示审核事件

指定审核的事件是否包括在“查看提交的任务”页面的任务中。

允许自定义列

指明您可以将自定义列附加到任务表，您可以在“查看提交的任务”选项卡和“用户历史记录”选项卡中查看这些任务表。例如，您可以将“用户 ID”列添加到显示在“用户历史记录”选项卡上的任务表中。

自定义列标题

指明自定义列的显示名称。

自定义列属性

指明将用于填充任务表中自定义列的属性。 例如，如果您要搜索针对某个组织的员工执行的任务，您可以附加组织列，从中显示每位员工所在的组织。

取消任务和事件

标识取消任务或事件的标准。 通过选择以下选项之一，您可以为该字段设置范围：

任务创建者须为当前用户

标识您可以取消或重新提交您创建的任务或事件。

任务创建者须在范围内

标识您可以取消或重新提交已被其他用户启动的任务，这些用户需符合赋予您访问该选项卡权限的管理角色的用户范围规则。

例如，由于您符合成员资格规则（包括“员工”组织中所有用户的范围）中的标准，您得到了“用户经理”角色，该角色包括“查看提交的任务”。 您可以取消或重新提交“员工”组织中所有用户提交的任务。

没有限制

标识任何用户均可以取消或重新提交任务或事件。

不允许

指定任务或事件不可被取消或重新提交。

重新提交任务和事件

标识重新提交任务或事件的标准。 通过选择以下选项之一，您可以设置该字段的范围：

任务创建者须为当前用户

标识您可以取消或重新提交您创建的任务或事件。

任务创建者须在范围内

标识您可以取消或重新提交已被其他用户启动的任务，这些用户需符合赋予您访问该选项卡权限的管理角色的用户范围规则。

例如，由于您符合成员资格规则（包括“员工”组织中所有用户的范围）中的标准，您得到了“用户经理”角色，该角色包括“查看提交的任务”。 您可以取消或重新提交“员工”组织中所有用户提交的任务。

没有限制

标识任何用户均可以取消或重新提交任务或事件。

不允许

指定任务或事件不可被取消或重新提交。

“用户历史记录”选项卡

通过“用户历史记录”选项卡，您可以查看与某用户相关的任务。 显示在此选项卡中的任务详细信息还可以在“查看提交的任务”选项卡中查看。

注意：您无法添加此选项卡以创建任务，如创建用户。

您可以使用该选项卡查看以下任务的历史记录：

- **对用户执行的任务**

  显示对所选用户执行的所有任务。

- **用户执行的任务**

  显示由所选用户执行的所有任务。

- **用户批准的工作流**

  显示用户已经批准作为工作流一部分的所有任务。

注意：您可以在此选项卡中查看的任务类型取决于选项卡的配置。“自定义用户历史记录”选项卡 (p. 483)提供更多信息。

搜索查看用户历史记录的属性

要查看已提交进行处理的任务，您可以使用“查看提交的任务”中的搜索功能。您可以根据以下标准搜索任务：

任务名称

将任务名称标识为搜索标准。 可以通过指定条件（例如，等于、包含、始于或终于“任务名称”字段的值）来细化搜索。 例如，您可以选择等于条件，然后在文本字段中输入“创建用户”，以此指定搜索标准“任务名称等于‘创建用户’”。

任务状态

将任务状态标识为搜索标准。您可以启用“任务状态等于”，然后选择条件，以此选择任务状态。 您可以根据以下条件进一步细化搜索：

- 已完成
- 进行中
- 已失败
- 已拒绝
- 部分完成
- 已取消
- 已排定

注意：有关详细信息，请参阅任务状态说明 (p. 476)。

任务优先级

将任务优先级标识为搜索标准。您可以启用“任务优先级等于”，然后选择条件，以此选择任务优先级。 您可以根据以下条件进一步细化搜索：

低

指定您可以搜索具有低优先级的任务。

中

指定您可以搜索具有中优先级的任务。

高

指定您可以搜索具有高优先级的任务。

日期范围

标识要搜索的已提交任务的日期范围。 您必须提供“起始”和“截至”日期。

自定义“用户历史记录”选项卡

管理员可以自定义“用户历史记录”选项卡，如下所述：

- 指定不同的任务名称和标签。
- 更改默认的显示属性。 默认情况下，用户可以输入用于确定在选项卡中显示哪些任务的条件。 管理员可以将选项卡配置为自动显示当天的任务，这样用户便无需输入搜索条件。
- 确定审核事件是否显示在“任务详细信息”页面中。
- 在任务显示中添加一列。
- 指定用于取消或重新提交任务和事件的条件。

遵循这些步骤:

1. 依次导航到“角色和任务”、“管理任务”、“管理管理任务”。

   将显示“选择管理任务”页面。

2. 在“搜索管理任务”字段中选择“名称”或“类别”，输入要搜索的字符串，然后单击“搜索”。

   CA Identity Manager 将显示符合搜索标准的管理任务。

3. 选择包括“用户历史记录”选项卡的任务，然后单击“选择”。

   CA Identity Manager 将显示管理任务的任务详细信息。

4. 单击“选项卡”选项卡。

5. 单击“用户历史记录”选项卡旁边的“编辑”图标。

   将显示选项卡详细信息。

6. 编辑字段以对“用户历史记录”选项卡进行自定义。

“用户历史记录”选项卡的配置设置

使用以下字段更改“用户历史记录”选项卡的外观和功能。

名称

定义任务的名称。

标签

定义任务的唯一标识符。 它用于 URL、Web 服务或属性文件中。 必须由字母、数字或下划线组成，且以字母或下划线开头。

隐藏选项卡

标识选项卡向用户显示，但不会被执行。 如果您选择了此选项，CA Identity Manager 将向用户显示一个错误。

显示加载的任务列表

显示当天已提交的任务。

注意：如果您已启用此选项，用户单击“查看提交的任务”便可直接看到当天提交的任务。

显示审核事件

指定审核的事件是否包括在“查看提交的任务”页面的任务中。

允许自定义列

指明您可以将自定义列附加到任务表，您可以在“查看提交的任务”选项卡和“用户历史记录”选项卡中查看这些任务表。例如，您可以将“用户 ID”列添加到显示在“用户历史记录”选项卡上的任务表中。

自定义列标题

指明自定义列的显示名称。

自定义列属性

指明将用于填充任务表中自定义列的属性。 例如，如果您要搜索针对某个组织的员工执行的任务，您可以附加组织列，从中显示每位员工所在的组织。

取消任务和事件

标识取消任务或事件的标准。 通过选择以下选项之一，您可以为该字段设置范围：

任务创建者须为当前用户

标识您可以取消或重新提交您创建的任务或事件。

任务创建者须在范围内

标识您可以取消或重新提交已被其他用户启动的任务，这些用户需符合赋予您访问该选项卡权限的管理角色的用户范围规则。

例如，由于您符合成员资格规则（包括“员工”组织中所有用户的范围）中的标准，您得到了“用户经理”角色，该角色包括“查看提交的任务”。 您可以取消或重新提交“员工”组织中所有用户提交的任务。

没有限制

标识任何用户均可以取消或重新提交任务或事件。

不允许

指定任务或事件不可被取消或重新提交。

重新提交任务和事件

标识重新提交任务或事件的标准。 通过选择以下选项之一，您可以设置该字段的范围：

任务创建者须为当前用户

标识您可以取消或重新提交您创建的任务或事件。

任务创建者须在范围内

标识您可以取消或重新提交已被其他用户启动的任务，这些用户需符合赋予您访问该选项卡权限的管理角色的用户范围规则。

例如，由于您符合成员资格规则（包括“员工”组织中所有用户的范围）中的标准，您得到了“用户经理”角色，该角色包括“查看提交的任务”。 您可以取消或重新提交“员工”组织中所有用户提交的任务。

没有限制

标识任何用户均可以取消或重新提交任务或事件。

不允许

指定任务或事件不可被取消或重新提交。

显示任务

确定显示在“用户历史记录”选项卡中的任务。

对用户执行的任务

显示对所选用户执行的所有任务。

用户执行的任务

显示由所选用户执行的所有任务。

用户批准的工作流

显示用户在工作流中批准的所有任务。

“查看用户活动”任务

用户活动是涉及特定用户的任务历史记录。 管理员可以使用“查看用户活动”任务跟踪以下用户信息：

- 对用户执行的任务
- 用户执行的任务
- 用户执行的工作流批准

查看用户活动

1. 依次导航到“用户”、“管理用户”、“查看用户活动”。

   将显示“选择用户”屏幕。

2. 搜索某个用户，然后单击“选择”。

   将显示“查看用户活动”屏幕。

注意：有关显示的用户活动的详细信息，请参阅用户控制台联机帮助。

清除已提交的任务

提交完每个任务后，随着任务永久数据库的不断增大，任务和事件的运行时性能也会降低。 存储步骤的垃圾收集功能可以缓解由于任务永久数据库存储空间不足而导致的潜在性能问题或系统中断。 通过存档任务的功能，管理员可以查看当前任务和事件信息以及已删除的任务和事件。

在用户控制台中，CA Identity Manager 管理员可以排定作业以便自动执行垃圾收集和定期存档。

重现选项卡

使用该选项卡可排定作业。 该选项卡上的字段如下所示：

立即执行

立即运行该作业。

排定新的作业

排定新的作业。

修改现有作业

指定您是否要修改一个已存在的作业。

注意：仅在已为该任务排定了作业时才会出现该字段。

作业名

指定想要创建或修改的作业的名称。

时区

指定服务器的时区。

注意：如果您的时区与服务器的时区不同，则会显示一个下拉框以便您可以在排定新作业时选择您的时区或者服务器的时区。 修改现有作业时不能更改时区。

按日排定

指定作业在每几天运行。

每（天数）

定义作业运行之间的天数。

按周排定

指定作业在一星期内的特定某天或某几天和特定时间运行。

周内某日

指定作业在一星期内的某天或某几天运行。

按月排定

指定作业在周内某日或月内某日运行（以月为基础）。

按年排定

指定作业在周内某日或月内某日运行（以年为基础）。

高级排定

指定其他排定信息。

Cron 表达式

有关填充该字段的信息，请参阅以下页面：

http://quartz-scheduler.org/api/2.1.0/org/quartz/CronExpression.html

执行时间

指定作业运行当天的时间（ 24 小时格式）。 例如，14:15。

立即执行作业

要立即执行作业，请使用“清除已提交的任务”向导。

遵循这些步骤:

1. 依次导航到“系统”、“清除已提交的任务”。

   此时会出现向导的“重现”步骤。

2. 依次选择“立即执行”和“下一步”。

   此时会出现向导的“清除已提交的任务”步骤。

3. 输入最小时长、存档、审核超时、时间限制和任务限制信息，然后单击“完成”。

   该作业会立即提交。

排定新的作业

要排定新的作业，请使用“清除已提交的任务”向导。

遵循这些步骤:

1. 依次导航到“系统”、“清除已提交的任务”。

   此时会出现“重现”步骤。

2. 选择排定新的作业，输入作业名称和该作业的排定信息，然后单击“下一步”。

   此时会出现“清除已提交的任务”。

3. 输入最小时长、存档、审核超时、时间限制和任务限制信息，然后单击“完成”。

   新作业已排定。

修改现有作业

要修改现有作业，请使用“清除已提交的任务”向导。

遵循这些步骤:

1. 依次导航到“系统”、“清除已提交的任务”。

   此时会出现“重现”步骤。

2. 选择“修改现有作业”，然后选择一项现有作业，修改排定信息，然后单击“下一步”。

   此时会出现“清除已提交的任务”。

3. 修改最小时长、存档、审核超时、时间限制和任务限制信息，然后单击“完成”。

   现有作业已修改。

删除周期任务

要删除周期任务，请遵循该步骤。

遵循这些步骤:

1. 导航到“系统”，选择“删除周期任务”。
2. 选择要删除的任务。
3. 单击“提交”。

清除已提交的任务选项卡

使用该选项卡可以指定任务的最小时长、存档、审核超时、时间限制和任务限制。 完成所有必填字段后单击“完成”。 该选项卡上的字段如下所示：

最小时长

指定处于最终状态（已完成、失败、已拒绝、已取消或已中止）的待清除任务的最小时长。 例如，如果指定了 1 个月，那么上个月中达到最终状态的所有任务都将被保留。 超过一个月之前达到最终状态的所有任务则可能被清除并存档。

这是必填字段。

存档

将任务备份到存档数据库，然后再将其从运行时数据库删除。

一旦运行作业，如果选择了存档，那么会将数据提交到存档数据库，并且从运行时任务持久性数据库中删除。 直到成功提交到存档数据库后才会删除数据。

审核超时

指定审核状态中的任务可能被清除之前的时间长度。 状态为审核的任务不会被视为处于最终状态，直到超过这个时间段为止。 处于审核状态的任务尚未提交。

时间限制

将清除限制为特定的时间长短。

任务限制

将清除限制为特定的任务数量。

删除周期任务

当某项任务无需按周期运行时，CA CA Identity Manager 管理员可以删除该任务。一旦删除该任务，就不再为其执行垃圾收集和存档。

使用“清除已提交的任务： 重现”向导排定的所有任务都列在此页中，CA CA Identity Manager 管理员可以选择要删除的任务。

注意：这些任务仍在数据库中，删除的仅是排定重现。

配置 Enterprise Log Manager 连接

使用此屏幕，可管理新增的 CA 用户活动报告 (CA UAR) 连接任务。

注意：CA Enterprise Log Manager 已更名。 现在称为 CA UAR。

该屏幕上的字段如下所列：

连接名称

指定用于单个 CA UAR 连接管理对象的唯一名称。

这是一个只读字段。

说明

说明 CA UAR 连接。

主机名

指定 CA UAR 服务器主机名或 IP 地址。

这是必填字段。

端口号

指定 CA UAR 服务器连接端口。

默认值：52520

这是必填字段。

认证机构签署的 SSL 证书

选中该项后，指定连接到 CA UAR 服务器时要执行的严格 SSL 证书检查。

如果您有自签署的 SSL 证书（例如，默认情况下与 CA UAR 一起安装的证书），则不得选中该复选框，因为根认证机构的受信路径不存在。

证书名称

指定用于身份验证的 CA UAR 证书的名称。

这是必填字段。

证书密码

指定 CA UAR 密码。

这是必填字段。

属性

不支持。 尝试将连接信息保存为测试时会检索版本。

删除企业日志管理器连接

从列表中选择连接，然后单击“删除”。 CA UAR 连接会被删除。

管理密钥

使用密钥来管理加密或解密数据的动态密钥。 如果您怀疑某个用户获得了未经授权的密钥访问权限，可以更改密钥库的密码。密钥库是存储密钥的数据库。一旦您更改此密码，CA Identity Manager 会对密钥值重新加密。

每个环境各有一套动态密钥和密钥库密码。 如果环境共享用户目录，则为每个环境使用相同的动态密钥和密钥库密码。

密钥库密码使用嵌入在 CA Identity Manager 服务器安装期间输入的加密代码或参数的密钥进行加密。 在群集中，所有节点共享动态密钥和密钥库密码的值。

加密操作使用最新的动态密钥用于对应的算法和环境。解密操作检查密钥 ID 是否存在于加密数据中，以便使用正确的密钥。 《配置指南》的“加密文本格式”一节提供更多信息。

遵循这些步骤:

1. 输入或修改密钥库的密码。
2. 如果需要其他密钥，请单击“添加密钥”。
3. 选择算法。
4. 为密钥输入密码。

   对于 PBE 和 RC2，最大密钥长度是 128 个字节。

   对于 AES，有效密钥大小是 16、24 和 32 个字节。
5. 单击“提交”。
6. 如果您修改了密钥库密码，请单击“提交”。

   CA Identity Manager 会对密钥值重新加密。

第 21 章： 任务持久性

此部分包含以下主题：

自动化的任务持久性无用单元收集和存档

在该版本中，管理员能够使用特定参数对作业进行排定和修改，以便通过“清除已提交的任务”任务来清除和存档任务持久性数据库中的任务和事件信息，以及根据需要删除这些周期任务。

在“系统”选项卡中，可以通过选择“清除已提交任务”启动一个向导。 然后，该向导将引导您完成设置和排定作业，以及是否存档数据的过程。 必要时，您还可以通过选择“系统”选项卡中的“删除周期任务”选择删除这些周期作业。

通过对任务进行排定以清理和存档任务数据，可以大大降低性能问题或系统运行中断的可能性。通过使用存档功能，您可以首先将任务备份到存档数据库中，然后再将其从运行时数据库删除。 如果您需要返回来查看这些删除的任务，请选择“查看提交的任务”中的“搜索存档”复选框，来搜索和查看所有已删除和存档任务的列表。

重现选项卡

使用该选项卡可排定作业。 该选项卡上的字段如下所示：

立即执行

立即运行该作业。

排定新的作业

排定新的作业。

修改现有作业

指定您是否要修改一个已存在的作业。

注意：仅当已为该任务排定了作业时才会出现该字段。

作业名

指定想要创建或修改的作业的名称。

时区

指定服务器的时区。

注意：如果您的时区与服务器的时区不同，则会显示一个下拉框以便您可以在排定新作业时选择您的时区或者服务器的时区。 修改现有作业时不能更改时区。

按周排定

指定一周中运行作业的特定一天或几天以及时间。

高级排定

指定其他排定信息。

周内某日

指定周内该作业运行的一天或几天。

执行时间

指定作业运行当天的时间（以 24 小时制的格式）。 例如，14:15。

Cron 表达式

有关填充该字段的信息，请参阅以下页面：

http://www.opensymphony.com/quartz/api/org/quartz/CronExpression.html

注意：当选中“高级排定”时会出现该字段。

更多信息

删除周期任务 (p. 489)
排定新的作业 (p. 488)
修改现有作业 (p. 489)
立即执行作业 (p. 488)

清除已提交的任务选项卡

使用该选项卡可以指定任务的最小时长、存档、审核超时、时间限制和任务限制。 完成所有必填字段后单击“完成”。 该选项卡上的字段如下所示：

最小时长

指定处于最终状态（已完成、失败、已拒绝、已取消或已中止）的待清除任务的最小时长。 例如，如果指定了 1 个月，那么上个月中达到最终状态的所有任务都将被保留。 超过一个月之前达到最终状态的所有任务则可能被清除并存档。

这是必填字段。

存档

将任务备份到存档数据库，然后再将其从运行时数据库删除。

一旦运行作业，如果选择了存档，那么会将数据提交到存档数据库，并且从运行时任务持久性数据库中删除。 直到成功提交到存档数据库后才会删除数据。

审核超时

指定审核状态中的任务可能被清除之前的时间长度。 状态为审核的任务不会被视为处于最终状态，直到超过这个时间段为止。 处于审核状态的任务尚未提交。

时间限制

将清除限制为特定的时间长短。

任务限制

将清除限制为特定的任务数量。

立即执行作业

要立即执行作业，请使用“清除已提交的任务”向导。

遵循这些步骤:

1. 依次导航到“系统”、“清除已提交的任务”。

   此时会出现向导的“重现”步骤。

2. 依次选择“立即执行”和“下一步”。

   此时会出现向导的“清除已提交的任务”步骤。

3. 输入最小时长、存档、审核超时、时间限制和任务限制信息，然后单击“完成”。

   该作业会立即提交。

排定新的作业

要排定新的作业，请使用“清除已提交的任务”向导。

遵循这些步骤:

1. 依次导航到“系统”、“清除已提交的任务”。

   此时会出现“重现”步骤。

2. 选择排定新的作业，输入作业名称和该作业的排定信息，然后单击“下一步”。

   此时会出现“清除已提交的任务”。

3. 输入最小时长、存档、审核超时、时间限制和任务限制信息，然后单击“完成”。

   新作业已排定。

修改现有作业

要修改现有作业，请使用“清除已提交的任务”向导。

遵循这些步骤:

1. 依次导航到“系统”、“清除已提交的任务”。

   此时会出现“重现”步骤。

2. 选择“修改现有作业”，然后选择一项现有作业，修改排定信息，然后单击“下一步”。

   此时会出现“清除已提交的任务”。

3. 修改最小时长、存档、审核超时、时间限制和任务限制信息，然后单击“完成”。

   现有作业已修改。

删除周期任务

要删除周期任务，请遵循该步骤。

遵循这些步骤:

1. 导航到“系统”，选择“删除周期任务”。
2. 选择要删除的任务。
3. 单击“提交”。

如何迁移任务持久性数据库

在之前的版本中，在“运行中”使用管理控制台即可完成迁移。 提供了命令行迁移工具，以在迁移大量任务时消除性能瓶颈。 您也能将迁移微调为特定环境、任务的状态以及在特定日期范围内创建和运行的任务。命令行工具 runmigration 位于以下文件夹中：

```
admin_tools/tools/tpmigration
```

为了迁移任务持久性数据库，您必须执行以下步骤：

1. 更新 tpmigration125.properties 文件
2. 设置 JAVA_HOME 变量。
3. 运行 runmigration 工具。

更新 tpmigration125.properties 文件

要设置任务持久性数据库迁移，您必须使用对象存储和任务持久性信息（包括存储值）更新 tpmigration.properties 文件。 Tpmigration125.properties 文件位于以下位置：

<IAM suite folder>/tools/tpmigration/com/ca/tp/migratetpto125

要设置迁移，完成属性文件中的以下信息：

```
############################################################
# The object store is required to obtain the environment details.
############################################################
os.db.hostname=<hostname>
os.db.dbname=<database-name or SID>
os.db.username=<db user name>
os.db.password=<db user's password>
os.db.port=<db port number>
os.db.dbType=<type of the database.  For ex. for SQL server sql2005 and for oracle
'oracle'>

############################################################
# Task persistence data where the old and new tables are.
############################################################
tp.db.hostname=<hostname>
tp.db.dbname=<database-name or SID>
tp.db.username=<db user name>
tp.db.password=<db user's password>
tp.db.port=<db port number>
tp.db.dbType=<type of the database.  For ex. for SQL server sql2005 and for oracle
'oracle'>
```

设置 JAVA_HOME 变量

为了迁移工具正常运行，您必须确保设置了环境变量 JAVA_HOME。

运行 runmigration 工具

要启动迁移，请使用以下程序。

通过命令行

1. 运行 runmigration 工具。

   对于 Windows：

   ```
   runmigration.bat
   ```

   对于 UNIX：

   ```
   runmigration.sh
   ```

2. 输入以下信息：

   - 该环境受保护的别名（“all”为所有环境）。

     注意：如果您不指定全部，则只能输入一个环境。

   - 任务状态。
     注意：如果您不指定全部，则只能输入一个任务状态。
   - 从 (1-8.x, 2-12.0) 迁移的 CA CA Identity Manager 版本。
   - 是否要指定要迁移的任务的日期范围 (y/n)。

     注意：如果选择“y”，您必须输入以下内容：

     - 输入开始日期 (mm/dd/yy)
     - 输入结束日期 (mm/dd/yy)

   迁移开始。

在迁移完成之后，状态指出迁移了多少任务。