IBM Cloud Identity Portal

管理指南

IBM Cloud Identity Portal

管理指南

IBM

Cloud Identity Portal 管理指南

© Copyright IBM Corporation 2015, 2017.

目录

© Copyright IBM Corp. 2015, 2017

第 1 章 IBM Cloud Identity Portal

欢迎使用 Cloud Identity Portal 文档，您可以在其中找到有关如何管理 Cloud Identity Service 的信息。

© Copyright IBM Corp. 2015, 2017

第 2 章 服务需求

服务需求包括 Cloud Identity Service 所支持的浏览器。

浏览器

Cloud Identity Portal 管理和自助服务应用程序所支持的浏览器。

表 *1.* 受支持的浏览器

浏览器	版本	操作系统
Microsoft Internet Explorer	最新版本和最新版本的前一版本。	Windows。
Mozilla Firefox	最新版本。	Windows 和 Mac。
Google Chrome	最新版本。	Windows 和 Mac。
Safari	最新版本和最新版本的前一版本。	Mac。

注：在最新版本和前一版本受支持的情况下，这些版本的所有修订版都受支持。例如，如果浏览器的最新版本为 24.*n*，那么版本 24.*n* 和 23.*n* 受支持。

注：Microsoft Edge 是当前最新的 Microsoft 浏览器。Microsoft Internet Explorer 11 是当前最新的 Internet Explorer 版本。

© Copyright IBM Corp. 2015, 2017

第 3 章 Cloud Identity Portal 概述

熟悉 Cloud Identity Portal 关键功能和概念。

特性和功能

Cloud Identity Portal 是一个综合管理环境，供您管理所有身份和访问管理过程。

公司信息

公司信息提供贵组织中负责管理或维护 Cloud Identity Portal 的个人的公司级别联系信息。

目录管理

目录管理是用于管理用户身份的系统和过程。用户可以组织成组，按角色进行定义，并可以与若干服务关联。

您可以管理用户、组、角色、服务和用户密码策略。您执行的添加和更改都会在 Cloud Identity Service 认证和授权上立即生效。

API 密钥管理

使用"API 密钥管理"来创建、编辑和移除 API 凭证，贵组织可以通过这些凭证来使用公共 Cloud Identity Portal API。

应用程序管理

应用程序管理是指对自助服务应用程序进行配置和定制。自助服务应用程序包含用户申请和维护其身份概要文件所需的所有应用程序。

配置自助服务应用程序包括配置自注册选项、密码重置选项和用户名恢复选项。

定制自助服务应用程序 UI 包括定制品牌形象、电子邮件模板、表列标签和用户概要文件区段标签。

Web 访问管理

Web 访问管理是指管理与受保护 Web 资源的网络连接。

您可以通过创建和管理与受保护 Web 资源的网络连接来管理 Web 访问。您还可以通过创建授权策略来控制对受保护资源的访问。授权策略包括访问控制表 (ACL)、受保护对象策略 (POP) 和全局用户策略。

© Copyright IBM Corp. 2015, 2017

联合单点登录

联合单点登录 (SSO) 使具有 Cloud Identity Service 帐户的用户能够使用现有身份访问其他第三方应用程序服务。Cloud Identity Service 环境可以支持多个联合合作伙伴。

对于支持使用 SAML 2.0 的联合单点登录的一些热门合作伙伴应用程序服务，提供了预先配置的模板。如果您要为其创建连接的合作伙伴不存在模板，那么可以使用定制配置。

身份供应

用户和组可以使用身份供给由外部目录同步或供应，也可以使用身份供给同步或供应到外部目录。

Cloud Identity Service 可以与超过 70 种身份存储库（例如 Active Directory、LDAP V3、关系数据库、SOAP 服务、消息队列和 SAP）连接。

请求管理

如果常规核准人不可用且没有委派核准人，Cloud Identity Portal 管理员可能需要管理服务的用户请求。

报告

Cloud Identity Service 针对审计存储库中的所有审计事件数据提供了特别报告功能。您可以使用一些预定义报告，并且可以定义自己的报告。

第 4 章 公司概况

公司概况信息提供了公司级别的联系信息。帐户联系人负有对 Cloud Identity Portal 进行维护的管理职责。

概述

公司概况信息提供了公司级别的联系信息。帐户联系人负有对 Cloud Identity Portal 进行维护的管理职责。使用 API 密钥管理来生成 API 凭证，贵组织可以通过这些凭证来使用公共 Cloud Identity Portal API。

添加帐户管理用户

您可以添加帐户管理用户。帐户管理用户有维护 Cloud Identity Portal 的管理职责。

过程

1. 在导航菜单中，单击**公司概况** > **帐户管理**，然后单击**帐户管理**和**添加新帐户**。
2. 在**用户名**字段中为用户输入用户名。单击**检查可用性**以检查帐户用户名是否唯一。
3. 输入该联系人的其余联系详细信息和凭证。

   注：密码可能需要最小字符数以及最小所指定字符类型数。使用字段帮助来发现密码需求。
4. 单击**保存**。

   该联系人在"帐户管理"页面中可用。

管理 API 密钥

生成 API 凭证，贵组织可以通过这些凭证来使用公共 Cloud Identity Portal API。

关于此任务

创建、编辑和移除 API 密钥。

过程

1. 在导航窗格中，单击**公司概况** > **API 密钥管理**。
2. 管理 API 密钥。

   添加 REST API 密钥

   a. 单击 **+ 添加新 API 密钥**。

© Copyright IBM Corp. 2015, 2017

b. 指定下列字段：

表 2. *API* 密钥字段

字段	描述
密钥别名	使用 50 个或更少的字母数字字符为 API 密钥创建易于识别的备用名称。
密钥描述	描述密钥的用途和所在位置。
访问令牌有效性	指定此令牌的有效时间（以秒计）。所输入值的近似小时数或天数将显示在此字段旁边。您将客户机标识、密钥和 grant_type 发送到 URL POST https://GmaApi/oauth/token 之后，将获得访问令牌。使用此访问令牌来调用 API。 **注：**该密钥将在您创建新的 API 密钥之后显示一次。在保存对新 API 密钥的更改后，该密钥将永远不再显示。 在访问令牌到期之后，请使用客户机标识、密钥和 grant_type 来获取新的访问令牌。或者，可以通过使用刷新令牌以及客户机标识和密钥来获取新的访问令牌。
刷新令牌有效性	指定**刷新令牌有效性**时间的秒数，它必须大于**访问令牌有效性**值。所输入值的近似小时数或天数将显示在此字段旁边。

编辑或删除 REST API 密钥

a. 通过在**缩小搜索范围**栏中进行搜索，或者通过单击密钥名称旁边的箭头，查看要编辑或删除的 API 密钥的详细信息。

b. 选择要编辑或删除的 API 密钥名称。

c. 执行下列其中一个操作：

- 编辑并更改表 1 中任何字段的值。
- 单击**移除密钥**以永久删除该密钥。

第 5 章 人员

人员管理是用于管理用户身份的系统和过程。用户可以组织成组，并按角色进行定义。

人员管理概述

人员管理任务包括管理用户、组和服务。

您可以创建、修改、删除和搜索用户、组和服务。您执行的添加和更改都会在 Cloud Identity Service 认证和授权上立即生效。例如，如果为用户创建了帐户记录，那么该用户就可以访问 Cloud Identity Service 和自助服务应用程序。您还可以将用户添加到组中以授予他们对特定 Web 应用程序的访问权。如果需要审批，那么服务成员资格可能不会立即生效。

用户

您可以添加、修改、删除和搜索用户记录。用户记录可以作为身份或帐户创建。帐户授予用户对自助服务应用程序以及可能对 Cloud Identity Service 管理的其他资源的登录访问权。身份只是有关用户的信息记录。

用户记录由若干用户身份属性组成。其中许多属性（例如，名字、姓氏和电子邮件地址）对大部分身份管理系统都是通用的。贵组织还有一些特定于您自己的应用程序集的属性。在为贵组织进行 Cloud Identity Service 初始配置期间，将从贵组织中已存在的记录或身份存储库源收集属性。大部分现有用户记录都是根据这些现有身份存储库创建的。

组

通过统一处理用户以最佳方式制定各种身份和访问管理策略决策。具有一些共同特征的用户可以分组在一起。例如，对于在公司同一个部门工作的一组用户，可以为其授予对指定 Web 应用程序的相同访问权。在此情况下，定义用户组，然后由一个访问控制表（ACL）策略引用该组。该策略授予（或拒绝）该组中的所有用户的应用程序访问权。

组的用户成员资格可以通过静态或动态方式定义。静态用户成员资格要求手动将每个用户添加到组并手动管理组成员资格。动态用户成员资格自动选择用户以授予成员资格。成员资格基于身份属性值、其他组/服务成员资格或管理者角色分配的任意匹配组合。例如，您可以将位于特定国家或地区的用户分组在一起。可以将账号属于特定帐号范围且同时是其他指定组成员的用户分组在一起。

© Copyright IBM Corp. 2015, 2017

动态用户成员资格使用动态供应策略来实现，在此策略中，您定义组成员资格选择条件。

模式管理

您可以通过添加定制身份属性来扩展用户身份记录中的信息帮助，从而管理 LDAP（轻量级目录访问协议）模式。

管理用户

您可以添加、修改、删除和搜索用户记录。

用户概述

用户记录可以作为身份或帐户创建。帐户授予用户对 Cloud Identity Service、自助服务应用程序以及由 Cloud Identity Service 管理的其他资源的登录访问权。身份只是有关用户的信息记录。

用户记录由若干用户身份属性组成。其中许多属性（例如，名字、姓氏和电子邮件地址）对几乎所有身份管理系统都是通用的。贵组织还有一些特定于您自己的应用程序集的属性。在为贵组织进行 Cloud Identity Service 初始配置期间，将从贵组织中已存在的记录或身份存储库源收集属性。

组和服务成员资格可以分配给用户，并可以为特定用户创建定制用户策略。用户策略定义最大登录失败次数、最长密码寿命、帐户到期日期以及用户的一天中的具体时间约束。

搜索用户

您可以搜索贵组织中的任何用户记录来查看该用户的详细信息或修改该用户的详细信息。

关于此任务

如果为用户输入了名字、用户名或电子邮件地址值，您可以搜索用户的这些属性值。只能使用名字、用户名或电子邮件地址的前几个字符。不能使用通配符。必须至少输入用户的名字、用户名或电子邮件地址的前 3 个字符。例如，要搜索电子邮件地址为 psmith@company.com 的帐户用户记录，可以输入 psm。输入的前几个字符越多，搜索准确性越高。

如果想要使用用户的名字来搜索记录，可以使用用户的名字或姓氏。例如，要搜索名为 Paul Smith 的用户，可以输入 pau 或 smi。还可以在搜索中输入以空格分隔的多个字符串，例如，可以输入 pau smi。

一次搜索最多可以返回 1000 条用户记录。

过程

1. 在导航窗格中，单击**人员** > **用户**。
2. 在**开始搜索**字段中，至少输入用户的名字、姓氏、用户名或电子邮件地址的前 3 个字符。 您可以在搜索中输入以空格分隔的多个字符串。

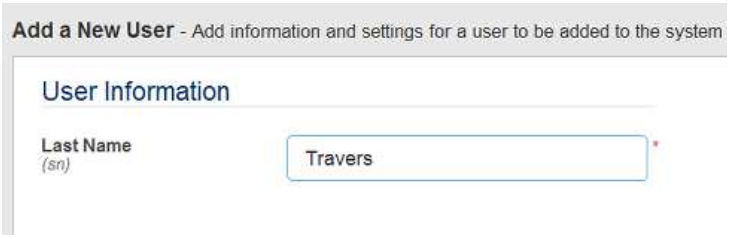
字段标签将更改为**过滤结果**。此时将列出与搜索条件匹配的用户。选择要修改或查看的用户。

添加用户记录

您可以添加用户记录。您可以将记录添加为帐户或身份。只有具有帐户的用户才能访问 Cloud Identity Service、受保护资源以及自助服务应用程序。

过程

1. 在导航窗格中，单击**人员** > **用户**，然后单击**添加用户**。

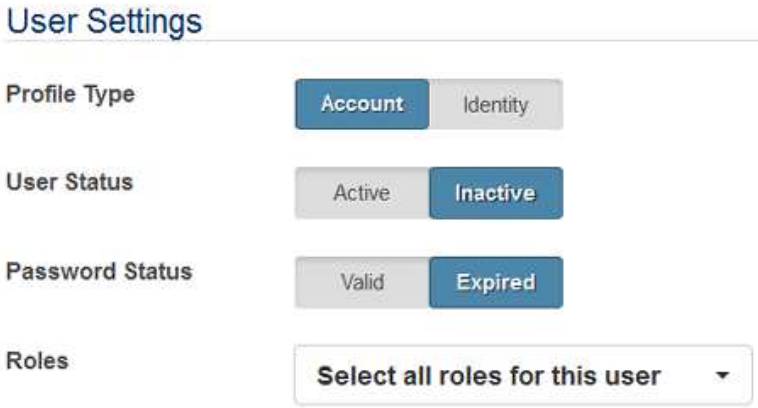


2. 在**姓氏**字段中输入用户姓氏。
3. 选择用户类型是帐户还是身份。

   帐户用于为用户授予对 Cloud Identity Service 的登录访问权。身份只是有关用户的信息记录。

   - 要创建只有身份的用户记录，请单击**身份**。
   - 要创建具有帐户的用户记录，单击**帐户**并完成以下步骤：
     a. 在**用户名**字段中为用户输入用户名。单击**检查可用性**以检查用户名是否唯一。

     b. 选择**活动**或**不活动**作为用户状态。活动状态允许用户登录 Cloud Identity Portal。



c. 选择**有效**或**到期**作为密码状态。到期状态强制用户在下次成功登录时更改其密码。如果状态为"有效"，那么用户可以在不更改密码的情况下登录。

d. 选择用户角色。单击**角色**菜单，然后选中每个适用于用户的角色。

注： 如果概要文件类型为"帐户"，那么保存记录时会自动分配 **gtwayPrincipalName** 属性。保存记录时，帐户记录会自动成为 **gatewaywamservice** 的成员。

4. 可选： 为用户添加更多身份属性。添加所需数目的属性。 例如，您可以添加中间名和移动电话。

a. 单击**添加其他属性**。

在搜索字段中输入一串字符来搜索要添加的属性。您可以搜索属性中的任何字符串。属性按注册表名称和可用的 Cloud Identity Service 名称（标签）列出。这两个名称都包含在搜索中。标签仅当可用时才会包含在内。 例如，要搜索 User Name，可以输入 `use` 或 `ser`。

b. 输入属性值。

注： **Password** 属性用于重置密码。该字段通常在用户自注册期间填充。您无法查看用户密码。

5. 单击**保存更改**以保存记录。

向用户添加组成员资格

您可以手动向用户添加组成员资格。您可以向静态或动态管理的组添加成员资格。

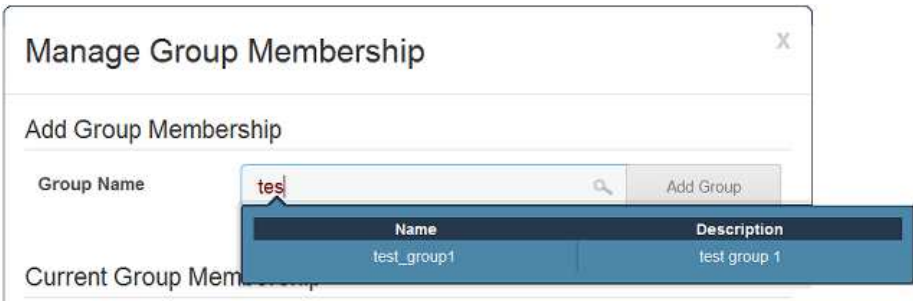
关于此任务

如果手动管理组，也可以向静态组添加用户。

注： 如果手动向用户添加动态管理的组的成员资格，那么该用户的持续成员资格在下次策略协调时由该组的策略确定。

过程

1. 搜索并选择用户。
2. 在**用户设置**中：
   - 如果组是您向其中添加用户的第一个组，单击**添加新组**。
   - 如果用户已经是一个或多个组的成员，单击**管理组成员资格**。



3. 在**组名**字段中，搜索想要将用户添加到的组。要搜索组，请至少输入该组名的前 3 个字符。
4. 选择组并单击**添加组**。
5. 单击**完成**。

向用户添加服务成员资格

您可以手动向用户添加服务成员资格。向用户添加服务成员资格遵从已就绪的任何服务审批。

关于此任务

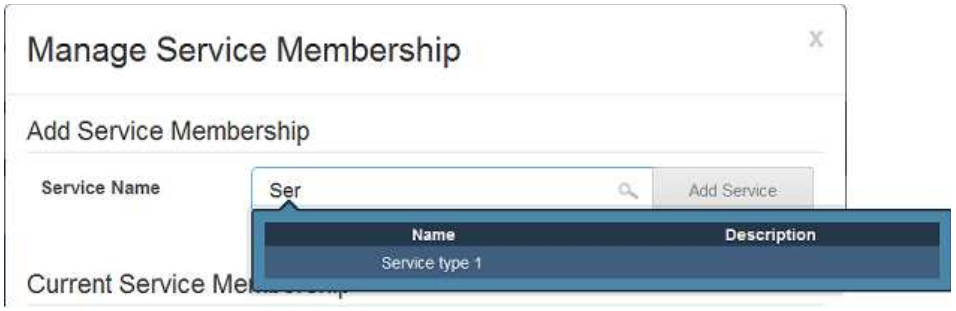
在向用户添加服务成员资格且该服务已有就绪的审批策略时，不会自动将该用户添加到该服务。在此情况下，将生成一个有关使该用户成为该服务成员的请求，然后向核准人发送暂挂服务请求电子邮件通知。

注：如果向用户添加动态管理的服务的成员资格，那么该用户的持续成员资格在下次策略协调时由该服务的策略确定。

您也可以在管理服务时将用户添加到服务成员资格。

过程

1. 搜索并选择用户。
2. 在**用户设置**中，单击**管理服务成员资格**。



3. 在**服务名称**字段中，搜索想要将用户添加到的服务。要搜索服务，请至少输入该服务名称的前 3 个字符。
4. 选择服务并单击**添加服务**。

向用户添加用户策略

用户策略用于定义一些密码验证限制、帐户到期日期和一天中的具体时间限制。全局用户策略应用于所有用户。定制用户策略应用于特定用户。

关于此任务

在用户级别设置的策略设置将覆盖全局策略中的对应设置。缺省情况下，所有用户级别的策略值均未设置。用户级别未设置的策略设置继承全局策略中的对应设置（如果有）。

过程

1. 搜索并选择用户。
2. 在**用户设置**中，单击**管理用户策略**。
3. 设置所需用户策略设置。
4. 单击**保存**。

   您可以将相同用户策略应用于其他用户。
5. 单击**完成**。

用户策略设置

表 *3.* 用户策略设置

设置	描述
最大登录失败次数	在帐户被锁定之前，用户可以尝试的最大登录失败次数。如果此选项设置为 0 或"未设置"，那么表示不限制登录失败尝试次数。 • **设置**。最大登录失败尝试次数。如果此选项设置为 0，那么表示不限制登录失败尝试次数。 • **未设置**。不限制登录失败尝试次数。
禁用时间间隔	指定超过"最大登录失败次数"计数之后是否锁定用户帐户。 • **设置**。超过"最大登录失败次数"计数之后锁定用户帐户。帐户被永久或暂时禁用。 • **未设置**。永远不会因为登录失败尝试而锁定用户帐户。"未设置"等同于将"最大登录失败次数"设置为 0 或"未设置"，用户可以进行无限次登录尝试。 • **永久禁用**。用户被永久锁定，直到 Cloud Identity Portal 管理员将该用户的用户状态设置为有效为止。 • **暂时禁用**。以秒为单位表示的时间，在此期间，用户帐户将在超过"最大登录失败次数"计数之后保持锁定状态。该帐户将在经过此时间间隔之后解锁。
最小长度	有效帐户密码所需的最少字符数。 • **设置**。密码的最少字符数。 • **未设置**。无最小密码长度。

表 3. 用户策略设置 (续)

设置	描述
最少字母数	帐户密码所需的最少字母字符数。 • **设置**。密码必须包含的最少字母字符数。 • **未设置**。不限制最小值。
最少非字母数	帐户密码所需的最少非字母字符（数字或特殊字符）数。 • **设置**。密码必须包含的最少非字母字符数。如果设置为 0，那么不限制最小值。 • **未设置**。不限制最小值。
最大重复字符数	帐户密码中允许的最大连续重复字符数。 • **设置**。允许的最大重复字符数。 • **未设置**。不限制重复字符数。
允许空格?	指定帐户密码是否可以包含空格。 • **设置**。指定是否允许空格。 – **是**。允许空格。 – **否**。不允许空格。 • **未设置**。允许空格。
密码到期?	密码创建之后保持有效的最长时间，之后将到期且必须更改。 • **是**。密码有效的天、小时、分钟和秒数。如果所有值都设置为 0，那么密码永不到期。 • **否**。密码永不到期。
跟踪密码复用?	指定重置密码时是否可以使用相同密码。 • **是**。用户重置或更改其密码时，不能使用相同密码。请指定新的唯一密码的数目，必须先设置此数目，然后才能复用旧密码。 • **否**。用户重置其密码时，可以使用相同密码。
帐户到期?	指定一个到期日期，在此日期之后所有帐户都设置为无效。该设置通常仅用于个人用户策略覆盖。例如，如果某个合同商对特定资源具有有限的访问期限，那么可以使用此选项来禁用特定日期的此访问权。 • **设置**。帐户的到期日期。以 YYYY/MM/DD 格式输入日期。 • **未设置**。有效期不受限，帐户有效性永不到期。
限制访问权?	指定用户可以访问系统的一天中具体时间约束。 • **是**。用户可以访问 Cloud Identity Service 的日期和一天中的具体时间。时间可以服务的本地时间或全球标准时间表示。 • **否**。用户可以随时访问 Cloud Identity Service。

重置用户密码

作为 Cloud Identity Portal 的管理员，您可以重置用户密码。

关于此任务

在以 Cloud Identity Portal 中的管理员身份重置用户密码时，会向该用户帐户记录添加密码属性。出于安全原因，用户帐户记录不会显示密码属性和密码值。当您添加密码属性并输入值时，就是在执行密码重置。在重置密码之后，当您再次访问该用户帐户记录时，将不会显示密码属性和值。

如果密码被重置的用户具有电子邮件地址，那么他们会收到一封电子邮件，通知其密码已被重置。

过程

1. 在导航窗格中，单击**目录管理** > **用户**。
2. 搜索并选择用户。
3. 单击**添加其他属性**。

4. 在搜索字段中输入一串字符来搜索密码属性，然后选择密码属性。 例如，输入 `pass`。

   属性按注册表名称和 Cloud Identity Service 名称（标签）列出。这两个名称都包含在搜索中。
5. 在**密码**字段中输入密码。 您输入的字符在显示中将使用星号字符代替。
6. 单击**保存更改**以保存记录。

管理组

通过以相同的方式处理用户组，可以最佳方式实现一些身份和访问管理决策。您可以通过手动选择用户来创建组，或者创建自动确定组成员资格的动态策略。

组概述

具有共同特征的用户可以分组在一起，以便对他们采用统一的处理方法。例如，对于在公司同一个部门工作的一组用户，可以为其授予对指定 Web 应用程序的相同访问权。

组的用户成员资格可以通过静态或动态方式定义。静态用户成员资格要求手动将每个用户添加到组并手动管理组成员资格。动态用户成员资格自动选择用户来授予成员资格，选择依据是用户身份属性值、其他组成员资格、其他服务成员资格或是否为其分配了管理者角色的任意匹配组合。例如，您可以将位于特定国家或地区的用户分组在一起。可以将账号属于特定帐号范围且同时是其他指定组成员的用户分组在一起。

动态用户成员资格使用动态供应策略来实现，在此策略中，您定义组成员资格选择条件。

可以为组定义任意数量的策略。可以通过协调策略按需应用策略。还可以根据计划应用策略。应用策略时，将评估其选择条件，并更新用户成员资格，以便移除不匹配的用户并添加匹配的用户。

搜索组

您可以搜索贵组织中的任何组来查看该组的详细信息，或者修改该组的详细信息以及管理该组的成员资格。

过程

1. 在导航窗格中，单击**人员** > **组**。
2. 在**过滤结果**字段中，至少输入组的前 3 个字符。字段标签将更改为**正在搜索**。

   此时将列出与搜索条件匹配的组。选择要修改或查看的组。

创建组

您可以创建新组。在创建组之后，可以通过静态或动态管理组来选择要成为组成员的用户。

过程

1. 在导航菜单中，单击**人员** > **组**，然后单击**添加组**。
2. 输入该组的名称和描述。 单击**检查可用性**来检查组名是否已被使用。
3. 单击**保存更改**以添加组。

下一步做什么

创建组后，您可以手动或动态向该组添加成员。

静态管理组成员资格

静态定义的用户成员资格要求手动添加和除去每个用户成员。

过程

1. 搜索并选择想要向其添加成员的组。
2. 单击**管理组成员资格**。

3. 在**用户名**字段中，搜索想要添加的用户。要搜索用户，请输入用户的名字、姓氏、用户名或电子邮件地址的前 3 个字符。
4. 选择用户并单击**添加成员资格**。
5. 添加所需的所有用户之后，单击**完成**。

以动态方式管理组成员资格

动态供应策略允许组的用户成员资格基于匹配条件。将自动选择与条件匹配的用户以授予该组的成员资格。

创建动态供应策略

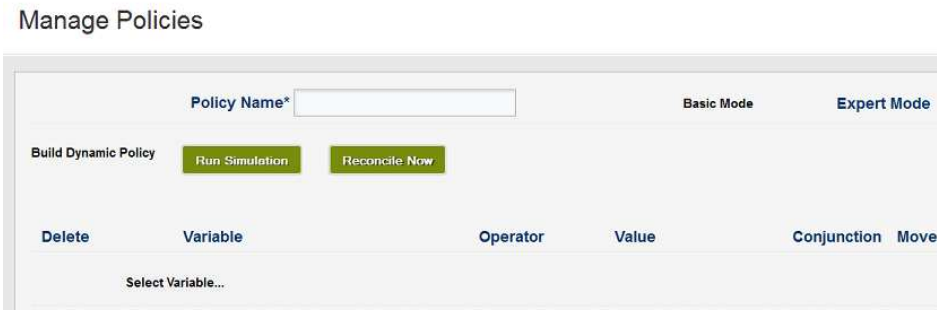
动态供应策略用来确定组的用户成员资格。

关于此任务

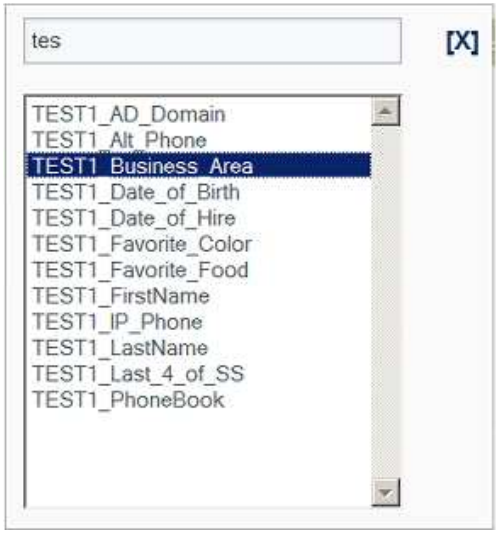
成员资格基于策略的选择条件。例如，您可以通过确定工作位置的属性或通过确定另一个组的工作位置和成员资格的属性来指定组成员资格。一个组可以有一个或多个策略。

过程

1. 搜索并选择想要将策略添加到的组。
2. 对于**动态供应策略**，单击**管理策略**。
3. 单击**添加新策略**。



4. 在**策略名称**字段中为策略输入有意义的名称。
5. 选择想要使用的变量，您可以选择要在策略中使用的任意类型的一个或多个变量。 您可以选择以下变量类型的任意组合：
   - **属性**。基于用户身份属性包含用户。
   - **组**。基于其他组成员资格包含或排除用户。
   - **服务**。基于服务成员资格包含或排除用户。
   - **管理者**。基于是否为其分配了管理者角色来包含用户。
6. 要将用户身份属性用作变量：
   a. 单击**选择变量**，然后单击**属性**。
   b. 单击**过滤属性**字段，然后输入属性的前几个字符。双击属性以将其选中。

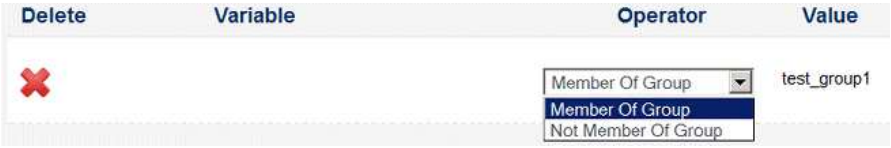


c. 选择**运算符**，然后输入属性**值**。

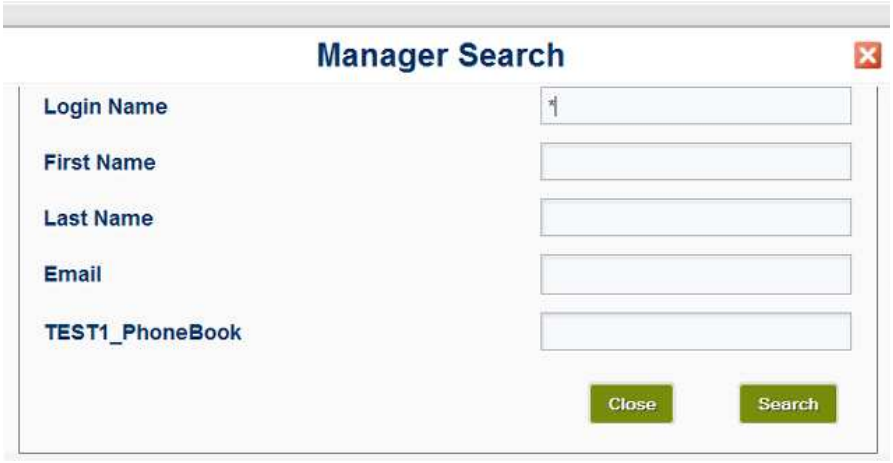
注：您可以使用通配符。例如，可以输入 11* 以表示以 11 开头的任何数字。

提示：如果贵组织具有使用日期值的用户属性，那么您可以将这种属性视为时间戳记。有关使用时间戳记的更多信息，请参阅第 21 页的『时间戳记值』。要搜索和查看贵组织正在使用的属性，请参阅第 26 页的『管理定制属性』。

7. 要将另一个组的成员资格或非成员资格用作变量：
   a. 单击**选择变量**，然后单击**组**。
   b. 单击**过滤组**字段，然后输入组的前几个字符。双击组以将其选中。
   c. 选择成员资格是取决于此另一组的成员资格还是非成员资格。



8. 要将服务的成员资格或非成员资格用作变量：
   a. 单击**选择变量**，然后单击**服务**。
   b. 单击**过滤服务**字段，然后输入服务的前几个字符。双击服务以将其选中。
   c. 选择成员资格是取决于此服务的成员资格还是非成员资格。
9. 要将管理者角色用作变量：
   a. 单击**选择变量**，然后单击**管理者**。



b. 在**管理者搜索**窗口中的任何字段中输入搜索条件来搜索用户。单击**搜索**。 这样仅返回分配了管理者角色并且与搜索条件匹配的用户。

注：您可以在搜索中使用通配符。例如，可以输入 Joh* 以表示以 Joh 开头的名称。

c. 选择用户。 您可以重复搜索以添加更多用户。

10. 使用**合取**字段来组合一个或多个变量以确定组成员资格。使用合取值 And 或 Or 将一个比较条件的结果与下一行组合起来。

变量（条件）分组将自顶向下进行，以便先前条件的结果与后续条件组合起来。

使用箭头图标可上下移动条件  。

在以下示例中，仅使用一个变量来确定成员资格：用户身份属性 TEST1_Business_Area。要成为成员，用户的 TEST1_Business_Area 属性必须具有值 London W4。

在以下示例中，使用两个变量确定成员资格。要成为成员，用户的 TEST1_Business_Area 属性必须具有值 London W4，并且用户必须是 Group1 的成员。

在以下示例中，使用三个变量确定成员资格。要成为成员，用户的 TEST1_Business_Area 属性必须具有值 London W4，并且用户必须是 Group1 的

成员或者 Group2 的成员。

11. 在定义了需要在策略中包含的所有条件之后，单击**保存**。

下一步做什么

模拟策略以检查成员资格是否符合预期。

时间戳记值：

如果要将属性和属性值视为时间戳记，那么可以使用 `$date$` 作为值的前缀。

`$date$` 前缀将采用缺省日期格式 yyyy-MM-dd HH:mm:ss。例如，您可以输入 `$date$1970-01-01 00:00:00` 以指定 1970 年 1 月 1 日午夜，也可以通过输入 `$date$now` 指定当前时间。

您还可以为时间戳记指定非缺省格式，方法是使用 SimpleDateFormat 将该格式包含在 `$date$` 前缀中。例如，对于 Z 时间戳记，您可以输入 `$date{yyyy-MM-dd HH:mm:ssZ}$1970-01-01 00:00:00-0400`，以在比 GMT/UTC 早 4 个小时的时区中表示 1970 年 1 月 1 日午夜。更改缺省格式会导致相同格式应用于所检索的属性值。您必须了解要检索的值的格式。所检索日期值的格式必须与要使用的格式一致。有关不同日期格式模式的更多信息，请参阅 SimpleDateFormat。

如果规则中指定的值或其比较值都未进行解析，那么将记录警告或错误。有关更多信息，请与 IBM 支持代表联系。全球标准时间 (UTC) 是缺省时区。

在以下示例中，使用了两个属性变量，以根据聘用日期来确定成员资格。要成为成员，用户的聘用日期必须在 2016 年 1 月 1 日之后且在当前日期和时间之前。

以专家方式创建动态供应策略

在某些情况下，无法使用基本属性比较和其他组或服务成员资格来确定组的策略选择条件。成员资格可能要求检查随其他属性值而变化的属性值（子字符串）。在此类情况下，必须以专家方式定义策略。

开始之前

要使用专家方式，必须充分了解并能够熟练地用 JavaScript 编码。

关于此任务

您可以用 JavaScript 以专家方式定义策略。

在策略评估期间，将针对注册表中的每个用户运行一次 JavaScript。JavaScript 检查用户及其成员资格的注册表属性，并决定是否将用户包含在组中。JavaScript 使用变量 **inGroup** 将此决定传达给 Cloud Identity Service。如果 JavaScript 的结果是 **inGroup** 等于 TRUE，那么将用户包含在组中，否则不包含用户。

JavaScript 可以使用三种方法来获取有关每个用户的 Cloud Identity Service 注册表属性和组信息。

- `String isMemberOfGroup(String groupName)`
- `String[] getAttributeValues(String attributeName)`
- `String evaluateAttribute(String attributeName, int operator, String constant)`

其中每种方法都使用可供 JavaScript 使用的另一个变量 **ldap** 进行调用。例如，要确定当前用户是否是名为 **accounting** 的组的成员，可以使用以下语句：

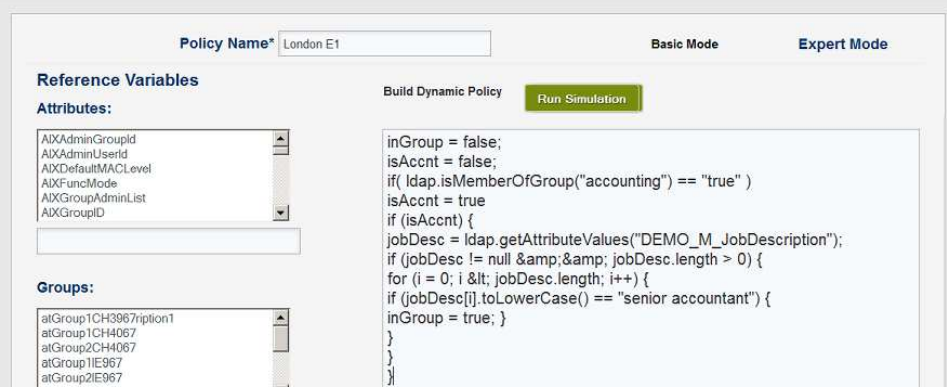
```
var isAccountant = ldap.isMemberOfGroup("accounting");
```

在以下 JavaScript 示例中，如果用户是 **accounting** 组的成员，同时在属性 **DEMO_M_JobDescription** 中具有值 **senior accountant**，那么将该用户包含在策略组中。

```
// assume user is not in group
inGroup = false;
isAccnt = false;
if( ldap.isMemberOfGroup("accounting") == "true" )
isAccnt = true
if (isAccnt) {
jobDesc = ldap.getAttributeValues("DEMO_M_JobDescription");
if (jobDesc != null && jobDesc.length > 0) {
for (i = 0; i < jobDesc.length; i++) {
if (jobDesc[i].toLowerCase() == "senior accountant") {
inGroup = true; }
}
}
}
```

过程

1. 搜索并选择想要将策略添加到的组。
2. 对于**动态供应策略**，单击**管理策略**。
3. 单击**添加新策略**。
4. 单击**专家方式**。



5. 输入想要用于确定成员资格的 JavaScript。

   属性、**组**和**服务**在各自的框中列出以供您参考。您可以在相应框下方的过滤器字段中输入前几个字符来搜索属性、组或服务。您可以复制并粘贴所选属性、组或服务。

6. 在定义了要在策略中使用的所有条件之后，单击**保存**以保存策略。

下一步做什么

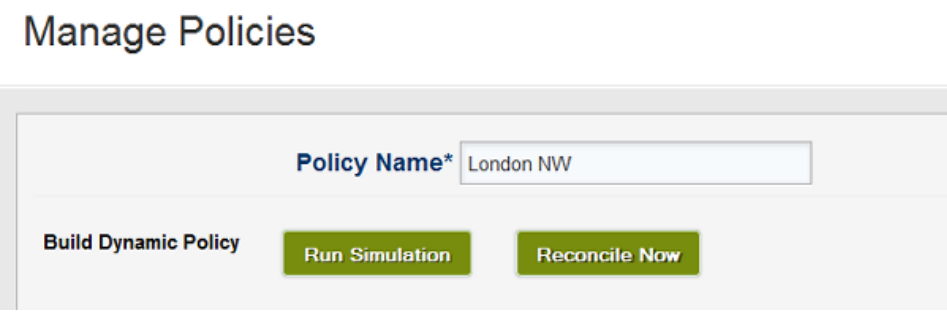
模拟策略以检查成员资格是否符合预期。

模拟策略

您可以模拟策略来评估组的用户成员资格，从而检查成员资格是否符合预期。模拟不会更改组的成员资格。它显示包含该组的建议成员资格的用户。可以 CSV 文件形式查看和保存结果。

过程

1. 如果没有选择策略，搜索并选择组。打开"管理策略"窗口以编辑策略。
2. 单击**运行模拟**。



3. 选择要运行的模拟类型。
   - **模拟目录中的所有用户**。该选项将策略选择与 Cloud Identity Service 中的所有用户进行比较。满足策略的用户将以添加或保留状态列示在结果中。不满足策略的用户将以从组中除去或未添加状态列示在结果中。
   - **模拟当前位于组中的所有用户**。该选项比较策略选择条件与当前位于组中的所有用户的属性。组中的每个用户以除去或保留状态列示在结果中。新用户不会以添加状态列出。

- **模拟单个用户**。该选项比较策略选择条件和所选用户。该用户以保留、除去、添加或未添加状态列示在结果中。使用用户名搜索用户。在**过滤用户**字段中输入用户名的前几个字符，单击**搜索用户**，然后选择用户。

4. 单击**运行模拟**。

   单个用户供应策略模拟的结果显示在"模拟供应策略"窗口中。

   关闭"模拟策略"窗口以返回到"管理策略"窗口，然后单击**取消**。
5. 单击"管理策略"窗口中的**刷新**以查看模拟结果。当模拟完成时，将显示复选标记图标和指向 CSV 文件的链接。

6. 查看结果。
   - 单击复选标记图标 ✔ 以打开"模拟结果"窗口。您可以通过清空或选中列标题复选框来选择要查看的结果列。关闭"模拟结果"窗口以返回到"管理策略"窗口。

     注：单击**清空模拟结果**以清除"模拟结果"窗口和"管理策略"窗口中的所有结果。
   - 单击 CSV 图标  可以 CSV 文件形式查看结果。您可以打开文件或保存文件。

下一步做什么

1. 协调策略。
2. 激活策略。

协调动态策略

在创建策略之后，可以协调该策略。在策略经过协调后，将根据策略选择条件来实现组的用户成员资格。

过程

1. 搜索并选择组。打开"管理策略"窗口以编辑策略。
2. 单击**立即协调**。

此时将显示警告消息。单击**确定**以协调策略。

下一步做什么

激活策略。

激活并计划动态策略

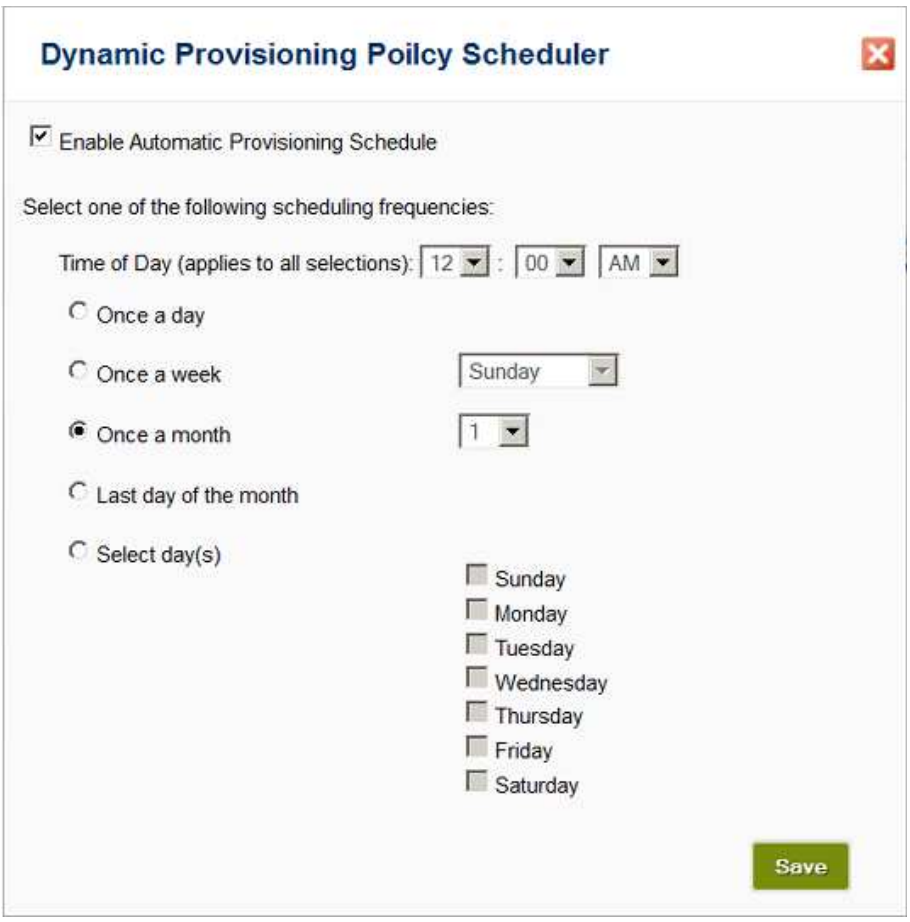
在创建和模拟策略并验证模拟结果之后，策略已准备就绪，可以对其进行激活和计划。激活策略按计划运行，因此每当运行计划时便会对组成员资格进行评估和更新。

过程

1. 如果没有选择策略，搜索并选择组。打开"管理策略"窗口以编辑策略。
2. 选择要激活的策略的**选择活动项**。

此时将显示警告消息。单击**确定**以激活策略。

3. 单击计划图标  以打开"动态供应策略计划程序"窗口。



4. 选中**启用自动供应计划**复选框。
5. 选择要运行计划的频率：
   - **每天一次**。选择**一天中的具体时间**。
   - **每周一次**。从下拉列表中选择周历日，然后选择**一天中的具体时间**。
   - **每月一次**。从下拉列表中选择月历日，然后选择**一天中的具体时间**。
   - **每月最后一天**。选择**一天中的具体时间**。
   - **选择若干天**。选中要运行计划的日期的复选框，然后选择**一天中的具体时间**。
6. 单击**保存**。

管理定制属性

用户记录由若干用户身份属性组成。您可以将定制属性添加到用于用户记录的身份属性集。

属性概述

用户记录由若干身份属性构成。大多数身份属性（例如，名字、姓氏和电子邮件地址）对于几乎所有身份管理系统都是通用的。

通用属性取自一组标准 LDAP（轻量级目录访问协议）属性。贵组织可能还有一些特定于您自己的应用程序集的属性。这些特定属性是定制属性。您可以创建更多定制属性。

搜索属性

您可以搜索可在身份记录中使用的任何属性。

过程

1. 在导航窗格中，单击**人员** > **模式管理**。
2. 在**开始搜索**字段中，请至少输入属性的前 3 个字符，字段标签将更改为**正在搜索**。

   此时将列出与搜索条件匹配的属性。选择要修改或查看的属性。

   您可以使用**显示缺省值**和**显示用户添加值**复选框来过滤列表。用户添加的属性为定制属性。您可以单击列标题以按该列对列表进行排序。

创建定制属性

您可以创建要在身份记录中使用的新定制属性。

开始之前

您必须对 LDAP（轻量级目录访问协议）、LDAP 模式以及贵公司的身份记录需求有基本的了解。

过程

1. 在导航窗格中，单击**人员** > **模式管理**。
2. 单击**添加新属性**。

3. 输入属性的名称和描述。 名称必须唯一，可以通过单击**检查可用性**来检查名称是否唯一。

   注：对于名称，可以使用字母数字字符 A-Z 和 0-9。可以使用特殊字符连字符 (-) 和下划线 (_)。不能使用空格。

   对于描述，可以使用字母数字字符 A-Z 和 0-9。可以使用特殊字符连字符 (-) 和下划线 (_)。还可以使用空格。
4. 输入属性设置。
5. 单击**保存更改**以添加属性。

属性设置

属性设置包括类型和多值用法。

表 4. 属性设置

设置	描述
类型	属性类型。 • **字符串**。Unicode (UTF-8) 字符串 • **布尔值**。 • **整数**
多值	指定属性是否可以具有许多不同的值。 • **True**。允许多值。 • **False**。只允许一个值。

管理用户的批量导入

您可以批量装入用户数据以在 Cloud Identity Portal 中创建用户身份记录。

开始之前

您需要具备对 JSON 和 System for Cross-domain Identity Management (SCIM) 文件的应用知识并具备对 REST API 的基本了解。

SCIM 文件

您将 System for Cross-domain Identity Management (SCIM) 文件上载到 Cloud Identity Portal 来批量装入用户数据。

SCIM 文件提供与平台无关的模式以 JSON 格式表示用户。有关 SCIM 的更多信息，请参阅 System for Cross-domain Identity Management。SCIM 文件包含一组操作，其中每个操作表示一个用户记录创建。操作通过 Cloud Identity Portal 管理 REST API 进行处理。每个成功的操作都会在 Cloud Identity Portal 中创建新用户记录。每个 SCIM 文件最多可以创建 5000 个操作，但您可以上载所需数量的文件。以下显示了示例 SCIM 文件的格式和内容。

```
{
 "operations": [
  {
   "method": "POST",
   "path": "/Users",
   "bulkId": "importtest1",
   "data": {
    "userName": "userimporttest1",
    "active": true,
    "password": "core1234",
    "emails": [{
     "value": "nomail@gmail.com",
     "type": "",
     "primary": "true"
    }],
    "name": {
     "familyName": "import",
     "middleName": "mid",
     "givenName": "ctest1"
    },
```

```
    "addresses": [{
     "streetAddress": "123 oak st",
     "locality": "fort worth",
     "region": "texas",
     "postalCode": "77077",
     "country": "USA",
     "type": "home",
     "primary": "true"
    }],
    "title": "title",
    "preferredLanguage": "en-US",
    "userType": "Contractor"
   }
  },
   {
   "method": "POST",
   "path": "/Users",
   "bulkId": "importtest1",
   "data": {
    "userName": "userimporttest2",
    "active": true,
    "password": "core1234",
    "emails": [{
     "value": "nomail2@gmail.com",
     "type": "",
     "primary": "true"
    }],
    "name": {
     "familyName": "import",
     "middleName": "mid",
     "givenName": "ctest2"
    },
    "addresses": [{
     "streetAddress": "123 oak st",
     "locality": "fort worth",
     "region": "texas",
     "postalCode": "77077",
     "country": "USA",
     "type": "home",
     "primary": "true"
    }],
    "title": "title",
    "preferredLanguage": "en-US",
    "userType": "Contractor"
   }
  }
 ]
}
```

表 *5.* 操作参数

参数	类型	是否必需	描述
method		是	方法要执行的操作。操作为 POST。
path	路径	是	指定要更新的对象的路径。路径是 /Users。
bulkId	字符串	是	事务标识。每个事务标识都有关联的响应状态。
data	对象	是	包含用户属性。
userName	字符串	是	指定用户的用户名。用户名必须唯一。

表 5. 操作参数 (续)

参数	类型	是否必需	描述
active	布尔值	是	指定用户记录是身份还是帐户。如果希望用户具有 Cloud Identity Service 帐户，设置为 true。如果没有帐户，那么用户无法向 Cloud Identity Service 进行认证，也无法访问自助服务应用程序。如果设置为 false，用户记录将创建为身份，而不是帐户。
password	字符串	可选	用于访问 Cloud Identity Service 和自助服务应用程序的密码。
emails	对象	可选	包含用户的电子邮件地址。
value	字符串	可选	有效电子邮件地址。
type	字符串	可选	电子邮件类型，例如，个人、办公室或社交。
primary	布尔值	可选	指定该电子邮件是否为用户的主要电子邮件地址。
name	对象	是	包含用户的名称属性。
familyName	字符串	是	用户的姓氏。
middleName	字符串	可选	用户的中间名字。
givenName	字符串	可选	用户的名字。
addresses	对象	可选	包含用户的邮政地址。
streetAddress	字符串	可选	邮政地址中的地点信息（街道、道路、位置或大道以及号码）。
locality	字符串	可选	所在地的名称，例如城市或县。
region	字符串	可选	范围大于所在地的地理区域的名称。例如，省/自治区/直辖市的全名。
postalCode	字符串	可选	邮政服务用来识别邮政服务区域的代码。
country	字符串	可选	国家或地区的名称。
type	字符串	可选	地址类型，例如，住宅或办公室。
primary	字符串	可选	指定该地址是否为用户的主要地址。
title	字符串	可选	人员的个人称谓，例如 Mr、Ms、Dr、Prof 和 Rev。
preferredLanguage	字符串	可选	用户的语言代码。例如，en-us 或 fr-ca。如果未指定，那么将使用 LDAP 中设置的首选语言。如果未设置首选语言，那么将使用缺省语言"美国英语"。
userType	字符串	可选	用户类型的名称，例如合同商。

导入用户

您可以导入 System for Cross-domain Identity Management (SCIM) 文件以在 Cloud Identity Portal 创建新用户。

开始之前

必须创建打算上载的 SCIM 文件。

过程

1. 在导航窗格中，单击**人员** > **导入用户**。
2. 单击**上载 SCIM** 以浏览并选择要上载的文件。

第 6 章 自助服务

自助服务应用程序管理是指对自助服务应用程序进行配置和定制。自助服务应用程序包含用户申请和维护其身份概要文件所需的所有应用程序。

配置自助服务应用程序

配置自助服务应用程序包括配置自注册选项、密码重置选项、用户名恢复选项和定义角色。

配置概述

自助服务应用程序在为贵组织进行 Cloud Identity Service 初始设置期间配置。您可以更改一些设置和选项来适应您的更改需要。

自助服务应用程序允许用户控制其 Cloud Identity Service 帐户的各个方面。例如，用户可以自注册帐户以获取对受保护资源的访问权，可以重置自己的密码，恢复自己的用户名以及更改自己的概要文件信息。对自助服务应用程序的访问权由用户角色确定。

自注册

自注册应用程序允许用户在 Cloud Identity Service 中申请帐户。在大多数情况下，所有用户都必须进行自注册，然后才能管理自己的概要文件和获取受保护资源（例如，Web 应用程序和服务器）的访问权。

您可以更改自注册选项，包括帐户的供应和批准方式。您可以对自注册表单上的区段和字段进行添加、除去和重新排列。

密码重置

密码重置应用程序可以配置为允许用户重置忘记的密码。您可以更改密码重置选项，包括必须回答的问题数量和是否使用电子邮件验证。

用户名恢复

用户无法想起用户名时，便无法登录或重置密码，因为无法确定其帐户。用户名恢复应用程序允许用户恢复其忘记的帐户用户名。您可以更改用户名恢复选项，包括是在屏幕上显示用户名，还是将用户名发送到用户的电子邮件地址。

© Copyright IBM Corp. 2015, 2017

自助服务概要文件

自助服务概要文件应用程序允许用户在注册并能够向 Cloud Identity Service 进行认证之后管理自己的帐户概要文件信息。您可以对概要文件设置表单上的区段和字段进行添加、除去和重新排列。

安全问题

安全问题用于在用户想要重置密码时验证用户身份。用户在自注册时必须提供安全问题答案。要在密码重置期间验证用户身份，自注册期间提供的答案必须与密码重置期间提供的答案匹配。

在为贵组织进行 Cloud Identity Service 初始配置期间，定义若干安全问题。您可以向已定义的问题中添加新问题，并可以隐藏问题。可以设置用户在自注册时必须提供答案的最小问题数。

角色

角色可以认为是贵组织中的职衔。例如，管理者、管理员或帮助台联系人。角色定义用户集合。角色用于控制对不同自助服务应用程序和操作的访问。

配置自注册选项和表单

您可以修改自注册供应和审批选项以及自注册表单中的字段。

配置自注册选项

自注册允许用户在 Cloud Identity Service 中申请帐户。自注册可以配置为以不同方式工作。您可以更改自注册选项，包括帐户的供应方式和审批选项。

过程

1. 在导航窗格中，单击**自助服务** > **自注册**。
2. 选择所需自注册选项。
3. 单击**保存更改**。

自注册选项：

自注册选项包括格式设置、审批和电子邮件选项。

表 *6.* 供应策略和格式设置选项

选项	描述
启用帐户申请	使用户能够使用电子邮件中发送的链接来申请帐户。 • **是**。用户可以使用电子邮件中的链接来申请帐户。用户通过电子邮件接收链接来申请帐户。通过单击该链接，用户可以通过成功自注册来申请帐户。 • **否**。用户不能使用电子邮件链接来申请帐户。

表 *6.* 供应策略和格式设置选项 *(续)*

选项	描述
启用 LDAP 身份验证	可以基于 LDAP 属性验证来供应用户帐户。用户身份记录必须存在，才能使用 LDAP 身份验证来供应用户。用户在自注册期间输入的属性值将与现有身份记录中的值进行比较。如果值匹配，那么可以供应该用户。要用于验证的 LDAP 属性必须在表单设置中选择并启用验证。 • **是**。如果成功验证了信息，那么可以为用户供应帐户。要用于验证的 LDAP 属性必须在表单设置中选择并启用验证。 **身份验证失败时**。当身份验证失败时，可以应用以下某个选项： – **拒绝注册**。拒绝用户注册。不创建帐户。 – **手动供应用户**。Cloud Identity Portal 管理员可以手动供应帐户。 – **自动供应用户**。自动为用户创建帐户。 **如果找到多个身份**。如果找到多个与用户输入的注册信息匹配的身份记录，可以应用以下某个选项： – **拒绝注册**。拒绝用户注册。不创建帐户。 – **手动供应用户**。Cloud Identity Portal 管理员必须手动供应用户帐户。 – **自动供应用户**。自动为用户创建帐户。 • **否**。无法基于 LDAP 属性验证来供应帐户。
首选用户名格式 **备用用户名格式**	首选和备用用户名格式。当用户进行自注册时，可以通过多种方法生成其用户名。存在首选格式的用户名时，将使用备选用户名格式。这两种格式必须不同。 • **允许用户选择用户名**。用户提供自己选择的用户名。 • **用户的电子邮件地址**。用户名设置为用户输入的电子邮件地址。 • **FirstName.LastName**。用户名由以句点分隔的用户名字和姓氏组成。例如，John.Smith。 • **FirstInitial.LastName**。用户名由以句点分隔的用户名字首字母缩写和姓氏组成。例如，J.Smith。 • **LastName.FirstInitial**。用户名由以句点分隔的用户姓氏和名字首字母缩写组成。例如，Smith.J。 • **FirstName.Middle.LastName**。用户名由以句点分隔的用户名字、中间名字首字母缩写和姓氏组成。例如，John.A.Smith。 • **填充来源**。用户名由用户针对指定 LDAP 属性输入的值组成。该属性必须存在于表单设置中。 • **调用定制方法**。用户名可以使用定制格式。 • **用户 UID**。

表 7. 审批和电子邮件选项

选项	描述
需要手动审批注册	Cloud Identity Service 用户手动批准用户注册。如果用户没有现有的身份记录，那么可以使用手动审批来供应帐户。手动审批也可以用于具有现有身份记录的用户。 • **是**。需要手动审批注册。您必须选择缺省核准人来批准注册。如果用户没有现有的身份记录，那么手动核准人是缺省核准人。如果用户有现有的身份记录，那么管理者可以批准注册。 – **需要管理者审批（如果可能）**。管理者批准注册。管理者只能批准具有现有身份记录的用户的注册。如果没有适用的管理者，那么由缺省核准人来批准注册。 在**缺省核准人**字段中搜索用户。输入用于批准注册的用户名字、姓氏或电子邮件地址的前 3 个字符。选择用户。 • **否**。不需要手动审批。
要求用户接受策略协议	必须接受策略协议才可注册。 • **是**。用户必须接受策略协议。 • **否**。用户无需接受策略协议。
需要身份验证问题	身份验证问题用于在用户重置密码时验证用户。这些问题的答案通常由用户在注册期间提供。 • **是**。用户必须提供身份验证问题的答案。 • **否**。用户无需提供注册期间的身份验证问题的答案。
注册暂挂时发送电子邮件	向用户发送电子邮件，值为**是**或**否**。
注册被拒绝时发送电子邮件	向用户发送电子邮件，值为**是**或**否**。
注册成功时发送电子邮件	向用户发送电子邮件，值为**是**或**否**。

配置自注册表单

自注册表单用于进行自注册。该表单包含用户在注册期间填写的一些字段。您可以对各个字段和区段进行重新排序，添加新区段，以及添加或除去字段。

过程

1. 在导航菜单中，单击**自助服务** > **自注册**，然后单击**表单设置**。

2. 添加字段：
   a. 单击**新增** > **新增字段**。

b. 选择属性和字段选项来定义字段。

c. 单击**保存更改**以添加字段。

3. 可选： 添加区段：

a. 单击**新增** > **新增区段**。

b. 输入该区段的**标签**、**副标题**和**标题**。 标签、副标题和标题用于在表单上标识该区段。

c. 单击**新增字段**以在该区段中输入新字段，选择属性和字段选项来定义字段。

d. 单击**保存更改**以保存该新区段。 您可以从主"自注册表单设置"窗口向该区段添加更多字段。

4. 要更改表单顺序并将某个区段或字段移到新位置，单击该字段或区段并拖动至新位置。

5. 单击**保存更改**以保存该表单。

表单选项：

表单选项用于设置自助服务应用程序中使用的字段特性。

根据所定义的表单，某些选项可能不可用。

表 *8.* 表单字段选项

选项	描述
LDAP 属性	要用作字段的 LDAP 属性。如果选择了要求输入另一个用户作为值的属性，将向该字段添加选择工具。例如，管理者属性可能要求输入另一个用户。 根据所定义的字段或表单，可能无法删除某些属性。
缺省值	字段的缺省值。如果字段可编辑，那么用户可以替换缺省值。
字段标签	用于标识字段的标签。

表 8. 表单字段选项 (续)

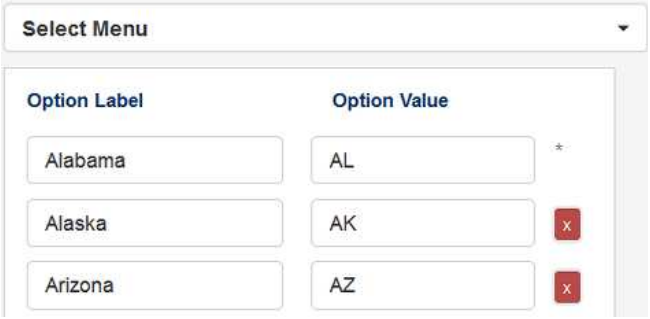
选项	描述
字段类型	• **复选框**。用户可以选择一个或多个选项作为字段输入。 • **密码字段**。密码字段带有掩码。 • **单选按钮**。用户可以从一些选项中选择一个选项作为字段输入。 • **选择菜单**。用户可以从一些选项中选择一个选项作为字段输入。 • **文本字段**。用户在字段中输入值以作为输入的文本。 • **文本区域**。自由格式的文本框。 对于**复选框**、**单选按钮**和**选择菜单**，请为字段添加选项。 • **选项标签**。用于标识选项的标签。 • **选项值**。选项的值。 在该示例中，选择菜单包含用于不同状态的一些选项。 
占位符	占位符标签。
工具提示	字段帮助文本。
是否可编辑	• **是**。用户可以在字段中输入值。 • **否**。用户不能在字段中输入值。某些字段中会填充现有数据。例如，在自注册期间，用户可能针对现有身份记录申请帐户，在此情况下，可以使用该身份记录中的字段值。
是否必需	• **是**。该字段为必填字段。 – 自注册表单。如果不为该字段提供值，用户无法完成自注册。 – 自助服务概要文件表单。提示用户输入任何未填充的必填字段的值。 • **否**。该字段为可选字段。
需要当前密码匹配	仅适用于密码 LDAP 属性。 • **是**。用户必须在单独的字段中输入两次密码。在每个字段中输入的值必须匹配以确认密码正确。 • **否**。仅在一个字段中输入一次密码。
带掩码	**是**。字段带掩码，在屏幕上看不到输入的值。输入的每个字符在屏幕上都替换为星号字符。

表 *8.* 表单字段选项 *(续)*

选项	描述
需要匹配字段	• **是**。用户必须在单独的字段中输入两次值。在每个字段中输入的值必须匹配以确认值正确。例如，当用户输入电子邮件地址时，您可以要求用户输入两次该地址。 • **否**。仅在一个字段中输入一次值。
验证	验证规则： • **是**。输入的值必须通过指定的验证规则。例如，日期可能需要通过格式验证规则，如 yyyy/mm/dd。 • **否**。不验证输入的值。 验证类型： • **日期**。值必须符合指定的日期格式。例如，yyyy/mm/dd。 • **电子邮件地址**。值必须对应于电子邮件地址格式。例如，*text_string*@*text_string*.com。 • **字母**。值必须仅包含字母字符。 • **最大字符长度**。值不能包含超过指定数量的字符。 • **最小字符长度**。值不能包含少于指定数量的字符。 • **数字**。值必须仅包含数字字符。 • **密码强度**。密码字段必须符合基本、标准或强验证规则。规则基于必须输入的字符数和字符类型。 • **美国电话号码**。值必须符合美国电话号码格式。 定制正则表达式。用于针对所输入值进行求值的正则表达式。如果表达式求值为 true，表示值有效。 • **模式**。正则表达式。例如，要将注册限制为北卡罗来纳州中的地址，使用正则表达式 ^NC$ 来表示 state 属性，其中，NC 定义为 state 属性的可选值。 • **错误消息**。输入的值无效时向用户显示的错误消息。

表 *9.* 表单区段选项

选项	描述
标签	区段标签。
副标题	副标题标签。
标题	标题。

自注册表单示例：

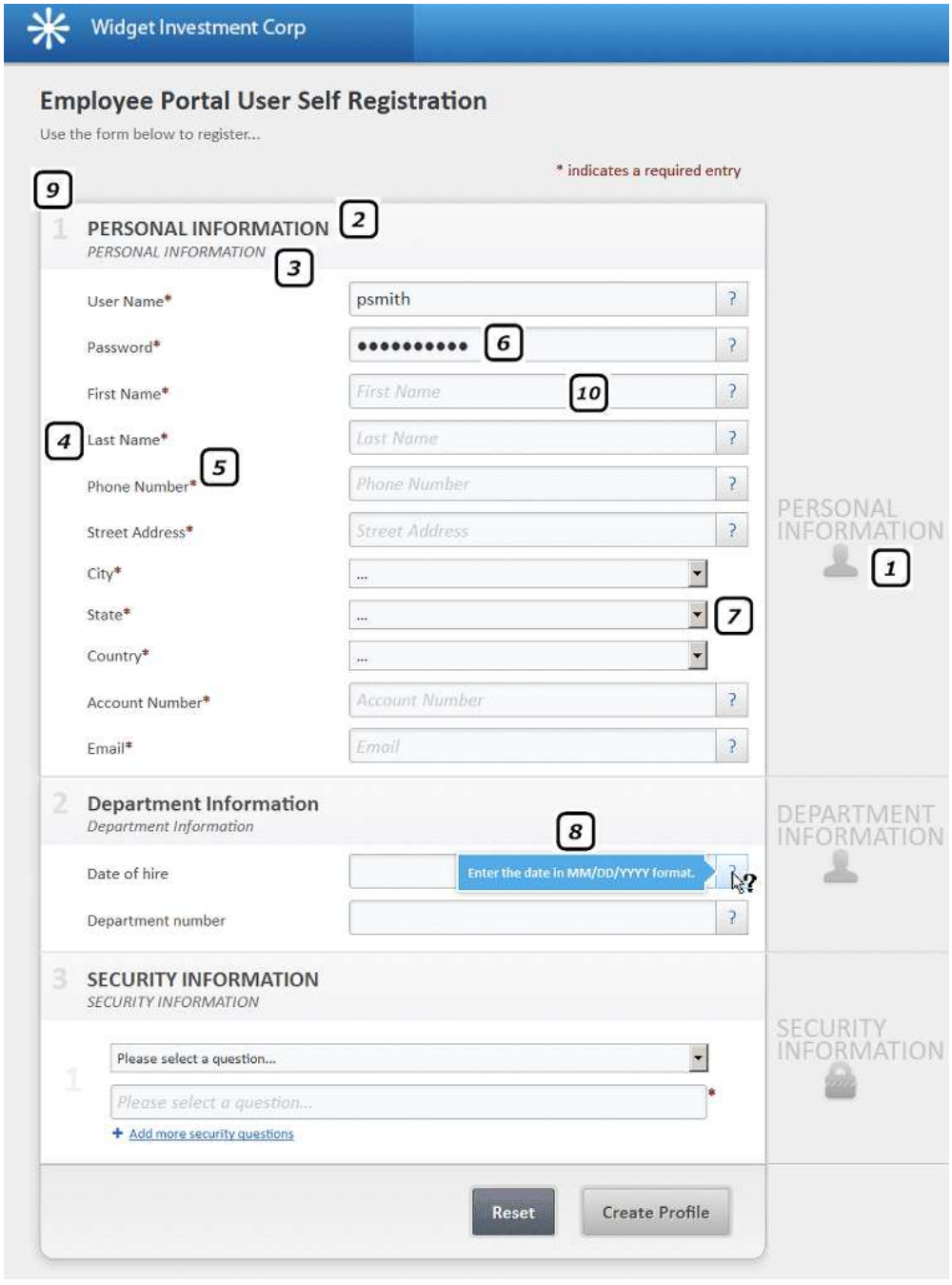


表 *10.* 自注册表单字段和区段元素

编号	描述
1	区段标签。
2	区段标题标签。
3	部分副标题标签。

表 *10.* 自注册表单字段和区段元素（续）

编号	描述
	字段标签。
	必填字段，由星号指示。
	带掩码的字段。密码字段始终带有掩码。
	选择菜单字段。
	工具提示字段帮助文本。
	部分编号。
	文本字段。

配置密码重置选项

您可以更改密码重置选项，包括必须回答的安全问题数量和是否使用电子邮件验证。

过程

1. 在导航窗格中，单击**自助服务** > **密码重置**.
2. 选择所需密码重置选项。
3. 单击**保存更改**。

密码重置选项

表 *11.* 密码重置选项

选项	描述
所需安全问题数	仅当**使用多因子认证**设置为**否**时才适用。它是用户为了能够重置其密码而必须回答的最小安全问题数。
最大失败尝试次数	仅当**使用多因子认证**设置为**否**时才适用。它是所有问题可接受的不正确回答总数。如果超过最大次数，那么用户将被锁定。

表 *11.* 密码重置选项（续）

选项	描述
需要电子邮件验证	仅当**使用多因子认证**设置为**否**时才适用。在用户请求密码重置之后，电子邮件验证要求用户单击通过电子邮件发送给他们的链接。 • **是**。需要电子邮件验证，以分钟为单位输入该链接有效的时间长度。用户必须在指定时间限制内使用该链接。 该链接将用户引导至密码重置窗口。  • **否**。不发送电子邮件。
成功重置时发送电子邮件	• **是**。向用户发送电子邮件以通知他们密码重置成功。 • **否**。不发送电子邮件。

配置用户名恢复选项和表单

您可以修改用户名恢复选项和字段。

配置用户名恢复选项

您可以配置用户名恢复选项，包括是在屏幕上显示用户名，还是将用户名发送到用户的电子邮件地址。

过程

1. 在导航窗格中，单击**自助服务** > **用户名恢复**。

2. 选择所需用户名恢复选项。
3. 单击**保存更改**。

用户名恢复选项：

表 *12.* 用户名恢复选项

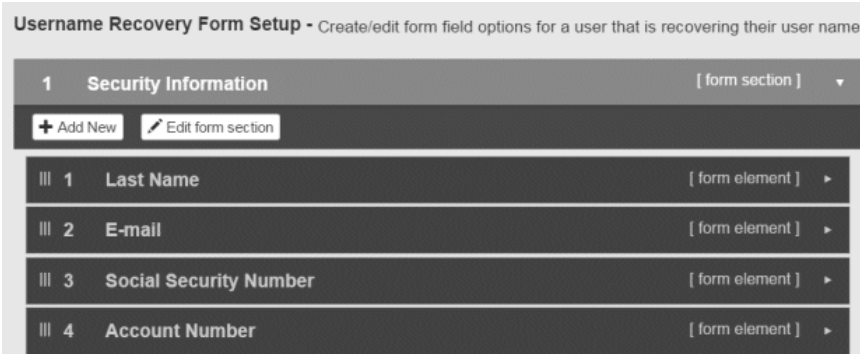
选项	描述
启用用户名恢复	• **是**。可以使用用户名恢复自助服务应用程序来恢复用户名。 • **否**。用户无法使用用户名恢复自助服务应用程序来恢复自己的用户名。
在屏幕上显示用户名	• **是**。用户名显示在用户名恢复自助服务应用程序的屏幕上。 • **否**。用户名在用户名恢复期间不显示在屏幕上。
将用户名发送到用户的电子邮件地址	• **是**。将用户名通过电子邮件发送给用户。 • **否**。不发送电子邮件。

配置用户名恢复表单

用户名恢复表单用于恢复用户名。该表单包含用户在用户名恢复期间填写的一些字段。您可以对各个字段和区段进行重新排序，添加新区段，以及添加或除去字段。

过程

1. 在导航菜单中，单击**自助服务** > **用户名恢复**，然后单击**表单设置**。



2. 添加字段：
   a. 单击**新增** > **新增字段**。
   b. 选择属性和字段选项来定义字段。
   c. 单击**保存更改**以添加字段。
3. 可选： 添加区段：
   a. 单击**新增** > **新增区段**。
   b. 输入该区段的**标签**、**副标题**和**标题**。 标签、副标题和标题用于在表单上标识该区段。
   c. 单击**新增字段**以在该区段中输入新字段，选择属性和字段选项来定义字段。
   d. 单击**保存更改**以保存该新区段。 您可以从主"用户名恢复表单设置"窗口向该区段添加更多字段。
4. 要更改表单顺序并将某个区段或字段移到新位置，单击该字段或区段并拖动至新位置。

5. 单击**保存更改**以保存该表单。

表单选项：

表单选项用于设置自助服务应用程序中使用的字段特性。

根据所定义的表单，某些选项可能不可用。

表 *13.* 表单字段选项

选项	描述
LDAP 属性	要用作字段的 LDAP 属性。如果选择了要求输入另一个用户作为值的属性，将向该字段添加选择工具。例如，管理者属性可能要求输入另一个用户。 根据所定义的字段或表单，可能无法删除某些属性。
缺省值	字段的缺省值。如果字段可编辑，那么用户可以替换缺省值。
字段标签	用于标识字段的标签。

表 *13.* 表单字段选项（续）

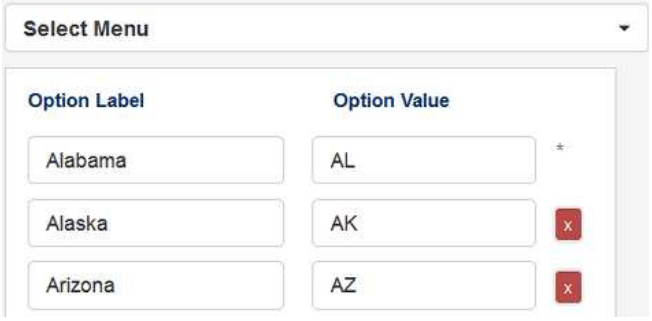
选项	描述
字段类型	• **复选框**。用户可以选择一个或多个选项作为字段输入。 • **密码字段**。密码字段带有掩码。 • **单选按钮**。用户可以从一些选项中选择一个选项作为字段输入。 • **选择菜单**。用户可以从一些选项中选择一个选项作为字段输入。 • **文本字段**。用户在字段中输入值以作为输入的文本。 • **文本区域**。自由格式的文本框。 对于**复选框**、**单选按钮**和**选择菜单**，请为字段添加选项。 • **选项标签**。用于标识选项的标签。 • **选项值**。选项的值。 在该示例中，选择菜单包含用于不同状态的一些选项。 
占位符	占位符标签。
工具提示	字段帮助文本。
是否可编辑	• **是**。用户可以在字段中输入值。 • **否**。用户不能在字段中输入值。某些字段中会填充现有数据。例如，在自注册期间，用户可能针对现有身份记录申请帐户，在此情况下，可以使用该身份记录中的字段值。
是否必需	• **是**。该字段为必填字段。 – 自注册表单。如果不为该字段提供值，用户无法完成自注册。 – 自助服务概要文件表单。提示用户输入任何未填充的必填字段的值。 • **否**。该字段为可选字段。
需要当前密码匹配	仅适用于密码 LDAP 属性。 • **是**。用户必须在单独的字段中输入两次密码。在每个字段中输入的值必须匹配以确认密码正确。 • **否**。仅在一个字段中输入一次密码。
带掩码	**是**。字段带掩码，在屏幕上看不到输入的值。输入的每个字符在屏幕上都替换为星号字符。

表 *13.* 表单字段选项 *(续)*

选项	描述
需要匹配字段	• **是**。用户必须在单独的字段中输入两次值。在每个字段中输入的值必须匹配以确认值正确。例如，当用户输入电子邮件地址时，您可以要求用户输入两次该地址。 • **否**。仅在一个字段中输入一次值。
验证	验证规则： • **是**。输入的值必须通过指定的验证规则。例如，日期可能需要通过格式验证规则，如 yyyy/mm/dd。 • **否**。不验证输入的值。 验证类型： • **日期**。值必须符合指定的日期格式。例如，yyyy/mm/dd。 • **电子邮件地址**。值必须对应于电子邮件地址格式。例如，*text_string*@*text_string*.com。 • **字母**。值必须仅包含字母字符。 • **最大字符长度**。值不能包含超过指定数量的字符。 • **最小字符长度**。值不能包含少于指定数量的字符。 • **数字**。值必须仅包含数字字符。 • **密码强度**。密码字段必须符合基本、标准或强验证规则。规则基于必须输入的字符数和字符类型。 • **美国电话号码**。值必须符合美国电话号码格式。 定制正则表达式。用于针对所输入值进行求值的正则表达式。如果表达式求值为 true，表示值有效。 • **模式**。正则表达式。例如，要将注册限制为北卡罗来纳州中的地址，使用正则表达式 `^NC$` 来表示 state 属性，其中，NC 定义为 state 属性的可选值。 • **错误消息**。输入的值无效时向用户显示的错误消息。

表 *14.* 表单区段选项

选项	描述
标签	区段标签。
副标题	副标题标签。
标题	标题。

用户名恢复表单示例：

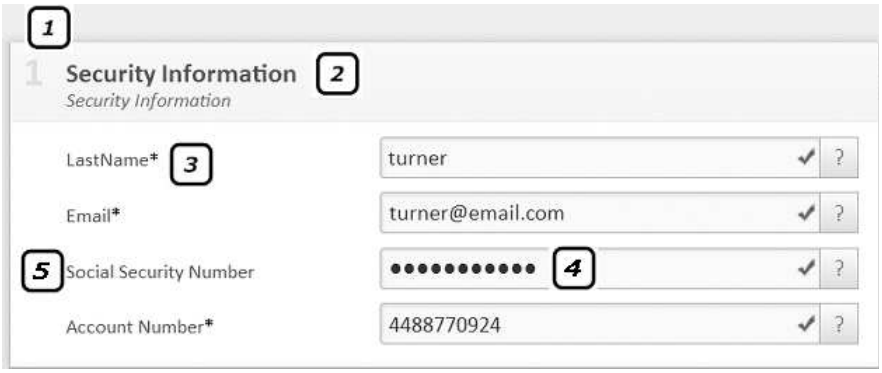


表 *15.* 用户名表单字段和区段元素

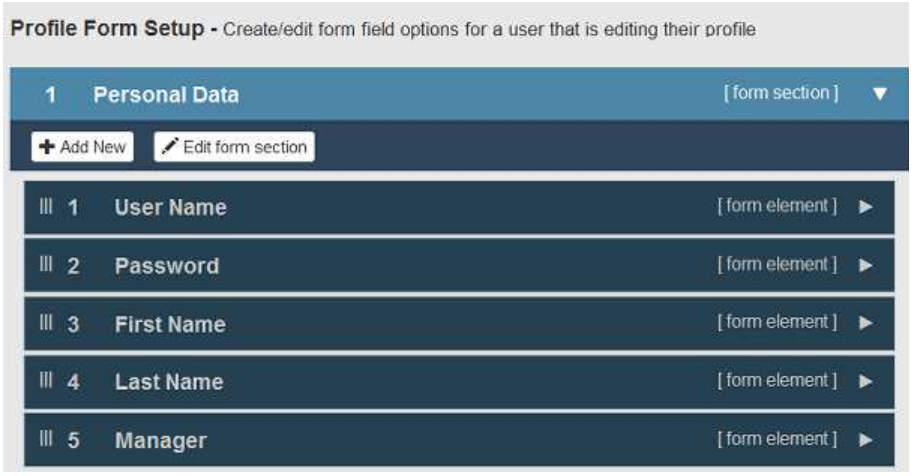
编号	描述
1	部分编号。
2	区段标签。
3	必填字段，由星号指示。
4	带掩码的字段。
5	字段标签。

配置自助服务概要文件表单

自助服务概要文件表单包含一些字段，这些字段构成了用户在自助服务概要文件应用程序中的概要文件。您可以对各个字段和区段进行重新排序，添加新区段，以及添加或除去字段。

过程

1. 在导航窗格中，单击**自助服务** > **自助服务门户网站**。



2. 要添加字段：
   a. 单击**新增** > **新增字段**。
   b. 选择属性和字段选项来定义字段。
   c. 单击**保存更改**以添加字段。
3. 要添加区段，请完成下列步骤：
   a. 单击**新增** > **新增区段**。
   b. 输入该区段的**标签**、**副标题**和**标题**。 标签、副标题和标题用于在表单上标识该区段。
   c. 单击**新增字段**以在该区段中输入新字段，选择属性和字段选项来定义字段。
   d. 单击**保存更改**以保存该新区段。 您可以从主"概要文件表单设置"窗口向该区段添加更多字段。
4. 要更改表单顺序并将某个区段或字段移到新位置，单击该字段或区段并拖动至新位置。

5. 单击**保存更改**以保存该表单。

表单选项

表单选项用于设置自助服务应用程序中使用的字段特性。

根据所定义的表单，某些选项可能不可用。

表 *16.* 表单字段选项

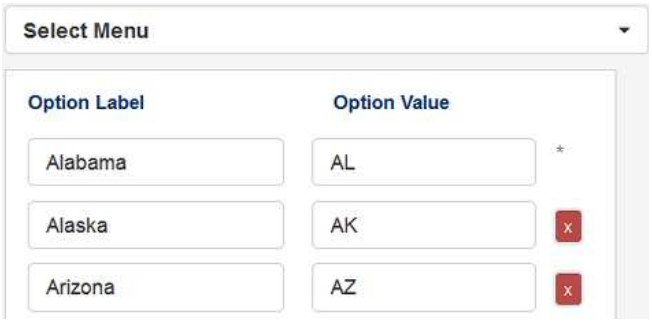
选项	描述
LDAP 属性	要用作字段的 LDAP 属性。如果选择了要求输入另一个用户作为值的属性，将向该字段添加选择工具。例如，管理者属性可能要求输入另一个用户。 根据所定义的字段或表单，可能无法删除某些属性。
缺省值	字段的缺省值。如果字段可编辑，那么用户可以替换缺省值。
字段标签	用于标识字段的标签。
字段类型	• **复选框**。用户可以选择一个或多个选项作为字段输入。 • **密码字段**。密码字段带有掩码。 • **单选按钮**。用户可以从一些选项中选择一个选项作为字段输入。 • **选择菜单**。用户可以从一些选项中选择一个选项作为字段输入。 • **文本字段**。用户在字段中输入值以作为输入的文本。 • **文本区域**。自由格式的文本框。 对于**复选框**、**单选按钮**和**选择菜单**，请为字段添加选项。 • **选项标签**。用于标识选项的标签。 • **选项值**。选项的值。 在该示例中，选择菜单包含用于不同状态的一些选项。 
占位符	占位符标签。
工具提示	字段帮助文本。
是否可编辑	• **是**。用户可以在字段中输入值。 • **否**。用户不能在字段中输入值。某些字段中会填充现有数据。例如，在自注册期间，用户可能针对现有身份记录申请帐户，在此情况下，可以使用该身份记录中的字段值。
是否必需	• **是**。该字段为必填字段。 – 自注册表单。如果不为该字段提供值，用户无法完成自注册。 – 自助服务概要文件表单。提示用户输入任何未填充的必填字段的值。 • **否**。该字段为可选字段。

表 *16.* 表单字段选项 *(续)*

选项	描述
需要当前密码匹配	仅适用于密码 LDAP 属性。 • **是**。用户必须在单独的字段中输入两次密码。在每个字段中输入的值必须匹配以确认密码正确。 • **否**。仅在一个字段中输入一次密码。
带掩码	**是**。字段带掩码，在屏幕上看不到输入的值。输入的每个字符在屏幕上都替换为星号字符。
需要匹配字段	• **是**。用户必须在单独的字段中输入两次值。在每个字段中输入的值必须匹配以确认值正确。例如，当用户输入电子邮件地址时，您可以要求用户输入两次该地址。 • **否**。仅在一个字段中输入一次值。
验证	验证规则： • **是**。输入的值必须通过指定的验证规则。例如，日期可能需要通过格式验证规则，如 yyyy/mm/dd。 • **否**。不验证输入的值。 验证类型： • **日期**。值必须符合指定的日期格式。例如，yyyy/mm/dd。 • **电子邮件地址**。值必须对应于电子邮件地址格式。例如，*text_string*@*text_string*.com。 • **字母**。值必须仅包含字母字符。 • **最大字符长度**。值不能包含超过指定数量的字符。 • **最小字符长度**。值不能包含少于指定数量的字符。 • **数字**。值必须仅包含数字字符。 • **密码强度**。密码字段必须符合基本、标准或强验证规则。规则基于必须输入的字符数和字符类型。 • **美国电话号码**。值必须符合美国电话号码格式。 定制正则表达式。用于针对所输入值进行求值的正则表达式。如果表达式求值为 true，表示值有效。 • **模式**。正则表达式。例如，要将注册限制为北卡罗来纳州中的地址，使用正则表达式 `^NC$` 来表示 state 属性，其中，NC 定义为 state 属性的可选值。 • **错误消息**。输入的值无效时向用户显示的错误消息。

表 *17.* 表单区段选项

选项	描述
标签	区段标签。
副标题	副标题标签。
标题	标题。

门户网站概要文件表单示例

表 *18.* 自注册表单字段和区段元素

编号	描述
1	区段标签。
2	字段标签。
3	必填字段，由星号指示。
4	文本字段。
5	文本字段，带有用户搜索工具。
6	带掩码的字段。密码字段始终带有掩码。

更改安全问题选项

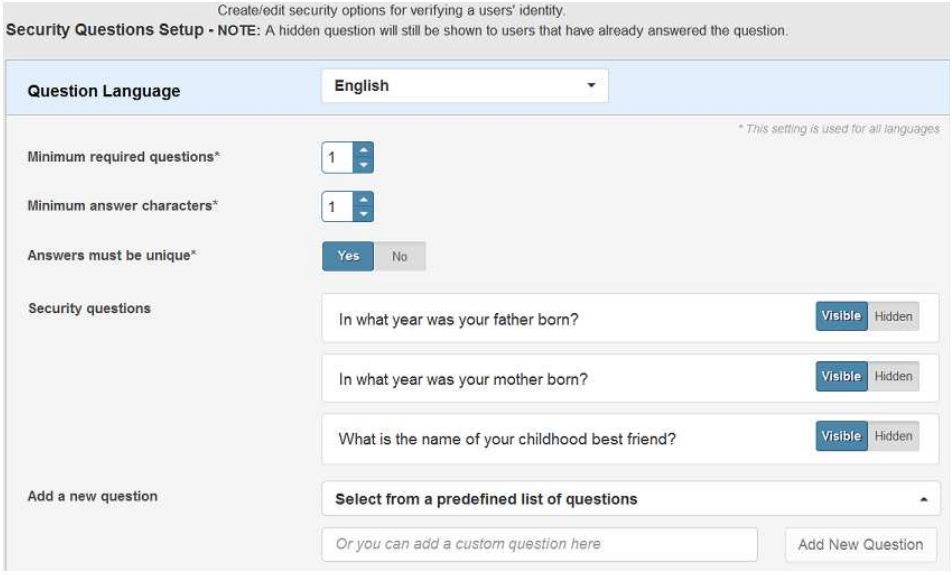
在为贵组织进行 Cloud Identity Service 初始配置期间，定义若干安全问题。安全问题答案用于在用户尝试重置密码时验证用户。您可以添加新安全问题。

关于此任务

用户在自注册时必须提供安全问题答案。用户可以从问题池中选择想要提供答案的问题。您可以添加新问题，并可以设置用户在自注册时必须提供答案的最小问题数。

过程

1. 在导航窗格中，单击**自助服务** > **安全问题**。



2. 可选： 从**问题语言**下拉列表中选择想要为用户提供本地语言支持的语言。

   可以选择的语言在为贵组织进行 Cloud Identity Service 初始配置期间定义。您可以为以缺省语言定义的问题添加翻译。

   a. 单击**选择要翻译的问题**，然后从列表中选择问题。

      可用问题是已使用缺省语言定义的问题。缺省语言为英语。

   b. 在文本字段中输入翻译，然后单击**添加翻译**。

3. 设置所需安全问题设置选项。
4. 单击**保存更改**。

安全问题选项

安全问题选项包括最少安全问题数量、问题唯一性和最短答案长度。

表 *19.* 安全问题选项

选项	描述
对答案启用加密盐和散列	指定是否对安全问题的答案进行加密盐和散列。散列对答案进行编码以使其成为定长字符串，以使答案更难以被发现。加密盐通过添加随机字符串以对散列进行随机化，以使答案更难以被解码。 **要点：**如果已启用加密盐和散列，那么不能禁用。
最少必需安全问题数	用户在注册时必须提供答案的最少安全问题数量。该选项并不是指密码重置期间必须回答的问题数量。例如，用户可以提供 5 个问题的答案，但在密码重置期间，只需 3 个答案。在此情况下，将从最初在注册期间回答的 5 个问题中随机选择 3 个问题。

表 *19.* 安全问题选项 *(续)*

选项	描述
最少答案字符数	作为答案必须输入的最小字符数。
答案必须唯一	• **是**。用户不能对不同问题输入相同答案。 • **否**。不同问题的答案可以相同。
用户具有安全问题时使安全选项卡成为缺省选项卡	登录自助服务门户网站时，指定当出现安全问题错误时，是否首先对用户显示安全问题选项卡。
安全问题	安全问题可以隐藏或可见。 • **可见**。问题可供用户在注册期间提供答案。 • **隐藏**。问题不可供用户在注册时使用，用户不能提供该问题的答案。
添加新问题	可通过使用两种方法来添加问题。 • **从预定义的问题列表中选择**。从问题列表中选择。 • **添加定制问题**。在文本字段中输入问题，然后单击**添加新问题**。 **要点：**新安全问题只能在保存后除去。在添加问题并保存更改之后，可以通过提交支持凭单来除去该问题。

管理角色

您可以添加和修改角色，但不能删除角色。

角色概述

角色可以认为是贵组织中的职衔。例如，管理者、管理员或帮助台联系人。角色用于控制对不同自助服务应用程序和操作的访问，以及用于在自助服务概要文件应用程序中控制对不同区段的访问。

添加角色

角色可以认为是贵组织中的职衔。例如，管理者、管理员或帮助台联系人。角色分配给用户。角色用于控制对不同自助服务应用程序和任务的访问。

关于此任务

角色可以分配到不同的实例。实例是自助服务应用程序的一组配置、选项和品牌形象。例如，实例可以定义一套颜色方案、文本翻译、表单布局和自注册选项。然后，对于定义的每个角色，可以为该角色选择实例。例如，可以为帮助台角色和管理者角色分配不同的实例。一个角色只能分配到一个实例，但一个实例可以有多个角色。

过程

1. 在导航窗格中，单击**自助服务** > **自助服务角色**。
2. 单击**添加新角色**。
3. 在**角色名称**字段中输入角色名称。
4. 可选： 从**实例**下拉列表中选择自助服务应用程序实例。

   自助服务应用程序可以具有不同的实例。实例定义自助服务应用程序中的窗口、字段、标签和其他 UI 元素。可以设计不同的实例来满足不同角色的需要。缺省 Cloud Identity Service 实例处于选中状态。一个角色只能分配到一个实例。

5. 选择所需角色设置。
6. 单击**保存更改**以保存角色。

角色设置：

角色设置用于控制分配了角色的用户对不同自助服务应用程序和操作的访问。角色设置包括概要文件管理、密码重置、用户名查找、自注册选项、搜索选项和概要文件查看与编辑许可权。

表 *20.* 角色设置

设置	描述
自助服务门户网站	这是允许用户管理其自己的用户信息概要文件的访问权。
区段访问权	自助服务门户网站和概要文件应用程序中的不同区段。 • **启动板**。对启动板的访问权。启动板在自助服务门户网站中提供了单一位置，用户可以从此位置访问已连接的 Web 应用程序和联合合作伙伴 Web 应用程序。 • **概要文件**。这是允许用户管理其自己的概要文件信息的访问权。 – **将概要文件显示为页面**。指定是将概要文件信息显示为页面还是显示为下拉标题。 • **直接下属**。访问以管理作为直接下属的用户的概要文件。 – **允许创建新用户**。可以创建新用户。 – **可以将帐户降级**. 可以将帐户降级为用户身份。 – **可以切换用户状态**。可以激活或取消激活用户帐户。如果帐户已取消激活，那么用户无法登录自助服务。 – **可以使密码到期**。可以使用户密码到期。 • **请求**。用来管理暂挂审批和重新认证请求的访问权。 • **服务**。用于查看所属服务列表以及请求服务的能力的访问权。 • **用户控制**。用于在"用户控制"页面中查看其他用户的概要文件信息的访问权。 – **允许创建新用户**。可以创建新用户。 – **可以将帐户降级**. 可以将帐户降级为用户身份。 – **可以切换用户状态**。可以激活或取消激活用户帐户。如果帐户已取消激活，那么用户无法登录自助服务。 – **可以使密码到期**。可以使用户密码到期。
区段设置	• **显示"检查用户名"按钮**。可以在创建新用户时检查用户名是否存在。
密码重置	用户对密码重置应用程序的访问权，用来重置其密码。该应用程序不需要认证。
用户名恢复	用户对用户名恢复应用程序的访问权，用来恢复其自己的用户名。该应用程序不需要认证。
自注册	用于自注册应用程序以进行自注册的访问权。该应用程序不需要认证。

表 *20.* 角色设置 *(续)*

设置	描述
用户搜索设置 **服务搜索设置**	在自助服务应用程序中搜索用户或服务时，用于排序和显示属性的优先级。 • **搜索结果优先级**。在搜索结果中，优先级较高的属性显示在优先级较低的属性的前面。要将属性添加到搜索结果，请从**添加新属性**列表中选择属性，然后单击  。单击属性并将其拖动至新位置以更改其优先级。 • **搜索结果过滤器**。可以应用属性过滤规则以从搜索中排除用户或服务。例如，您可以排除具有特定角色的用户。要添加排除过滤器，请单击**添加排除过滤器**。从**当属性**列表中选择要作为排除依据的属性。在**等于**字段中输入想要排除的属性值。
查看许可权	用户概要文件的查看和编辑许可权。对于自助服务应用程序中的概要文件，您可以将身份属性指定为可查看和可编辑。 • **任何用户概要文件**。所有用户的概要文件。 • **用户自己的概要文件**。用户自己的概要文件。 • **直接下属概要文件**。用户直接下属的概要文件。 • **组成员概要文件**。具有指定组成员资格的用户的概要文件。 • **服务成员概要文件**。具有指定服务成员资格的用户的概要文件。 • **角色成员概要文件**。具有指定角色的用户的概要文件。 要添加属性查看和编辑许可权： 1. 单击**添加查看许可权过滤器**。 2. 从**查看以下内容时应用**列表中选择要对其应用属性查看和编辑许可权的用户概要文件。 对于"角色成员概要文件"，从**属于**列表中选择角色。 对于"组成员概要文件"和"服务成员概要文件"，从**属于**列表中搜索并选择组或服务。要搜索组或服务，请至少输入该组或服务名称的前 3 个字符。 3. 从**添加属性**菜单中选择要对其应用许可权的属性，然后单击 。您可以添加所需数量的属性。 单击相应的**是**或**否**来指定是否将属性设置为可查看和可编辑。 4. 单击**保存更改**。

定制自助服务应用程序的 UI

定制自助服务应用程序 UI 的过程包括定制品牌形象、文本键标签、电子邮件模板、自助服务概要文件应用程序中的标签以及自助服务应用程序套件页面的标签。

自助服务 UI 定制概述

自助服务应用程序在为贵组织进行 Cloud Identity Service 初始设置期间配置。您可以定制自助服务应用程序的品牌形象。您可以更改发送给用户的电子邮件的内容，并可以更改 UI 列标签和其他文本键。

品牌形象

您可以控制自助服务应用程序的品牌形象。品牌形象包括应用程序颜色方案、徽标、图标和表单元素的视觉呈现。

文本键

文本键用于提供应用程序页眉和页脚、错误消息、按钮标签、属性标签和表单区段标签的缺省文本。您可以更改文本键的文本。

电子邮件模板

电子邮件模板用于提供为响应某个事件而发送给用户的电子邮件的内容。例如，当批准注册请求或重置密码时发送的邮件内容。您可以更改邮件内容。可以更改使用的字体和段落样式方面。

门户网站

自助服务概要文件门户网站或应用程序允许用户在注册并能够向 Cloud Identity Service 进行认证之后管理自己的帐户概要文件信息。您可以更改用于标注表列标题的文本和用于其他 UI 元素的文本。

套件页面

套件页面是单独的自助服务应用程序页面，用户访问这些页面以管理其 Cloud Identity Service 身份或帐户方面的信息。套件页面包括自注册、密码重置、用户名恢复和目录查找。您可以更改用于标注套件页面中的区段和标题的文本。

定制品牌形象

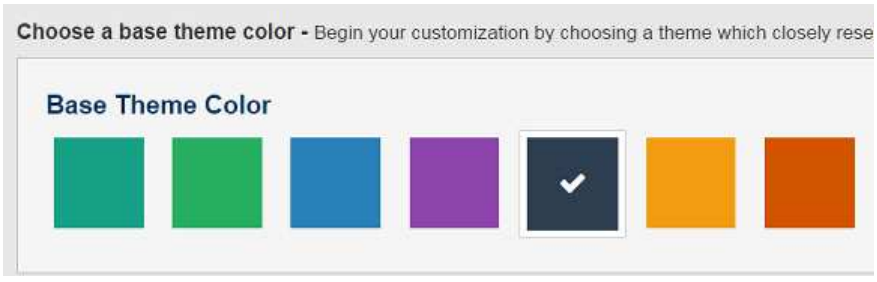
您可以通过更改自助服务应用程序中使用的颜色、徽标、图标和图像来定制品牌形象。

选择基本主题颜色

您可以选择要用作所有自助服务应用程序的基本背景色的颜色。

过程

1. 在导航菜单中，单击**自助服务** > **品牌形象**，然后单击**主题**。



2. 选择基本主题颜色。 将显示预览。
3. 单击**保存**。

选择主题颜色

您可以选择一些自助服务 UI 元素的单独基本颜色。还可以选择要用于消息和按钮的颜色。

关于此任务

选定颜色将覆盖基本主题颜色。

过程

1. 在导航窗格中，单击**自助服务** > **品牌形象**，然后单击**颜色**。

2. 使用以下某种方法更改元素的颜色。
   - 单击颜色选择方框。
   - 输入 HTML 颜色代码。

   您可以选择以下自助服务 UI 元素的颜色。
   - 基本
     - 标题
     - 表
     - 概要文件
     - 链接
     - 错误
   - 按钮
     - 主项
     - 辅助
     - 备用

- 消息
  - 基本
  - 成功
  - 正在装入
  - 反馈
  - 警报
  - 错误

3. 单击**保存**。

选择图像

您可以替换自助服务应用程序中使用的图像、徽标和图标。

关于此任务

通过上载文件以替换当前使用的图像文件来更改图像。

注：替代文件将覆盖当前文件。如果当前文件不是原始文件，可以先保存文件的当前版本，然后再进行替换。原始文件始终可供下载和复用。图像文件最大大小为 50 KB。

过程

1. 在导航菜单中，单击**自助服务 > 品牌形象**，然后单击**图像**。
2. 可选： 下载当前使用的文件，单击**下载当前文件**。
3. 上载替代文件，单击**选择新文件**。

图像文件：

图像文件用于自助服务图标、图像和徽标。

表 *21.* 图像文件

文件	描述
徽标图像	标题徽标。该徽标具有透明背景时视觉效果最佳。不能更改其大小。超出当前高度或宽度会导致图像扭曲。
错误图标	失败操作或错误图像。该徽标具有透明背景时视觉效果最佳。不能更改其大小。超出当前高度或宽度会导致图像扭曲。
收藏夹图标	显示在浏览器中的收藏夹图标。该图标必须为 16 X 16 像素，以便可以正确地显示为浏览器中的书签图标。
表单元素	复选框和单选按钮图像。该图像精灵在单个文件中包含表单元素每种状态的所有图像。每个图像都不得超过缺省图像的高度或宽度，否则在装入浏览器中时将会被修剪（裁剪）。
页面背景	用于概要文件管理的平铺背景图像。装入页面时，该图像垂直平铺（复制）并左对齐。
数据正在装入指示符	数据正在装入图像。您可以使用静态或动画图像。不得更改其大小。
预装入器图像	区段正在装入图像。您可以使用静态或动画图像。不得更改其大小。
搜索字段图标	支持自动补全或搜索的输入字段图像。必须使用静态图像。不得更改其大小。
正在搜索图标	正在执行搜索图像。您可以使用静态或动画图像。不得更改其大小。

表 *21.* 图像文件 *(续)*

文件	描述
成功图标	成功操作图标。该图标具有透明背景时视觉效果最佳。不能更改其大小。超出当前高度或宽度会导致图像扭曲。
页面图标	自助服务屏幕上的页面图标。该图像精灵在单个文件中包含用户工具页面每个区段的所有图像。每个图像都不得超过缺省图像的高度或宽度，否则在装入浏览器中时将会被修剪（裁剪）。

定制登录页面和错误页面

您可以替换用于 Cloud Identity Service 登录页面和错误页面的样式表、徽标和页面标题。还可以更改和添加显示在页面底部的文本元素。

开始之前

如果要替换样式表文件，那么必须很了解 CSS。样式表用来控制页面上 UI 元素的缩放大小、定位和样式。

关于此任务

通过上载文件以替换当前使用的徽标文件或样式表文件，更改徽标或样式表。输入文本以更改页面标题和文本元素。文本元素显示在页面底部。您还可以提供对文本元素的本地语言支持。

注：原始文件提供了对于定制登录页面和错误页面很有用的示例。

注：替代样式表文件或徽标文件将覆盖当前文件。如果当前文件不是原始文件，那么可以先下载并保存文件的当前版本，然后再进行替换。原始文件始终可供下载和复用。图像文件最大大小为 50 KB。

过程

1. 在导航菜单中，单击**自助服务** > **品牌形象**，然后单击**全局**。
2. 可选： 上载新的样式表文件，单击**上载样式表**。
3. 可选： 在**页面标题**字段中输入新的页面标题。
4. 可选： 上载新的徽标文件，单击**上载徽标**。
5. 可选： 在**文本元素**字段中为文本元素输入新文本。

   注：您可以添加文本元素的翻译版本，以在 Cloud Identity Service 配置可用的任何语言中提供本地语言支持。
6. 可选： 单击**添加新的文本元素**，以输入新的文本元素。

   注：新的文本元素按顺序显示在前一元素之下。

   注：可以通过**预览更改**来预览您作出的更改。
7. 单击**保存更改**。

定制常规自助服务 UI 文本键

对于用来标注在所有自助服务应用程序中使用的按钮、字段、列、LDAP 属性和其他元素的常规文本键，您可以添加文本和更改文本。

过程

1. 在导航菜单中，单击**自助服务** > **内容管理**，然后单击**常规**。
2. 从**文本键**下拉列表中选择想要定制的文本键。 针对以下常规文本键，您可以添加文本和更改文本键：
   - **自动完成**。"服务"和"用户查找"表中使用的自动完成表文本键。
   - **按钮标签**。在所有自助服务应用程序中使用的按钮标签。
   - **错误消息传递**。在屏幕顶部显示的常规错误消息传递。
   - **页脚文本**。在自助服务应用程序底部显示的页脚文本。
   - **表单标签**。表单中使用的标签。
   - **表单字段占位符文本**。表单中使用的占位符文本。
   - **表单字段工具提示文本**。表单字段工具提示。
   - **标题文本**。自助服务应用程序顶部出现的文本。
   - **LDAP 属性**。LDAP 属性名称。LDAP 属性文本键可以用于搜索 LDAP 属性。
   - **用户概要文件布局**。概要文件区段布局标题。
   - **验证消息传递（定制）**。定制验证消息传递。用于客户提供的正则表达式验证。
   - **验证消息传递（标准）**。标准验证消息传递。
3. 更改所需文本键，然后单击**保存更改**。

配置电子邮件模板

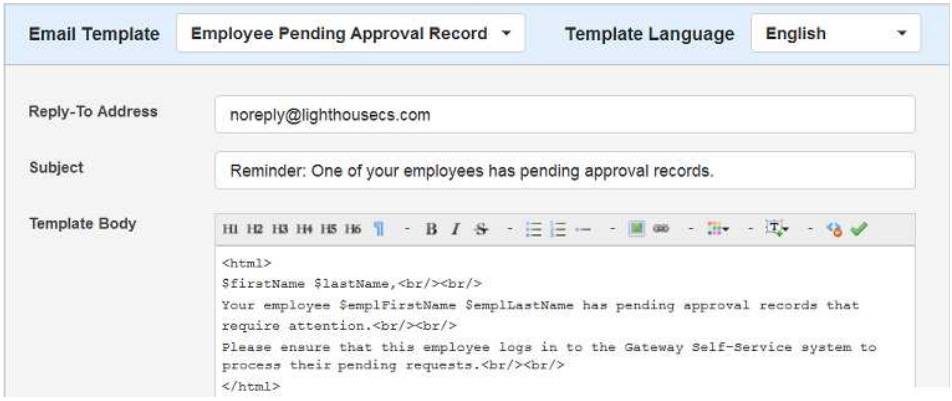
电子邮件模板用于提供发送给用户的电子邮件所用的内容。您可以更改电子邮件模板的内容和格式。

开始之前

要编辑模板正文中的信息，需要具备有关 HTML 的基本知识并能够熟练使用 HTML。

过程

1. 在导航菜单中，单击**自助服务** > **内容管理**，然后单击**电子邮件模板**。



2. 从**电子邮件模板**菜单中，选择要配置的模板。
3. 您可以更改以下标题详细信息：
   - **回复地址**。发件人的地址。

- **主题**。有关电子邮件用途的描述。

4. 输入或修改模板正文中的消息文本。

   使用**模板正文**菜单栏来设置文本格式，插入段落、图片、链接和属性。每个图标都会在模板正文中插入相应的 HTML 标记或属性。请突出显示文本，或者将光标定位在要应用格式设置或者要插入属性、链接或图片的位置。

5. 单击**保存更改**。

电子邮件模板格式设置和内容选项

表 22. 电子邮件模板正文、格式和内容选项

格式和内容选项	描述
	插入标题 1 - 6。标题 1 - 6 的字体大小分别是 36、30、24、18、14 和 12 像素。
	插入段落。
	粗体、斜体和删除线的文本格式设置。
	项目符号列表、编号列表和列表项的列表格式设置。
	插入图片。指定图片链接的 URL。您可指定图片的替代文本。替代文本用于满足辅助功能选项需求。您还可指定是否阻止链接创建额外对话框。额外对话框是指弹出窗口。
	在 Web 页面中插入链接。指定页面链接的 URL。锚点标记中将突出显示一个区域以供您输入链接文本：**您的链接文本**。输入供电子邮件收件人单击以访问链接页面的文本。
	文本颜色。

表 22. 电子邮件模板正文、格式和内容选项（续）

格式和内容选项	描述
	输入属性。提供了一些属性。 • 审批创建时间。请求服务的日期和时间。 • 审批宽限期。为批准服务请求授予的时间长度。 • 核准人名字。负责批准或拒绝请求的管理员的名字。 • 核准人姓氏。负责批准或拒绝请求的管理员的姓氏。 • 客户名称。贵组织的名称。 • 客户网上存在的名称。贵组织网上存在的名称，在初始设置过程期间定义。 • 连接名称。与 Cloud Identity Service 的安全连接的名称。 • 取消供应指示信息。用于删除帐户的指示信息。 • 电子邮件地址。用户的电子邮件地址。 • 电子邮件分钟数。密码重置链接保持有效的时间长度。 • 员工名字。具有暂挂请求的员工的名字。 • 员工姓氏。具有暂挂请求的员工的姓氏。 • 名字。用户的名字。 • 姓氏。用户的姓氏。 • 密码分钟数。用户单击重置链接后可更改密码的时间长度。 • 密码重置 URL。用于重置密码的链接。 • 供应指示信息。用于创建帐户的指示信息。 • 原因。所执行操作或所请求操作的原因。 • 请求者名字。提交服务请求的用户的名字。 • 请求者姓氏。提交服务请求的用户的姓氏。 • 服务描述。服务的摘要描述。 • 服务名称。请求的服务的名称。 • 用户名。用户的用户名。
	除去所选文本的格式设置。
	预览电子邮件。

定制自助服务概要文件应用程序

您可以定制自助服务门户网站概要文件应用程序。您可以更改用于标注门户网站列和其他元素的文本键。

关于此任务

自助服务概要文件应用程序允许用户管理自己的帐户概要文件信息，并允许用户查看和请求服务。还用于管理直接下属、服务请求和委派用户。

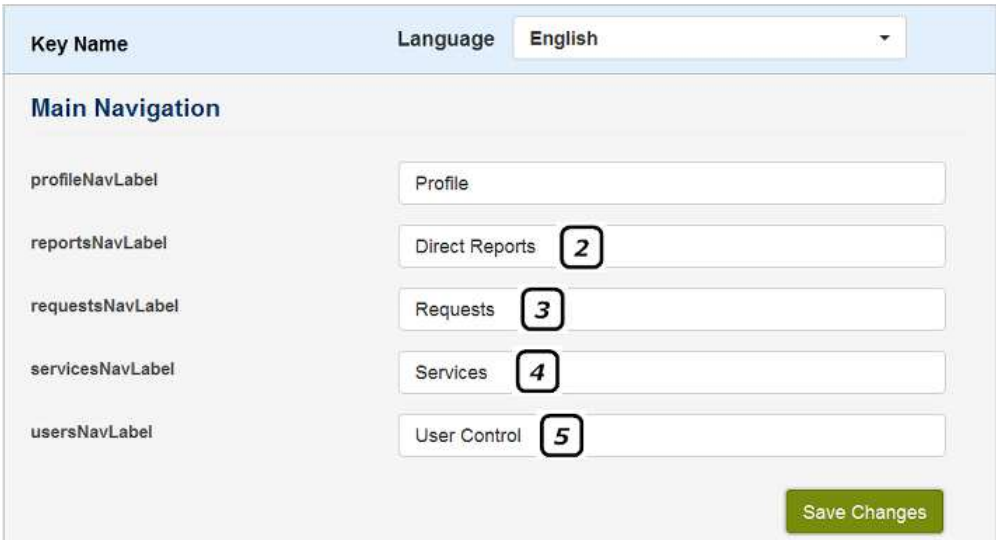
您可以更改用于标注整个门户网站中的表列标题的文本和用于其他 UI 元素的文本。

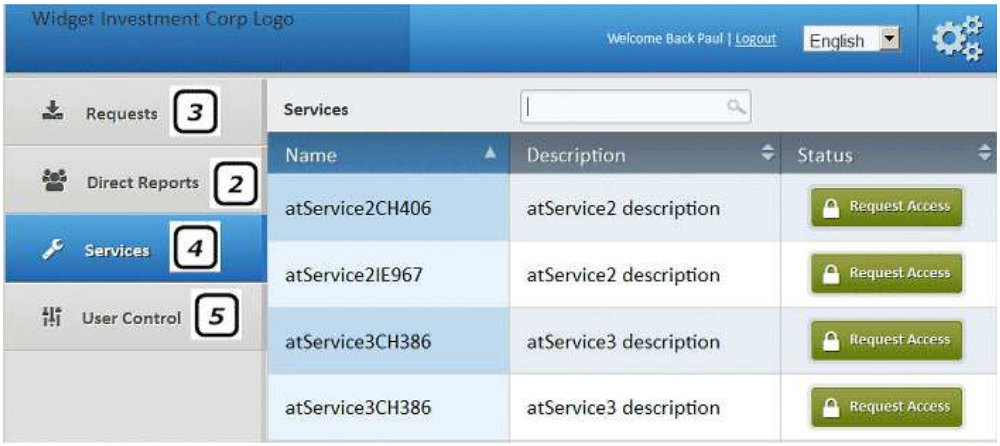
过程

1. 在导航菜单中，单击**自助服务** > **内容管理**，然后单击**门户网站**。
2. 从**文本键**菜单中选择要定制的 UI 区段。 您可以更改以下 UI 区域的文本键：
   - **主要导航**。
   - **服务表列**。
   - **直接下属表列**。
   - **请求表列**。
   - **用户控制表列**。
   - **表标签**。
   - **搜索标签**。
3. 更改所需标签和文本，然后单击**保存更改**。

主要门户网站导航键名和标签

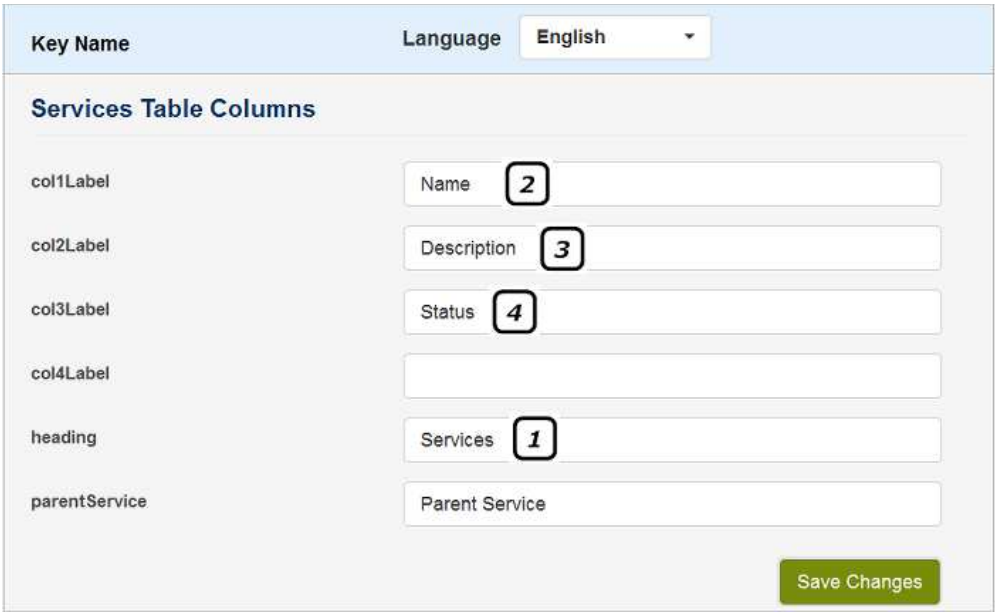
主要门户网站导航键名用于在自助服务门户网站主页上标注主要区段。

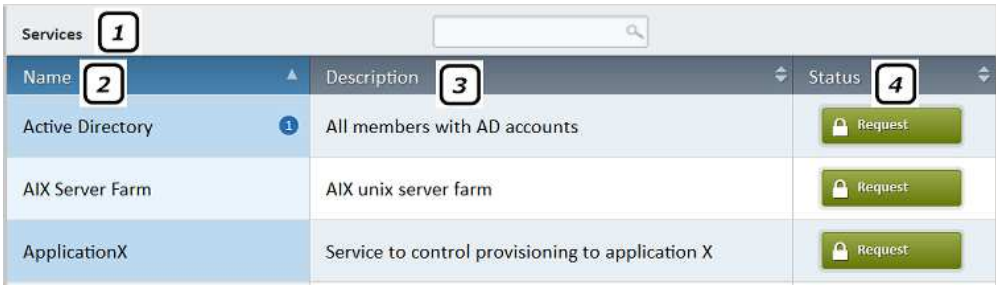




"服务"页面键名和标签

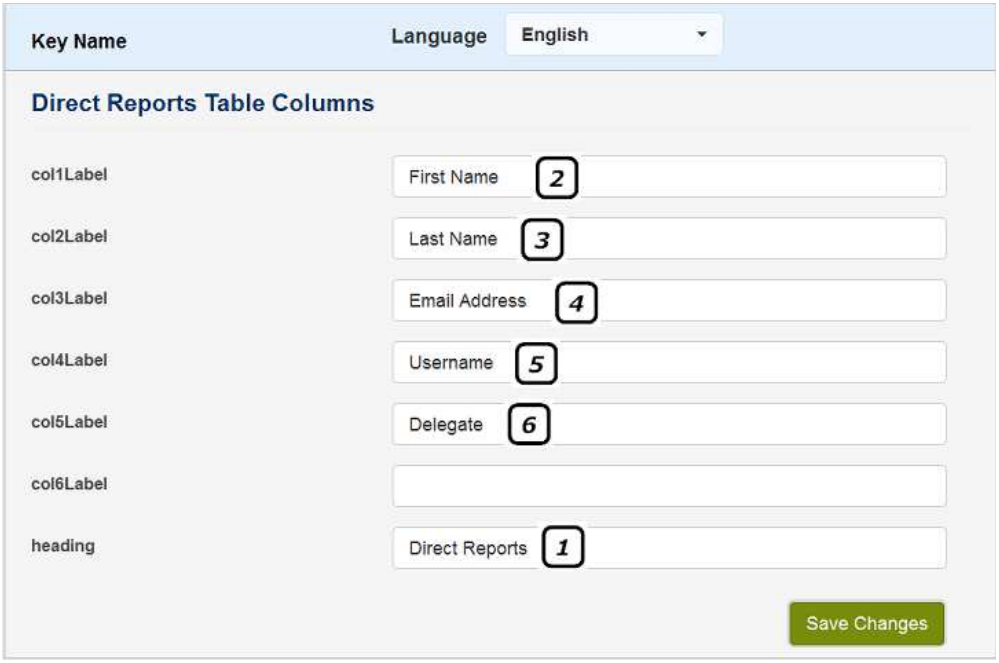
"服务"页面键名用于标注"服务"页眉和表列。

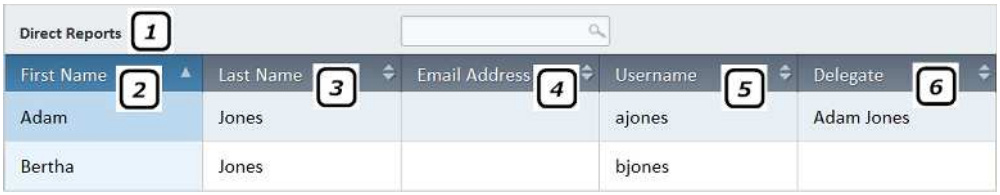




"直接下属"页面键名和标签

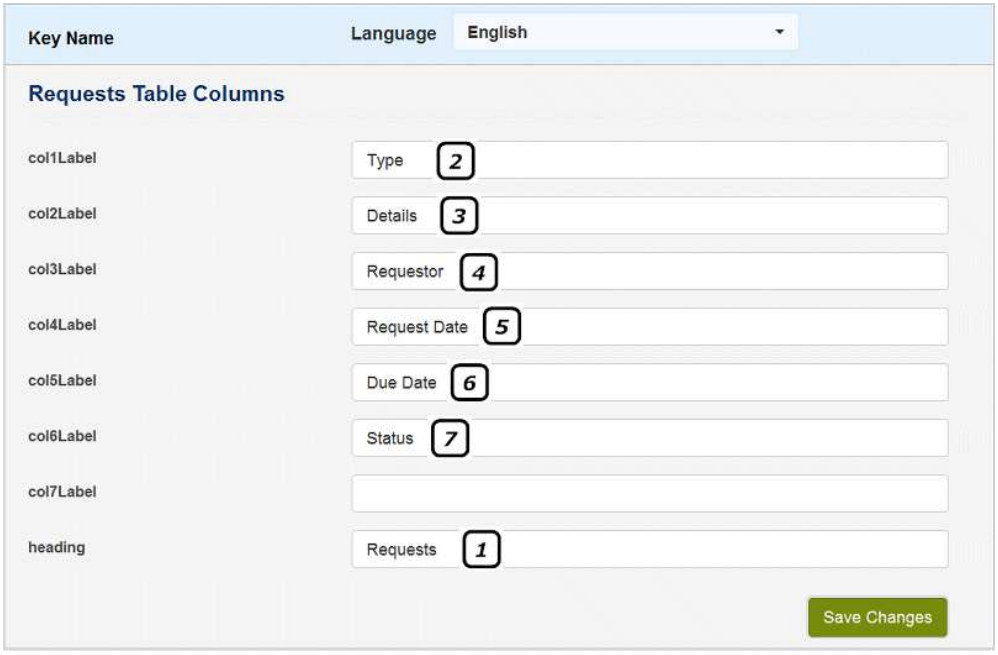
直接下属键名用于标注"直接下属"页眉和表列。





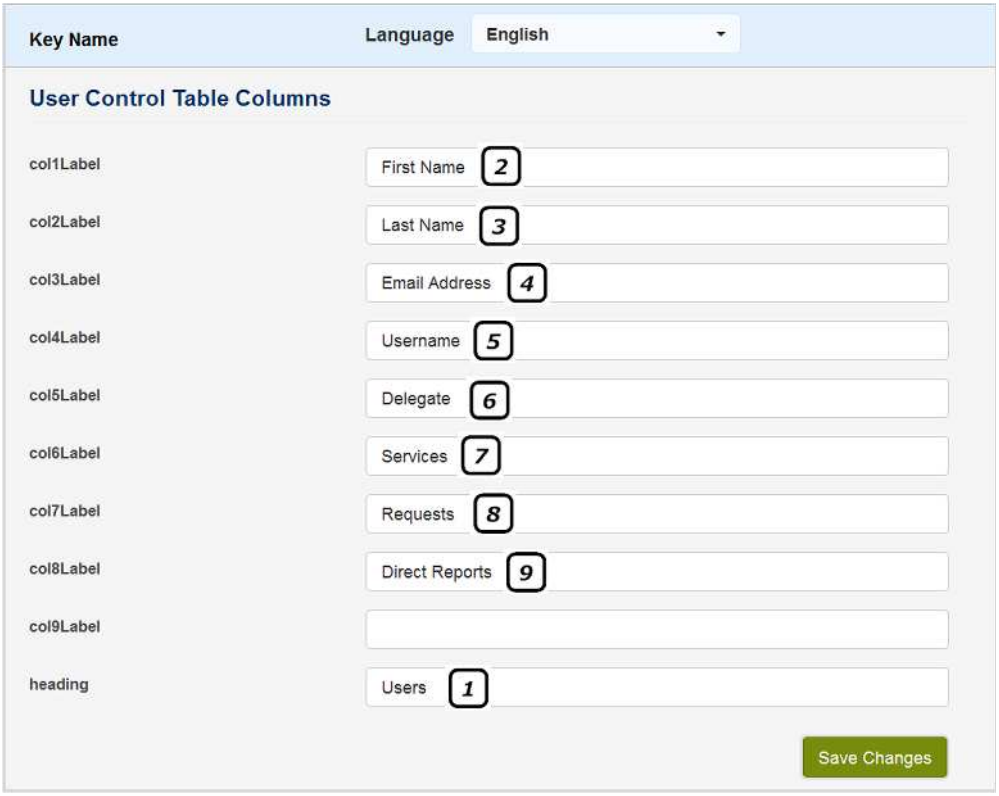
"请求"页面键名和标签

"请求"页面键名用于标注"请求"页眉和表列。



"用户控制"页面键名和标签

"用户控制"页面键名用于标注"用户控制"页眉和表列。



定制自助服务套件页面的 UI

您可以定制自助服务应用程序套件页面。您可以更改用于标注自助服务应用程序的标题、字段和其他元素的文本键。

关于此任务

自助服务应用程序允许用户管理若干自助服务任务，包括自注册、密码重置和用户名恢复。您可以更改用于标注所有自助服务应用程序中的字段和标题的文本。

您可以更改的文本项取决于针对自助服务应用程序配置的选项。

过程

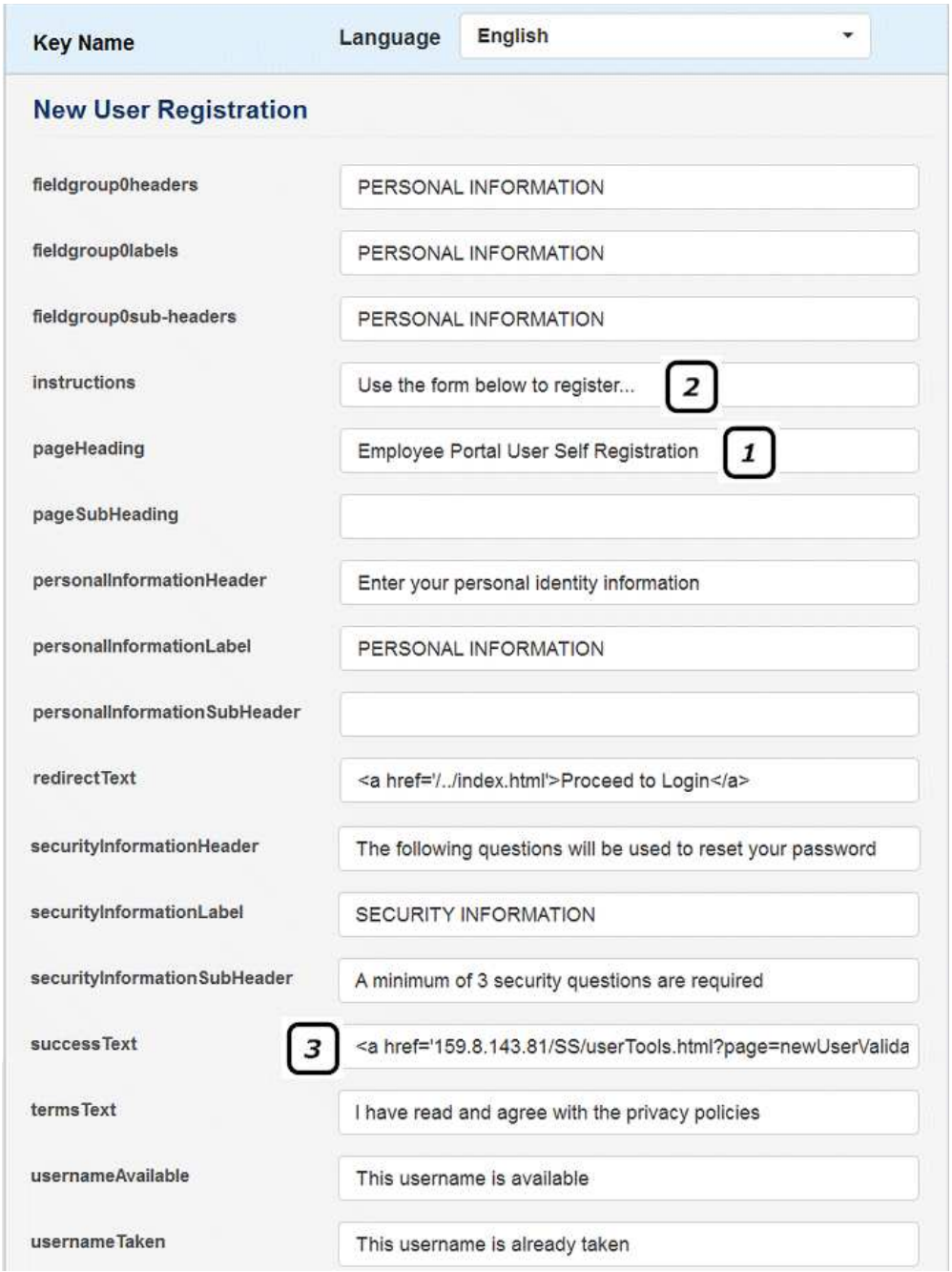
1. 在导航菜单中，单击**自助服务** > **内容管理**，然后单击**套件页面**。
2. 从**文本键**菜单中选择要定制的自助服务应用程序。 您可以更改以下自助服务应用程序的文本键：
   - **新用户注册**。
   - **密码重置**。

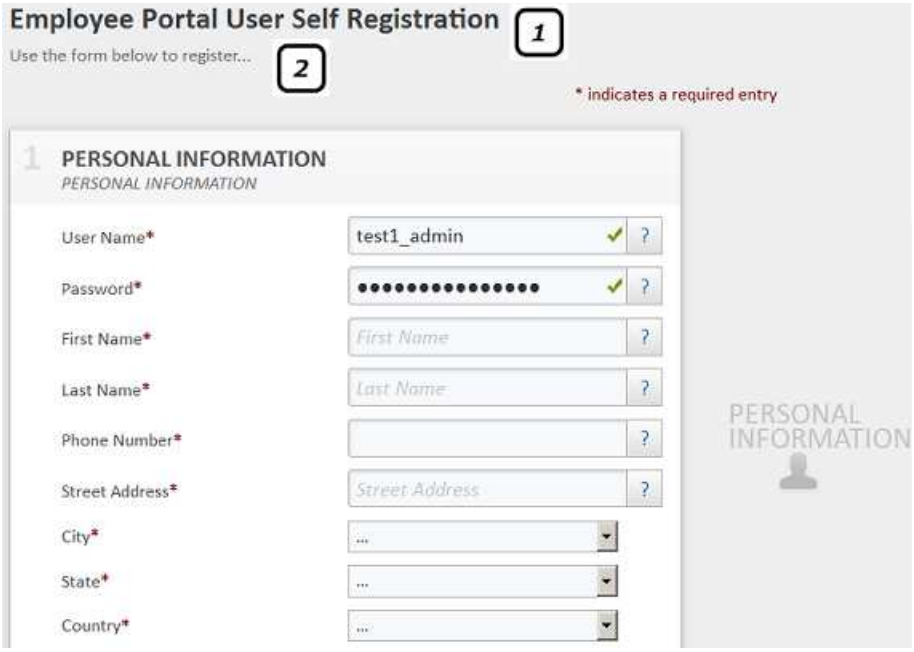
- **密码重置验证。**
- **用户名恢复。**
- **目录查找文本。**

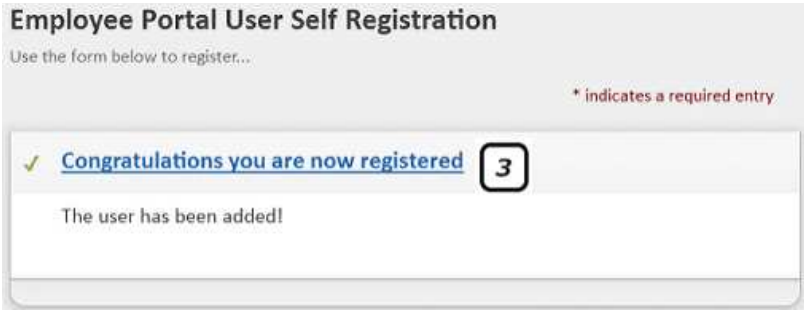
3. 更改所需文本键，然后单击**保存更改**。

用户注册键名

用户注册键名用于在自助服务的"用户注册"页面中标注标题和字段。

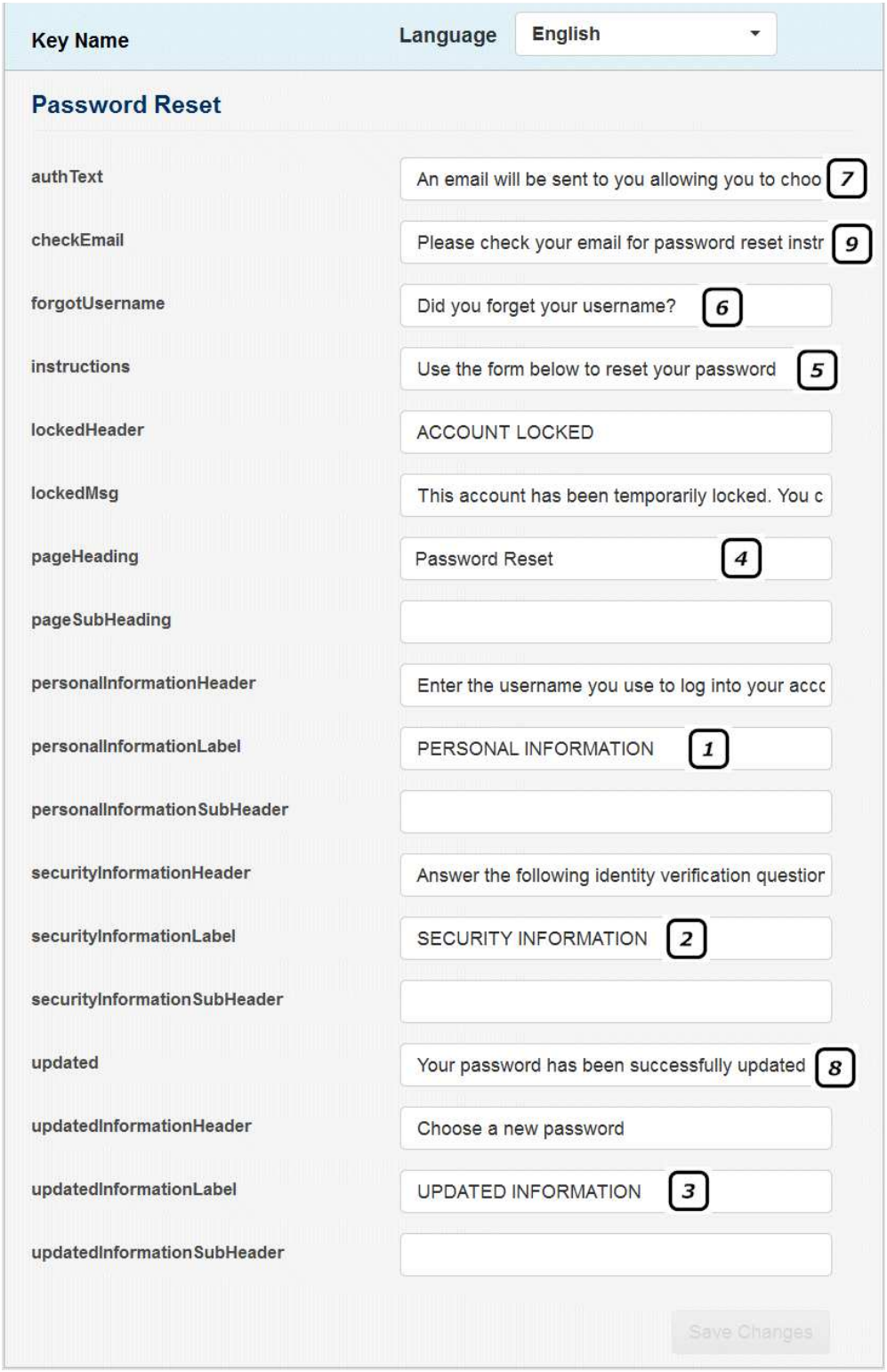


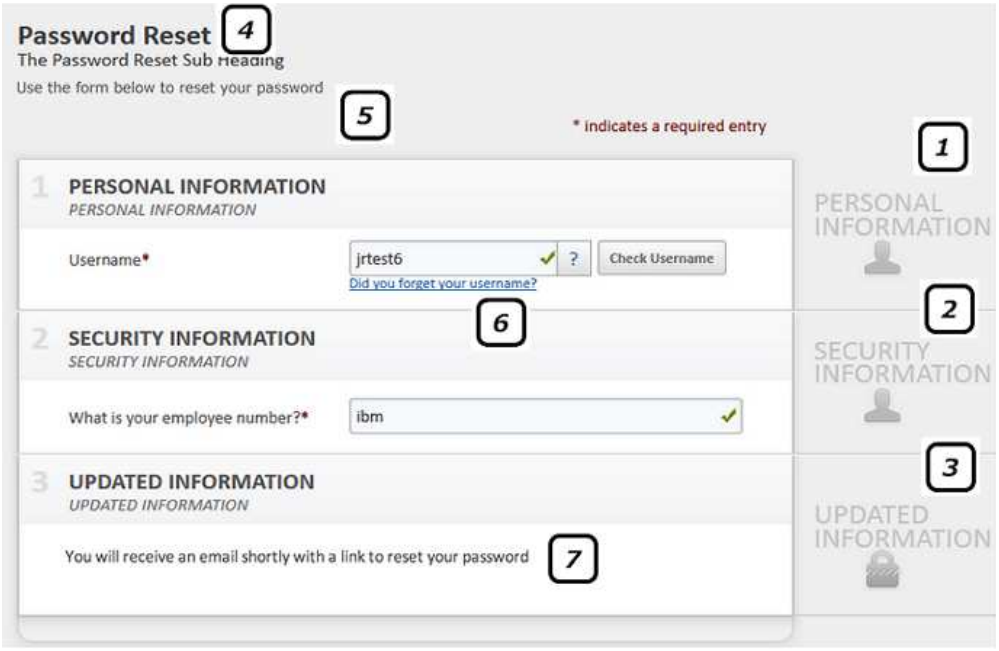

Employee Portal User Self Registration
1
Use the form below to register...
2
* indicates a required entry
1 PERSONAL INFORMATION
PERSONAL INFORMATION
User Name*
test1_admin
Password*
First Name*
First Name
Last Name*
Last Name
Phone Number*
Street Address*
Street Address
City*
State*
Country*
PERSONAL INFORMATION

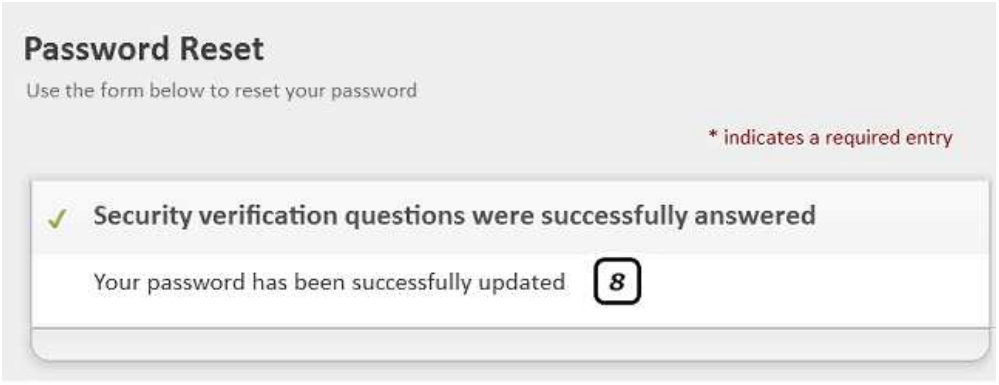

Employee Portal User Self Registration
Use the form below to register...
* indicates a required entry
Congratulations you are now registered
3
The user has been added!

密码重置键名

密码重置键名用于在自助服务应用程序的"密码重置"中标注标题、区段和字段。



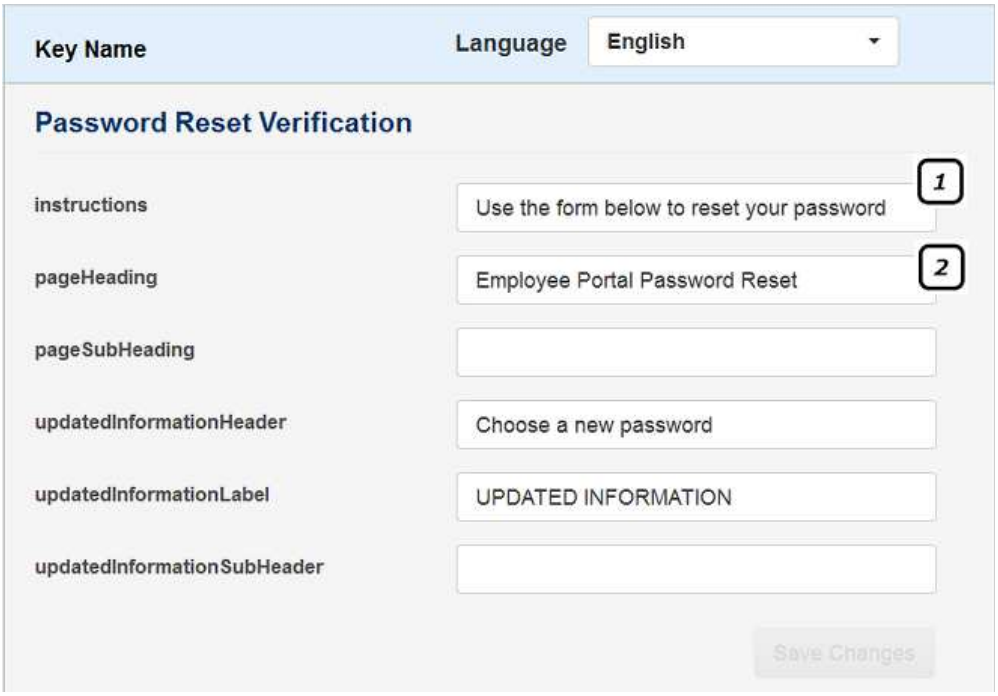

Password Reset
4
The Password Reset Sub Heading
Use the form below to reset your password
5
* indicates a required entry
1
1 PERSONAL INFORMATION
PERSONAL INFORMATION
PERSONAL INFORMATION
Username*
jrtest6
?
Check Username
Did you forget your username?
6
2
2 SECURITY INFORMATION
SECURITY INFORMATION
SECURITY INFORMATION
What is your employee number?*
ibm
3
3 UPDATED INFORMATION
UPDATED INFORMATION
UPDATED INFORMATION
You will receive an email shortly with a link to reset your password
7

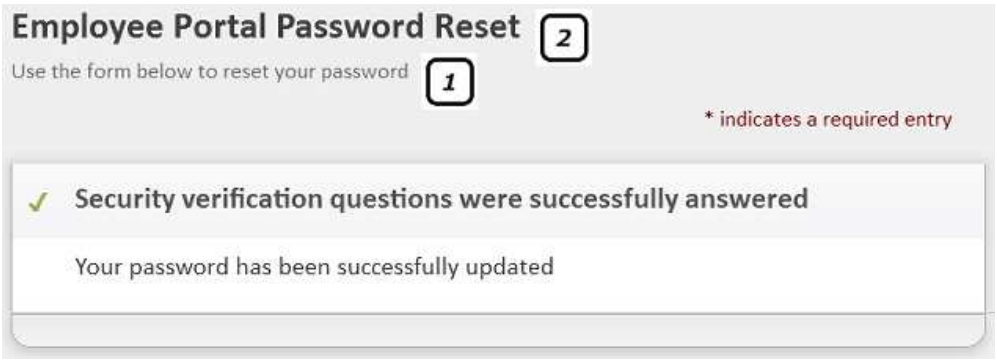

Password Reset
Use the form below to reset your password
* indicates a required entry
Security verification questions were successfully answered
Your password has been successfully updated
8


Security verification questions were successfully answered
Please check your email for password reset instructions
9

密码重置验证键名

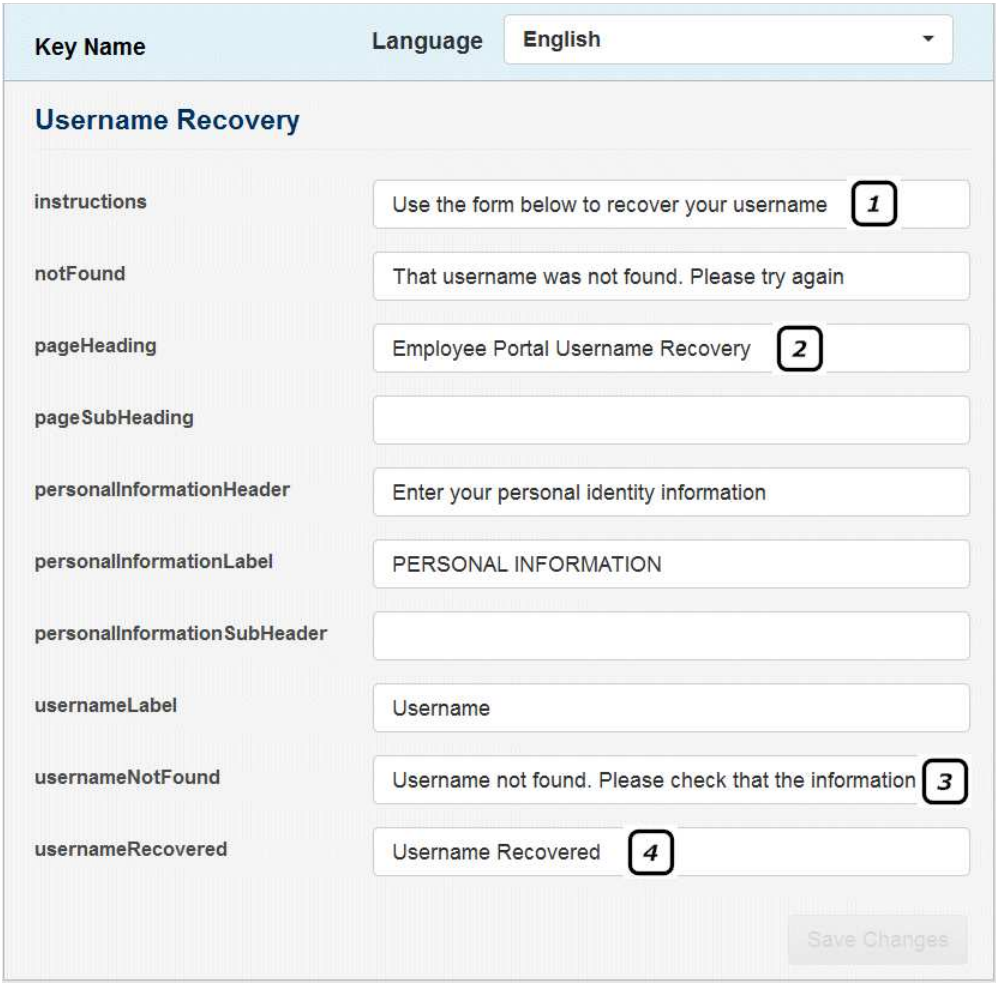
密码重置验证键名用于在自助服务的"密码重置验证"页面中标注标题和字段。

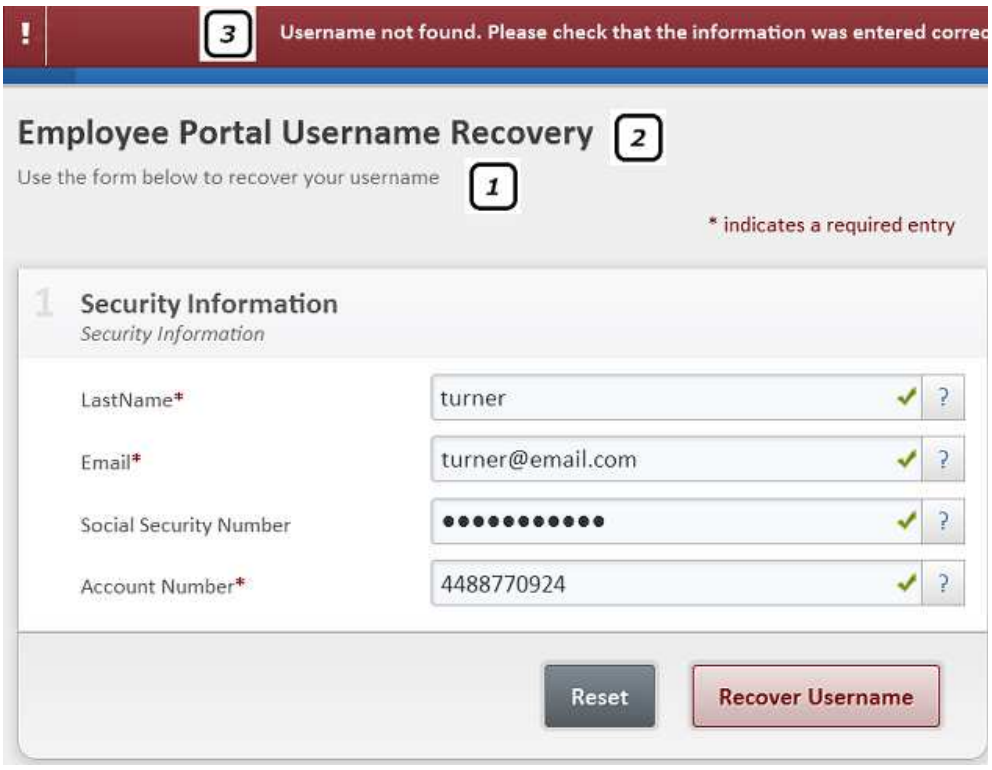


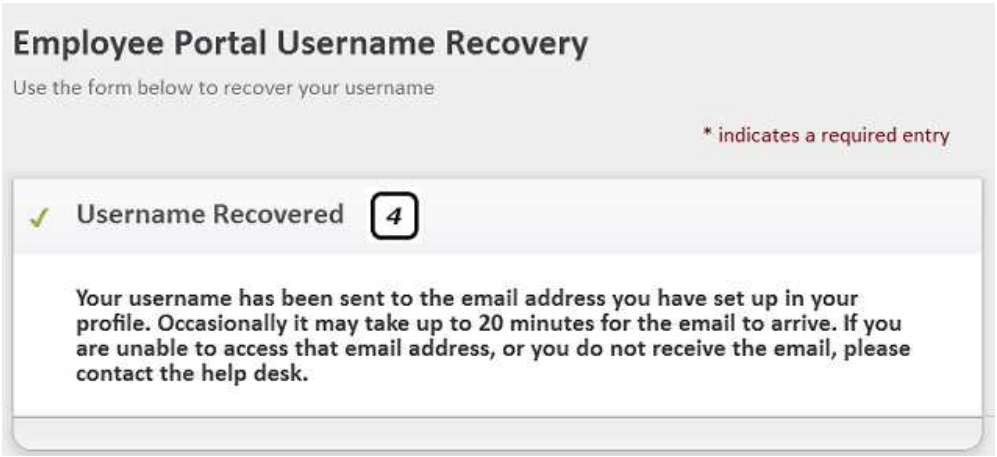


用户名恢复键名

用户名恢复键名用于在自助服务的"用户名恢复"页面中标注标题和字段。

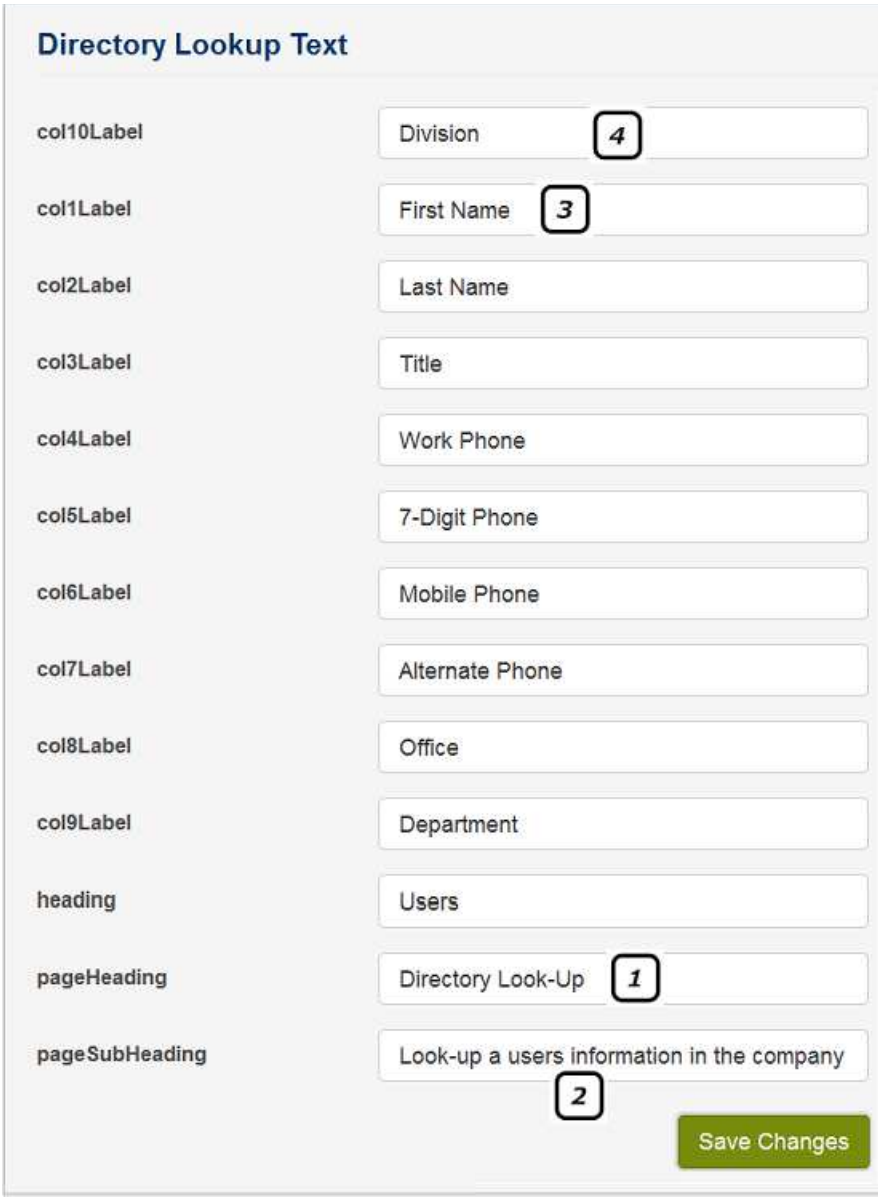


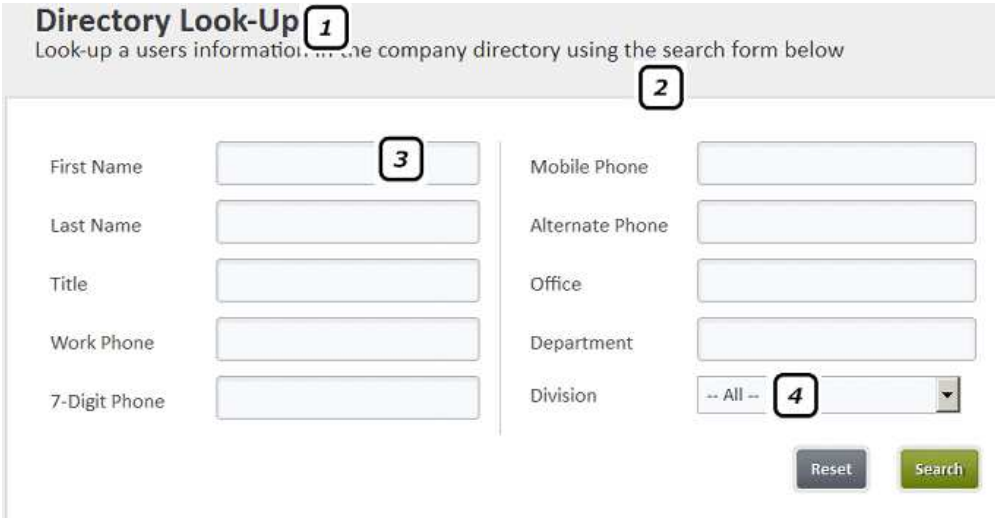

!
3
Username not found. Please check that the information was entered correc
Employee Portal Username Recovery
2
Use the form below to recover your username
1
* indicates a required entry
1
Security Information
Security Information
LastName*
turner
Email*
turner@email.com
Social Security Number
Account Number*
4488770924
Reset
Recover Username


Employee Portal Username Recovery
Use the form below to recover your username
* indicates a required entry
Username Recovered
4
Your username has been sent to the email address you have set up in your profile. Occasionally it may take up to 20 minutes for the email to arrive. If you are unable to access that email address, or you do not receive the email, please contact the help desk.

目录查找键名

目录查找键名用于在自助服务的"目录查找"页面中标注标题和字段。





添加实例

您可以添加一些实例以供贵组织中的不同角色使用。

关于此任务

实例是自助服务应用程序的一组配置和选项。例如，实例可以定义文本翻译、表单布局、自注册选项和其他自助服务应用程序选项。对于定义的每个角色，可以为该角色选择实例。例如，可以为帮助台角色和管理者角色分配不同的实例，从而为他们授予对不同自助服务应用程序选项的访问权。一个角色只能分配到一个实例，但一个实例可以供多个角色使用。

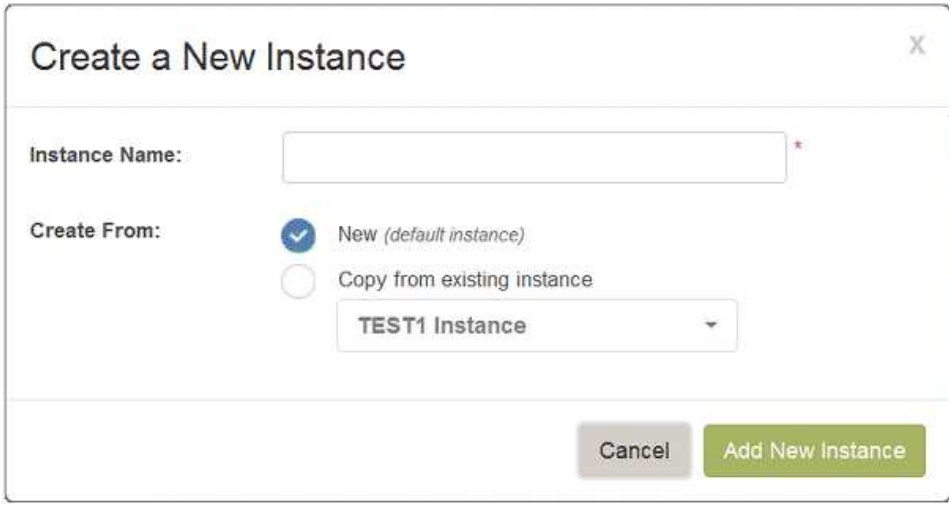
您可以选择在以下情况下使用的实例：

- 配置自助服务应用程序
- 定制自助服务应用程序的 UI

需要时可以通过大多数自助服务配置和定制任务创建实例。在以下示例中，将从**自助服务** > **内容管理**创建实例。

过程

1. 在导航窗格中，单击**内容管理**。
2. 单击**添加新实例**。



3. 在**实例名称**字段中输入实例名称。
4. 选择实例是基于缺省实例还是其他实例。
   - **新建**。实例基于为缺省实例创建的配置选项。
   - **从现有实例复制**。实例基于为所选实例创建的配置选项。
5. 单击**添加新实例**。

添加本地语言支持

您可以添加本地语言支持，以便自助服务应用程序、消息和电子邮件中的文本都以您选择的语言显示。

添加语言

您可以向 Cloud Identity Portal 添加受支持的语言。添加的语言可以用于在自助服务应用程序中提供以所选语言显示的文本。

过程

1. 在导航窗格中，单击**自助服务** > **内容管理**。
2. 从**添加新语言**菜单中选择要添加的语言。 该菜单显示所有受支持的语言列表。
3. 单击**添加新语言**。

提供翻译文本

您可以提供翻译的文本，从而为自助服务应用程序用户提供本地语言支持。

关于此任务

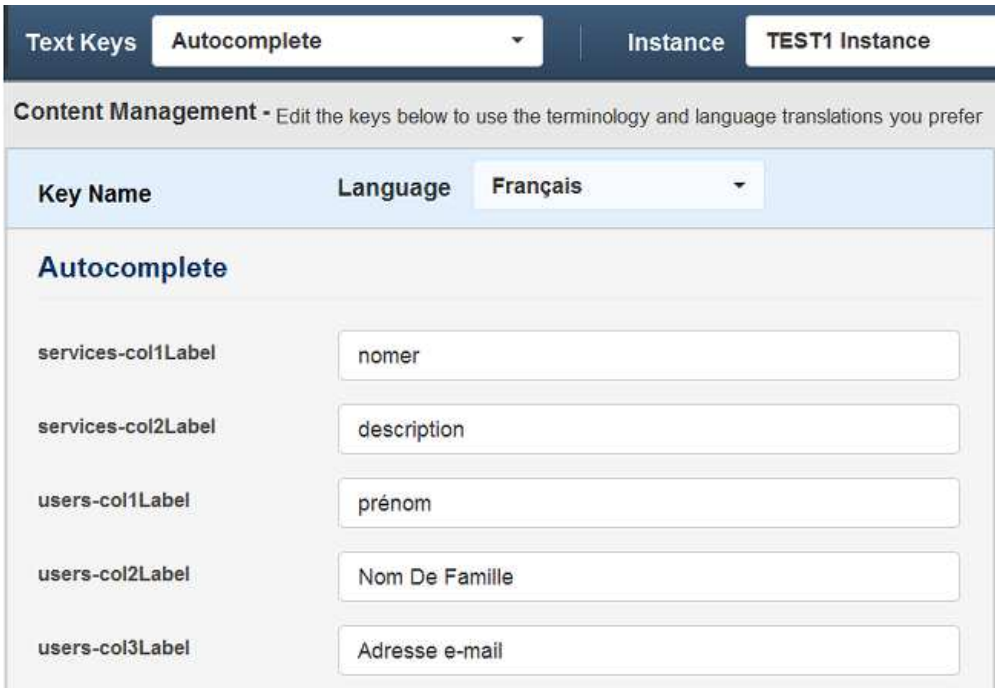
您可以为自助服务应用程序的许多方面（包括电子邮件模板和安全问题）提供文本。您可以从一些受支持的语言中进行选择。

您可以选择一种语言来为以下内容提供本地语言文本：

- 安全问题
- 自助服务应用程序 UI 文本

- 电子邮件模板
- 自助服务概要文件门户网站
- 自助服务应用程序套件页面，包括自注册、密码重置、用户名恢复和目录查找

在以下示例中，自动完成文本键翻译为法语。



第 7 章 应用程序

应用程序管理包括管理与公司保护的 Web 资源的网络连接、与联合第三方 Web 应用程序的网络连接以及管理用户供应和服务。

管理服务

服务提供角色或组功能之外的额外功能。一般而言，服务用于提供用户身份和 Cloud Identity Service 外部系统之间的链接。

服务概述

一般而言，服务用于提供用户身份和可能需要将用户供应到的 Cloud Identity Service 外部系统之间的链接。

您可以使用 Cloud Identity Service 来管理服务，包括服务成员资格。服务成员资格可以手动管理，也可以使用动态供应策略进行管理。每个服务都必须具有服务所有者。服务所有者是一个用户，通常将其定义为服务链接到的外部系统的所有者或管理员。服务类别可以用来将相关服务组合在一起，以使自助服务用户更容易管理其服务。

服务的用户成员资格可以通过静态或动态方式定义。静态用户成员资格要求您将每个用户手动添加到服务以及手动管理成员资格。动态用户成员资格自动选择用户来授予成员资格，选择依据是用户身份属性值、其他组成员资格、其他服务成员资格或是否为其分配了管理者角色的任意匹配组合。

动态用户成员资格使用动态供应策略来实现，在此策略中，您定义成员资格选择条件。

可以为服务定义任意数量的动态策略。可以通过协调策略按需应用策略。还可以根据计划应用策略。应用策略时，将评估其选择条件，并更新用户成员资格，从而除去不匹配的用户并添加匹配的用户。

服务包括用于在服务之间创建依赖关系（包括父子关系和容器映射）的选项。父子关系用于强制先获取父服务中的成员资格，再获取任何子服务中的成员资格。容器映射用于定义一些服务，当获取了该容器的成员资格时，这些服务直接请求每个内含服务中的用户成员资格。

通知用于向各个收件人发送通知电子邮件。通知可以包括特定于服务的供应信息和取消供应信息。

重新认证用于控制随着时间的推移，哪些用户仍保持为服务成员。重新认证策略的定义方式与动态供应策略相同。根据服务的定义方式，符合重新认证策略条件的任何成

© Copyright IBM Corp. 2015, 2017

员都会向其管理者和/或服务所有者发送重新认证请求。管理者或服务所有者将认证该用户是否仍属于该服务。对于基于策略的服务成员资格和手动控制的服务成员资格，可能需要重新认证。可计划重新认证策略以使重新认证按指定频率发生。

审批用于控制哪些用户可以获取服务成员资格。对于动态控制的成员资格和手动控制的成员资格，可能需要审批。审批可能要求管理者和/或服务所有者进行操作。审批可以应用于成员资格和重新认证过程。

搜索服务

您可以搜索贵组织中的任何服务来查看该服务的详细信息，或者修改该服务的详细信息以及管理该服务的成员资格。

过程

1. 在导航菜单中，单击**应用程序 > 服务**，然后单击**常规**。
2. 在**过滤结果**字段中，至少输入服务的前 3 个字符。字段标签将更改为**正在搜索**。

   此时将列出与搜索条件匹配的服务。选择要修改或查看的服务。

搜索服务类别

您可以搜索任何服务类别，以查看或修改该类别的详细信息，以及管理该类别下分组的服务。

过程

1. 在导航菜单中，单击**应用程序 > 服务**，然后单击**类别管理**。
2. 在**过滤结果**字段中，至少输入服务类别的前 3 个字符。字段标签将更改为**正在搜索**。

   将列示与搜索条件匹配的类别。选择要修改或查看的类别。

创建服务

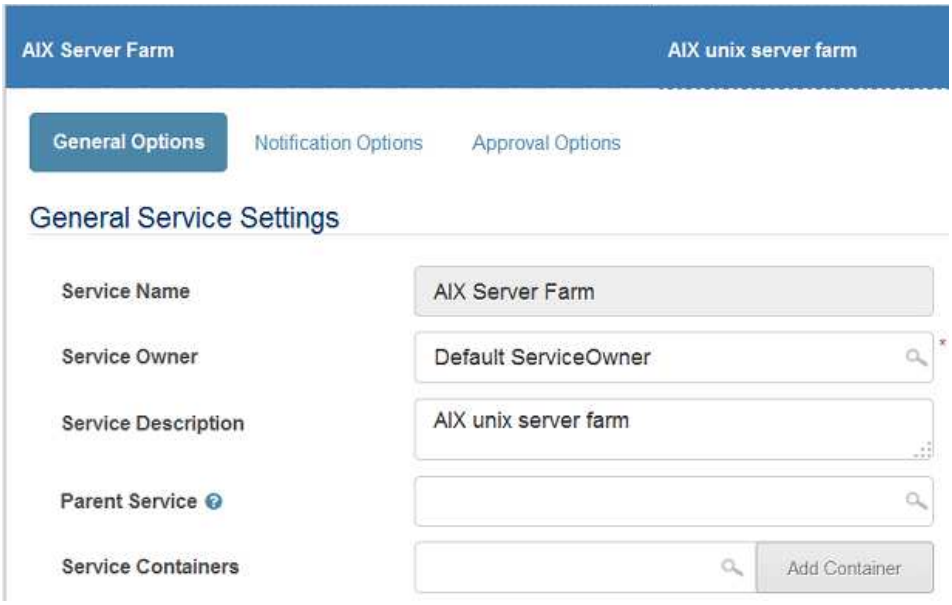
您可以添加新服务。在添加服务之后，您可以通过静态或动态管理服务来选择要成为服务成员的用户。

过程

1. 在导航菜单中，单击**应用程序 > 服务**，然后单击**添加服务**。
2. 输入服务的名称、服务所有者和描述。

   服务名称必须唯一。单击**检查可用性**来检查服务名称是否已被使用。

   要搜索并选择用户以作为服务所有者，请在**服务所有者**字段中至少输入搜索条件的前 3 位。您可以搜索用户的名字、姓氏或电子邮件地址。从返回的列表中选择用户。
3. 单击**保存更改**以添加服务。 该服务已保存。您将返回到服务列表。
4. 搜索并选择服务以输入**常规选项**、**通知选项**、**审批选项**和**表单选项**。



下一步做什么

创建服务之后，您可以手动或动态向服务添加成员，并可以创建重新认证策略。

服务设置

服务设置包括常规、通知和审批选项。

表 23. 常规选项

设置	描述
服务名称	服务名称。
服务所有者	服务所有者的用户名。
服务描述	服务的描述。
父服务	指定父服务成员资格对于服务成员资格是否为必需。在获取父服务的成员资格之后，用户才有资格获取成员资格。要搜索并选择父服务，请至少输入服务名称的前 3 个字符。
内含服务	指定内含服务。容器映射用于定义一些服务，当获取了该容器的成员资格时，这些服务直接请求每个内含服务中的用户成员资格。要搜索并选择内含服务，请至少输入服务名称的前 3 个字符，选择该服务，然后单击**添加服务**。
请求指示信息	用户请求服务时向用户显示的指示信息。
需要 SOD 调出	职责分离。指定在触发审批过程之前是否需要工作流程在外部系统上记录服务请求审批。
在自助服务 UI 中隐藏服务	指定是否在自助服务概要文件应用程序中显示服务。
允许重复的成员资格请求	指定是否允许重复的成员资格请求。 • **开启**。服务不能包含永久性成员。用户成员资格会自动到期。必须重新请求成员资格。 • **关闭**。用户成员资格不会自动到期。
动态供应策略	管理策略。使用动态供应策略管理服务的成员资格。
重新认证策略	管理策略。使用重新认证策略管理服务的重新认证。

表 *23.* 常规选项 *(续)*

设置	描述
服务成员	静态（手动）管理服务成员资格。
分配到类别	可以将服务分配到一个或多个服务类别。服务类别用来将相关服务组合在一起，从而使用户更容易在自助服务应用程序中管理他们的服务。 单击**管理类别**以打开"将服务分配到类别"窗口。要搜索并选择类别，请在**类别名称**字段中至少输入类别名称的前 3 位。从返回的列表中选择类别，然后单击**添加类别**。将服务添加到所需数目的类别，然后单击**完成**。

表 *24.* 通知选项

设置	描述
收件人类型	组、服务或用户。向组或服务的所有成员或者向用户发送通知电子邮件。当发生某个事件（例如，向服务添加了用户）时将会发送通知。
收件人名称	向其发送通知的组、服务或用户的名称。要搜索并选择组或服务，请至少输入该组或服务名称的前 3 个字符。从返回的列表中选择组或服务。要搜索并选择用户，请至少输入搜索条件的前 3 位。您可以搜索用户的名字、姓氏或电子邮件地址。从返回的列表中选择用户。
供应指示信息	将用户添加到服务时用户必须遵循的指示信息。
取消供应指示信息	从服务除去用户时用户必须遵循的指示信息。
将分配/撤销通知给成员	指定在服务中添加或除去用户时是否向用户发送通知。
将分配/撤销通知给管理者	指定在服务中添加或除去用户时是否向用户管理者发送通知。

表 *25.* 审批和重新认证选项

设置		描述
审批需求	**拖欠操作**	服务审批请求在到期日期之前未获批准时要执行的操作。
	操作到期期限	拖欠操作到期前的天数。
	管理者审批	指定用户管理者是否必须予以审批，然后才能为用户授予服务成员资格。 • **动态** – 选中此复选框：当动态策略生效时，将自动生成服务请求审批通知电子邮件，以通知管理者他们必须手动批准的暂挂服务请求。 – 清空此复选框：代表管理者自动进行审批。 • **请求**。选中此复选框：向请求服务的用户的管理者发送请求。必须批准这些请求，用户才能成为服务成员。
	服务所有者	指定服务所有者是否必须予以批准，然后才能为用户授予服务成员资格。 • **动态** – 选中此复选框：当动态策略生效时，将自动生成服务请求审批通知电子邮件，以通知服务所有者他们必须手动批准的暂挂服务请求。 – 清空此复选框：代表服务所有者自动进行审批。 • **请求**。选中此复选框：向请求服务的用户的服务所有者发送请求。必须批准这些请求，用户才能成为服务成员。

表 25. 审批和重新认证选项 (续)

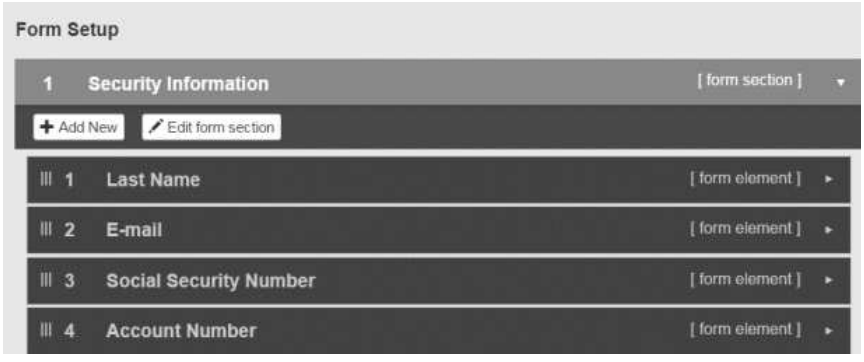
设置		描述
重新认证设置	**拖欠操作**	服务成员资格在到期日期之前未进行重新认证时要执行的操作。到期日期是重新认证计划设置的日期。
	操作到期期限	拖欠操作到期前的天数。
	管理者审批	指定用户管理者是否必须予以批准后才能重新认证用户。 • **动态** – 选中此复选框：将自动生成重新认证审批通知电子邮件，以通知管理者他们必须手动批准的暂挂重新认证请求。 – 清空此复选框：代表管理者自动进行审批。 • **请求**。选中此复选框：向管理者发送请求。必须批准请求才能重新认证用户。
	服务所有者	指定服务所有者是否必须予以批准后才能重新认证用户。 • **动态** – 选中此复选框：将自动生成重新认证审批通知电子邮件，以通知服务所有者他们必须手动批准的暂挂重新认证请求。 – 清空此复选框：代表服务所有者自动进行审批。 • **请求**。选中此复选框：向服务所有者发送请求。必须批准请求才能重新认证用户。

配置服务表单

用户或服务所有者在请求或撤销服务访问权时必须填写表单。每个表单都包含若干字段，用户或服务所有者在请求或撤销服务访问权时必须填写这些字段。您可以对各个字段和区段进行重新排序，添加新区段，以及添加或除去字段。

过程

1. 单击要编辑的表单的**编辑表单**，您可以编辑以下表单：
   - **请求访问权表单**。当用户请求对服务的访问权时，由用户填写。
   - **撤销访问权表单**。当服务所有者想要除去用户对服务的访问权时，由服务所有者填写。



2. 添加字段：
   a. 单击**新增** > **新增字段**。
   b. 选择属性和字段选项来定义字段。
   c. 单击**保存更改**以添加字段。
3. 添加区段：
   a. 单击**新增** > **新增区段**。
   b. 输入该区段的**标签**、**副标题**和**标题**。 标签、副标题和标题用于在表单上标识该区段。
   c. 单击**新增字段**以在该区段中输入新字段，选择属性和字段选项来定义字段。
   d. 单击**保存更改**以保存该新区段。 您可以从主"表单设置"窗口向该区段添加更多字段。
4. 要更改表单顺序并将某个区段或字段移到新位置，单击该字段或区段并拖动至新位置。

5. 单击**保存更改**以保存该表单。

表单选项：

表单选项用于设置自助服务应用程序中使用的字段特性。

根据所定义的表单，某些选项可能不可用。

表 *26.* 表单字段选项

选项	描述
LDAP 属性	要用作字段的 LDAP 属性。如果选择了要求输入另一个用户作为值的属性，将向该字段添加选择工具。例如，管理者属性可能要求输入另一个用户。 根据所定义的字段或表单，可能无法删除某些属性。
缺省值	字段的缺省值。如果字段可编辑，那么用户可以替换缺省值。
字段标签	用于标识字段的标签。

表 26. 表单字段选项（续）

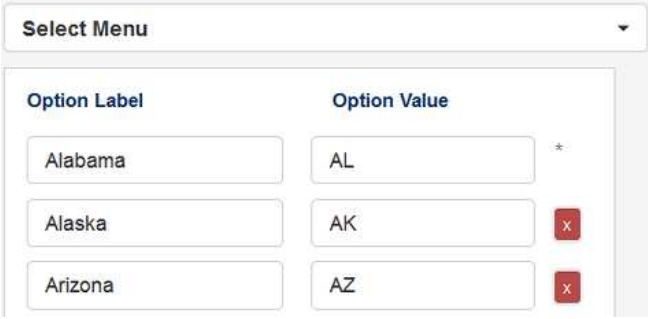
选项	描述
字段类型	• **复选框**。用户可以选择一个或多个选项作为字段输入。 • **密码字段**。密码字段带有掩码。 • **单选按钮**。用户可以从一些选项中选择一个选项作为字段输入。 • **选择菜单**。用户可以从一些选项中选择一个选项作为字段输入。 • **文本字段**。用户在字段中输入值以作为输入的文本。 • **文本区域**。自由格式的文本框。 对于**复选框**、**单选按钮**和**选择菜单**，请为字段添加选项。 • **选项标签**。用于标识选项的标签。 • **选项值**。选项的值。 在该示例中，选择菜单包含用于不同状态的一些选项。 
占位符	占位符标签。
工具提示	字段帮助文本。
是否可编辑	• **是**。用户可以在字段中输入值。 • **否**。用户不能在字段中输入值。某些字段中会填充现有数据。例如，在自注册期间，用户可能针对现有身份记录申请帐户，在此情况下，可以使用该身份记录中的字段值。
是否必需	• **是**。该字段为必填字段。 – 自注册表单。如果不为该字段提供值，用户无法完成自注册。 – 自助服务概要文件表单。提示用户输入任何未填充的必填字段的值。 • **否**。该字段为可选字段。
需要当前密码匹配	仅适用于密码 LDAP 属性。 • **是**。用户必须在单独的字段中输入两次密码。在每个字段中输入的值必须匹配以确认密码正确。 • **否**。仅在一个字段中输入一次密码。
带掩码	**是**。字段带掩码，在屏幕上看不到输入的值。输入的每个字符在屏幕上都替换为星号字符。

表 *26.* 表单字段选项 *(续)*

选项	描述
需要匹配字段	• **是**。用户必须在单独的字段中输入两次值。在每个字段中输入的值必须匹配以确认值正确。例如，当用户输入电子邮件地址时，您可以要求用户输入两次该地址。 • **否**。仅在一个字段中输入一次值。
验证	验证规则： • **是**。输入的值必须通过指定的验证规则。例如，日期可能需要通过格式验证规则，如 yyyy/mm/dd。 • **否**。不验证输入的值。 验证类型： • **日期**。值必须符合指定的日期格式。例如，yyyy/mm/dd。 • **电子邮件地址**。值必须对应于电子邮件地址格式。例如，*text_string*@*text_string*.com。 • **字母**。值必须仅包含字母字符。 • **最大字符长度**。值不能包含超过指定数量的字符。 • **最小字符长度**。值不能包含少于指定数量的字符。 • **数字**。值必须仅包含数字字符。 • **密码强度**。密码字段必须符合基本、标准或强验证规则。规则基于必须输入的字符数和字符类型。 • **美国电话号码**。值必须符合美国电话号码格式。 定制正则表达式。用于针对所输入值进行求值的正则表达式。如果表达式求值为 true，表示值有效。 • **模式**。正则表达式。例如，要将注册限制为北卡罗来纳州中的地址，使用正则表达式 `^NC$` 来表示 state 属性，其中，NC 定义为 state 属性的可选值。 • **错误消息**。输入的值无效时向用户显示的错误消息。

表 *27.* 表单区段选项

选项	描述
标签	区段标签。
副标题	副标题标签。
标题	标题。

创建服务类别

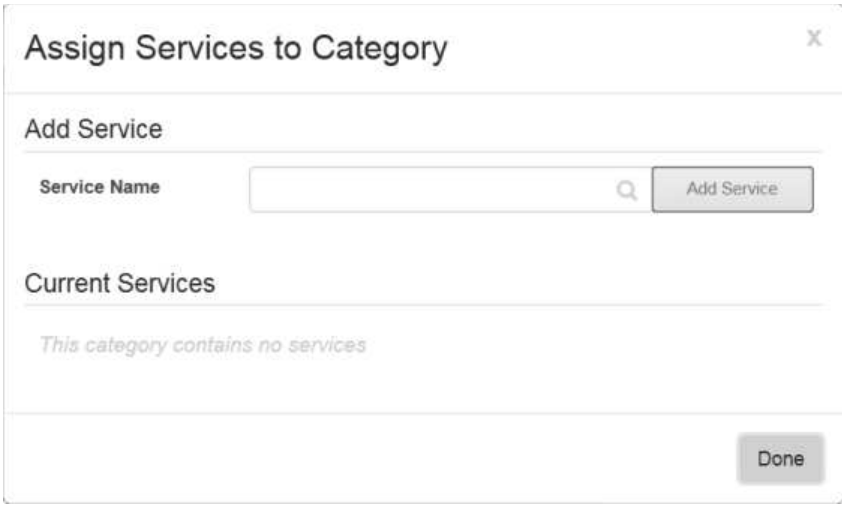
您可以创建服务类别以将相关服务组合在一起。服务组使用户更容易在自助服务 应用程序中管理他们的服务。

过程

1. 在导航菜单中，单击**应用程序** > **服务**，然后单击**类别管理**和**添加新类别**。
2. 输入名称，输入描述，并为该类别选择图标。

类别名称必须是唯一的。可以通过在**选择下列其中一个**搜索字段中输入字符串来搜索图标。

3. 单击**添加类别**以添加服务类别。 将保存该类别。您将返回到服务类别列表。
4. 搜索并选择该类别，以对其添加服务。
5. 单击**管理服务**以打开"将服务分配到类别"窗口。



要搜索并选择服务，请在**服务名称**字段中至少输入服务名称的前 3 位。从返回的列表中选择服务，然后单击**添加服务**。

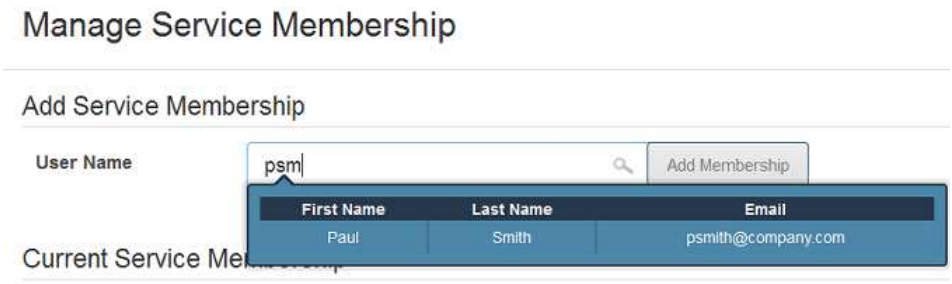
添加所需的所有服务，然后单击**完成**。

静态管理服务成员资格

静态定义的用户成员资格要求手动添加和除去每个用户成员。

过程

1. 搜索并选择想要向其添加成员的服务。
2. 单击**管理服务成员资格**。



3. 在**用户名**字段中，搜索想要添加的用户。要搜索用户，请输入用户的名字、姓氏、用户名或电子邮件地址的前 3 个字符。
4. 选择用户并单击**添加成员资格**。
5. 添加所需的所有用户之后，单击**完成**。

以动态方式管理服务成员资格

动态供应策略允许服务的用户成员资格基于匹配条件。将自动选择与条件匹配的用户以授予该服务的成员资格。

创建动态供应策略

动态供应策略用于确定服务的用户成员资格。

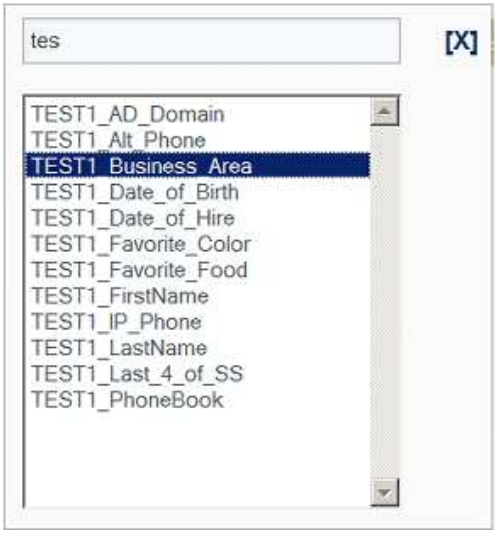
关于此任务

成员资格基于策略的选择条件。例如，您可以通过确定工作位置的属性或通过确定某个组的工作位置和成员资格的属性来指定服务成员资格。一个服务可以有一个或多个策略。

过程

1. 搜索并选择想要将策略添加到的服务。
2. 对于**动态供应策略**，单击**管理策略**。
3. 单击**添加新策略**。

4. 在**策略名称**字段中为策略输入有意义的名称。
5. 选择想要使用的变量，您可以选择要在策略中使用的任意类型的一个或多个变量。 您可以选择以下变量类型的任意组合：
   - **属性**。基于用户身份属性包含用户。
   - **组**。基于组成员资格包含或排除用户。
   - **服务**。基于其他服务成员资格包含或排除用户。
   - **管理者**。基于是否为其分配了管理者角色来包含用户。
6. 要将用户身份属性用作变量：
   a. 单击**选择变量**，然后单击**属性**。
   b. 单击**过滤属性**字段，然后输入属性的前几个字符。双击属性以将其选中。



c. 选择**运算符**，然后输入属性**值**。

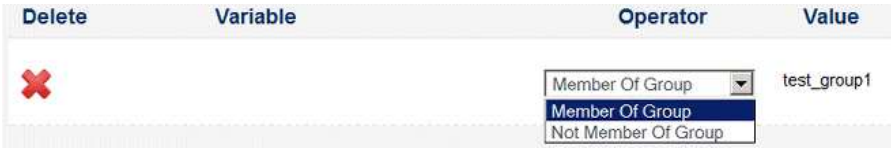
注：您可以使用通配符。例如，可以输入 11* 以表示以 11 开头的任何数字。

提示：如果要将属性和属性值视为时间戳记，那么可以使用 $date$ 作为值的前缀。此前缀将采用缺省日期格式 yyyy-MM-dd HH:mm:ss。例如，您可以输入 $date$1970-01-01 00:00:00 以表示 1970 年 1 月 1 日午夜。

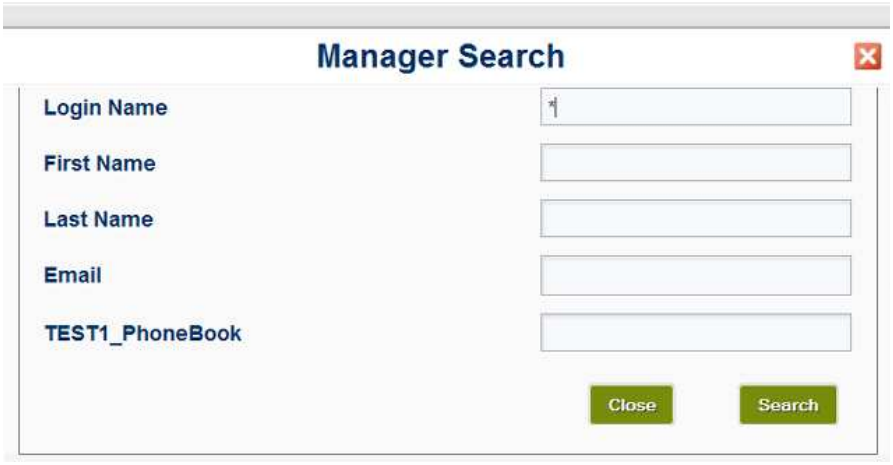
您还可以为时间戳记指定非缺省格式，方法是使用 SimpleDateFormat 将该格式包含在 $date$ 前缀中。例如，对于 Z 时间戳记，您可以输入 $date{yyyy-MM-dd HH:mm:ssZ}$1970-01-01 00:00:00-0400，以在比 GMT/UTC 早 4 个小时的时区中表示 1970 年 1 月 1 日午夜。更改缺省格式会导致相同格式应用于所检索的属性值。您必须了解要检索的值的格式，并且它们与要使用的格式一致。有关不同格式模式的更多信息，请参阅 SimpleDateFormat。

如果规则中指定的值或其比较值都未进行解析，那么将记录警告或错误。有关更多信息，请与 IBM 支持代表联系。全球标准时间 (UTC) 是缺省时区。

7. 要将某个组的成员资格或非成员资格用作变量：
   a. 单击**选择变量**，然后单击**组**。
   b. 单击**过滤组**字段，然后输入组的前几个字符。双击组以将其选中。
   c. 选择成员资格是取决于该组的成员资格，还是成员资格取决于该其他组的非成员资格。



8. 要将另一个服务的成员资格或非成员资格用作变量：
   a. 单击**选择变量**，然后单击**服务**。
   b. 单击**过滤服务**字段，然后输入服务的前几个字符。双击服务以将其选中。
   c. 选择成员资格是取决于该其他服务的成员资格，还是成员资格取决于该其他服务的非成员资格。
9. 要将管理者角色用作变量：
   a. 单击**选择变量**，然后单击**管理者**。



   b. 在**管理者搜索**窗口中的任何字段中输入搜索条件来搜索用户。单击**搜索**。 这样仅返回分配了管理者角色并且与搜索条件匹配的用户。

      注：您可以在搜索中使用通配符。例如，可以输入 `Joh*` 以表示以 Joh 开头的名称。
   c. 选择用户。 您可以重复搜索以添加更多用户。
10. 使用**合取**字段来组合一个或多个变量以确定服务成员资格。使用合取值 `And` 或 `Or` 将一个比较条件的结果与下一行组合起来。

    变量（条件）分组自顶向下，因此先前条件的结果将与后续条件组合起来。

    使用箭头图标可上下移动条件  。

    在以下示例中，仅使用一个变量来确定成员资格：用户身份属性 TEST1_Business_Area。要成为成员，用户的 TEST1_Business_Area 属性必须具有值 London W4。

    在以下示例中，使用两个变量确定成员资格。要成为成员，用户的 TEST1_Business_Area 属性必须具有值 London W4，并且用户必须是 Group1 的成员。

在以下示例中，使用三个变量确定成员资格。要成为成员，用户的 TEST1_Business_Area 属性必须具有值 London W4，并且用户必须是 Group1 的成员或者 Group2 的成员。

11. 在定义了需要在策略中包含的所有条件之后，单击**保存**。

下一步做什么

模拟策略以检查成员资格是否符合预期。

以专家方式创建动态供应策略

在某些情况下，无法使用基本属性比较和其他服务或组成员资格来确定服务的策略选择条件。成员资格可能要求检查随其他属性值而变化的属性值（子字符串）。在此类情况下，必须以专家方式定义策略。

开始之前

要使用专家方式，必须充分了解并能够熟练地用 JavaScript 编码。

关于此任务

您可以用 JavaScript 以专家方式定义策略。

在策略评估期间，将针对注册表中的每个用户运行一次 JavaScript。JavaScript 检查用户及其成员资格的注册表属性，并决定是否将用户包含在服务中。JavaScript 使用变量 **inGroup** 将此决定传达给 Cloud Identity Service。如果 JavaScript 的结果是 **inGroup** 等于 TRUE，那么将用户包含在服务中，否则不包含用户。

JavaScript 可以使用三种方法来获取有关每个用户的 Cloud Identity Service 注册表属性和组信息。

- `String isMemberOfGroup(String groupName)`
- `String[] getAttributeValues(String attributeName)`

- `String evaluateAttribute(String attributeName, int operator, String constant)`

其中每种方法都使用可供 JavaScript 使用的另一个变量 **ldap** 进行调用。例如，要确定当前用户是否是名为 **accounting** 的组的成员，可以使用以下语句：

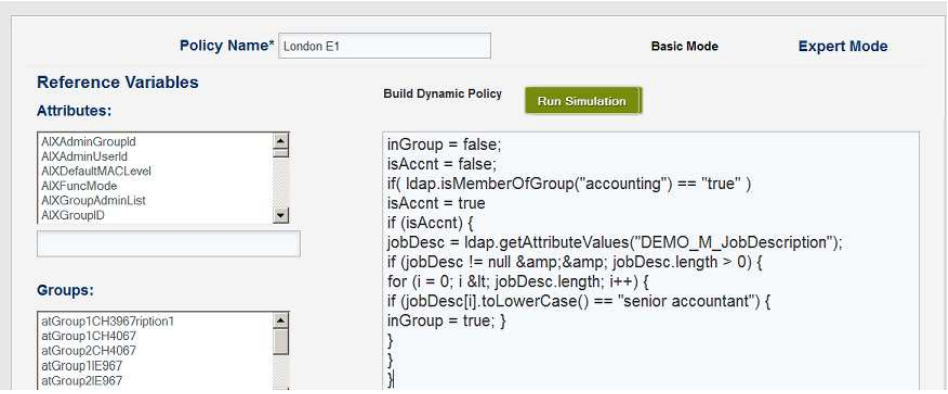
```
var isAccountant = ldap.isMemberOfGroup("accounting");
```

在以下 JavaScript 示例中，如果用户是 **accounting** 组的成员，同时在属性 **DEMO_M_JobDescription** 中具有值 **senior accountant**，那么将该用户包含在策略中。

```
// assume user is not in group
inGroup = false;
isAccnt = false;
if( ldap.isMemberOfGroup("accounting") == "true" )
isAccnt = true
if (isAccnt) {
jobDesc = ldap.getAttributeValues("DEMO_M_JobDescription");
if (jobDesc != null && jobDesc.length > 0) {
for (i = 0; i < jobDesc.length; i++) {
if (jobDesc[i].toLowerCase() == "senior accountant") {
inGroup = true; }
}
}
}
```

过程

1. 搜索并选择想要将策略添加到的服务。
2. 对于**动态供应策略**，单击**管理策略**。
3. 单击**添加新策略**。
4. 单击**专家方式**。



5. 输入想要用于确定成员资格的 JavaScript。

   属性、**组**和**服务**在各自的框中列出以供您参考。您可以在相应框下方的过滤器字段中输入前几个字符来搜索属性、组或服务。您可以复制并粘贴所选属性、组或服务。

6. 在定义了要在策略中使用的所有条件之后，单击**保存**以保存策略。

下一步做什么

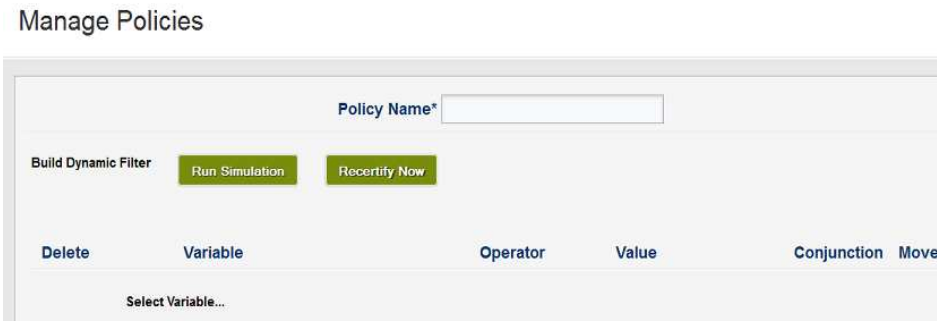
模拟策略以检查成员资格是否符合预期。

创建重新认证策略

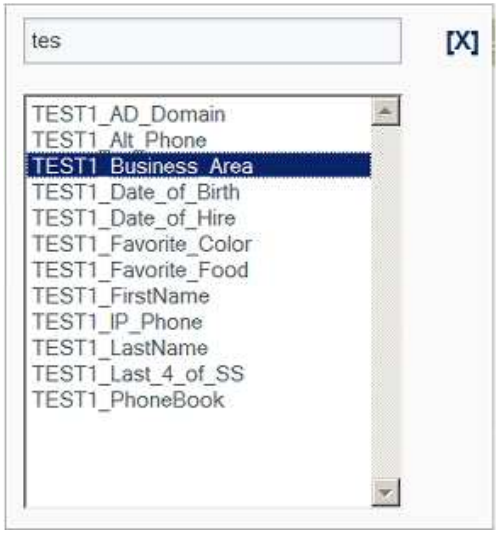
重新认证策略用于确定哪些用户仍保持为服务成员。重新认证策略的定义方式与动态供应策略相同。持续成员资格基于用户身份属性值、其他组成员资格、其他服务成员资格和管理者角色。一个服务可以有一个或多个重新认证策略。

过程

1. 搜索并选择想要将重新认证策略添加到的服务。
2. 对于**重新认证策略**，单击**管理策略**。
3. 单击**添加新策略**。



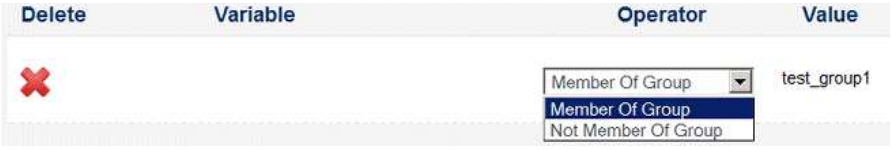
4. 在**策略名称**字段中为策略输入有意义的名称。
5. 选择想要使用的变量，您可以选择要在策略中使用的任意类型的一个或多个变量。 您可以选择以下变量类型的任意组合：
   - **属性**。基于用户身份属性包含用户。
   - **组**。基于其他组成员资格包含或排除用户。
   - **服务**。基于其他服务成员资格包含或排除用户。
   - **管理者**。基于是否为其分配了管理者角色来包含用户。
6. 要将用户身份属性用作变量：
   a. 单击**选择变量**，然后单击**属性**。
   b. 单击**过滤属性**字段，然后输入属性的前几个字符。双击属性以将其选中。



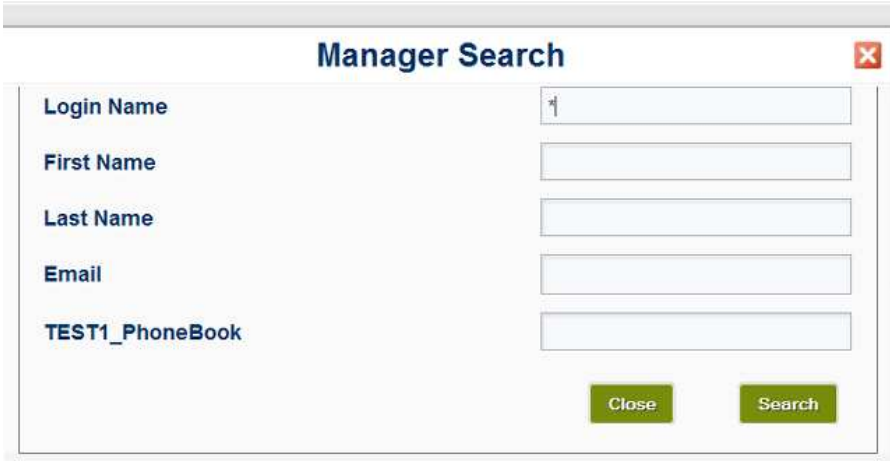
c. 选择**运算符**，然后输入属性**值**。

注：您可以使用通配符。例如，可以输入 11* 以表示以 11 开头的任何数字。

7. 要将某个组的成员资格或非成员资格用作变量：
   a. 单击**选择变量**，然后单击**组**。
   b. 单击**过滤组**字段，然后输入组的前几个字符。双击组以将其选中。
   c. 选择持续成员资格是取决于该组的成员资格，还是持续成员资格取决于该组的非成员资格。



8. 要将另一个服务的成员资格或非成员资格用作变量：
   a. 单击**选择变量**，然后单击**服务**。
   b. 单击**过滤服务**字段，然后输入服务的前几个字符。双击服务以将其选中。
   c. 选择持续成员资格是取决于该其他服务的成员资格，还是持续成员资格取决于该其他服务的非成员资格。
9. 要将管理者角色用作变量：
   a. 单击**选择变量**，然后单击**管理者**。



b. 在**管理者搜索**窗口中的任何字段中输入搜索条件来搜索用户。单击**搜索**。 这样仅返回分配了管理者角色并且与搜索条件匹配的用户。

注：您可以在搜索中使用通配符。例如，可以输入 Joh* 以表示以 Joh 开头的名称。

c. 选择用户。 您可以重复搜索以添加更多用户。

10. 使用**合取**字段来组合一个或多个变量以确定服务的持续成员资格。使用合取值 And 或 Or 将一个比较条件的结果与下一行组合起来。

变量（条件）分组自顶向下，因此先前条件的结果将与后续条件组合起来。

使用箭头图标可上下移动条件  。

在以下示例中，仅使用一个变量来确定持续成员资格：用户身份属性 TEST1_Business_Area。要成为成员，用户的 TEST1_Business_Area 属性必须具有值 London W4。

在以下示例中，使用两个变量确定持续成员资格。要成为成员，用户的 TEST1_Business_Area 属性必须具有值 London W4，并且用户必须是 Group1 的成员。

在以下示例中，使用三个变量确定持续成员资格。要成为成员，用户的 TEST1_Business_Area 属性必须具有值 London W4，并且用户必须是 Group1 的

成员或者 Group2 的成员。

11. 在定义了需要在策略中包含的所有条件之后，单击**保存**。

下一步做什么

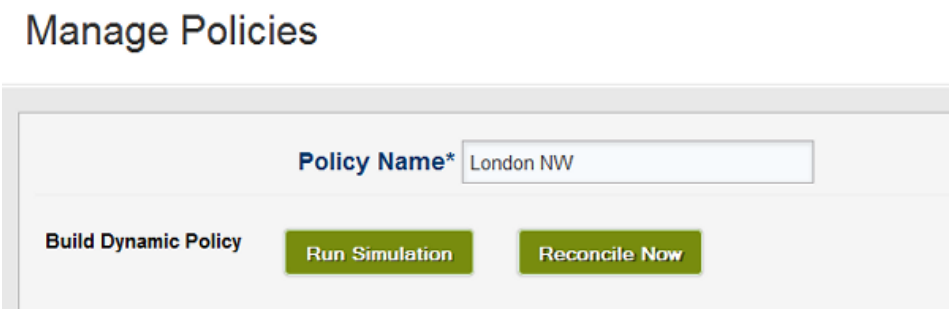
模拟策略以检查持续成员资格是否符合预期。

模拟策略

您可以模拟策略来评估服务的用户成员资格，从而检查成员资格是否符合预期。您可以模拟动态供应策略和重新认证策略。模拟不会更改服务的成员资格。它显示包含该服务的建议成员资格的用户。可以 CSV 文件形式查看和保存结果。

过程

1. 如果没有选择策略，搜索并选择服务。打开"管理策略"窗口以编辑策略。
2. 单击**运行模拟**。



3. 选择要运行的模拟类型。
   - 动态供应策略。
     - **模拟目录中的所有用户**。该选项将策略选择与 Cloud Identity Service 中的所有用户进行比较。满足策略的用户将以添加或保留状态列示在结果中。不满足策略的用户将以从服务中除去或未添加状态列示在结果中。
     - **模拟当前位于组中的所有用户**。该选项比较策略选择条件与当前位于服务中的所有用户的属性。服务中的每个用户以除去或保留状态列示在结果中。新用户不会以添加状态列出。
     - **模拟单个用户**。该选项比较策略选择条件和所选用户。该用户以保留、除去、添加或未添加状态列示在结果中。使用用户名搜索用户。在**过滤用户**字段中输入用户名的前几个字符，单击**搜索用户**，然后选择用户。

- 重新认证策略。
  - **模拟所有当前服务成员**。该选项比较策略选择条件与当前位于服务中的所有用户的属性。服务中的每个用户以包含或排除状态列示在结果中。新用户不会以添加状态列出。
  - **模拟单个服务成员**。该选项比较策略选择条件和所选用户。该用户以包含、排除、添加或未添加状态列示在结果中。使用用户名搜索用户。在**过滤用户**字段中输入用户名的前几个字符，单击**搜索用户**，然后选择用户。

4. 单击**运行模拟**。
   - 单个用户供应策略模拟的结果显示在"模拟供应策略"窗口中。
   - 单个用户重新认证策略模拟的结果显示在"模拟重新认证策略"窗口中。

   关闭"模拟策略"窗口以返回到"管理策略"窗口，然后单击**取消**。
5. 单击"管理策略"窗口中的**刷新**以查看模拟结果。当模拟完成时，将显示复选标记图标和指向 CSV 文件的链接。

6. 查看结果。
   - 单击复选标记图标 ✔ 以打开"模拟结果"窗口。您可以通过清空或选中列标题复选框来选择要查看的结果列。关闭"模拟结果"窗口以返回到"管理策略"窗口。

     注：单击**清空模拟结果**以清除"模拟结果"窗口和"管理策略"窗口中的所有结果。

- 单击 CSV 图标 可以 CSV 文件形式查看结果。您可以打开文件或保存文件。

下一步做什么

- 对于动态供应策略，协调策略并激活策略。
- 对于重新认证策略，重新认证策略并激活策略。

协调动态策略

在创建策略之后，可以协调该策略。在策略经过协调后，将根据策略选择条件来实现服务的用户成员资格。

过程

1. 搜索并选择服务。打开"管理策略"窗口以编辑策略。
2. 单击**立即协调**。

此时将显示警告消息。单击**确定**以协调策略。

下一步做什么

激活策略。

激活并计划动态策略

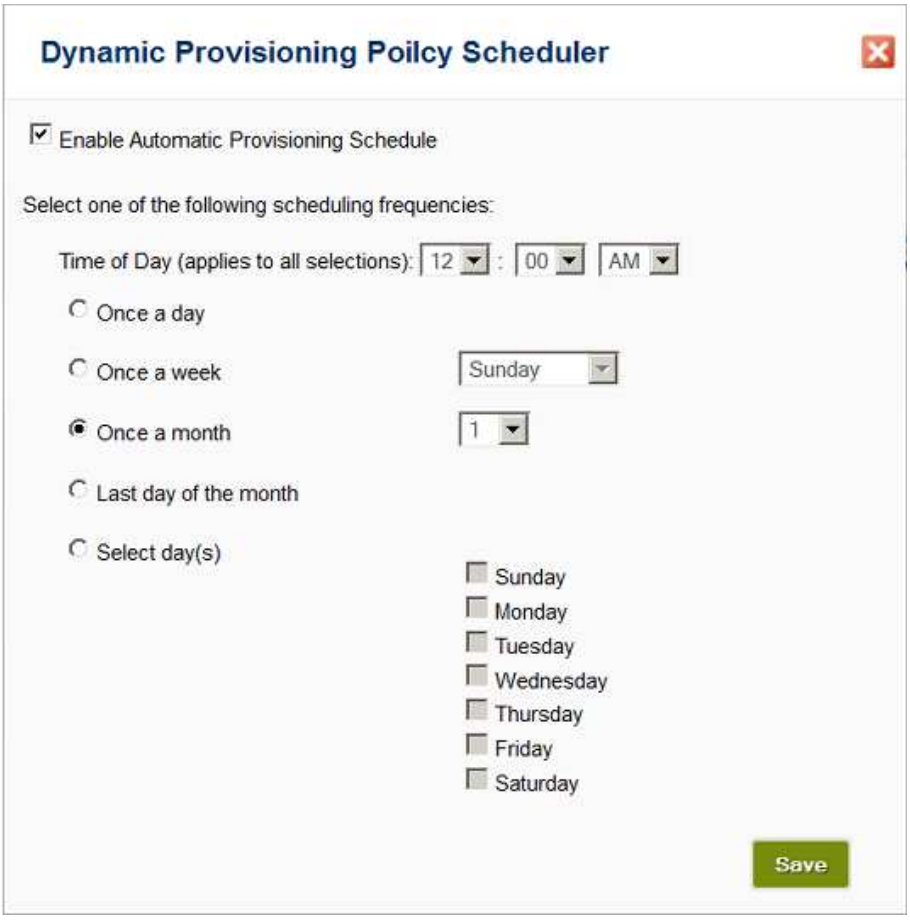
在创建和模拟策略并验证模拟结果之后，策略已准备就绪，可以对其进行激活和计划。激活策略按计划运行，因此每当运行计划时便会对服务成员资格进行评估和更新。

过程

1. 如果没有选择策略，搜索并选择服务。打开"管理策略"窗口以编辑策略。
2. 选择要激活的策略的**选择活动项**。

此时将显示警告消息。单击**确定**以激活策略。

3. 单击计划图标 以打开"动态供应策略计划程序"窗口。



4. 选中**启用自动供应计划**复选框。
5. 选择要运行计划的频率：
   - **每天一次**。选择**一天中的具体时间**。
   - **每周一次**。从下拉列表中选择周历日，然后选择**一天中的具体时间**。
   - **每月一次**。从下拉列表中选择月历日，然后选择**一天中的具体时间**。
   - **每月最后一天**。选择**一天中的具体时间**。
   - **选择若干天**。选中要运行计划的日期的复选框，然后选择**一天中的具体时间**。
6. 单击**保存**。

重新认证策略

在创建重新认证策略之后，可以重新认证策略。当策略被重新认证之后，将根据重新认证策略选择条件来实现服务的用户成员资格。立即运行协调会生成无法撤回的重新认证审批请求。

过程

1. 搜索并选择服务。打开"管理策略"窗口以编辑策略。
2. 单击**立即重新认证**。

此时将显示警告消息。

3. 单击**确定**以重新认证策略。

下一步做什么

激活策略。

激活并计划重新认证策略

在创建和模拟策略并验证模拟结果之后，策略已准备就绪，可以对其进行激活和计划。激活策略按计划运行，因此每当运行计划时便会为用户请求服务重新认证。

过程

1. 如果没有选择策略，搜索并选择服务。打开"管理策略"窗口以编辑策略。
2. 选择要激活的策略的**选择活动项**。

此时将显示警告消息。单击**确定**以激活策略。

3. 单击计划图标  以打开"重新认证计划"窗口。

4. 选中**启用计划执行**复选框。
5. 在**每日开始时间**中选择一天中运行策略的具体时间。
6. 选择计划类型：
   - **静态计划**。
     a. 在**开始日期**中选择策略启动的日期。以 YYYY/MM/DD 格式输入日期。
     b. 从**重复时间间隔**中选择用于运行策略的频率。
   - **滚动计划**。
     a. 以天为单位在**重复时间间隔**中输入时间间隔频率。从第一个时间间隔开始，每经过您输入的天数，策略便运行一次。例如，如果您输入 30，从今天开始 30 天后、60 天后以及 90 天后都将运行一次策略。
7. 单击**保存更改**。

管理 Web 访问

管理 Web 访问包括管理与贵公司内部的受保护 Web 资源的网络连接。

Web 访问概述

您可以通过创建和管理与受保护 Web 资源的网络连接来管理 Web 访问。您还可以通过创建授权策略来控制对受保护资源的访问。授权策略包括访问控制表 (ACL)、受保护对象策略 (POP) 和全局用户策略。

受保护资源

受保护资源是指想要通过 Cloud Identity Service 进行保护的 Web 应用程序和服务器。受保护资源的常见示例包括 Web 门户网站、Java™ Platform, Enterprise Edition 应用程序服务器、IIS 上运行的 Microsoft .NET Web 应用程序和静态 HTML 内容服务器。

当用户经过认证之后，来自该用户的请求将通过 Cloud Identity Service 传递到受保护资源。Cloud Identity Service 将检查每个请求并与您的授权策略进行比较。有诸多因素（例如角色、组和服务成员资格、一天中的具体时间以及网络 IP）会影响用户是否有权访问某资源或执行某事务。

使用 Web 应用程序界面来定义和管理与客户机应用程序服务器的连接。还可以管理在每个客户机应用程序服务器上构成连接对象空间的连接和路径（受保护）对象的附加策略。

授权策略

访问控制表 (ACL) 定义哪些用户可以访问哪些受保护资源，以及这些用户可以对有权访问的资源执行哪些操作。受保护对象策略 (POP) 通过规定一天中的具体时间约束以及规定 IP 地址范围约束来限定对资源的访问。通过将策略附加到结点或路径对象可以实施策略。当策略附加到连接时，策略将应用于该连接和所有子对象。如果其他策略是在较低级别附加的，那么继承的策略将被覆盖。

搜索 Web 应用程序连接

您可以搜索与受保护 Web 应用程序的网络连接以查看、修改或除去连接。

过程

1. 在导航窗格中，单击**应用程序 > 连接管理**，然后单击 **Web 应用程序**。
2. 在**搜索**字段中，至少输入连接的前 3 个字符。 字段标签将更改为**正在搜索**。

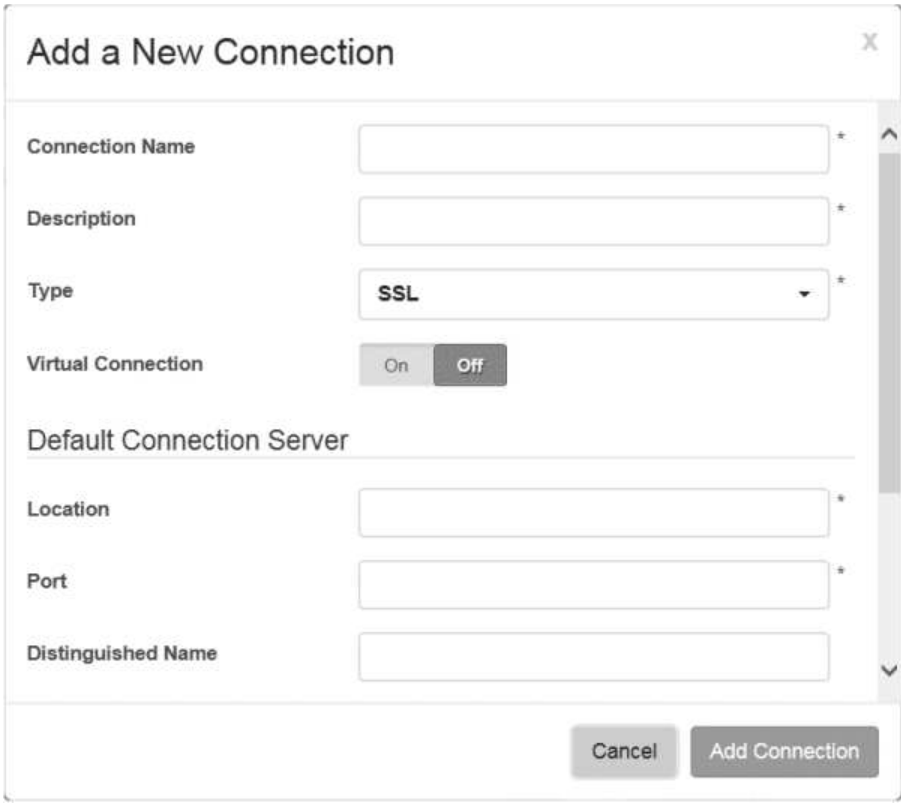
   此时将列出与搜索条件匹配的连接。选择要修改或查看的连接。

创建 Web 连接

连接表示从 Cloud Identity Service Web 代理服务器到一个或多个客户机应用程序服务器上的端点的逻辑连接。多个服务器连接可以添加到一个连接。

过程

1. 在导航菜单中，单击**应用程序** > **连接管理**，然后单击 **Web 应用程序**。



2. 输入连接名称和其他基本连接设置。
3. 输入缺省连接服务器的设置。 您可以添加更多服务器连接。
4. 单击**添加连接**。
5. 可选： 输入可选设置。
6. 可选： 选择或添加 ACL（访问控制表）。
7. 可选： 选择或添加 POP（受保护对象策略）。
8. 可选： 创建受保护对象。
9. 单击**保存**。

连接设置

连接设置包括连接类型和名称、服务器主机信息和可选设置。

基本设置

表 *28.* 基本连接设置

设置	描述
连接名称	连接名称。连接名称确定用于访问该连接所连接的应用程序服务器的 URL 路径。例如，如果连接名为 webapp_1，那么应用程序服务器根的 URL 为 https://*client_Cloud_Identity_Service_address*/webapp_1/。
描述	连接描述。

表 28. 基本连接设置 (续)

设置	描述
类型	连接协议，TCP 或 SSL。
虚拟连接	虚拟连接与虚拟主机进行通信。客户机请求中使用 HTTP 主机头将这些请求定向到所连接服务器的相应位置。 用户可以使用所连接服务器的主机名 (`http://protected-server/resource`) 直接访问资源，而不是使用 WebSEAL 服务器的主机名以及可能修改的资源路径 (`http://webseal/connection/resource`) 进行间接访问。使用所连接服务器的主机名直接访问资源不需要 URL 过滤。
连接服务器	创建新连接时不使用。要为连接设置的服务器地址、路径和端口。单击**添加服务器**以添加服务器连接。有关添加服务器的更多信息，请参阅第 113 页的『添加连接服务器』。

连接策略和规则

表 29. 连接访问策略和规则

设置	描述
访问控制表 (ACL)	通过 ACL 限制对资源的访问。从列表中选择**添加新列表**以创建 ACL，请参阅第 117 页的『创建访问控制表』。
受保护对象策略 (POP)	通过 POP 限制对资源的访问。从列表中选择**添加新策略**以添加 POP，请参阅第 115 页的『创建受保护对象策略』。

连接对象空间

连接对象空间表示连接下方的受保护对象的逻辑路径。例如，目录、文件、程序或位置的路径。您可以将所需数量的受保护对象添加到连接。

表 30. 连接对象空间

设置	描述
对象名称	对象名称。受保护对象必须根据其所表示的对象命名。例如，如果对象表示名为 `page1.jsp` 的页面，且该页面位于结点的根，那么路径对象必须使用名称 `page1.jsp` 进行创建。
ACL	应用于对象的 ACL。
POP	应用于连接的 POP。
子代	子对象。

可选设置

表 31. 可选设置

设置	描述
有状态连接	指定连接支持有状态应用程序。缺省情况下，连接是无状态的。
布尔值规则	允许通过连接在布尔值规则头 (AM_AZN_FAILURE) 中发送来自授权规则的被拒绝请求和失败原因信息。
线程限制	定义工作者线程使用的软硬限制。

表 *31.* 可选设置 *(续)*

设置	描述
HTTP 基本认证头	定义 WebSEAL 逆向代理服务器如何在 HTTP 基本认证 (BA) 头中将客户机身份信息传递到 Web 应用程序服务器。用于处理客户机身份信息的选项。 • **过滤**。缺省选项。当 WebSEAL 认证设置为 BA 头信息时使用此选项。 WebSEAL BA 头用于所有后续 HTTP 事务。对于后端服务器，WebSEAL 始终显示为登录状态。 允许将使用客户机证书的 WebSEAL 认证与此选项一起使用。 如果后端服务器需要实际的客户机身份（来自浏览器），可以使用 CGI 变量 HTTP_IV_USER、HTTP_IV_GROUP 和 HTTP_IV_CREDS。对于脚本和 servlet，使用对应的 Cloud Identity Service 特定 HTTP 头。 – iv-user – iv-groups – iv-creds • **忽略**。不允许将使用 BA 头的 WebSEAL 认证与此选项一起使用。此选项将 BA 头用于原始客户机用户名和密码。 允许将使用客户机证书的 WebSEAL 认证与此选项一起使用。 • **提供**。不允许将使用 BA 头的 WebSEAL 认证与此选项一起使用。此选项将 BA 头用于原始客户机用户名和假密码。 允许将使用客户机证书的 WebSEAL 认证与此选项一起使用。

表 *31.* 可选设置 *(续)*

设置	描述
客户机头	客户机头将特定于 Cloud Identity Service 的客户机用户身份信息插入到主机连接的 HTTP 头中。头类型可以包括以下 HTTP 头类型的任意组合。 • 缺省头。 – **短用户名**。将用户登录名插入到名为 iv-user 的 HTTP 头中，并将其添加到发送到连接主机的所有后端请求。 – **长用户名**。将 Cloud Identity Service 用户专有名称插入到名为 iv-user-l 的 HTTP 头中，并将其添加到发送到连接主机的所有后端请求。 – **组名**。将用户所属组的列表（以逗号分隔）插入到名为 iv-groups 的 HTTP 头中，并将其添加到发送到连接主机的所有后端请求。 – **用户凭证**。将 Base64 编码字符串形式的 Cloud Identity Service 用户凭证插入到名为 iv-creds 的 HTTP 头中。将其添加到发送到连接主机的所有后端请求。 – **插入客户机 IP 地址**。将用户 IP 地址插入到名为 iv-remote-address 的 HTTP 头中，并将其添加到发送到连接主机的所有后端请求。 • 定制头。 – 必须配置并启用定制属性以使定制头的 Cloud Identity Service 设置可用。将所选属性插入到 HTTP 头中。必须输入该头的名称。
HTTP 头编码	指定生成 HTTP 头以发送到连接主机时使用的编码。该编码可防止由于转换为非 UTF-8 代码页而可能发生的任何潜在数据损失。用于编码的可用值。 • **UTF-8 二进制**。未编码的 UTF-8 数据。该设置能够在不损失数据的情况下传输数据，客户无需对数据进行 URI 解码。必须谨慎使用此设置，因为它不包括在 HTTP 规范中。 • **UTF-8 URI 编码**。URI 编码的 UTF-8 数据。所有空格和非 ASCII 字节都编码为 %XY，其中 X 和 Y 是十六进制值 (0-F)。 • **本地代码页二进制**。未编码的本地代码页数据。该方式由 WebSEAL V5.1 之前的版本使用。使用该方式允许从先前版本进行迁移，可在升级后的环境中使用。使用时请务必谨慎，因为使用此方式可能会导致数据损失。 • **本地代码页 URI 编码**。URI 编码的本地代码页数据。不能转换为本地代码页的任何 UTF-8 字符将转换为问号 (?). 使用该选项时请务必谨慎，并且请仅在本地代码页产生所需字符串的环境中使用。
基本认证	指示连接主机也是 WebSEAL 服务器。如果启用，那么将使用专用认证设置来认证服务器之间的连接。 • **WebSEAL 用户名**。Cloud Identity Service WebSEAL 服务器用于向连接主机进行认证的用户标识。 • **WebSEAL 密码**。Cloud Identity Service WebSEAL 服务器用于向连接主机进行认证的密码。

表 31. 可选设置 (续)

设置	描述
相互认证	启用客户机认证以使用证书进行连接。 • **证书**。要使用的证书。
结点 Cookie	通过 Cookie 脚本插入标识。
Cookie 位置	仅当启用**结点 Cookie** 时适用。指定连接主机提供的页面中通过 Cookie 脚本插入标识的位置。 • 无。如果指定了**无**，那么缺省情况下在响应主体开头写入脚本。 • **头**。为符合 HTML 4.01，在 <head> </head> 标记之间插入脚本。 • **尾部**。将脚本追加到（而不是添加为前缀）从后端服务器返回的 HTML 页面。 • **尾部焦点处**。在脚本中使用 onfocus 事件处理程序以确保在多连接/多浏览器窗口场景中使用正确的连接 Cookie。 • **XHTML 1.0**。在解释该文档的浏览器上插入符合 XHTML 1.0（和 HTML 4.01）的 JavaScript 块。
Cookie 处理	• **脚本 Cookie**。在 Cookie 中提供连接标识以处理脚本生成的服务器相对 URL。 • **保留 Cookie 路径**。通过在重新编写的 Cookie 名称中包含每个 Cookie 路径，确保连接主机为 Cookie 设置唯一的 Set-Cookie 头名称属性。 • **保留 Cookie 名称**。确保连接主机设置的 Set-Cookie 头不会被 Cloud Identity Service 重写以在 Cookie 名称中包含连接名称。
透明路径结点	非虚拟选项。指定连接是否使用透明路径。假设连接主机上的所有内容都是从与 */connection_name* 匹配的上下文根提供的，而不是使用 */connection_name* 向所有过滤的 URL 添加前缀。透明路径消除了 Cloud Identity Service 过滤服务器相对 URL 的需要。

基本连接设置：

表 32. 基本连接设置

设置	描述
连接名称	连接名称。连接名称确定用于访问该连接所连接的应用程序服务器的 URL 路径。例如，如果连接名为 webapp_1，那么应用程序服务器根的 URL 为 https://*client_Cloud_Identity_Service_address*/webapp_1/。
描述	连接描述。
类型	连接协议，TCP 或 SSL。

表 32. 基本连接设置 (续)

设置	描述
虚拟连接	虚拟连接与虚拟主机进行通信。客户机请求中使用 HTTP 主机头将这些请求定向到所连接服务器的相应位置。 用户可以使用所连接服务器的主机名 (`http://protected-server/resource`) 直接访问资源，而不是使用 WebSEAL 服务器的主机名以及可能修改的资源路径 (`http://webseal/connection/resource`) 进行间接访问。使用所连接服务器的主机名直接访问资源不需要 URL 过滤。
连接服务器	创建新连接时不使用。要为连接设置的服务器地址、路径和端口。单击**添加服务器**以添加服务器连接。有关添加服务器的更多信息，请参阅第 113 页的『添加连接服务器』。

缺省连接服务器设置：

表 33. 连接服务器设置

设置	描述
位置	构成连接的端点的主机名或 IP 地址。
端口	用于连接到主机系统的端口。缺省为缺省 HTTPS 端口 443。仅当需要建立与不同端口的连接时才需要指定此值。
专有名称	建立与应用程序服务器的连接时提交给 Cloud Identity Service 的证书 DN。该字段可以用于增强安全性，因为其功能是允许 Cloud Identity Service 先验证服务器的认证身份，然后再建立与该服务器的连接。
虚拟主机	随着 Web 请求传输到应用程序服务器的 HTTP 主机头。对于符合 HTTP V1.1 的 Web 服务器，需要该头以将请求路由到相应的虚拟主机配置。 **注：**仅当虚拟主机名不同于**位置**字段中指定的值时才为必需。
查询脚本路径	这是查询内容工具的位置，该工具可以选择性安装在客户机应用程序服务器上。查询内容工具允许 Cloud Identity Service 检查其 Web 空间，并通过"连接对象空间"面板中显示的路径对象层次结构表示其 Web 空间。如果未指定，那么此值缺省为 `/cgi-bin/query_contents`。
区分大小写的 URL	控制在对发送到连接主机的请求执行授权检查时，Cloud Identity Service 是否不区分 URL 的大小写。成功 ACL 检查之后，在向服务器发送请求时将复原 URL 的原始大小写。

表 *33.* 连接服务器设置 *(续)*

设置	描述
Win32 支持	控制 Cloud Identity Service 是否对旧 Windows 文件路径执行授权检查。Cloud Identity Service 基于 URL 中指定的文件路径对发送到连接主机的客户机请求执行安全性检查。 此安全性检查会作出一定的妥协，因为 Win32 文件系统允许使用两种不同的方法访问长文件名。第一种方法认知完整文件名，例如，`abcdefghijkl.txt`。第二种方法识别旧 8.3 文件名格式（例如，`abcdef~1.txt`）以便兼容较早版本。 在 Windows 环境中添加主机连接时，请务必将访问控制仅限制于一个对象表示。该限制也防止发生绕过安全性机制的后门访问的可能性。因此，Win32 支持选项提供了一些保护措施。 • 防止使用 8.3 文件名格式。用户无法使用短格式 (8.3) 文件名来避免长文件名上的显式 ACL。输入任何短格式文件名时，Cloud Identity Service 将返回"403 被禁止"错误。 • 不允许目录和文件名以句点结尾。如果文件或目录包含结尾句点，将返回"403 被禁止"错误。 • 通过设置**区分大小写 URL** 选项强制实施不区分大小写。

可选连接设置：

表 *34.* 可选设置

设置	描述
有状态连接	指定连接支持有状态应用程序。缺省情况下，连接是无状态的。
布尔值规则	允许通过连接在布尔值规则头 (AM_AZN_FAILURE) 中发送来自授权规则的被拒绝请求和失败原因信息。
线程限制	定义工作者线程使用的软硬限制。

表 *34.* 可选设置 *(续)*

设置	描述
HTTP 基本认证头	定义 WebSEAL 逆向代理服务器如何在 HTTP 基本认证 (BA) 头中将客户机身份信息传递到 Web 应用程序服务器。用于处理客户机身份信息的选项。 • **过滤**。缺省选项。当 WebSEAL 认证设置为 BA 头信息时使用此选项。 WebSEAL BA 头用于所有后续 HTTP 事务。对于后端服务器，WebSEAL 始终显示为登录状态。 允许将使用客户机证书的 WebSEAL 认证与此选项一起使用。 如果后端服务器需要实际的客户机身份（来自浏览器），可以使用 CGI 变量 HTTP_IV_USER、HTTP_IV_GROUP 和 HTTP_IV_CREDS。对于脚本和 servlet，使用对应的 Cloud Identity Service 特定 HTTP 头。 – iv-user – iv-groups – iv-creds • **忽略**。不允许将使用 BA 头的 WebSEAL 认证与此选项一起使用。此选项将 BA 头用于原始客户机用户名和密码。 允许将使用客户机证书的 WebSEAL 认证与此选项一起使用。 • **提供**。不允许将使用 BA 头的 WebSEAL 认证与此选项一起使用。此选项将 BA 头用于原始客户机用户名和假密码。 允许将使用客户机证书的 WebSEAL 认证与此选项一起使用。

表 *34.* 可选设置 *(续)*

设置	描述
客户机头	客户机头将特定于 Cloud Identity Service 的客户机用户身份信息插入到主机连接的 HTTP 头中。头类型可以包括以下 HTTP 头类型的任意组合。 • 缺省头。 – **短用户名**。将用户登录名插入到名为 iv-user 的 HTTP 头中，并将其添加到发送到连接主机的所有后端请求。 – **长用户名**。将 Cloud Identity Service 用户专有名称插入到名为 iv-user-l 的 HTTP 头中，并将其添加到发送到连接主机的所有后端请求。 – **组名**。将用户所属组的列表（以逗号分隔）插入到名为 iv-groups 的 HTTP 头中，并将其添加到发送到连接主机的所有后端请求。 – **用户凭证**。将 Base64 编码字符串形式的 Cloud Identity Service 用户凭证插入到名为 iv-creds 的 HTTP 头中。将其添加到发送到连接主机的所有后端请求。 – **插入客户机 IP 地址**。将用户 IP 地址插入到名为 iv-remote-address 的 HTTP 头中，并将其添加到发送到连接主机的所有后端请求。 • 定制头。 – 必须配置并启用定制属性以使定制头的 Cloud Identity Service 设置可用。将所选属性插入到 HTTP 头中。必须输入该头的名称。
HTTP 头编码	指定生成 HTTP 头以发送到连接主机时使用的编码。该编码可防止由于转换为非 UTF-8 代码页而可能发生的任何潜在数据损失。用于编码的可用值。 • **UTF-8 二进制**。未编码的 UTF-8 数据。该设置能够在不损失数据的情况下传输数据，客户无需对数据进行 URI 解码。必须谨慎使用此设置，因为它不包括在 HTTP 规范中。 • **UTF-8 URI 编码**。URI 编码的 UTF-8 数据。所有空格和非 ASCII 字节都编码为 %XY，其中 X 和 Y 是十六进制值 (0-F)。 • **本地代码页二进制**。未编码的本地代码页数据。该方式由 WebSEAL V5.1 之前的版本使用。使用该方式允许从先前版本进行迁移，可在升级后的环境中使用。使用时请务必谨慎，因为使用此方式可能会导致数据损失。 • **本地代码页 URI 编码**。URI 编码的本地代码页数据。不能转换为本地代码页的任何 UTF-8 字符将转换为问号 (?). 使用该选项时请务必谨慎，并且请仅在本地代码页产生所需字符串的环境中使用。
基本认证	指示连接主机也是 WebSEAL 服务器。如果启用，那么将使用专用认证设置来认证服务器之间的连接。 • **WebSEAL 用户名**。Cloud Identity Service WebSEAL 服务器用于向连接主机进行认证的用户标识。 • **WebSEAL 密码**。Cloud Identity Service WebSEAL 服务器用于向连接主机进行认证的密码。

表 *34.* 可选设置 *(续)*

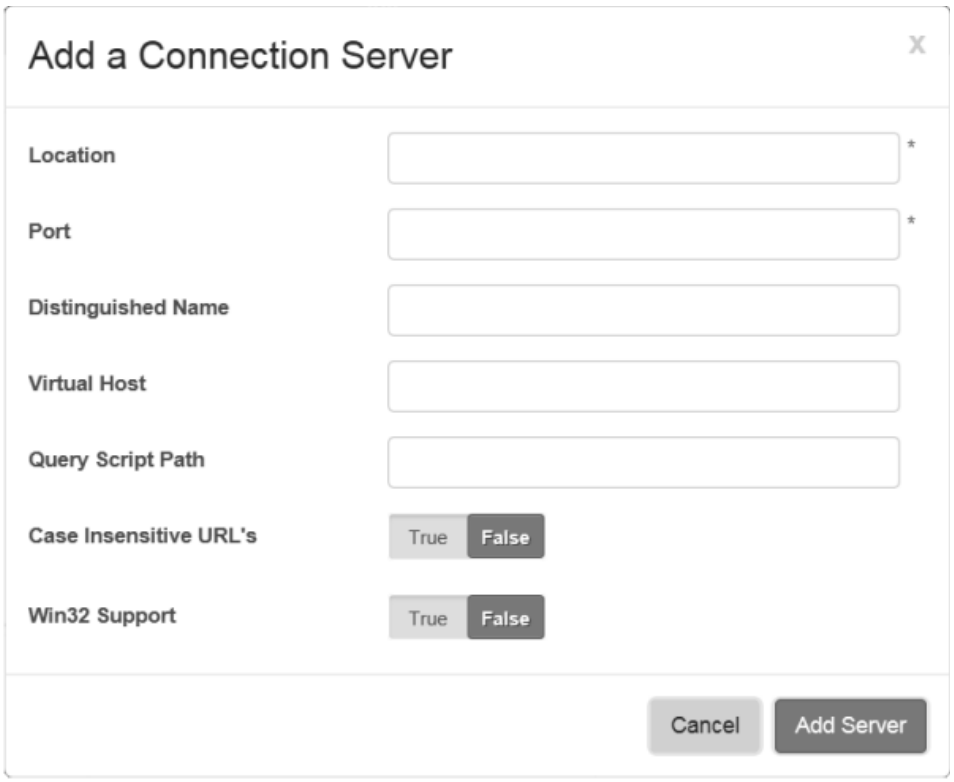
设置	描述
相互认证	启用客户机认证以使用证书进行连接。 • **证书**。要使用的证书。
结点 Cookie	通过 Cookie 脚本插入标识。
Cookie 位置	仅当启用**结点 Cookie** 时适用。指定连接主机提供的页面中通过 Cookie 脚本插入标识的位置。 • 无。如果指定了**无**，那么缺省情况下在响应主体开头写入脚本。 • **头**。为符合 HTML 4.01，在 `<head> </head>` 标记之间插入脚本。 • **尾部**。将脚本追加到（而不是添加为前缀）从后端服务器返回的 HTML 页面。 • **尾部焦点处**。在脚本中使用 onfocus 事件处理程序以确保在多连接/多浏览器窗口场景中使用正确的连接 Cookie。 • **XHTML 1.0**。在解释该文档的浏览器上插入符合 XHTML 1.0（和 HTML 4.01）的 JavaScript 块。
Cookie 处理	• **脚本 Cookie**。在 Cookie 中提供连接标识以处理脚本生成的服务器相对 URL。 • **保留 Cookie 路径**。通过在重新编写的 Cookie 名称中包含每个 Cookie 路径，确保连接主机为 Cookie 设置唯一的 Set-Cookie 头名称属性。 • **保留 Cookie 名称**。确保连接主机设置的 Set-Cookie 头不会被 Cloud Identity Service 重写以在 Cookie 名称中包含连接名称。
透明路径结点	非虚拟选项。指定连接是否使用透明路径。假设连接主机上的所有内容都是从与 */connection_name* 匹配的上下文根提供的，而不是使用 */connection_name* 向所有过滤的 URL 添加前缀。透明路径消除了 Cloud Identity Service 过滤服务器相对 URL 的需要。

添加连接服务器

要为连接设置的连接服务器地址、路径和端口。

过程

1. 如果想要为其创建连接服务器的连接尚未打开，搜索并选择该连接。
2. 从**连接服务器**中，单击**添加新服务器**。



3. 输入连接服务器设置。

表 *35.* 连接服务器设置

设置	描述
位置	构成连接的端点的主机名或 IP 地址。
端口	用于连接到主机系统的端口。缺省为缺省 HTTPS 端口 443。仅当需要建立与不同端口的连接时才需要指定此值。
专有名称	建立与应用程序服务器的连接时提交给 Cloud Identity Service 的证书 DN。该字段可以用于增强安全性，因为其功能是允许 Cloud Identity Service 先验证服务器的认证身份，然后再建立与该服务器的连接。
虚拟主机	随着 Web 请求传输到应用程序服务器的 HTTP 主机头。对于符合 HTTP V1.1 的 Web 服务器，需要该头以将请求路由到相应的虚拟主机配置。 **注：**仅当虚拟主机名不同于**位置**字段中指定的值时才为必需。
查询脚本路径	这是查询内容工具的位置，该工具可以选择性安装在客户机应用程序服务器上。查询内容工具允许 Cloud Identity Service 检查其 Web 空间，并通过"连接对象空间"面板中显示的路径对象层次结构表示其 Web 空间。如果未指定，那么此值缺省为 `/cgi-bin/query_contents`。
区分大小写的 URL	控制在对发送到连接主机的请求执行授权检查时，Cloud Identity Service 是否不区分 URL 的大小写。成功 ACL 检查之后，在向服务器发送请求时将复原 URL 的原始大小写。

表 35. 连接服务器设置（续）

设置	描述
Win32 支持	控制 Cloud Identity Service 是否对旧 Windows 文件路径执行授权检查。Cloud Identity Service 基于 URL 中指定的文件路径对发送到连接主机的客户机请求执行安全性检查。 此安全性检查会作出一定的妥协，因为 Win32 文件系统允许使用两种不同的方法访问长文件名。第一种方法认知完整文件名，例如，abcdefghijkl.txt。第二种方法识别旧 8.3 文件名格式（例如，abcdef~1.txt）以便兼容较早版本。 在 Windows 环境中添加主机连接时，请务必将访问控制仅限制于一个对象表示。该限制也防止发生绕过安全性机制的后门访问的可能性。因此，Win32 支持选项提供了一些保护措施。 • 防止使用 8.3 文件名格式。用户无法使用短格式 (8.3) 文件名来避免长文件名上的显式 ACL。输入任何短格式文件名时，Cloud Identity Service 将返回"403 被禁止"错误。 • 不允许目录和文件名以句点结尾。如果文件或目录包含结尾句点，将返回"403 被禁止"错误。 • 通过设置**区分大小写 URL** 选项强制实施不区分大小写。

4. 单击**添加服务器**。

创建受保护对象策略

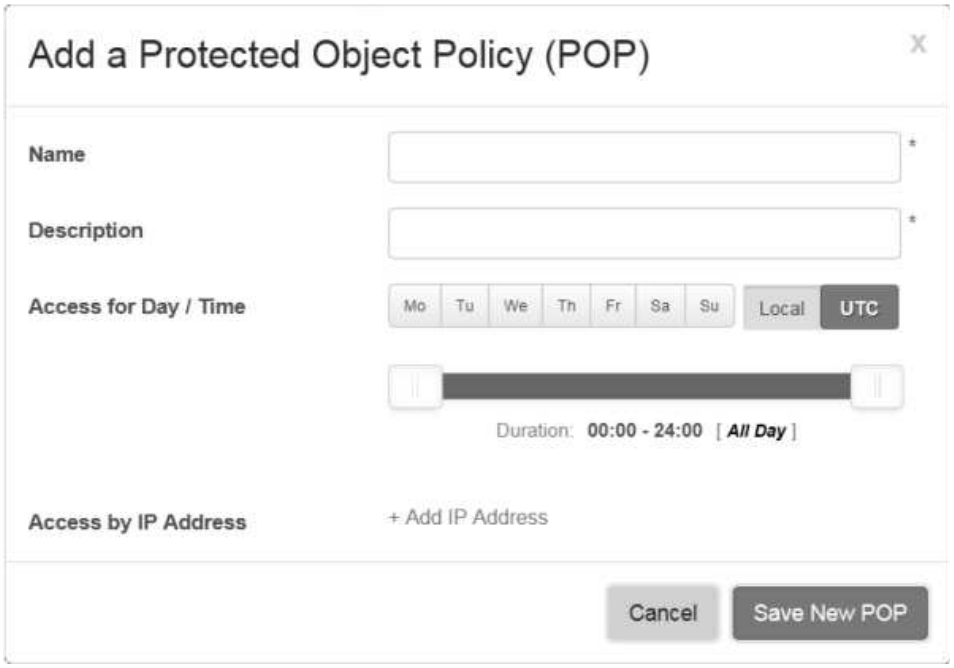
使用受保护对象策略 (POP) 来限定访问需求。使用一天中的具体时间和网络位置来限定访问需求。

关于此任务

策略仅在附加到连接后生效。

过程

1. 如果想要为其创建 POP 的连接尚未打开，搜索并选择该连接。
2. 从**受保护对象策略 (POP)** 下拉列表中选择**添加新策略**。



3. 输入名称和描述。
4. 输入其余 POP 设置。

设置	描述	
日期/时间访问	指定允许访问的日期和一天中的具体时间。时间可以服务主机环境的本地时间或全球标准时间表示。选择要允许访问的日期。使用滑动条将访问权限制于所选时间范围。	
按 IP 地址访问	受保护对象策略 (POP) 的 IP 认证设置。按 IP 地址和认证级别限定访问。可以允许或阻止来自指定 IP 地址的用户访问资源。单击**添加 IP 地址**以添加 IP 地址约束。	
	任何其他网络	用作与 POP 中没有指定的任何网络匹配的网络范围。使用此方法来创建一个缺省条目，该条目可以拒绝所有不匹配的 IP 地址，或者允许符合认证级别需求的任何人访问。
	IP 地址	网络值为 TCP/IP 地址。网络和网络掩码选项必须以相同的 IP 版本指定。
	网络掩码	网络掩码值为 TCP/IP 地址。网络和网络掩码选项必须以相同的 IP 版本指定。 网络掩码中的数字 0 充当通配符，表示该子网的所有 IP 地址。例如，网络掩码为 255.255.255.0 的 IP 地址 9.1.2.3 适用于 9.1.2.[0-255] 范围中的所有 IP 地址。
	禁止	禁止访问。
	认证级别	这是特定于应用程序的整数值，用于定义递升式认证级别。支持 1000 以下的所有整数值。0 是最低级别。认证级别在为贵组织进行 Cloud Identity Service 初始配置期间定义。
多因子认证		指定是否启用多因子认证。

5. 单击**保存新 POP**。

示例

POP 的缺省设置为在任意认证级别允许所有网络访问：

- **认证级别**为 0

在以下示例中，起源于一组 IP 地址的客户机访问被认为是安全的。另一个网络范围被认为较不安全，需要更高级别的认证。来自任何其他网络范围的访问必须被拒绝。必须为 POP 创建两个 IP 认证条目，一个用于安全 IP 地址范围，一个用于不安全 IP 地址。

第一个范围适用于以 IP 地址 9.180.168.* 访问 Web 资源的任何客户机。

- **IP 地址**为 9.180.168.0
- **网络掩码**为 255.255.255.0
- **认证级别**为 0

第二个范围使用**任何其他网络**和**禁止**选项来排除 IP 地址。源 IP 地址与 9.180.168.* 范围不匹配的 Web 客户机缺省为此范围并且将被拒绝。只有 IP 地址位于范围 9.180.168.* 中的 Web 客户机能够访问该 POP 保护的 Web 资源。该示例可以应用于企业防火墙使用的网络地址转换 (NAT) 范围。

- 启用**任何其他网络**。
- **禁止**为 true。

该策略的"受保护对象策略"页面显示两个 IP 范围。

创建访问控制表

访问控制表 (ACL) 提供用户、组和服务以及一组许可权之间的映射。您可以创建新 ACL 以授予用户、组成员和服务成员对受保护资源的访问权。

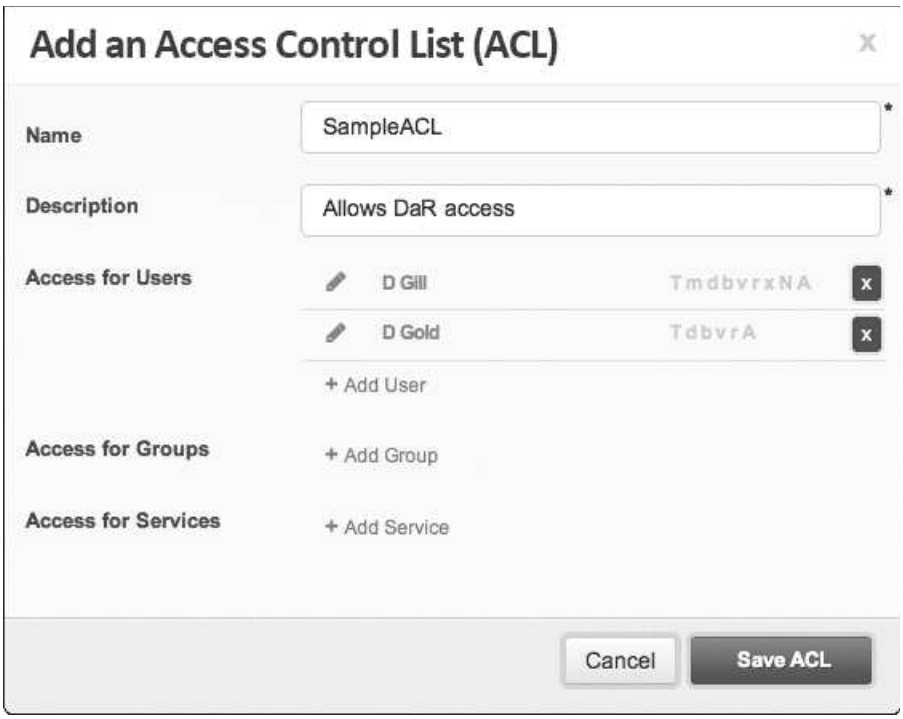
关于此任务

ACL 由一组 ACL 条目组成。每个 ACL 条目使用一列许可权指定用户、组和服务，这些许可权将授予这些用户、组和服务。ACL 仅在添加到连接后生效。

要点：缺省 ACL 不得修改或删除。

过程

1. 如果想要为其创建 ACL 的连接尚未打开，搜索并选择该连接。
2. 从**访问控制表 (ACL)** 下拉列表中选择**添加新列表**。



3. 输入名称和描述。
4. 输入其余 ACL 设置。

设置	描述
用户访问权	单个用户的访问权。将为每个添加的用户授予资源访问权。单击**添加用户**以添加用户。要搜索并选择用户，请输入用户的名字、姓氏、用户名或电子邮件地址的前 3 个字符。选择每个条目的许可权。您可以将以下许可权用于 Cloud Identity Service 用户、组和服务： • **r**。读。允许用户查看对象。 • **x**。执行。允许用户从对象运行文件或脚本。 • **T**。遍历。允许用户访问层次结构中级别较低的对象。 **注：**所有其他许可权适用于管理功能，不适用于 Cloud Identity Service 用户、组和服务。
组访问权	组成员访问权。将为所添加组的每个成员授予资源访问权。单击**添加组**以添加组。要搜索并选择组，请至少输入组名的前 3 个字符。选择每个条目的许可权。
服务访问权	服务成员访问权。将为所添加服务的每个成员授予资源访问权。单击**添加服务**以添加服务。要搜索并选择服务，请至少输入服务名称的前 3 个字符。选择每个条目的许可权。
未经认证的访问权	指定未经认证用户的访问许可权。未经认证用户可能需要许可权。例如，可能想要通过设置遍历许可权，允许未经认证的用户访问层次结构中较低级别的资源。要设置许可权，单击**允许**，然后选择未经认证用户的许可权。

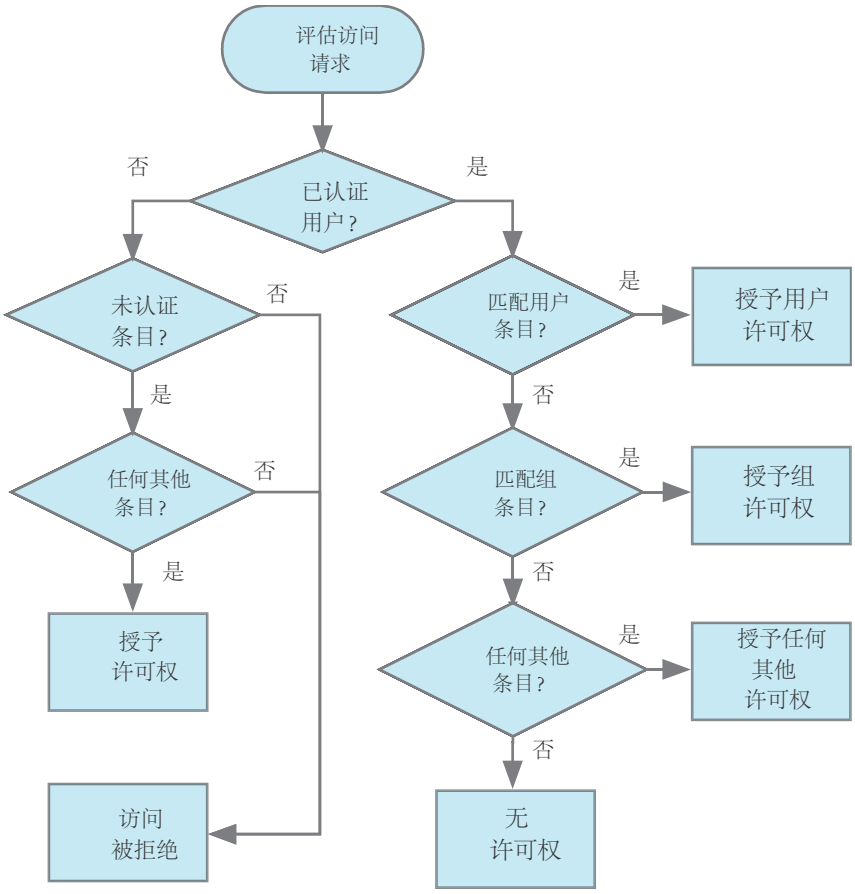
设置	描述
任何其他访问权	指定用户、组或服务访问权中未指定的所有其他已认证用户的访问许可权。所有已认证用户可能需要许可权。例如，可能想要通过设置遍历许可权，允许所有已认证用户访问层次结构中较低级别的资源。要设置许可权，单击**允许**，然后选择所有其他已认证用户的许可权。

5. 单击**保存新 ACL**。

访问控制表评估

当用户尝试访问受保护资源时，将评估适用于该受保护资源的访问控制表（ACL）以确定是否授予访问权。

评估的第一个阶段是确定请求访问的用户是（已认证）否（未认证）有活动登录会话。



当已认证用户尝试访问受保护资源时，将按照以下顺序执行评估。

- 将用户标识与用户 ACL 条目进行匹配。找到用户条目匹配项时评估停止。授予的许可权为匹配用户条目中的许可权。
- 如果没有匹配的用户条目，那么确定用户所属的组，并将这些组与 ACL 中的组条目匹配。找到任何组匹配项时评估停止。如果匹配了多个组条目，那么产生的许可权为匹配条目中最宽松的许可权。
- 如果没有匹配的用户或组条目，那么授予"任何其他"条目（如果存在）的许可权。

- 如果没有匹配的用户或组条目，也没有"任何其他"条目，那么该用户无许可权。

当未认证用户尝试访问受保护资源时，将按照以下方法执行评估。

- 如果 ACL 不包含"未认证"条目，那么拒绝访问。
- 如果 ACL 不包含"任何其他"条目，那么拒绝访问。
- 如果 ACL 包含"未认证"条目和"任何其他"条目，那么授予的许可权是同时授予"未认证"和"任何其他"条目的许可权。授予未认证用户的许可权不会超过"任何其他"条目中授予的许可权。

创建受保护对象

受保护对象表示通过连接可以访问的逻辑路径元素。

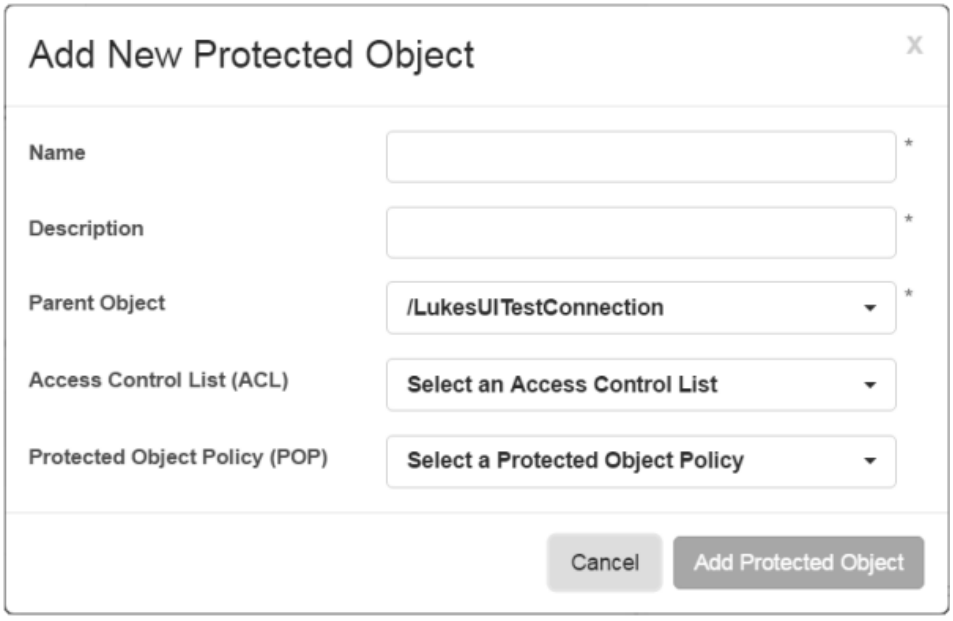
关于此任务

连接对象空间表示来自连接的受保护对象的逻辑路径。例如，目录、文件、程序或位置的路径。您可以将所需数量的受保护对象添加到连接。您可以向下从连接选择任何现有对象，从而创建所需深度和复杂度的层次结构。

您可以将访问控制表 (ACL) 和受保护对象策略 (POP) 附加到受保护对象。当策略附加到对象时，策略将应用于该对象和所有子对象。如果其他策略是在较低级别附加的，那么继承的策略将被覆盖。

过程

1. 如果想要为其添加受保护对象的连接尚未打开，搜索并选择该连接。
2. 从**连接对象空间**中单击**添加新受保护对象**。



3. 输入名称和描述。

   受保护对象必须根据其所表示的对象命名。例如，如果对象表示名为 `page1.jsp` 的页面，且该页面位于结点的根，那么路径对象必须使用名称 `page1.jsp` 进行创建。
4. 输入其余对象设置。

设置	描述
父对象	受保护对象的父对象。父级对象可以是连接对象，或者连接之下的任何现有受保护对象。
访问控制表 (ACL)	要附加到对象的 ACL。
受保护对象策略 (POP)	要附加到对象的 POP。

5. 单击**添加受保护对象**。

管理启动板服务

用户可通过 自助服务 门户网站中的启动板使用 Web 连接及联合合作伙伴 Web 连接。用户必须添加至相应服务才能通过启动板访问 Web 连接。

向启动板服务添加用户

用户可通过启动板（其 自助服务 门户网站中的单个位置）访问 Web 应用程序。

关于此任务

对于每个 Web 连接及所创建的联合合作伙伴连接，将创建对应服务。系统对该服务指定与连接相同的名称，对于联合 Web 应用程序，系统指定与连接别名相同的名称。为使用户可从启动板使用该 Web 应用程序，必须将该用户添加至相应服务。

注： 非虚拟连接名称以正斜杠开头，例如，`/my_connection_1`。非虚拟连接的服务名称也以正斜杠开头。

注： 如果联合合作伙伴连接别名已更改，那么将创建带有新别名的新服务。该连接先前使用的服务中的成员将迁移至新服务，旧服务将被移除。

可通过手动管理服务或使用策略动态管理服务来向服务添加用户。

过程

向启动板服务添加用户。

- 通过手动管理服务来添加用户。
- 通过动态管理服务来添加用户。

管理联合 SSO Web 访问

联合 SSO（单点登录）Web 访问管理包括管理与第三方应用程序的网络连接。联合单点登录 (SSO) 使具有 Cloud Identity Service 帐户的用户能够使用现有身份访问其他第三方应用程序服务。

联合 SSO 概述

联合单点登录 (SSO) 使具有 Cloud Identity Service 帐户的用户能够无缝访问一个或多个合作伙伴组织提供的服务，而不必在该合作伙伴站点进行单独登录。

当用户单击联合登录 URL 时，Cloud Identity Service 构造一个可供合作伙伴组织验证（并因此信任）的数字签名令牌。该令牌由用户浏览器提交到在其中创建会话的合作伙伴单点登录 URL。

联合合作伙伴关系涉及两个不同的角色，分别用于涉及的双方：身份提供者 (IdP) 和服务提供者 (SP)。身份提供者以数字令牌形式提供可信身份。服务提供者验证该数字令牌，为用户创建会话，并允许该用户访问其应用程序环境。Cloud Identity Service 是身份提供者，合作伙伴是服务提供者。

单个 Cloud Identity Service 环境可以支持多个联合合作伙伴。对于每个联合登录 URL，必须定义用于描述合作伙伴联合特性的连接详细信息。每个连接都必须有个人证书和签署者证书提供的公用和专用密钥对。

对于支持使用 SAML 2.0 的联合单点登录的一些热门合作伙伴应用程序服务，Cloud Identity Portal 提供了预先配置的模板。如果您要为其创建连接的合作伙伴不存在模板，那么可以使用定制配置。

密钥管理

每个连接都必须有公用和专用密钥对。这些密钥由个人证书和签署者证书提供。

签署者证书表示与某个个人证书关联的证书和公用密钥。签署者证书的目的是验证个人证书。专用密钥的所有者能够建立与合作伙伴应用程序服务的连接。签署者证书显式信任与关联个人证书所有者建立的连接或者由该所有者建立的连接。

Cloud Identity Portal 中只能启用一个个人证书。您不必显式选择要在定义连接时使用的个人证书。缺省情况下，启用的个人证书将用于您创建的所有连接。对于您创建的每个连接，必须选择相应的签署者证书。签署者证书通常由服务提供者提供。您可以导入签署者证书。您也可以针对低敏感度、非生产和其他快速使用需求创建自签名证书和密钥。

连接管理

您可以创建任意数量的连接来支持任意数量的联合合作伙伴。针对一些热门合作伙伴应用程序服务，提供了一些预配置的模板。您可以使用这些模板来创建与联合合作伙伴的连接。模板会预先配置尽可能多的合作伙伴连接详细信息。如果某合作伙伴不存在模板，或者您想要创建与内部应用程序或服务的连接，可以使用通用模板来创建连接。成功创建的每个连接都会生成登录 URL。该 URL 用于启动单点登录合作伙伴。

某些提供者允许用户首次成功登录尝试时在服务提供者端创建用户记录。该用户记录创建称为自动供应。

管理联合合作伙伴连接

管理合作伙伴连接

搜索联合 Web 应用程序连接

您可以搜索与联合 Web 应用程序的网络连接，以查看、修改或移除连接。

过程

1. 在导航窗格中，单击**应用程序** > **连接管理**，然后单击**联合应用程序**。
2. 在**搜索**字段中，至少输入连接的前 3 个字符。 字段标签将更改为**正在搜索**。

   此时将列出与搜索条件匹配的连接。选择要修改或查看的连接。

向联合合作伙伴添加连接

您可以创建任意数量的连接来支持任意数量的联合合作伙伴。针对一些热门合作伙伴应用程序服务，提供了一些预配置的模板。

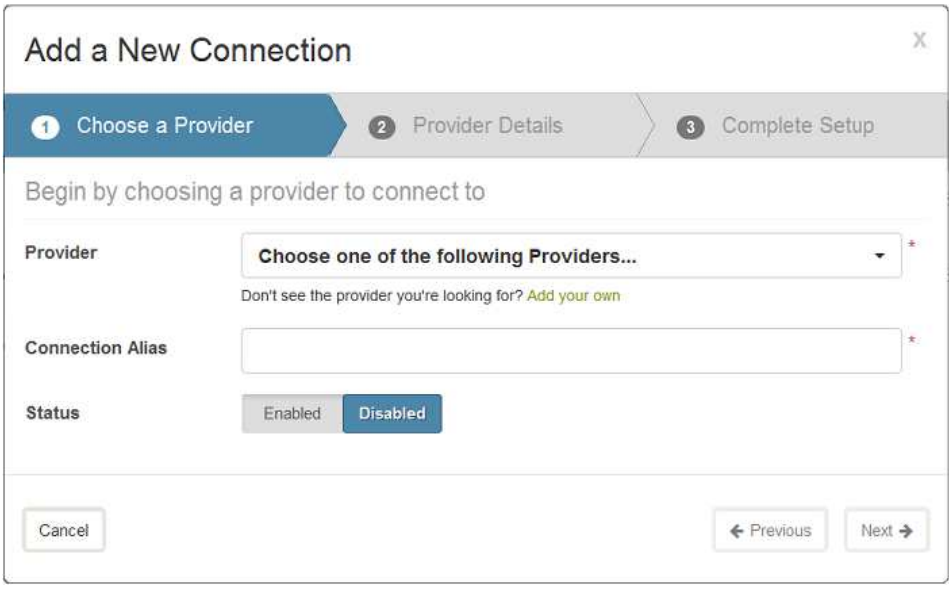
关于此任务

Cloud Identity Portal 提供了一些模板以用于为联合合作伙伴添加连接。您可以使用通用模板添加指向其他提供者的连接。通用模板还可以用于为内部应用程序创建连接。

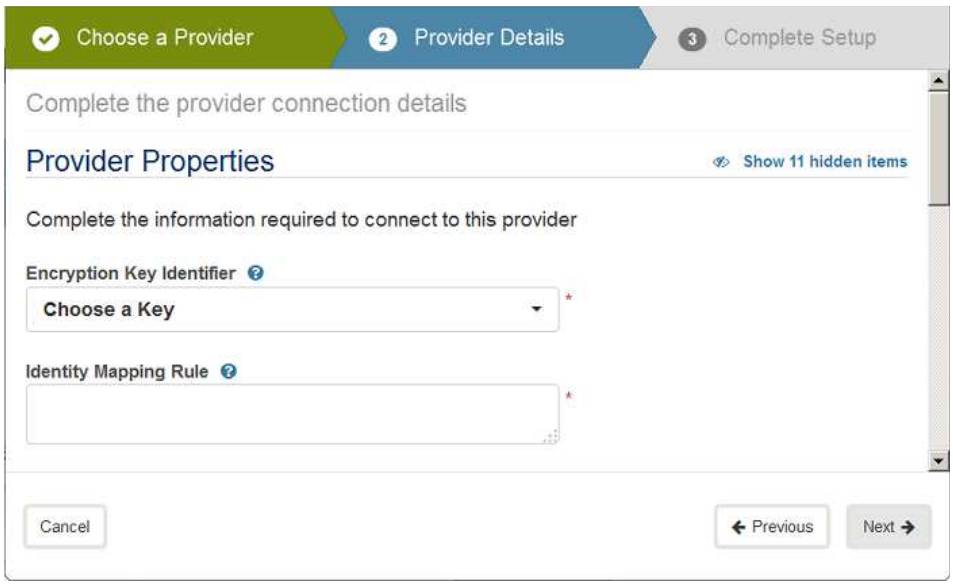
某些提供者允许用户首次成功登录尝试时在服务提供者端创建用户记录。自动供应模板可供允许创建用户记录的合作伙伴使用。要自动供应用户记录，服务提供者通常需要附加信息。此附加信息通过将 Cloud Identity Service LDAP 属性映射到对应合作伙伴属性来提供。

过程

1. 在导航菜单中，单击**应用程序** > **连接管理**，然后单击**联合应用程序** > **添加新连接**。



2. 从**提供者**菜单中选择提供者名称。
   - 要基于合作伙伴模板创建连接，请从**提供者**菜单中选择提供者。在可能的情况下，可通过图标识别提供者。如果没有可用的提供者图标，使用通用图表。
   - 要为没有模板的合作伙伴或内部应用程序创建连接，请单击**添加自有项**或从**提供者**菜单中选择**通用 SAML2.0 服务提供者**。
3. 在**连接别名**字段中输入连接别名。
4. 单击**下一步**。



5. 输入提供者特性详细信息。

   注：由于验证连接是在服务器端完成的，因此，无法指示所有必填字段。

   注：对于基于模板的连接，为您输入了一些详细信息。预先输入的缺省字段在连接设置期间处于隐藏状态。如果您想要查看或编辑缺省字段，单击**显示隐藏项**。您可以编辑缺省字段的值或设置。更改缺省字段的设置或值可能导致连接无效。

   要编辑缺省字段，请单击**启用缺省字段编辑**。此时将显示一个警告。单击**启用字段**以编辑缺省字段。

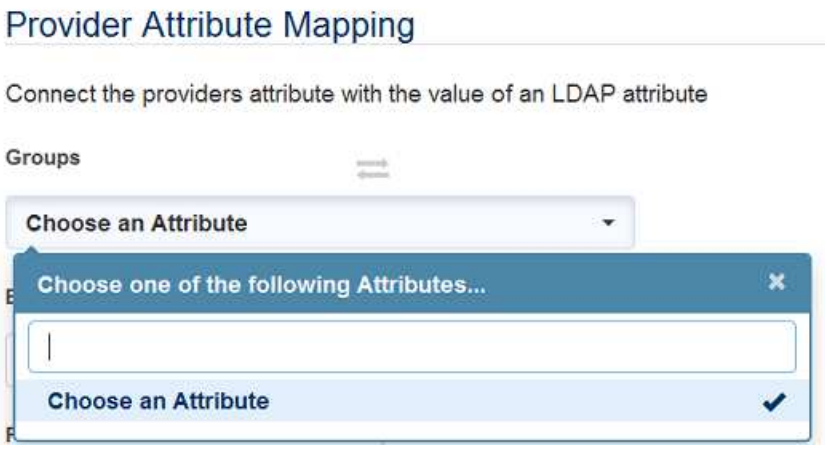
   要点：对于 Clarizen 连接，根据您使用的 Clarizen 环境，"断言使用者服务 URL" 可能具有下列其中一个值：

   - EU 环境。`https://eu1.clarizen.com/Clarizen/Pages/Integrations/SAML/SamlResponse.aspx`
   - SV 环境。`https://app2.clarizen.com/Clarizen/Pages/Integrations/SAML/SamlResponse.aspx`
   - TB 环境。`https://app.clarizentb.com/Clarizen/Pages/Integrations/SAML/SamlResponse.aspx`

   模板缺省值是 `https://app2.clarizen.com/Clarizen/Pages/Integrations/SAML/SamlResponse.aspx`。如果您需要更改值，请使用**启用缺省字段编辑**。

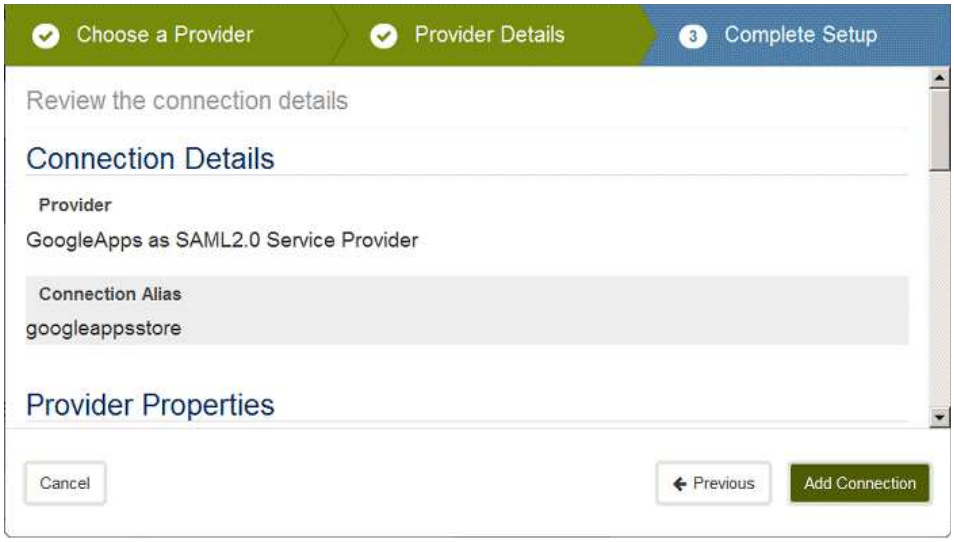
6. 对于需要属性映射的提供者，输入提供者属性映射。

   某些提供者需要将一些属性映射到 Cloud Identity Service LDAP 属性。映射的属性将装入到 SAML 断言中并由服务提供者用于识别用户。LDAP 属性中存储的值将映射到提供者变量。



7. 可选： 输入并映射到其他属性。 如果提供者接受其他属性映射，那么您可以添加其他属性。
   a. 在**添加属性映射**字段中输入合作伙伴属性的名称，然后单击**添加属性**。

   b. 从**选择属性**字段中选择要映射到的 LDAP 属性。
8. 单击**下一步**。



9. 单击**添加连接**。

联合合作伙伴连接设置：

联合合作伙伴的连接设置包括连接别名、状态、登录 URL、属性映射特性和服务提供者特性。

表 *36.* 提供者信息

设置	描述
提供者	服务提供者。
连接别名	连接别名。
状态	连接状态。如果连接被禁用，那么连接将失败。
登录 URL	用于启动单点登录合作伙伴的 URL。

表 *37.* 属性映射

设置	描述
提供者属性映射	所需提供者属性映射。某些提供者需要将一些属性映射到 Cloud Identity Service LDAP 属性。所需属性装入到 SAML 断言并由服务提供者用于识别用户。
添加属性映射	可选属性映射。

表 *38.* 提供者属性

设置	描述
断言使用者服务 URL	接收断言的服务提供者的端点。
公司名称	服务提供者公司名称。
启用	指定是否启用合作伙伴。如果不启用合作伙伴，那么连接将失败。
加密断言	指定是否加密断言。
加密断言属性	指定是否加密断言属性。
加密密钥标识	加密密钥的名称。
加密名称标识	指定是否必须对名称标识加密。
身份映射规则	可选的 JavaScript 内部映射规则，用于修改构建 SAML 2.0 令牌所需的信息。必须提供 JavaScript 映射规则的内容。
身份映射规则参考	可选的 JavaScript 内部映射规则，用于修改构建 SAML 2.0 令牌所需的信息。必须提供映射规则 REST API 管理的 JavaScript 映射规则的相对 URI，例如，`/iam/access/v8/mapping-rules/mapping_rule_id`。当指定了 **`identityMappingRuleReference`** 时，它将优先于 **`identityMappingRule`**。
提供者标识	用于标识服务提供者的唯一标识。
会话终止时间期限	服务提供者必须废弃针对主体建立的安全上下文的秒数。
签署断言	指定是否签署断言。
签名验证密钥标识	签名验证密钥的名称。
签署认证响应	指定是否签署认证响应。
验证认证请求	指定是否验证认证请求的数字签名。

快速连接合作伙伴端配置

单点登录 (SSO) 快速连接合作伙伴端配置。

对于 Cloud Identity Service 中配置的合作伙伴，需要将快速连接模板生成的登录 URL 提供给用户。登录 URL 使用户能够通过 SAML SSO 使用链接（通常从 Cloud Identity Service 提供给用户）来登录合作伙伴站点。在合作伙伴端配置中，管理员必须使用

Cloud Identity Service 登录 URL 和 SAML 断言验证证书为服务提供者 (SP) 合作伙伴配置 SAML 2.0 SSO 设置。在合作伙伴端配置中，某个过程或方法用于在合作伙伴端创建用户。某些合作伙伴支持即时 (JIT) 供应。在 JIT 供应中，如果 Cloud Identity Service 用户不存在于合作伙伴端，那么会使用通过 SAML 断言传递的属性来自动创建该用户。

为使 SSO 可用于所有合作伙伴，Cloud Identity Service 用户名通常必须与 SP 使用的用户名匹配。此需求的例外情况是启用了 JIT 供应的合作伙伴，此时 SAML 主题映射到 SP 端的联合标识。

快速连接合作伙伴端设置

为使单点登录能够与预先配置的快速连接联合模板配合使用，某些合作伙伴端设置必须仅使用特定的值或设置。下表并没有列出所有合作伙伴端 SAML 2.0 设置。该表列出了联合模板仅支持某些值或选项的特定设置。

管理员可以在接口级别覆盖快速连接联合模板的特性。Cloud Identity Service 同时支持身份提供者 (IdP) 和 SP 启动的 SSO。

注：针对所有 SP 的 SAML 断言（回复）均使用相同密钥进行签署。

表 *39.* 快速连接联合模板的 *SAML 2.0* 设置

合作伙伴	应用程序和 SAML 2.0 设置	自动供应支持	IdP 或 SP 启动的 SSO
ADFS	1. 在"ADFS 声明提供者信任特性"的**高级**选项卡中，**安全散列算法**必须设置为 **RSA-SHA1**。 2. SAML2.0 认证请求不得由 ADFS 签署。	否	SP
Adobe Creative Cloud	不适用	否	SP
Adobe Echo Sign Provisioning	不适用	否	IdP 和 SP
Agiloft	不适用	是	SP
Aha	不适用	是	IdP 和 SP
Amazon Web Services (AWS)	• 在 AWS 中为 SSO 创建 IAM 角色。IAM 角色建立与身份提供者的信任并为联合用户定义许可权。 • 选择**用于身份访问的角色**和**将 Web SSO 访问权授予 SAML 提供者**选项。 • SAML 断言中的**角色**和**角色会话名称**字段为必填。	否	IdP
ANCILE uAlign			IdP 和 SP
AnswerHub			IdP 和 SP
ArcGIS		是	IdP 和 SP
Asana	不适用	否	IdP 和 SP
Assembla			IdP

表 39. 快速连接联合模板的 *SAML 2.0* 设置 (续)

合作伙伴	应用程序和 SAML 2.0 设置	自动供应支持	IdP 或 SP 启动的 SSO
BambooHR	不适用	否	IdP 和 SP
BIME	不适用	否	SP
Bitium	不适用	否	IdP 和 SP
BlueJeans	对于 IdP 启动的 SSO，必须在目标标识中输入 RelayState。	是	IdP 和 SP
Bonusly	不适用	否	IdP 和 SP
Boomi Atmosphere®		否	IdP 和 SP
Box	无论启用还是禁用自动供应，都需要以下设置。 1. 必须针对 SP 启动的 SSO 签署 SAML 请求。 2. 用于签署 SAML 请求的签名算法必须是 RSA-SHA1。 3. 如果 BOX 组和电子邮件别名将通过 SAML 断言发送，那么必须使用以下属性名称： • 对于 BOX 组，使用 `groups` 作为属性名称。 • 对于 BOX 电子邮件别名，使用 `email_aliases` 作为属性名称。 如果启用 BOX 自动供应，那么必须使用以下属性名称。 1. 对于名字，使用 `firstname` 作为属性名称。 2. 对于姓氏，使用 `lastname` 作为属性名称。	是	IdP 和 SP
Brightcove	不适用	否	IdP 和 SP
Chatter	Chatter 在 Salesforce 开发者帐户中可用。有关 SAML SSO 配置的信息，请参阅 Salesforce SAML 设置。	是	IdP 和 SP
Citrix 应用程序	SP 启动的 SSO 需要每个应用程序的单独目标标识。 Citrix 应用程序。 • Citrix OpenVoice • Citrix Online • GoTo Assist • GoToAssist Concierge • GoToAssist Remote Support • GoToAssist Seeit • GoToAssist ServiceDesk • GoTo Webinar		
Citrix Sharefile		否	IdP 和 SP

表 *39.* 快速连接联合模板的 *SAML 2.0* 设置 *(续)*

合作伙伴	应用程序和 SAML 2.0 设置	自动供应支持	IdP 或 SP 启动的 SSO
Clarizen	不适用	否	IdP 和 SP
ClearSlide	不适用	是	IdP 和 SP
Cloud Drop	• Salesforce 开发者帐户必须可用。有关 SAML SSO 配置的信息，请参阅 Salesforce SAML 设置。 • 从 Salesforce AppExchange 中，搜索 Cloud Drop 应用程序并将其安装在 Salesforce 开发者帐户中	是	IdP 和 SP
Cloud Passage	如果启用自动供应，需要以下设置。 • **admin**。指定用户是否为 Halo 站点管理员。 • **ghostport_access**。指定用户是否为 GhostPorts 用户。 • **portal_access**。指定用户是否具有门户网站访问权。 • **firstname**。 • **lastname**。 • **email**。 • **sms**。用户的移动电话号码，用于接收 SMS 认证代码。 • **Yubikey（可选）**。用户的 YubiKey 密钥值。 • **帐户标识**。用于向身份提供者标识贵组织的 Halo 帐户的标识。作为使用者 URL 在断言中传递此标识。	是	IdP
Concur	不适用	否	IdP
CrashPlan	不适用	否	IdP
Data.com	Data.com 在 Salesforce 开发者帐户中可用。有关 SAML SSO 配置的信息，请参阅 Salesforce SAML 设置。	是	IdP 和 SP
Datadog	IdP 和 SP 启动的 SSO 都需要单独的 ACS URL。 • IdP。 `https://app.datadoghq.com/account/saml/assertion/id/`*`AccountID`* • SP。`https://app.datadoghq.com/account/saml/assertion`	是	IdP 和 SP
Desk.com	不适用	是	IdP 和 SP
DeskPRO	不适用	是	IdP 和 SP
DocuSign	不适用	否	IdP 和 SP
Dropbox	不适用	否	IdP 和 SP

表 *39.* 快速连接联合模板的 *SAML 2.0* 设置 *(续)*

合作伙伴	应用程序和 SAML 2.0 设置	自动供应支持	IdP 或 SP 启动的 SSO
DupeBlocker	• Salesforce 开发者帐户必须可用。有关 SAML SSO 配置的信息，请参阅 Salesforce SAML 设置。 • 从 Salesforce AppExchange 中，搜索 DupeBlocker 应用程序并将其安装在 Salesforce 开发者帐户中	是	IdP 和 SP
Egnyte	• 将**缺省用户映射**设置为**电子邮件地址**。 • 将**使用域特定颁发者值**设置为**启用**。URL 为 `https://egnyte domain.egnyte.com`。	否	IdP 和 SP
eSignLive		是	IdP 和 SP
Fairsail		是	IdP 和 SP
GitHub	不适用	是	IdP 和 SP
Google Analytics	与 Google Apps SAML 设置相同。	否	IdP 和 SP

表 39. 快速连接联合模板的 *SAML 2.0* 设置 (续)

合作伙伴	应用程序和 SAML 2.0 设置	自动供应支持	IdP 或 SP 启动的 SSO
Google Apps	• 缺省情况下，Google Apps 模板不支持域特定颁发者。仅支持将静态值 `google.com` 用作颁发者/提供者标识。 • 当在 Google Apps 上配置 SAML2.0 SSO 时，不得选择**使用域特定颁发者**选项。 • 必须验证域名。 • 对于 SP 启动的 SSO，必须在每个应用程序的 URL 中提供特定目标标识。 Google Apps 应用程序。 • Google Admin • Google Books • Google Code • Google Drive • Google Forms • Google Groups • Google Hangouts • Google Keep • Google Maps • Google Photos • Google Play • Google Sheets • Google Slides • Google Translate • Google Trends • Google Videos • Google + • Blogger • Gmail	否	IdP 和 SP
Google Calendar	与 Google Apps SAML 设置相同。	否	IdP 和 SP
Google Docs	与 Google Apps SAML 设置相同。	否	IdP 和 SP
Google Finance	与 Google Apps SAML 设置相同。	否	IdP 和 SP
Google Site	与 Google Apps SAML 设置相同。	否	IdP 和 SP
GoToMeeting	贵组织的有效域必须针对 SAML2.0 SSO 进行注册和验证。	否	IdP 和 SP
Greenhouse	不适用	是	IdP 和 SP
HappyFox	不适用	是	IdP 和 SP
Huddle	不适用	是	IdP 和 SP
IBM® Bluemix®	不适用	是	IdP 和 SP

表 *39.* 快速连接联合模板的 *SAML 2.0* 设置 *(续)*

合作伙伴	应用程序和 SAML 2.0 设置	自动供应支持	IdP 或 SP 启动的 SSO
IBM Blueworks Live™	不适用	是	IdP 和 SP
IBM Cloud Security Enforcer	• 提供认证 URL 和目标 URL 以实现仪表板和启动板访问，例如： – `https://`*`my_domainName`*`/isam/mtfim/sps/saml20ip/saml20/logininitial?PartnerId=https://`*`partner provider_domain name`*`/idaas/mtfim/sps/idaas/saml20 &NameIdFormat=Email&Target=https://`*`partnerProvider_Domainname`*`/ui/launchpad` – `https://`*`my_domainName`*`/isam/mtfim/sps/saml20ip/saml20/logininitial?PartnerId=https://`*`partner provider_domain name`*`/idaas/mtfim/sps/idaas/saml20 &NameIdFormat=Email&Target=https://`*`partnerProvider_Domainname`*`/ui/dashboard` • 为了确保访问仪表板，SAML 断言必须包含值为 **admin** 的属性 **groups**。	否	IdP 和 SP
IBM Connections Cloud	对于 IdP 启动的 SSO，必须为每个应用程序提供目标标识。 IBM Connections Cloud 应用程序。 • IBM Connections™ Activities • IBM Connections Chat • IBM Connections Files • IBM Connections Meetings • IBM Connections Notebook • IBM Connections ToDo • IBM SmartCloud® Notes® Web • IBM Verse®	否	IdP 和 SP
IBM Kenexa® Talent Suite		否	IdP 和 SP
IBM MaaS360®		否	SP
IBM Softlayer	不适用	否	IdP
Igloo Software	必须在 ACS（断言使用者服务）URL 中提供提供者标识和目标标识。	是	IdP 和 SP
Informatica Cloud		是	IdP 和 SP

表 39. 快速连接联合模板的 *SAML 2.0* 设置 (续)

合作伙伴	应用程序和 **SAML 2.0** 设置	自动供应支持	**IdP 或 SP 启动的 SSO**
Intacct	Intacct 的 **SSO 颁发者 URL** 必须为 `https://saml.intacct.com`。	否	IdP 和 SP
Invision	不适用	否	IdP
JIRA (Altassian)	不适用	否	IdP 和 SP
Kanban Tool			IdP 和 SP
kiteworks	不适用	是	IdP 和 SP
Knowledge	Salesforce 开发者帐户必须可用。有关 SAML SSO 配置的信息，请参阅 Salesforce SAML 设置。	是	IdP 和 SP
Lesson.ly		否	IdP 和 SP
LiquidPlanner	不适用	否	IdP 和 SP
Litmos			IdP
LivePerson	不适用	否	IdP
LogMeIn	提供认证 URL 和目标 URL，例如： • `https://my_DomainName/isam/mtfim/sps/saml20ip/saml20/logininitial?RequestBinding=HTTPPost&PartnerId=https://accounts.logme.in&NameIdFormat=Email&Target=https://secure.logmein.com/central/Central.aspx`	是	IdP 和 SP
Lucidchart	在 SAML 中，选择**在 SAML 请求中发送 Nameid 格式**。	是	IdP 和 SP
Mozy	提供包含 **RequestBinding**、**PartnerID** 和 **NameIDFormat** 的认证 URL，例如： • `https://my_domain/isam/mtfim/sps/saml20ip/saml20/logininitial?RequestBinding=HTTPPost&PartnerId=https://auth2.mozy.com/mozy_domain/saml&NameIdFormat=Email`	否	IdP 和 SP
Namely	不适用	否	IdP 和 SP
NetSuite	不适用	否	IdP
New Relic	不适用	否	IdP 和 SP
Office 365	• 登录 Microsoft Office 365 并添加域。 • 验证该域。 • 使用 power shell 命令联合域。使用 Azure Active Directory Module for Windows PowerShell 工具。	否	SP
Okta	不适用	是	IdP 和 SP
OneDrive / SkyDrive	OneDrive 在 Office 365 帐户中可用。有关更多信息，请参阅 Office 365 SAML 设置。	否	SP
OpenDataSoft	必须在 SSO URL 中提供目标标识。	否	IdP 和 SP

表 *39.* 快速连接联合模板的 *SAML 2.0* 设置 *(续)*

合作伙伴	应用程序和 SAML 2.0 设置	自动供应支持	IdP 或 SP 启动的 SSO
OpenDNS		否	IdP 和 SP
PagerDuty	不适用	是	IdP 和 SP
ProofHQ	不适用	是	IdP 和 SP
Redbooth	不适用	否	IdP 和 SP
Remedyforce	获取 Remedyforce 帐户。有关 SAML SSO 配置的信息，请参阅 Salesforce SAML 设置。	是	IdP 和 SP
Roambi Business	必须在 SSO URL 中提供目标标识。	否	IdP 和 SP
Sales Cloud	注册 Salesforce Service Cloud 帐户。有关 SAML SSO 配置的信息，请参阅 Salesforce SAML 设置。	是	IdP 和 SP
Salesforce	如果启用 JIT 供应，那么需要以下设置： • **请求签名方法**必须设置为 **RSA-SHA1**。 • **断言解密证书**必须设置为**断言未加密**。 • **SAML 身份位置**必须设置为**身份位于 Subject 语句的 NameIdentifier 元素中**。 • **服务提供者启动的请求绑定**必须设置为 **HTTP 重定向**。 • **SAML 身份类型**必须设置为**来自用户对象的联合标识**。 • **用户供应类型**必须设置为**标准**。	是	IdP 和 SP
Samanage	不适用	是	IdP 和 SP
SAP Netweaver		否	IdP 和 SP
Service Cloud	注册 Salesforce Service Cloud 帐户。有关 SAML SSO 配置的信息，请参阅 Salesforce SAML 设置。	是	IdP 和 SP
ServiceNow	不适用	否	IdP 和 SP
SharePoint Online	SharePoint Online 在 Office 365 帐户中可用。有关更多信息，请参阅 Office 365 SAML 设置。	否	SP
Skilljar		是	IdP 和 SP
Slack	**服务提供者标识**必须设置为 `https://`*`DomainName`*`.slack.com/`。	是	IdP 和 SP
Small Improvements		否	IdP 和 SP
Soonr Workplace	不适用	否	IdP 和 SP

表 *39.* 快速连接联合模板的 *SAML 2.0* 设置 *(续)*

合作伙伴	应用程序和 **SAML 2.0** 设置	自动供应支持	**IdP** 或 **SP** 启动的 **SSO**
SpringCM	提供认证 URL 和目标 URL，例如： • `https://`*`ISAM_DomainName`*`/isam/mtfim/sps/saml20ip/saml20/logininitial?PartnerId=https://`*`Partner_DomainName`*`/atlas/sso&NameIdFormat=Email&Target=https://`*`Partner_Provider_DomainName`*`/atlas/Documents/BrowseDocuments.aspx?aid=`*`ID`*	否	IdP 和 SP
StatusPage	不适用	否	IdP 和 SP
SuccessFactors	需要以下设置。 • **需要必需签名**必须设置为**断言**。 • **启用 SAML 标志**必须设置为**启用**。 • **SAML 概要文件**必须设置为**浏览器/发布概要文件**。 • **NameID 格式**必须设置为**未指定**。 • **启用 SP 启动的登录 (AuthnRequest)** 必须设置为**是**。 • 必须选择**缺省颁发者**。	否	IdP 和 SP
SugarCRM	不适用	否	IdP 和 SP
Symantec End-point Manager			IdP 和 SP
Syncplicity	不适用	否	SP
Tableau			IdP 和 SP
TOPdesk		否	IdP 和 SP
Unifyle	不适用	是	IdP 和 SP
UserVoice			IdP 和 SP
Ustream		否	IdP 和 SP
VersionOne	必须在 SSO URL 中提供目标标识。	否	IdP 和 SP
WalkMe	• Salesforce 开发者帐户必须可用。有关 SAML SSO 配置的信息，请参阅 Salesforce SAML 设置。 • 在 Salesforce 开发者帐户上安装 WalkMe 应用程序。	是	IdP 和 SP
WebEx	• 在 SAML 断言中，**NameID 格式**必须为电子邮件。 • 在 Cloud Identity Portal 中创建用户时，**UID** 和 **gtwayPrincipalName** 必须不同。**gtwayPrincipalName** 必须采用电子邮件格式，而 **UID** 必须与提供者的用户名相同。	是	IdP 和 SP
WordPress	不适用	是	IdP 和 SP

表 *39.* 快速连接联合模板的 *SAML 2.0* 设置 *(续)*

合作伙伴	应用程序和 SAML 2.0 设置	自动供应支持	IdP 或 SP 启动的 SSO
Workday	• 对于 IdP 和 SP 启动的 SSO，**服务提供者标识**选项必须设置为 `http://www.workday.com/`。 • 对于 SP 启动的 SSO，必须选择**不抑制 SP 启动的认证请求**选项。 • 必须清除**签署 SP 启动的认证请求**选项。	否	IdP 和 SP
Yammer	Yammer 在 Office 365 帐户中可用。有关更多信息，请参阅 Office 365 SAML 设置。	否	SP
Zendesk	不适用	否	IdP 和 SP
Zoho 应用程序	不适用 Zoho 应用程序。 • Site 24x7 (Service Desk Plus) • ZoHo Books • Zoho Bugtracker • Zoho Campaigns • Zoho Chat • Zoho Connect • Zoho CRM • Zoho Docs • Zoho Forms • Zoho Invoice • Zoho Mail • Zoho Meeting • Zoho Projects • Zoho Reports • Zoho SalesIQ • Zoho Sites • Zoho Social • Zoho Support • Zoho Survey • Zoho Vault	否	IdP 和 SP
Zscaler	无论是启用还是禁用了自动供应，对于 IdP 启动的 SSO，必须向登录 URL 追加目标标识，例如： • `https://my_domain/isam/mtfim/sps/saml20ip/saml20/logininitial?PartnerId=zscalerbeta.net&Target=http://gateway.zscalerbeta.net/test`	是	IdP 和 SP
Zuora	对于 IdP SSO 登录，必须提供联合标识。	否	IdP

管理启动板服务

用户可通过 自助服务 门户网站中的启动板使用 Web 连接及联合合作伙伴 Web 连接。用户必须添加至相应服务才能通过启动板访问 Web 连接。

向启动板服务添加用户

用户可通过启动板（其 自助服务 门户网站中的单个位置）访问 Web 应用程序。

关于此任务

对于每个 Web 连接及所创建的联合合作伙伴连接，将创建对应服务。系统对该服务指定与连接相同的名称，对于联合 Web 应用程序，系统指定与连接别名相同的名称。为使用户可从启动板使用该 Web 应用程序，必须将该用户添加至相应服务。

注： 非虚拟连接名称以正斜杠开头，例如，/my_connection_1。非虚拟连接的服务名称也以正斜杠开头。

注： 如果联合合作伙伴连接别名已更改，那么将创建带有新别名的新服务。该连接先前使用的服务中的成员将迁移至新服务，旧服务将被移除。

可通过手动管理服务或使用策略动态管理服务来向服务添加用户。

过程

向启动板服务添加用户。

- 通过手动管理服务来添加用户。
- 通过动态管理服务来添加用户。

管理密钥

您可以管理用来保护连接的客户机证书和服务器证书。

创建客户机证书

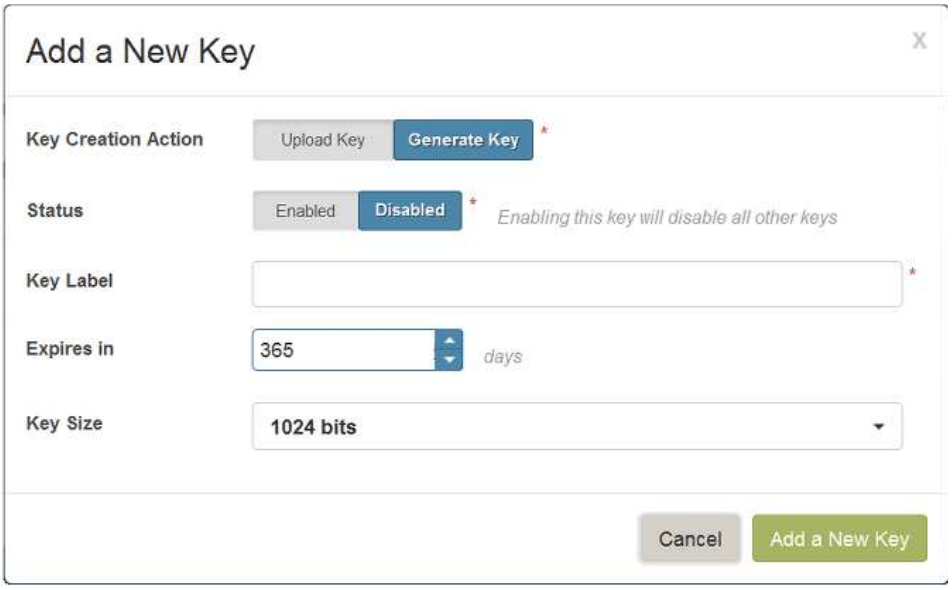
客户机证书包含专用密钥和公用密钥。客户机证书由客户机系统用来向远程服务器发出已认证请求。您可以创建客户机证书，或者，如果您要使用现有证书文件，那么可以将此文件上载到 Cloud Identity Portal。

关于此任务

缺省情况下，启用的证书将用于您创建的每个连接。同一时间只能启用一个密钥。

过程

1. 在导航菜单中，单击**应用程序** > **密钥管理**，然后单击**客户机证书**和**添加新密钥**。



2. 输入客户机证书密钥设置。
3. 单击**添加新密钥**。

客户机证书密钥设置

客户机证书密钥设置包括密钥标签、到期时间和密钥大小。

表 *40.* 客户机证书密钥设置

设置	描述
密钥创建操作	• **上载密钥**。如果您有想要使用的证书文件，可以上载此文件。 • **生成密钥**。如果您没有证书文件，Cloud Identity Portal 可以生成密钥。
状态	• **启用**。如果您启用密钥，那么将禁用先前启用的密钥和所有其他证书密钥。同一时间只能启用一个密钥。 **要点：**如果启用密钥，那么将禁用先前启用的密钥。使用先前启用密钥的所有连接均无效。 • **禁用**。密钥被禁用。
密钥标签	• 对于上载的密钥，当状态设置为"启用"时必须输入标签。密钥标签是正在上载的证书文件的名称。 • 对于生成的密钥，这是表示证书的唯一标识。标签提供的名称用于在执行密钥管理功能时引用证书。
密钥文件	仅对于上载的密钥，单击**浏览**以浏览并选择要上载的文件。支持 JKS、PEM 和 P12 格式。
密钥密码	仅对于上载的密钥，这是密钥密码。该密码必须与您要上载的证书文件中的密码匹配。
到期时间	密钥有效的天数。
密钥大小	密钥大小。

搜索客户机证书

搜索要启用、禁用或移除的证书。

过程

1. 在导航菜单中，单击**应用程序** > **密钥管理**，然后单击**客户机证书**。
2. 在**缩小搜索范围**字段中，输入搜索条件。

   您可以搜索证书密钥标签中包含的任意 3 个字符的字符串。例如，要搜索具有密钥标签 certificate1 的证书，可以输入 cer 或 te1。 将列示与搜索条件匹配的证书。您可以选择要启用、禁用、除去或替换的证书。

启用和禁用密钥

同一时间只能启用一个密钥。

关于此任务

启用证书密钥时，将自动禁用先前启用的密钥。只能通过启用其他密钥来禁用当前启用的密钥。

要点：如果启用密钥，那么将禁用先前启用的密钥。使用先前启用密钥的所有连接均无效。

过程

1. 搜索并选择要启用的密钥。

2. 单击**启用**。 密钥已启用。所有新连接现在都使用新启用的证书密钥。

下载证书

您可以下载证书。

关于此任务

对于合作伙伴加密认证请求并验证认证签名的合作伙伴连接，您可以下载该连接中使用的专用证书密钥的公用证书。

公用证书将在合作伙伴端接口配置中使用。

过程

1. 搜索并选择想要为其下载公用证书的密钥。
2. 单击**下载公用证书**。
3. 保存该文件。

除去密钥

可以移除不再需要的证书。必须先禁用密钥才能将其除去。

过程

1. 搜索并选择想要除去的密钥。
2. 单击**除去密钥**。

   此时将要求您确认除去操作。单击**除去密钥**。 密钥已被除去。

替换密钥

在使用证书的任何环境中，需要更新证书及其密钥。可能还需要替换到期的证书。

过程

1. 搜索并选择想要替换的密钥。
2. 单击**替换密钥**。

创建服务器证书

服务器证书用来识别服务器。如果您要添加现有服务器证书文件，那么可以将此文件上载到 Cloud Identity Portal。

过程

1. 在导航菜单中，单击**应用程序** > **密钥管理**，然后单击**服务器证书**和**添加新密钥**。

2. 在**密钥标签**字段中输入密钥标签。 密钥标签必须与正在上载的证书文件的名称匹配。
3. 单击**浏览**以浏览并选择要上载的证书文件。
4. 单击**添加新密钥**。

搜索服务器证书

搜索要移除或替换的证书。

过程

1. 在导航菜单中，单击**应用程序** > **密钥管理**，然后单击**服务器证书**。
2. 在**缩小搜索范围**字段中，输入搜索条件。

您可以搜索个人证书密钥标签中包含的任意 3 个字符的字符串。例如，要搜索具有密钥标签 certificate1 的证书，可以输入 cer 或 te1。 将列示与搜索条件匹配的证书。您可以选择要除去或替换的证书。

除去密钥

可以移除不再需要的证书。

关于此任务

要点：移除证书时，使用该证书的任何连接都将失败。要使连接保持有效，必须为连接选择有效证书。

过程

1. 搜索并选择想要除去的密钥。
2. 单击**除去密钥**。

   此时将要求您确认除去操作。单击**除去密钥**。 证书已被除去。

替换密钥

在使用证书的任何环境中，需要更新证书及其密钥。可能需要替换到期的证书。

过程

1. 搜索并选择想要替换的密钥。
2. 单击**替换密钥**。

供应身份

身份管理供给允许身份数据在外部身份存储库和 Cloud Identity Service 身份管理环境之间流动。身份供应可以为入站供应和出站供应。

身份供应概述

用户记录可以由外部身份存储库使用身份管理供给供应，也可以使用身份管理供给来供应到外部身份存储库。

Cloud Identity Service 可以与许多类型的身份存储库（例如 Active Directory、LDAP V3、关系数据库、SOAP 服务、消息队列和 SAP）连接。通过集成这些其他身份存储库，可以通过定义入站连接在 Cloud Identity Service 中自动添加、修改和删除用户。通过使用出站连接，可以在外部存储库中添加、修改和删除用户。

身份存储库

身份数据可以保存在贵组织中的许多不同系统中。这些系统称为身份存储库。每个存储库可能包含不同类型的身份数据。例如，某些可能包含简单的帐户相关数据以供特定应用程序（例如 SQL 数据库）使用。其他身份存储库可能包含对各种系统（例如 Oracle PeopleSoft）有意义的更全面的身份数据。这些存储库中的数据由身份属性组成。身份属性用于标识用户和构成用户记录。例如，用户记录可能由用户名、名字、姓氏、电子邮件地址和作业角色组成。Cloud Identity Service 充当身份管理 (IDM) 系统，其作用是使用身份供应功能使身份数据在贵组织中的不同存储库中保持准确、一致且最新。

供给管理

当存储库与 Cloud Identity Service 集成时，定义如何连接这些系统以及如何在这些系统之间供应身份数据便成了在存储库之间同步数据的关键。供给管理使身份数据（例如属性，组、角色和帐户信息）能够在其他身份存储库和 Cloud Identity Service 之间流动。

IDM 系统可以认为是集中星型模型。Cloud Identity Service 位于所有身份存储库的中央以充当中心。身份数据在 Cloud Identity Service 和其他身份存储库之间来回流动。从身份存储库流向 Cloud Identity Service 的数据称为入站数据，从 Cloud Identity Service 流出的数据称为出站数据。

身份管理供给包含许多类型的业务规则，这些规则定义 Cloud Identity Service 如何与其他身份存储库交互：

- 连接信息。连接信息确定 Cloud Identity Service 与存储库连接的方式和时间，以及如何解析和解释来自该存储库的信息。
- 供应策略。主供应策略确定 Cloud Identity Service 向存储库传输身份数据或从中接收身份数据的情况。供应策略还确定要忽略的数据。
- 属性和组映射信息。不同身份存储库中的属性和组不使用相同的命名约定。身份属性可以在不同的存储库之间映射到 Cloud Identity Service 中包含的信息。Cloud Identity Service 身份管理供给的映射功能允许简单和复杂的映射逻辑，包括组之间的映射。

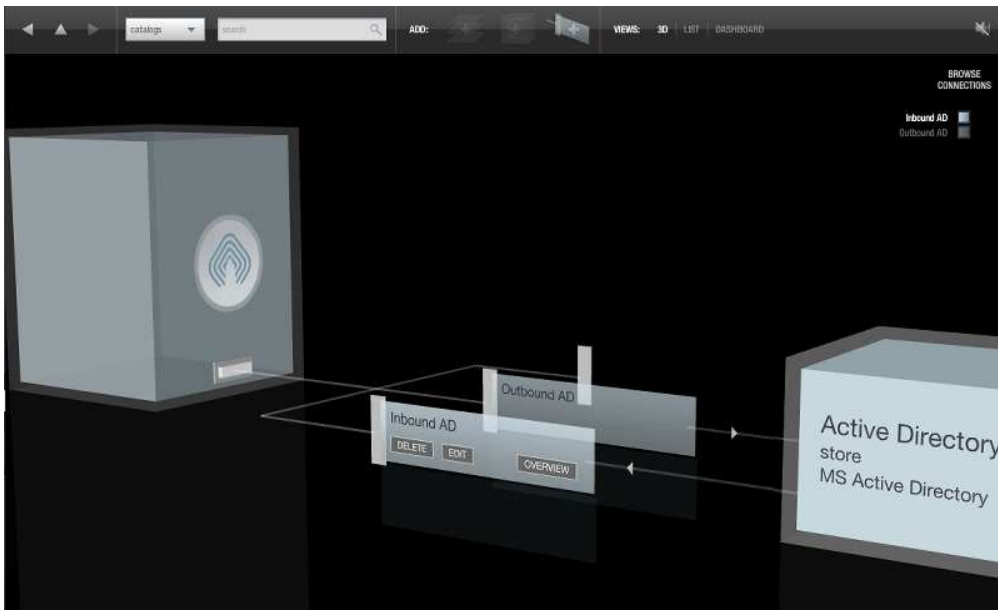
组装行

在 Cloud Identity Service 中，身份管理供给称为组装行。组装行在为贵组织进行 Cloud Identity Service 初始设置期间配置。组装行使用模板组装行 (TAL) 进行定义。每个 TAL 都包含一些可配置的连接选项。

供给管理 UI

供给管理 UI 提供了对配置管理供给的图形表示。

Cloud Identity Service 可以与许多类型的身份存储库（例如 Active Directory、LDAP V3、关系数据库、SOAP 服务、消息队列、SAP 和 PeopleSoft）连接。通过集成这些其他身份存储库，可以将用户自动添加到 Cloud Identity Service，并且可以将 Cloud Identity Service 用户添加到外部存储库。



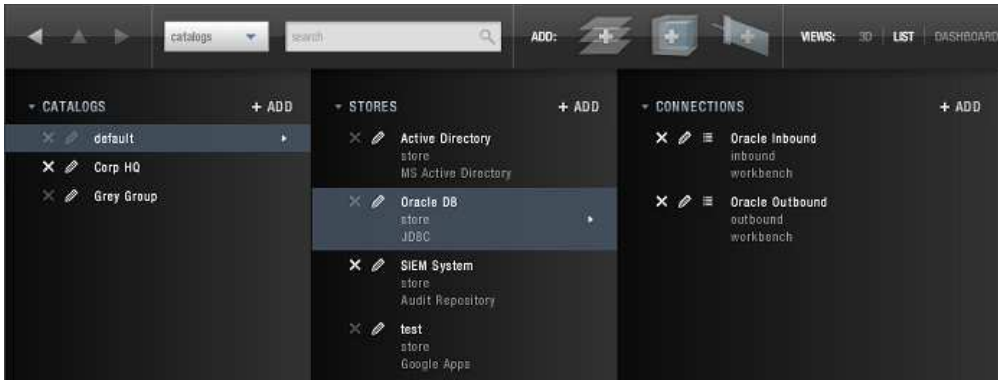
目录、库和连接

目录提供了用于对连接到 Cloud Identity Service 服务的外部身份存储库进行分组的方法。例如，可以针对公司的某个部门（例如，财务或 IT）定义目录。库是分组到目录之下的外部身份存储库。Cloud Identity Service 能够支持最常见的身份存储库，例如 Active Directory、LDAP V3、关系数据库、SOAP 服务、消息队列和 SAP。

连接定义 Cloud Identity Service 如何与外部身份存储库连接和交互。连接可以为入站和出站连接。

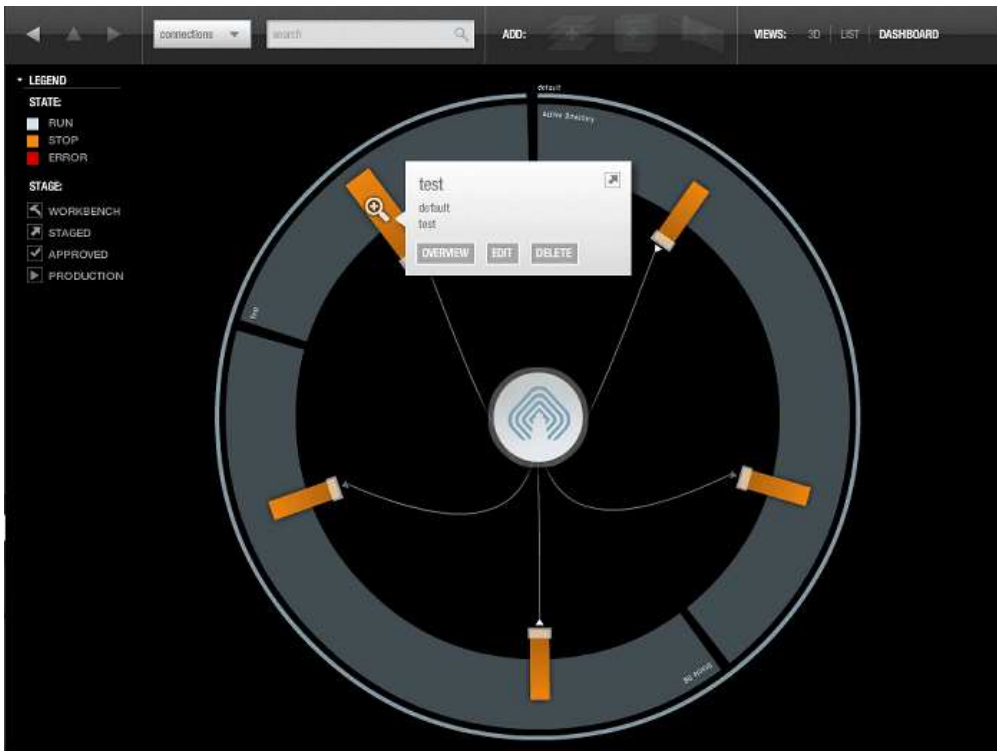
"列表"视图

您可以在"列表"视图中查看供给管理系统，从而更轻松地浏览、查看、添加和编辑目录、库和连接。

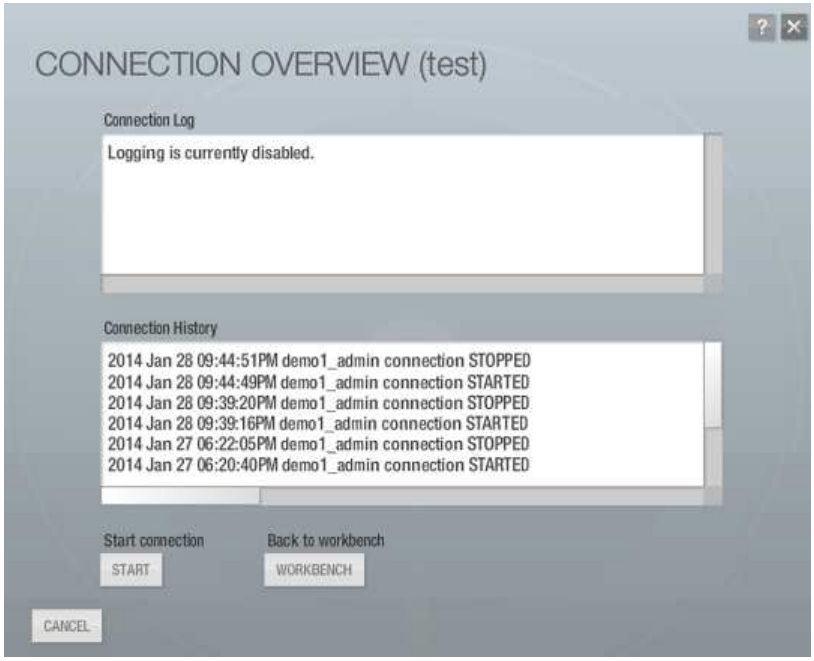


"仪表板"视图

在建立与库的连接之后，管理员可以从"仪表板"查看整个供给管理系统。颜色编码指示连接的状态。



管理员可以查看每个连接的事件历史记录，并可以启动和停止连接。



管理逆向代理设置

您可以管理逆向代理设置，以更改受保护资源的用户会话的超时值。

过程

单击**应用程序** > **逆向代理设置**。

逆向代理设置

用户会话的超时值将应用于受 Cloud Identity Service 保护的所有 Web 资源的所有会话。

超时值

超时值用于设置所有已认证或未认证用户会话的最大生存期超时值。超时值确定授权凭证信息保持有效的时间长度。达到指定的超时限制时，用户必须重新认证。缺省会话条目生存期超时值为 3600 秒。值为 0 表示禁用超时功能（超时值不受限）。

不活动超时值

不活动超时值用于设置用户会话不活动超时值。例如，如果用户处于不活动状态的时间长度超过不活动超时值，那么会话将结束或者标记为需要重新认证。缺省登录会话不活动超时值为 600 秒。值为 0 表示禁用此不活动超时功能（不活动超时值不受限）。

第 8 章 移动应用程序

用户可通过 IBM 移动应用以使用他们的移动设备访问自助服务应用程序。

IBM 移动应用也是接收一次性密码 (OTP) 和推送通知以向自助服务应用程序认证的必备软件。

概述

IBM 移动应用允许用户从其移动设备访问自助服务应用程序。

IBM 移动应用能做些什么?

用户可通过 IBM 移动应用从其设备发出服务请求，管理员可批准和拒绝服务请求。您可访问链接至服务的应用程序。IBM 移动应用还具有一次性密码生成器，用于向自助服务应用程序进行两步认证。

为什么您需要 IBM 移动应用?

您需要该程序以从移动设备访问自助服务应用程序以及从您的移动设备启动服务应用程序。

如果您的公司使用多因子认证以通过推送通知或一次性密码 (OTP) 访问自助服务应用程序(OTP)，那么您也需要该应用程序。

IBM 移动应用支持哪些移动设备?

IBM 移动应用支持运行 iOS V10.0.0 或更高版本的 Apple 设备及运行 Lollipop 或更高版本的 Android 设备。

什么是多因子认证 (MFA)?

MFA 要求使用来自不同源的多种认证方法以验证用户的身份。Cloud Identity Service 使用两步 MFA。您的身份是通过输入用户名和密码并输入代码或接受发送给您的移动设备的通知来验证的。

两步验证按以下方式工作。

1. 使用用户名和密码按常规方式登录自助服务应用程序。
2. 系统会向您的移动设备发送验证通知（使用 SMS 消息、所生成 OTP 或以推送通知形式）。
3. 在移动设备上，通过输入代码或接受通知来验证您的身份。

© Copyright IBM Corp. 2015, 2017

入门

通过下载和安装 IBM 移动应用，然后将您的设备连接至您的 Cloud Identity Service 帐户，开始使用该应用程序。

下载应用程序

在您的设备上安装该应用程序。

过程

1. 启动 App Store (iOS) 或 Google Play Store (Android) 应用程序。
2. 搜索 IBM 移动应用。
3. 点击**获取**和**安装**以下载应用程序。
4. 点击应用程序图标以打开应用程序。

登录

在您的移动设备上登录 Cloud Identity Service 帐户。

关于此任务

可扫描 QR 代码以登录您的帐户，也可使用一次性密码 (OTP) 代码。您的会话到期时，可通过输入用户名和密码再次登录。

使用 QR 代码进行登录

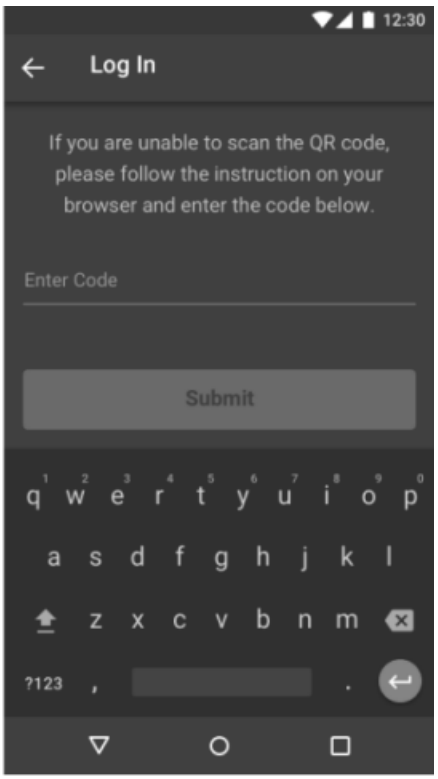
扫描 QR 代码以登录您的帐户。如果无法扫描 QR 代码，那么可手动输入代码。

过程

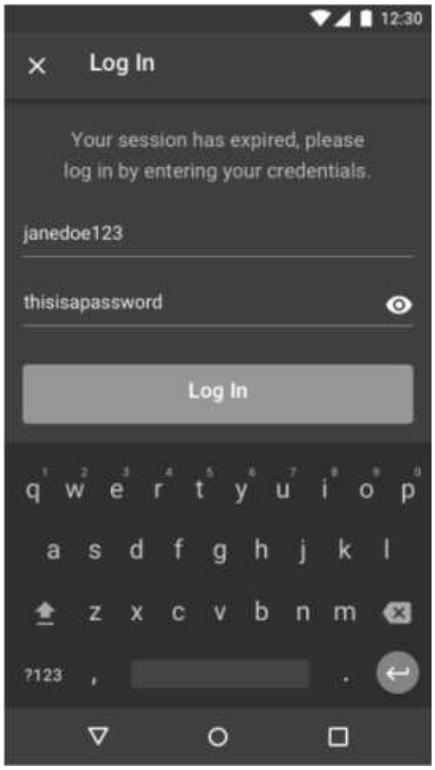
1. 在您的设备上找到并打开 IBM 移动应用，然后点击**登录**。

   系统会向您发送 QR 代码。

2. 在另一设备上，转至 ***company*.ibm.com** 并扫描 QR 代码。如果您无法扫描 QR 代码，点击**无法扫描 QR 代码**并遵循指示信息以手动输入代码。



3. 如果会话到期，请输入用户名和密码，然后点击**登录**。

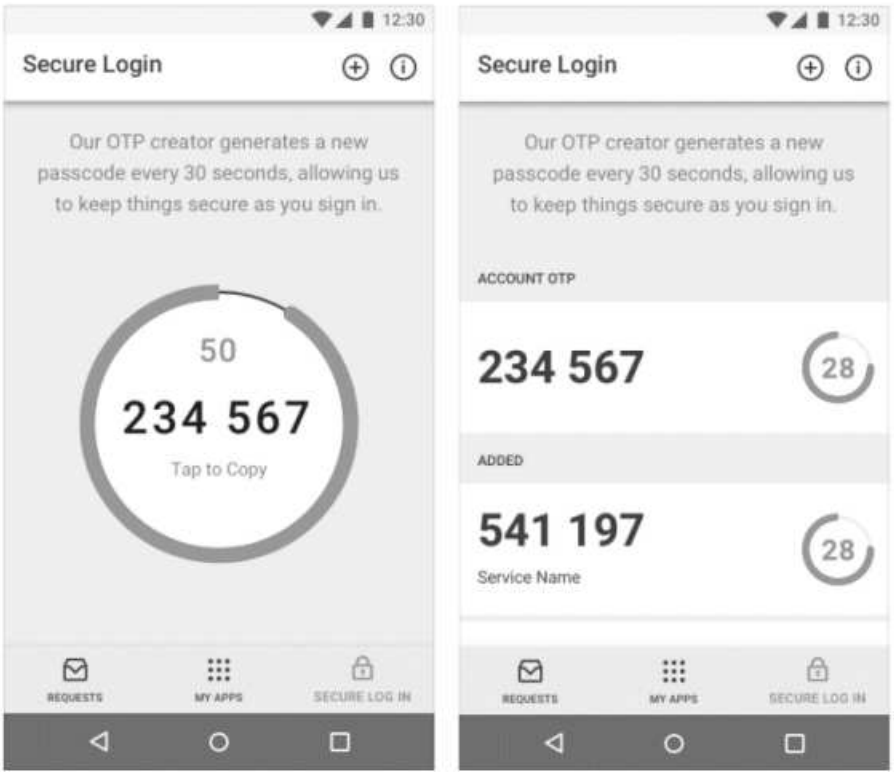


使用一次性密码登录

使用 OTP 代码登录。

过程

在您的设备上找到并打开 IBM 移动应用，点击**安全登录**，然后选择您要使用的 OTP 生成服务。



可通过扫描 QR 代码或手动输入代码来添加 OTP 生成服务。

管理您的设备

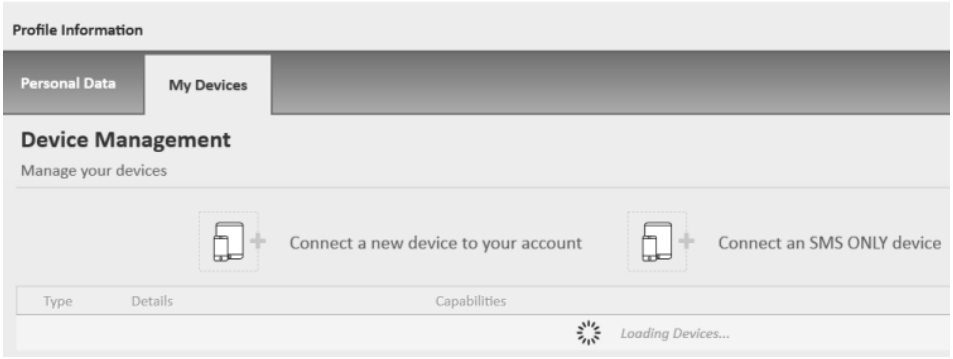
从 Cloud Identity Service 自助服务门户网站注册并管理您的设备。

关于此任务

添加新设备并移除您不再使用的旧设备。通过扫描 QR 代码或手动输入代码，可添加仅启用 SMS 的设备和启用所有方法的设备。您应在首次登录自助服务门户网站时注册设备。

过程

1. 从您的计算机登录自助服务门户网站。
2. 选择**概要文件** > **我的设备**。



3. 添加或移除设备。

删除应用程序

如果不再使用该设备或者不再需要访问 Cloud Identity Service，请删除该应用程序。

关于此任务

注：删除 IBM 移动应用不会移除任何对您的 Cloud Identity Service 帐户有效的两步验证。

过程

1. 在您的设备上找到并选择该 IBM 移动应用。
2. 点击**删除**。

入门

通过下载和安装 IBM 移动应用，然后将您的设备连接至您的 Cloud Identity Service 帐户，开始使用该应用程序。

下载应用程序

在您的设备上安装该应用程序。

过程

1. 启动 App Store (iOS) 或 Google Play Store (Android) 应用程序。
2. 搜索 IBM 移动应用。
3. 点击**获取**和**安装**以下载应用程序。
4. 点击应用程序图标以打开应用程序。

登录

在您的移动设备上登录 Cloud Identity Service 帐户。

关于此任务

可扫描 QR 代码以登录您的帐户，也可使用一次性密码 (OTP) 代码。您的会话到期时，可通过输入用户名和密码再次登录。

使用 *QR* 代码进行登录：

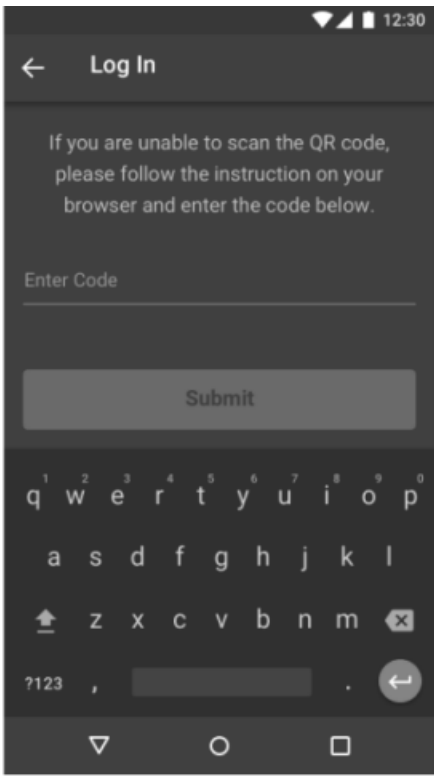
扫描 QR 代码以登录您的帐户。如果无法扫描 QR 代码，那么可手动输入代码。

过程

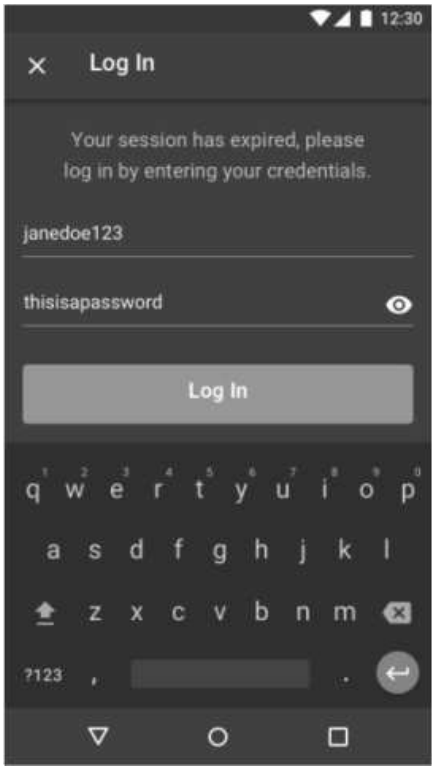
1. 在您的设备上找到并打开 IBM 移动应用，然后点击**登录**。

   系统会向您发送 QR 代码。

2. 在另一设备上，转至 ***company*.ibm.com** 并扫描 QR 代码。如果您无法扫描 QR 代码，点击**无法扫描 QR 代码**并遵循指示信息以手动输入代码。



3. 如果会话到期，请输入用户名和密码，然后点击**登录**。

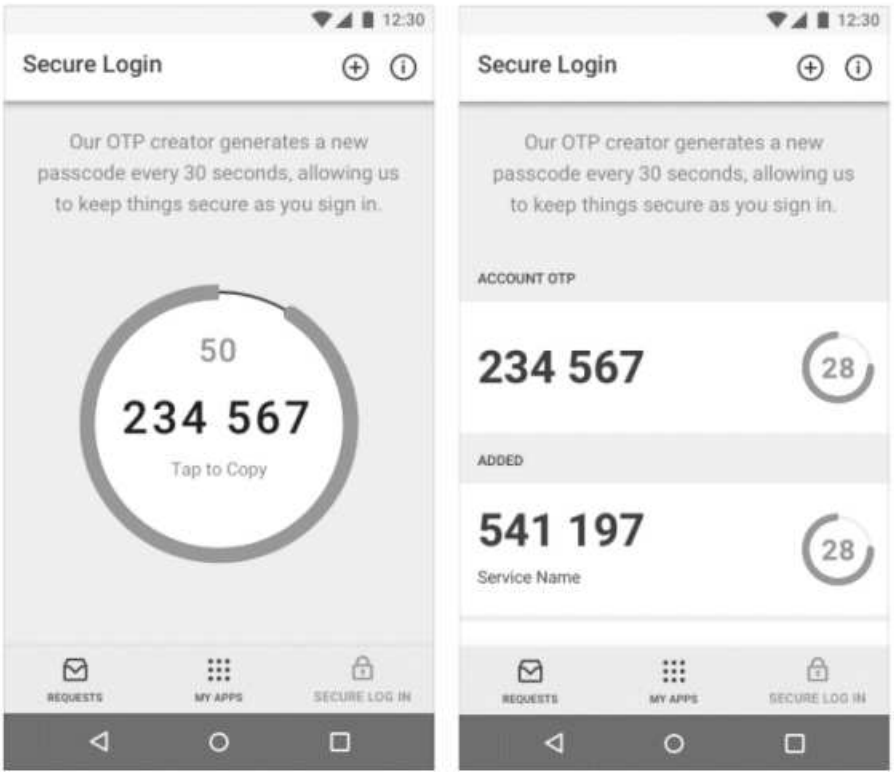


使用一次性密码登录：

使用 OTP 代码登录。

过程

在您的设备上找到并打开 IBM 移动应用，点击**安全登录**，然后选择您要使用的 OTP 生成服务。



可通过扫描 QR 代码或手动输入代码来添加 OTP 生成服务。

管理您的设备

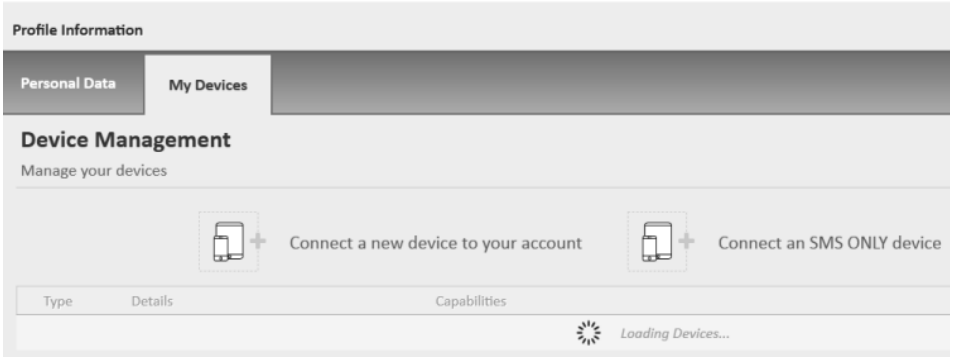
从 Cloud Identity Service 自助服务门户网站注册并管理您的设备。

关于此任务

添加新设备并移除您不再使用的旧设备。通过扫描 QR 代码或手动输入代码，可添加仅启用 SMS 的设备和启用所有方法的设备。您应在首次登录自助服务门户网站时注册设备。

过程

1. 从您的计算机登录自助服务门户网站。
2. 选择**概要文件** > **我的设备**。



3. 添加或移除设备。

删除应用程序

如果不再使用该设备或者不再需要访问 Cloud Identity Service，请删除该应用程序。

关于此任务

注：删除 IBM 移动应用不会移除任何对您的 Cloud Identity Service 帐户有效的两步验证。

过程

1. 在您的设备上找到并选择该 IBM 移动应用。
2. 点击**删除**。

入门

通过下载和安装 IBM 移动应用，然后将您的设备连接至您的 Cloud Identity Service 帐户，开始使用该应用程序。

下载应用程序

在您的设备上安装该应用程序。

过程

1. 启动 App Store (iOS) 或 Google Play Store (Android) 应用程序。
2. 搜索 IBM 移动应用。
3. 点击**获取**和**安装**以下载应用程序。
4. 点击应用程序图标以打开应用程序。

登录

在您的移动设备上登录 Cloud Identity Service 帐户。

关于此任务

可扫描 QR 代码以登录您的帐户，也可使用一次性密码 (OTP) 代码。您的会话到期时，可通过输入用户名和密码再次登录。

使用 *QR* 代码进行登录：

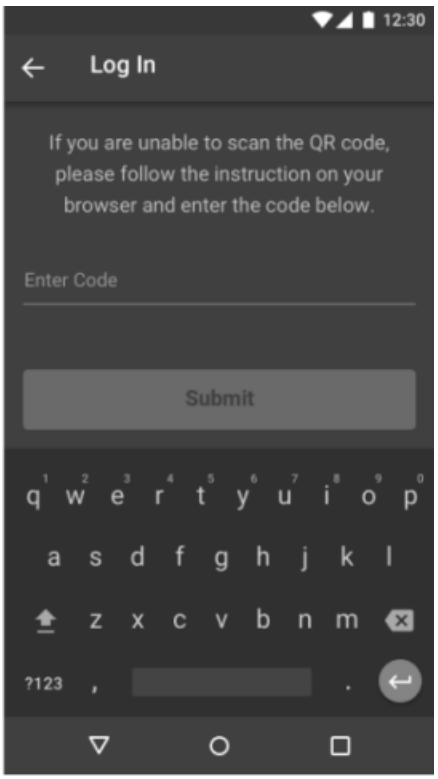
扫描 QR 代码以登录您的帐户。如果无法扫描 QR 代码，那么可手动输入代码。

过程

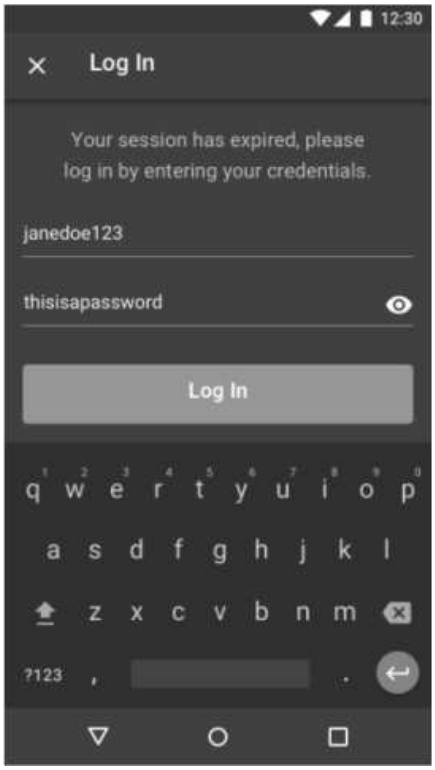
1. 在您的设备上找到并打开 IBM 移动应用，然后点击**登录**。

   系统会向您发送 QR 代码。

2. 在另一设备上，转至 ***company*.ibm.com** 并扫描 QR 代码。如果您无法扫描 QR 代码，点击**无法扫描 QR 代码**并遵循指示信息以手动输入代码。



3. 如果会话到期，请输入用户名和密码，然后点击**登录**。

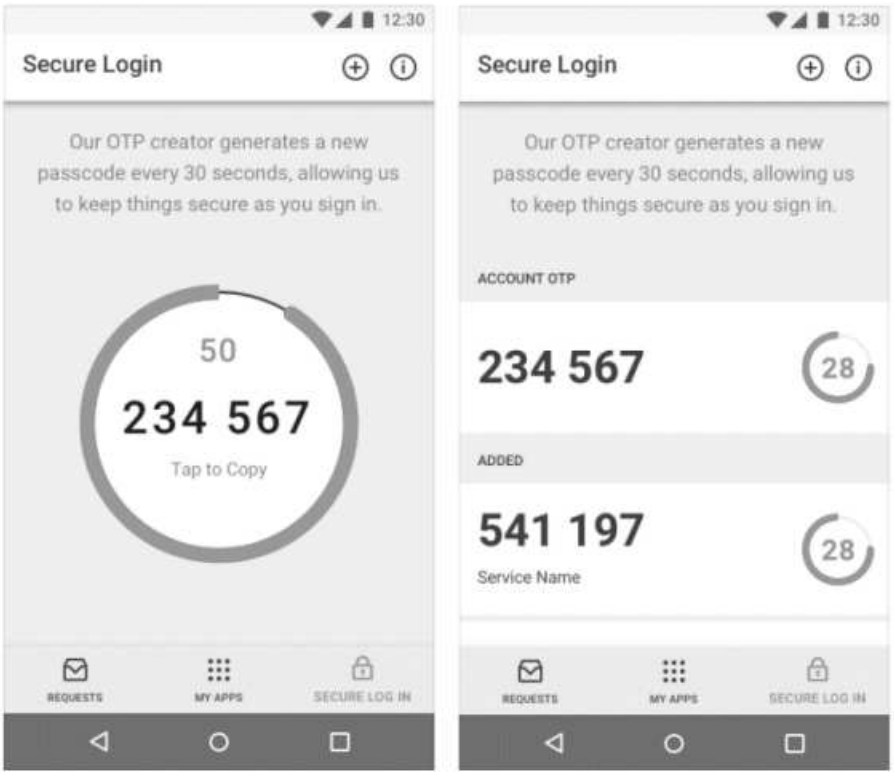


使用一次性密码登录：

使用 OTP 代码登录。

过程

在您的设备上找到并打开 IBM 移动应用，点击**安全登录**，然后选择您要使用的 OTP 生成服务。



可通过扫描 QR 代码或手动输入代码来添加 OTP 生成服务。

管理您的设备

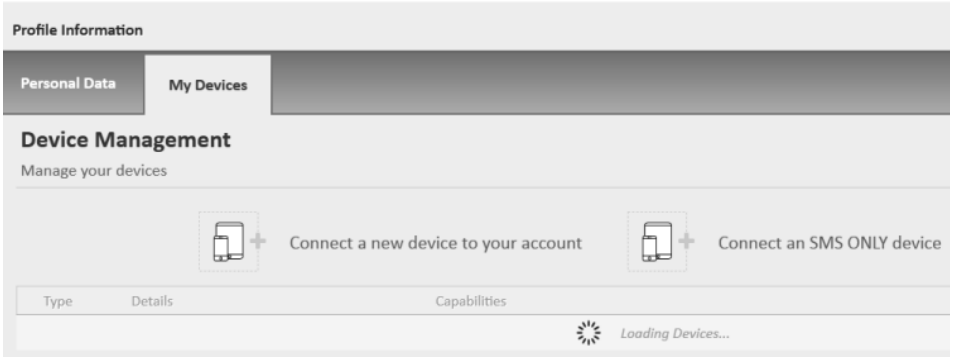
从 Cloud Identity Service 自助服务门户网站注册并管理您的设备。

关于此任务

添加新设备并移除您不再使用的旧设备。通过扫描 QR 代码或手动输入代码，可添加仅启用 SMS 的设备和启用所有方法的设备。您应在首次登录自助服务门户网站时注册设备。

过程

1. 从您的计算机登录自助服务门户网站。
2. 选择**概要文件** > **我的设备**。



3. 添加或移除设备。

删除应用程序

如果不再使用该设备或者不再需要访问 Cloud Identity Service，请删除该应用程序。

关于此任务

注：删除 IBM 移动应用不会移除任何对您的 Cloud Identity Service 帐户有效的两步验证。

过程

1. 在您的设备上找到并选择该 IBM 移动应用。
2. 点击**删除**。

入门

通过下载和安装 IBM 移动应用，然后将您的设备连接至您的 Cloud Identity Service 帐户，开始使用该应用程序。

下载应用程序

在您的设备上安装该应用程序。

过程

1. 启动 App Store (iOS) 或 Google Play Store (Android) 应用程序。
2. 搜索 IBM 移动应用。
3. 点击**获取**和**安装**以下载应用程序。
4. 点击应用程序图标以打开应用程序。

登录

在您的移动设备上登录 Cloud Identity Service 帐户。

关于此任务

可扫描 QR 代码以登录您的帐户，也可使用一次性密码 (OTP) 代码。您的会话到期时，可通过输入用户名和密码再次登录。

使用 *QR* 代码进行登录：

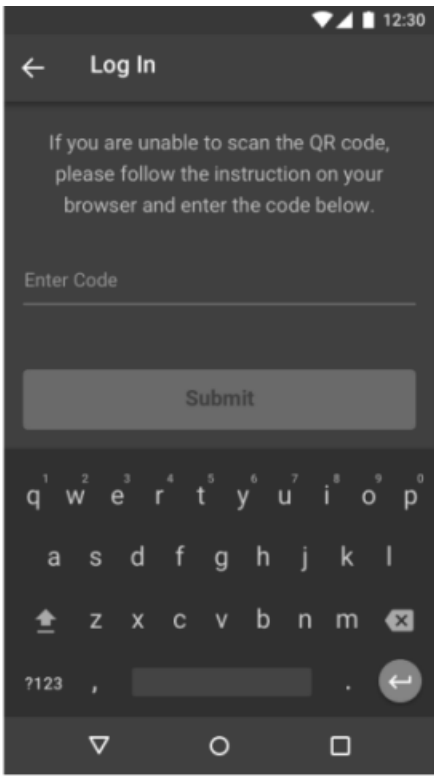
扫描 QR 代码以登录您的帐户。如果无法扫描 QR 代码，那么可手动输入代码。

过程

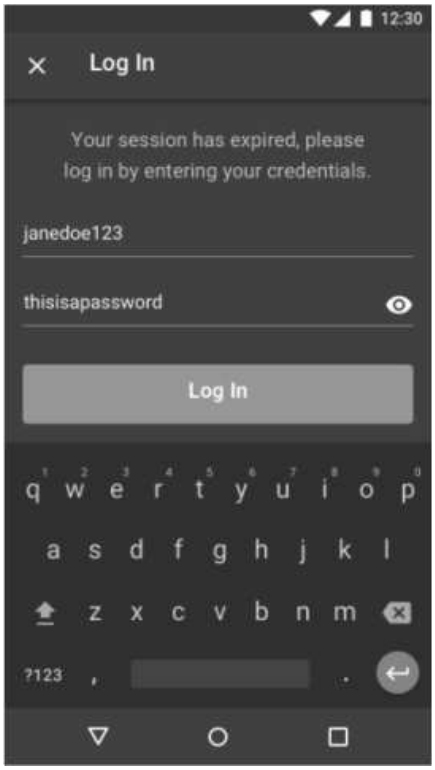
1. 在您的设备上找到并打开 IBM 移动应用，然后点击**登录**。

   系统会向您发送 QR 代码。

2. 在另一设备上，转至 ***company*.ibm.com** 并扫描 QR 代码。如果您无法扫描 QR 代码，点击**无法扫描 QR 代码**并遵循指示信息以手动输入代码。



3. 如果会话到期，请输入用户名和密码，然后点击**登录**。

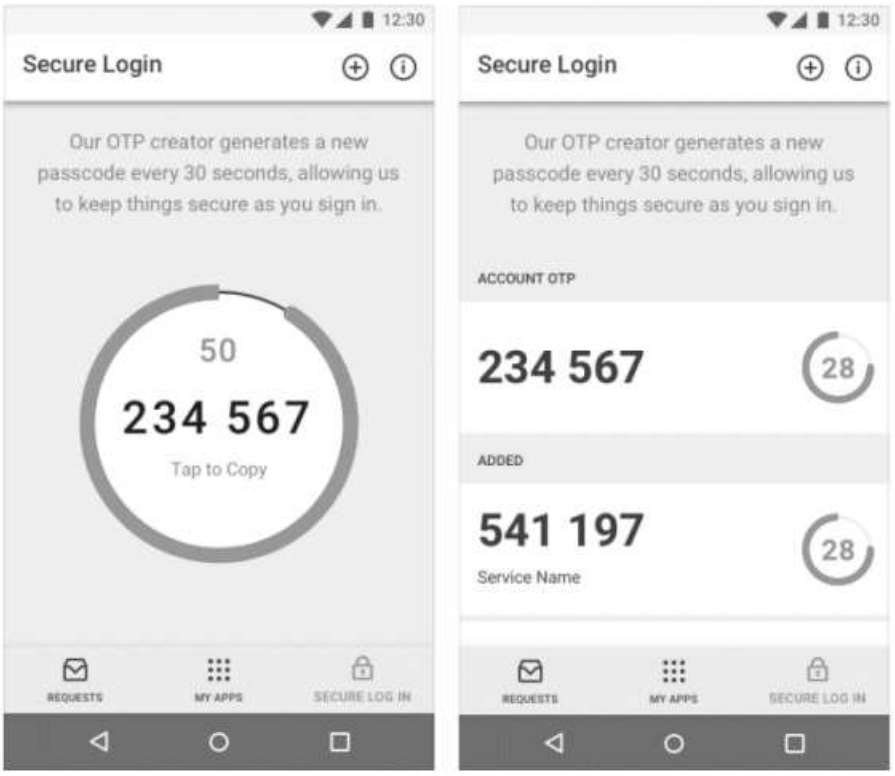


使用一次性密码登录：

使用 OTP 代码登录。

过程

在您的设备上找到并打开 IBM 移动应用，点击**安全登录**，然后选择您要使用的 OTP 生成服务。



可通过扫描 QR 代码或手动输入代码来添加 OTP 生成服务。

管理您的设备

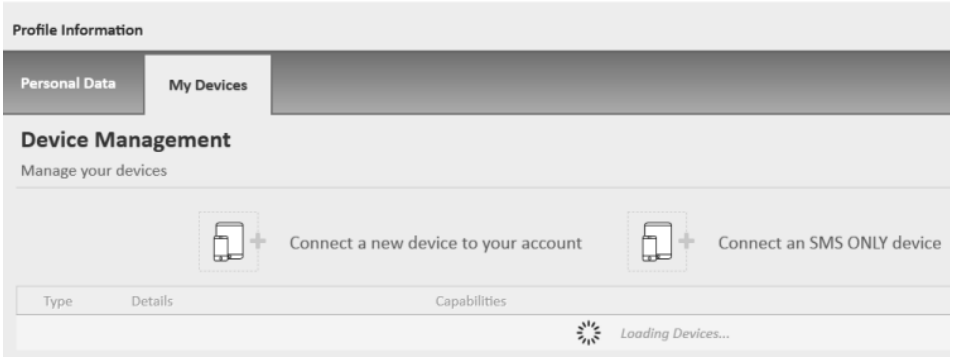
从 Cloud Identity Service 自助服务门户网站注册并管理您的设备。

关于此任务

添加新设备并移除您不再使用的旧设备。通过扫描 QR 代码或手动输入代码，可添加仅启用 SMS 的设备和启用所有方法的设备。您应在首次登录自助服务门户网站时注册设备。

过程

1. 从您的计算机登录自助服务门户网站。
2. 选择**概要文件** > **我的设备**。



3. 添加或移除设备。

删除应用程序

如果不再使用该设备或者不再需要访问 Cloud Identity Service，请删除该应用程序。

关于此任务

注：删除 IBM 移动应用不会移除任何对您的 Cloud Identity Service 帐户有效的两步验证。

过程

1. 在您的设备上找到并选择该 IBM 移动应用。
2. 点击**删除**。

入门

通过下载和安装 IBM 移动应用，然后将您的设备连接至您的 Cloud Identity Service 帐户，开始使用该应用程序。

下载应用程序

在您的设备上安装该应用程序。

过程

1. 启动 App Store (iOS) 或 Google Play Store (Android) 应用程序。
2. 搜索 IBM 移动应用。
3. 点击**获取**和**安装**以下载应用程序。
4. 点击应用程序图标以打开应用程序。

登录

在您的移动设备上登录 Cloud Identity Service 帐户。

关于此任务

可扫描 QR 代码以登录您的帐户，也可使用一次性密码 (OTP) 代码。您的会话到期时，可通过输入用户名和密码再次登录。

使用 *QR* 代码进行登录：

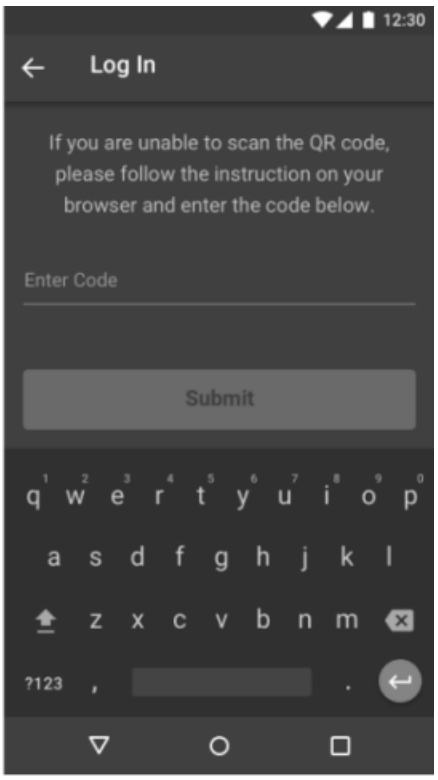
扫描 QR 代码以登录您的帐户。如果无法扫描 QR 代码，那么可手动输入代码。

过程

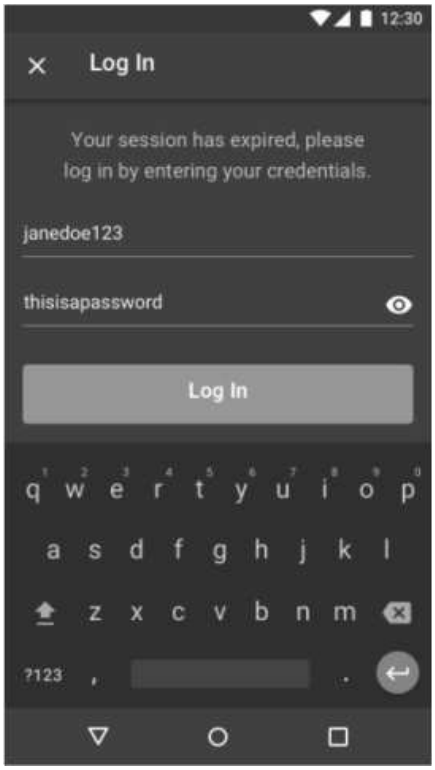
1. 在您的设备上找到并打开 IBM 移动应用，然后点击**登录**。

   系统会向您发送 QR 代码。

2. 在另一设备上，转至 ***company*.ibm.com** 并扫描 QR 代码。如果您无法扫描 QR 代码，点击**无法扫描 QR 代码**并遵循指示信息以手动输入代码。



3. 如果会话到期，请输入用户名和密码，然后点击**登录**。

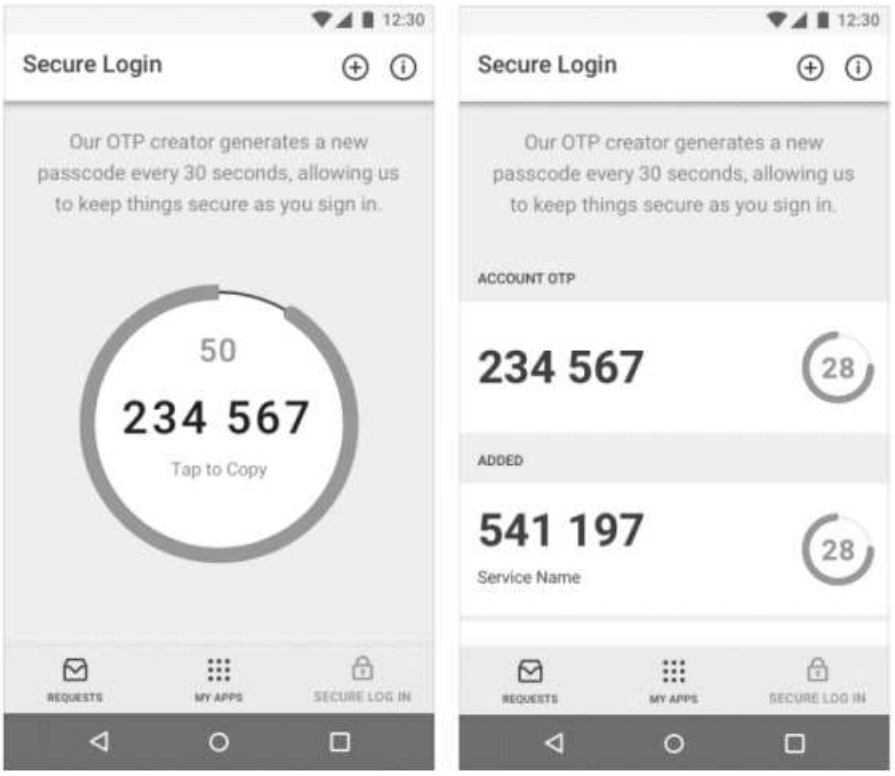


使用一次性密码登录：

使用 OTP 代码登录。

过程

在您的设备上找到并打开 IBM 移动应用，点击**安全登录**，然后选择您要使用的 OTP 生成服务。



可通过扫描 QR 代码或手动输入代码来添加 OTP 生成服务。

管理您的设备

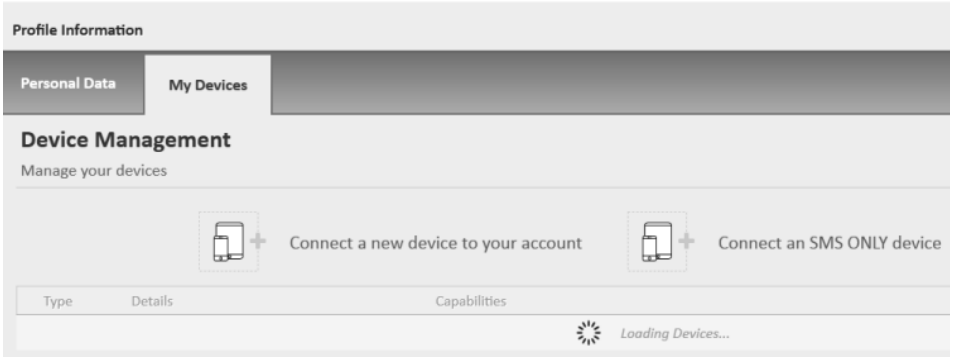
从 Cloud Identity Service 自助服务门户网站注册并管理您的设备。

关于此任务

添加新设备并移除您不再使用的旧设备。通过扫描 QR 代码或手动输入代码，可添加仅启用 SMS 的设备和启用所有方法的设备。您应在首次登录自助服务门户网站时注册设备。

过程

1. 从您的计算机登录自助服务门户网站。
2. 选择**概要文件** > **我的设备**。



3. 添加或移除设备。

删除应用程序

如果不再使用该设备或者不再需要访问 Cloud Identity Service，请删除该应用程序。

关于此任务

注：删除 IBM 移动应用不会移除任何对您的 Cloud Identity Service 帐户有效的两步验证。

过程

1. 在您的设备上找到并选择该 IBM 移动应用。
2. 点击**删除**。

管理服务和启动应用程序

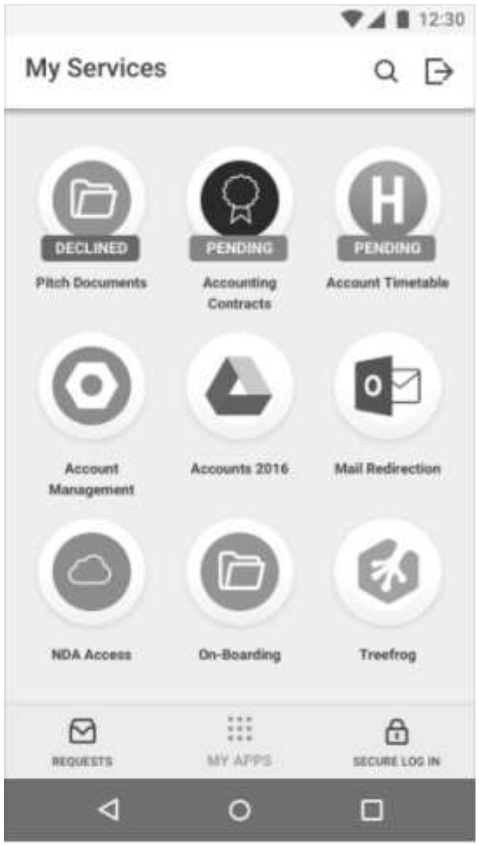
使用 IBM 移动应用查看服务及请求对服务的访问。

查看服务和启动应用程序

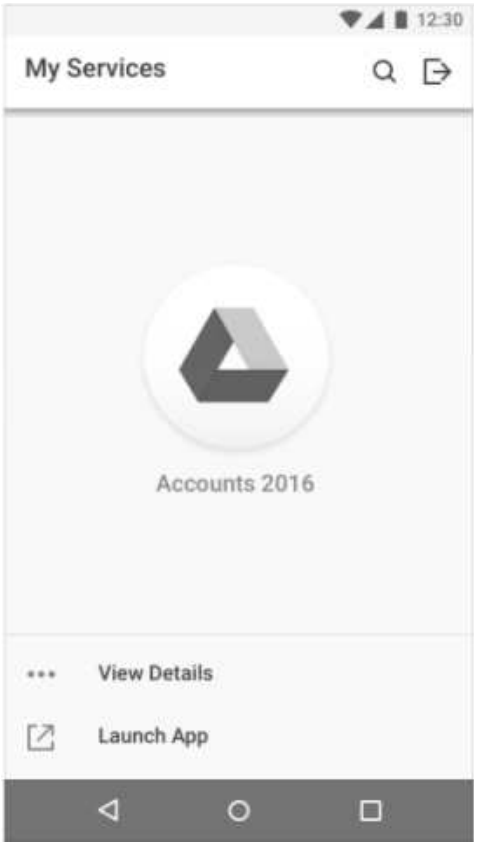
可查看您可访问的服务，并可启动链接的应用程序。

过程

1. 在您的设备上打开 IBM 移动应用，然后点击**我的应用程序**。



2. 点击用于打开服务的图标。



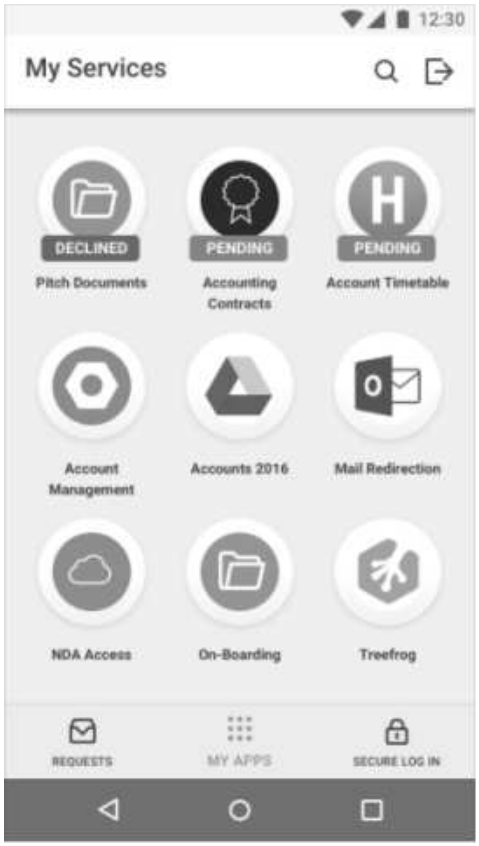
3. 点击**查看详细信息**以查看服务的详细信息，或点击**启动应用程序**以启动链接至该服务的应用程序。

请求对服务的访问

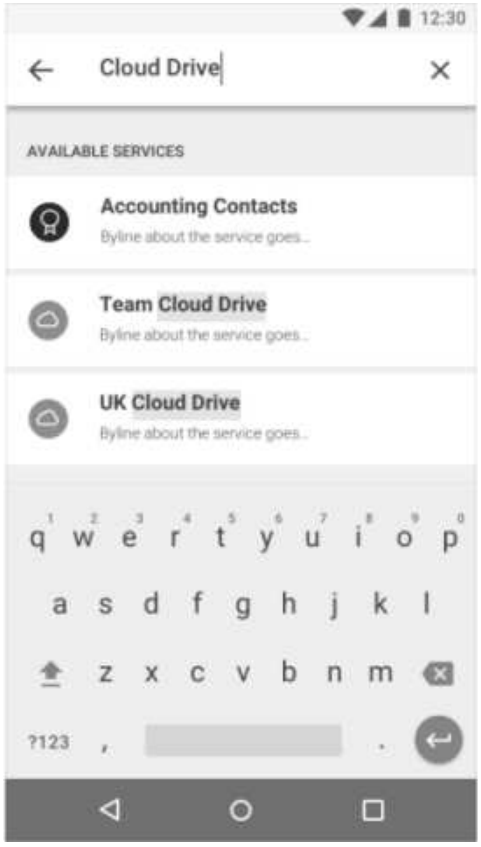
要获取对服务及链接的应用程序的访问，请搜索该服务并提交请求。

过程

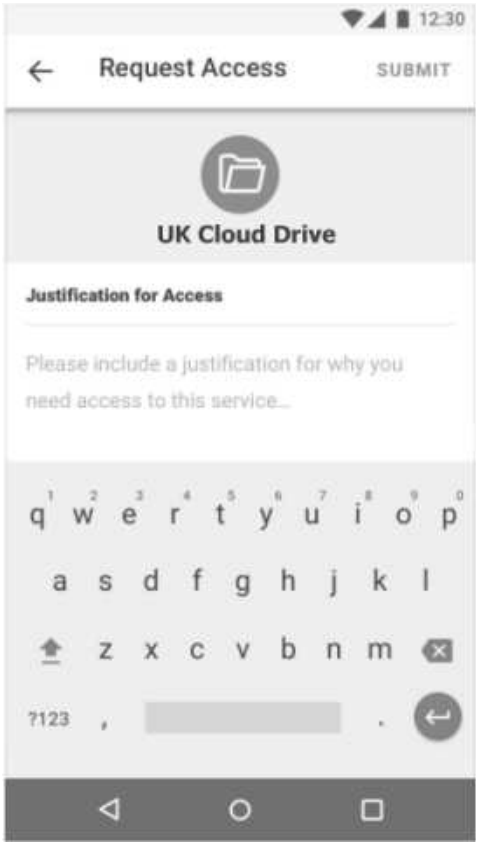
1. 在您的设备上打开 IBM 移动应用，然后点击**我的应用程序**。



2. 从可用服务中搜索该服务。



3. 点击该服务以选择该服务，输入请求该服务的理由，然后点击**提交**。



服务状态将更改为暂挂。您的管理员可接受或拒绝您的请求。

管理服务和启动应用程序

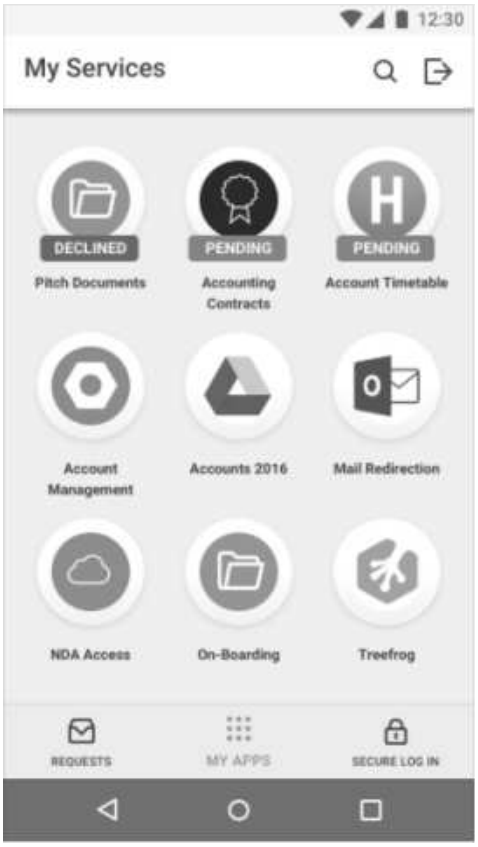
使用 IBM 移动应用查看服务及请求对服务的访问。

查看服务和启动应用程序

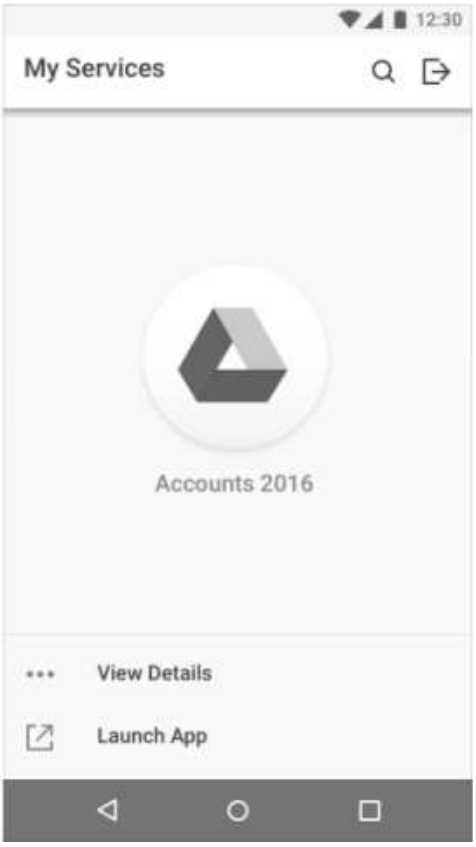
可查看您可访问的服务，并可启动链接的应用程序。

过程

1. 在您的设备上打开 IBM 移动应用，然后点击**我的应用程序**。



2. 点击用于打开服务的图标。



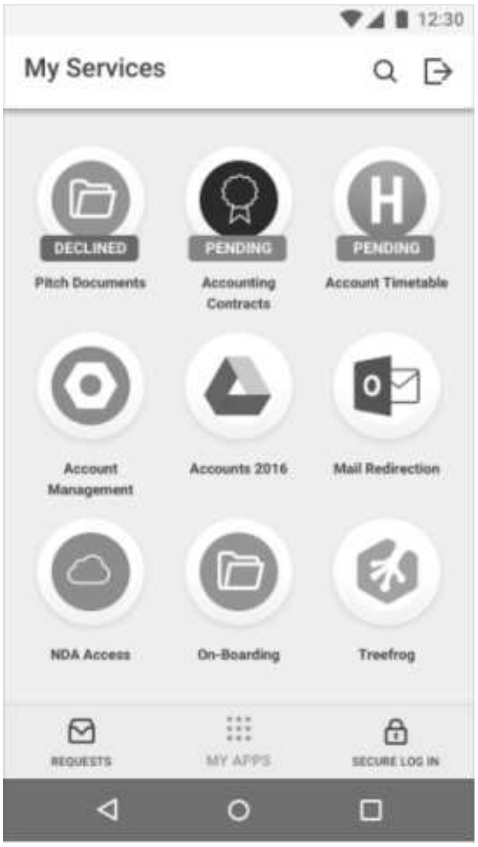
3. 点击**查看详细信息**以查看服务的详细信息，或点击**启动应用程序**以启动链接至该服务的应用程序。

请求对服务的访问

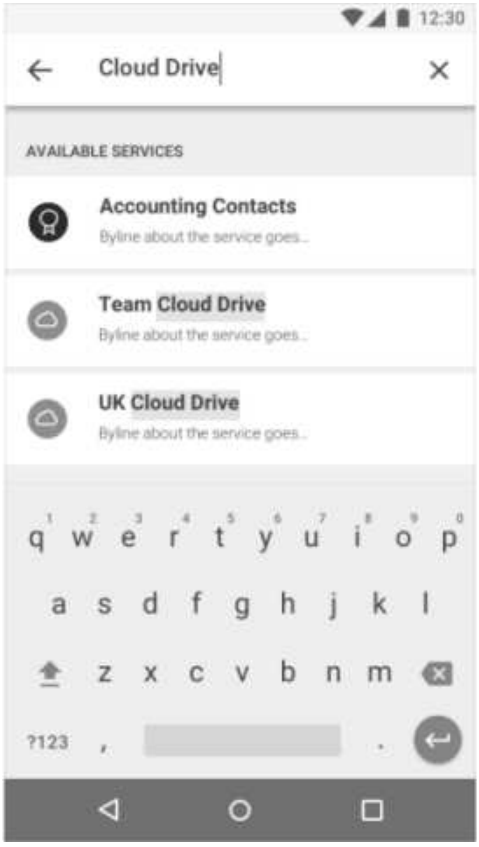
要获取对服务及链接的应用程序的访问，请搜索该服务并提交请求。

过程

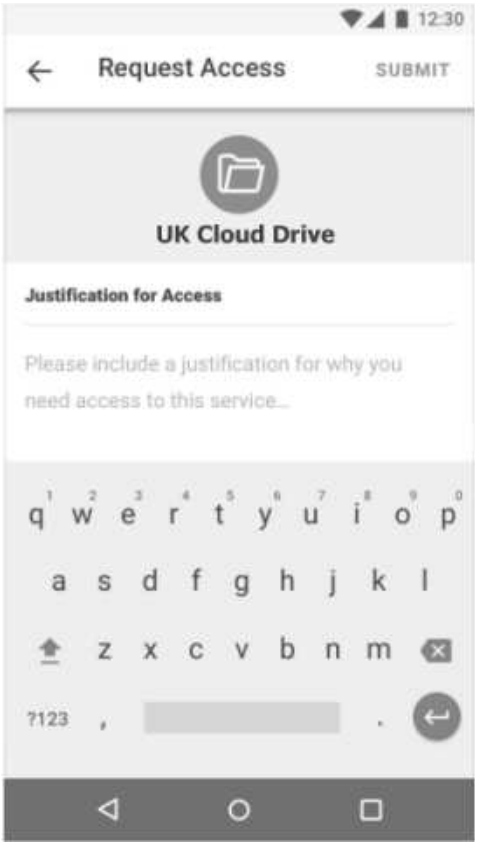
1. 在您的设备上打开 IBM 移动应用，然后点击**我的应用程序**。



2. 从可用服务中搜索该服务。



3. 点击该服务以选择该服务，输入请求该服务的理由，然后点击**提交**。



服务状态将更改为暂挂。您的管理员可接受或拒绝您的请求。

管理服务和启动应用程序

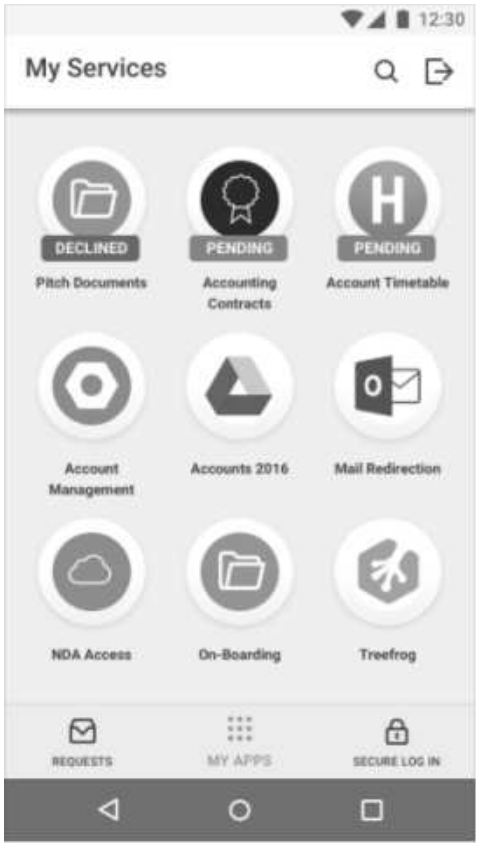
使用 IBM 移动应用查看服务及请求对服务的访问。

查看服务和启动应用程序

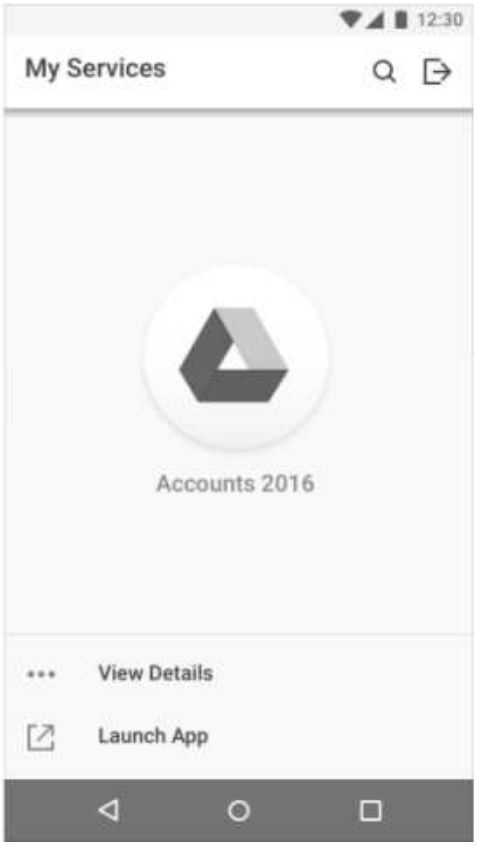
可查看您可访问的服务，并可启动链接的应用程序。

过程

1. 在您的设备上打开 IBM 移动应用，然后点击**我的应用程序**。



2. 点击用于打开服务的图标。



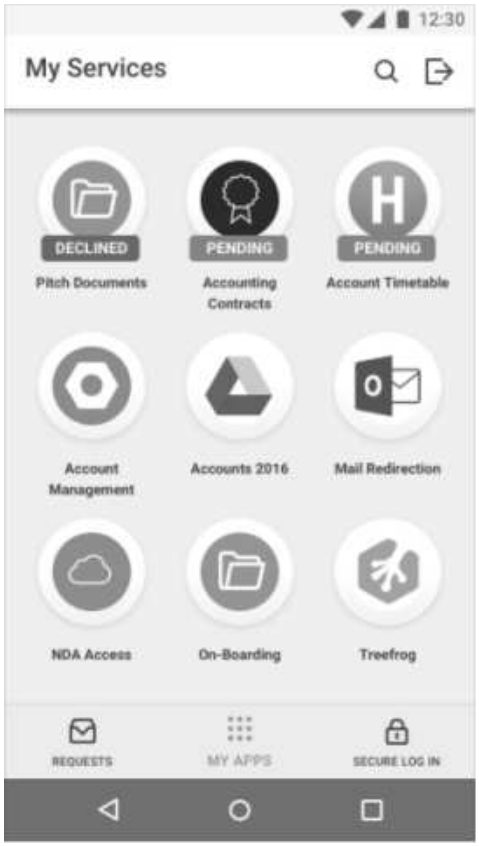
3. 点击**查看详细信息**以查看服务的详细信息，或点击**启动应用程序**以启动链接至该服务的应用程序。

请求对服务的访问

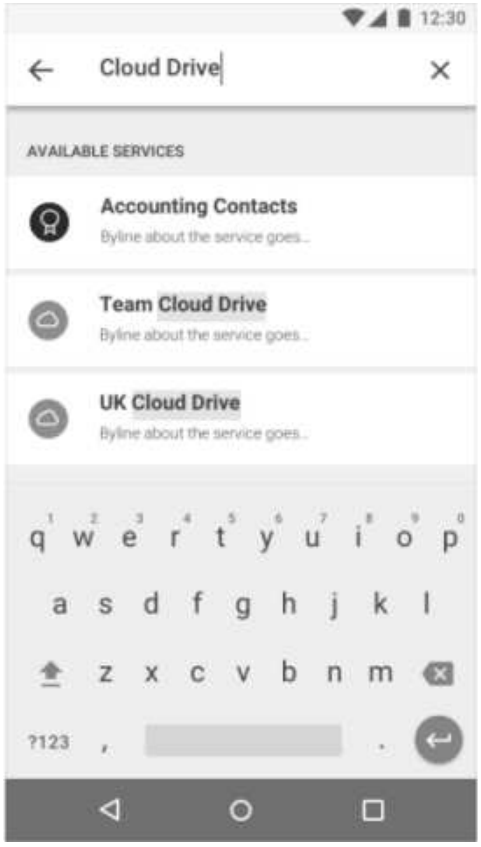
要获取对服务及链接的应用程序的访问，请搜索该服务并提交请求。

过程

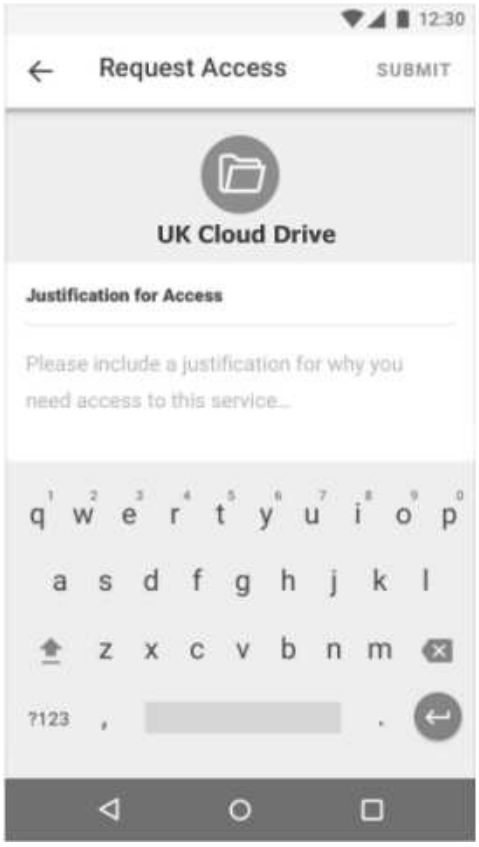
1. 在您的设备上打开 IBM 移动应用，然后点击**我的应用程序**。



2. 从可用服务中搜索该服务。



3. 点击该服务以选择该服务，输入请求该服务的理由，然后点击**提交**。



服务状态将更改为暂挂。您的管理员可接受或拒绝您的请求。

管理请求

使用 IBM 移动应用批准和拒绝服务请求。

关于此任务

此任务可供用户经理批准或拒绝员工的访问服务请求。可通过按员工或服务进行搜索来选择请求。

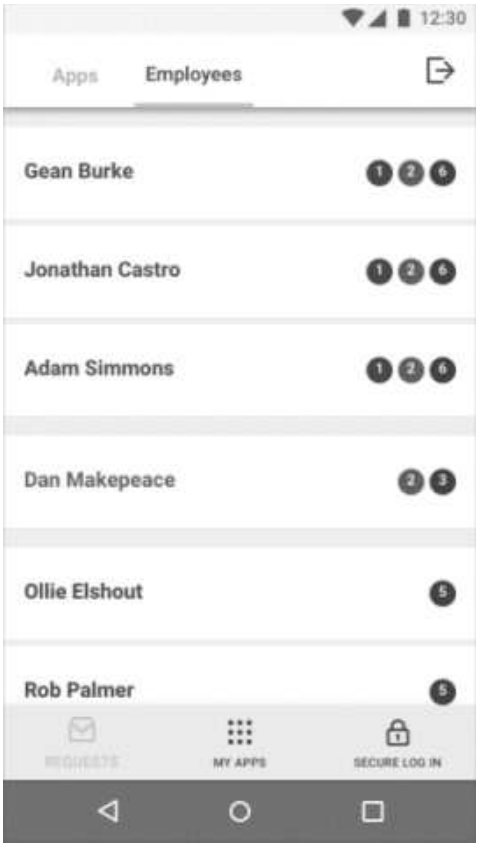
将显示对应每个受管用户的未完成审批的数目及其状态。已过期审批将显示为红色。接近到期审批将显示为黄色。未到期审批或接近过期审批显示为深灰色。

按员工搜索

按员工搜索审批。

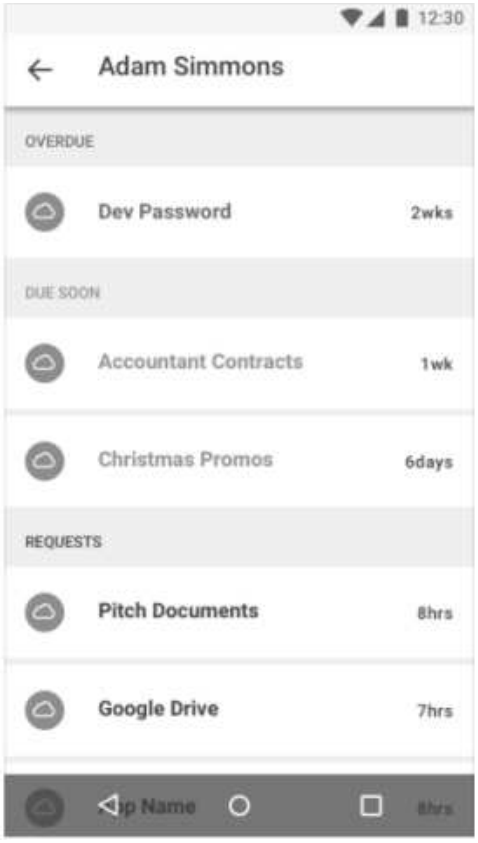
过程

1. 在您的设备上打开 IBM 移动应用，点击**请求**，然后点击**员工**。



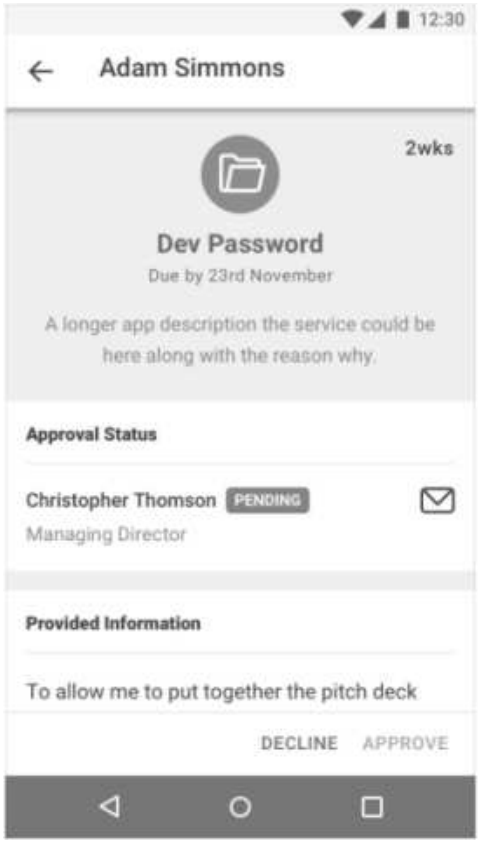
   员工请求是按审批到期日期和时间排序的。具有最多过期请求的员工显示在最前。还会显示请求数目和请求状态。

2. 点击您要管理其请求的员工。

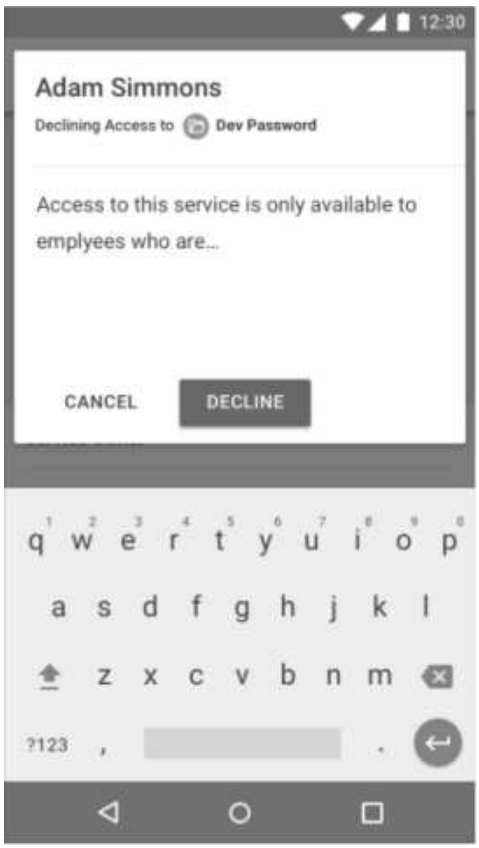


请求现在将按服务及到期日期和时间排序。

3. 点击服务以查看针对该服务的请求。



4. 批准或拒绝请求：
   - 点击**批准**以批准该请求。
   - 点击**拒绝**以拒绝该请求，必要时输入理由。

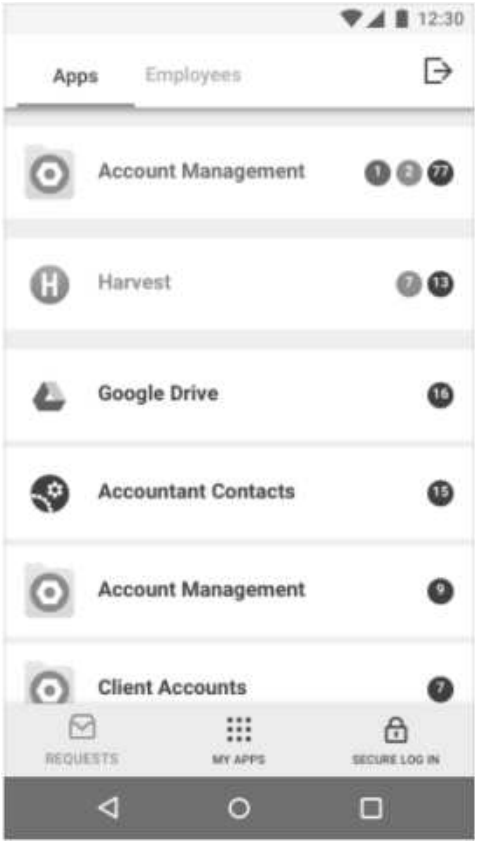


按服务搜索

按服务搜索审批。

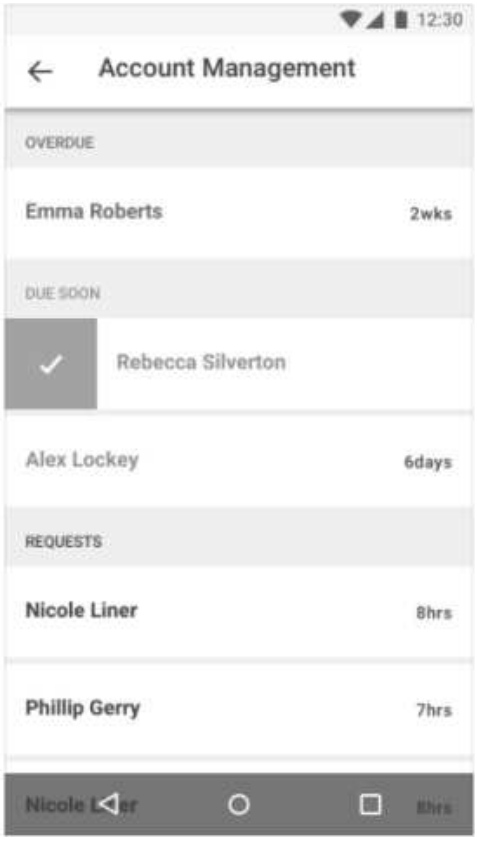
过程

1. 在您的设备上打开 IBM 移动应用，点击**请求**，然后点击**应用程序**。



   请求是按审批到期日期和时间排序的。具有最多过期请求的服务显示在最前。还会显示请求数目和请求状态。

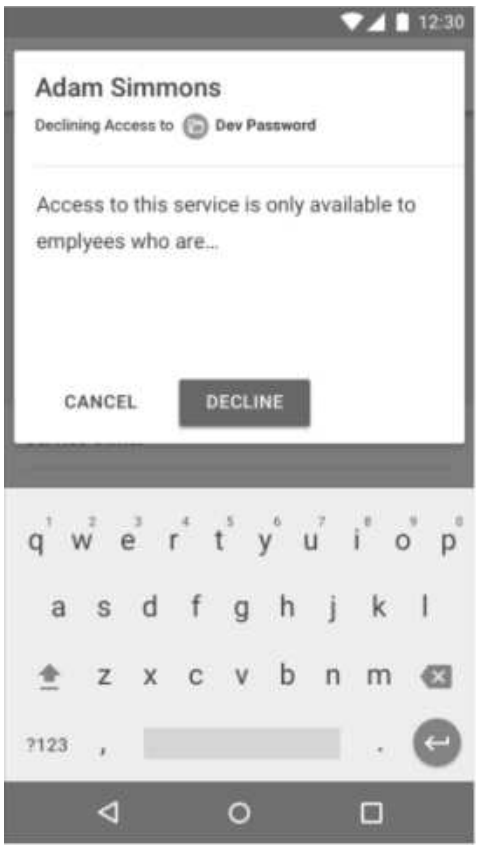
2. 点击您要管理对应请求的服务。



请求现在将按员工及到期日期和时间排序。

3. 选择您要管理其请求的员工，然后批准或拒绝请求：

   - 点击  以批准该请求。
   - 点击  以拒绝该请求，必要时输入理由。



管理请求

使用 IBM 移动应用批准和拒绝服务请求。

关于此任务

此任务可供用户经理批准或拒绝员工的访问服务请求。可通过按员工或服务进行搜索来选择请求。

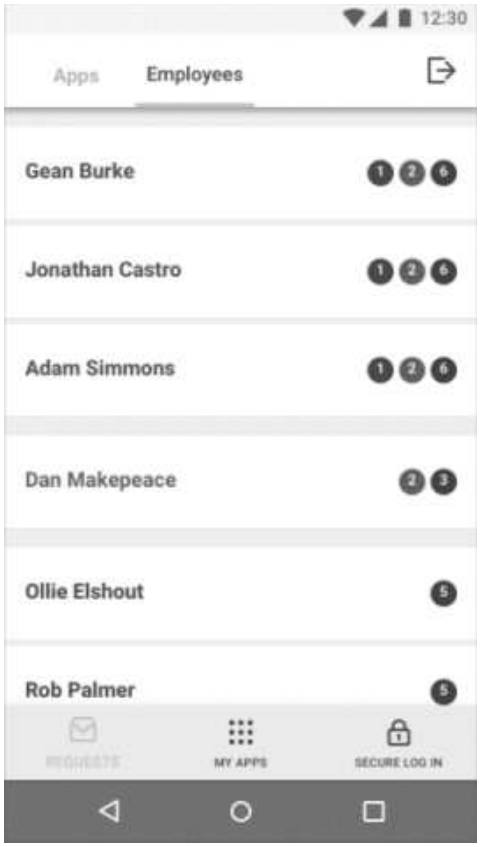
将显示对应每个受管用户的未完成审批的数目及其状态。已过期审批将显示为红色。接近到期审批将显示为黄色。未到期审批或接近过期审批显示为深灰色。

按员工搜索

按员工搜索审批。

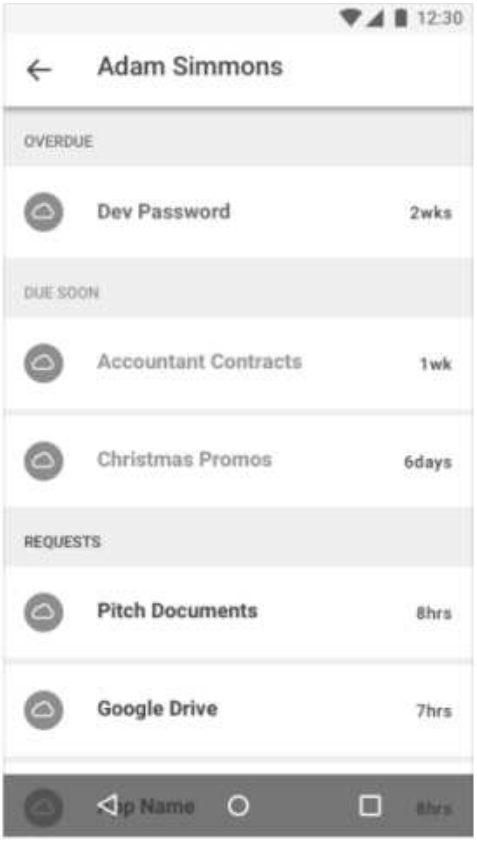
过程

1. 在您的设备上打开 IBM 移动应用，点击**请求**，然后点击**员工**。



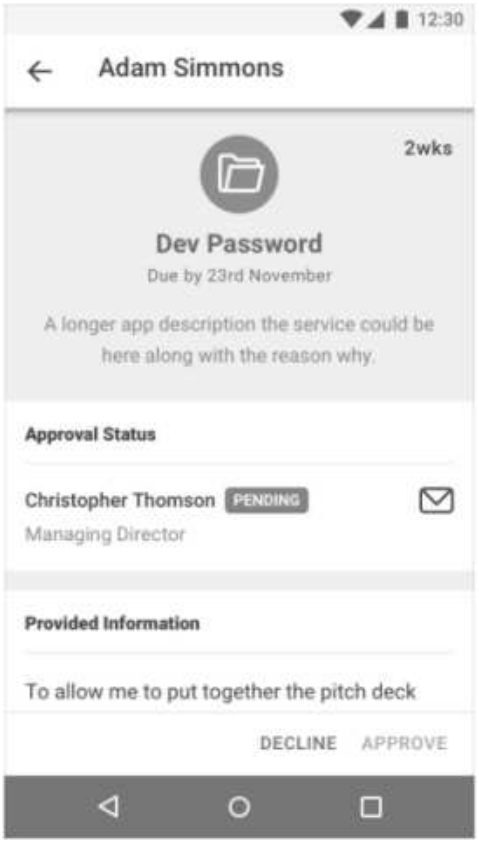
   员工请求是按审批到期日期和时间排序的。具有最多过期请求的员工显示在最前。还会显示请求数目和请求状态。

2. 点击您要管理其请求的员工。

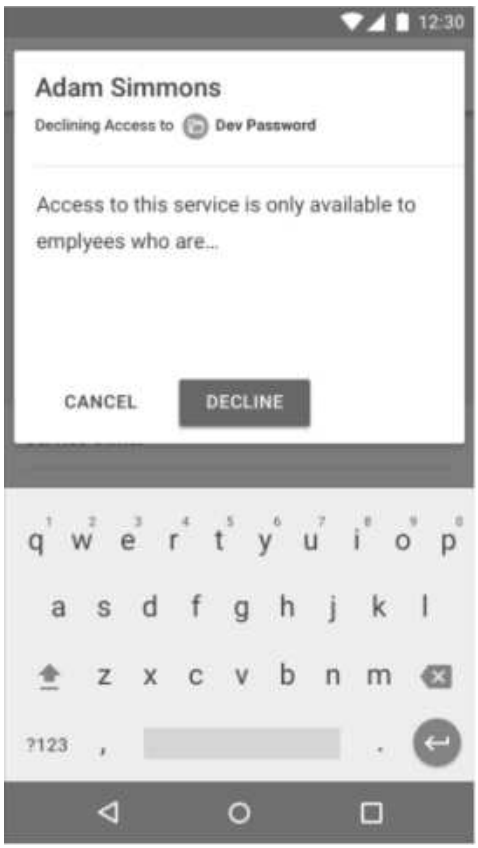


请求现在将按服务及到期日期和时间排序。

3. 点击服务以查看针对该服务的请求。



4. 批准或拒绝请求：
   - 点击**批准**以批准该请求。
   - 点击**拒绝**以拒绝该请求，必要时输入理由。

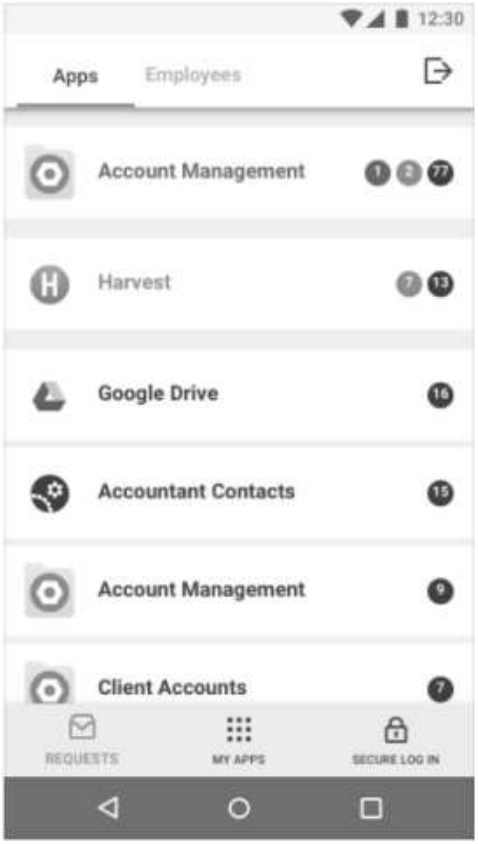


按服务搜索

按服务搜索审批。

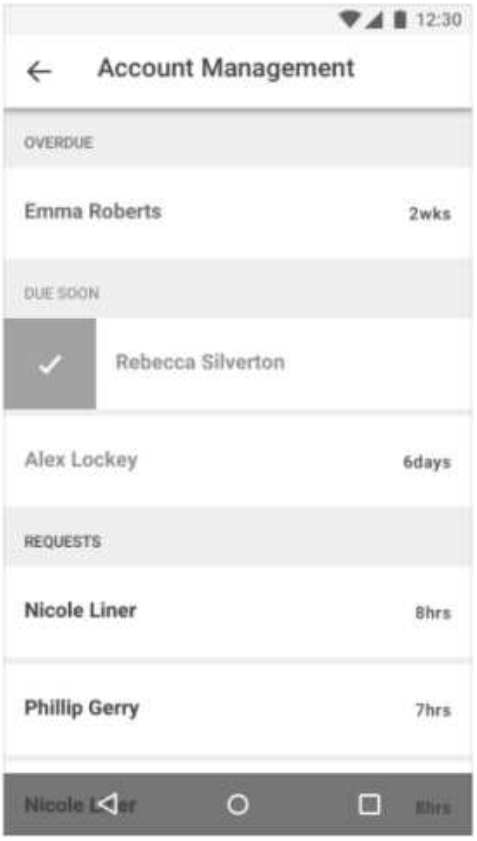
过程

1. 在您的设备上打开 IBM 移动应用，点击**请求**，然后点击**应用程序**。



   请求是按审批到期日期和时间排序的。具有最多过期请求的服务显示在最前。还会显示请求数目和请求状态。

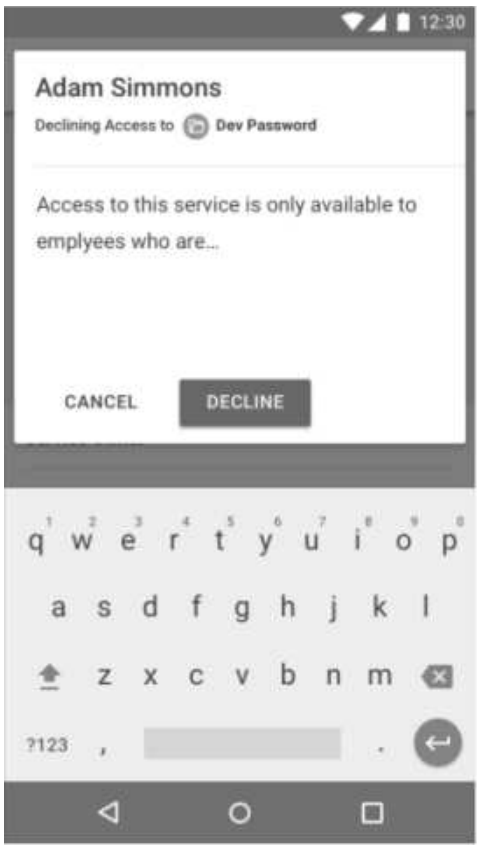
2. 点击您要管理对应请求的服务。



请求现在将按员工及到期日期和时间排序。

3. 选择您要管理其请求的员工，然后批准或拒绝请求：

   - 点击  以批准该请求。
   - 点击  以拒绝该请求，必要时输入理由。



管理请求

使用 IBM 移动应用批准和拒绝服务请求。

关于此任务

此任务可供用户经理批准或拒绝员工的访问服务请求。可通过按员工或服务进行搜索来选择请求。

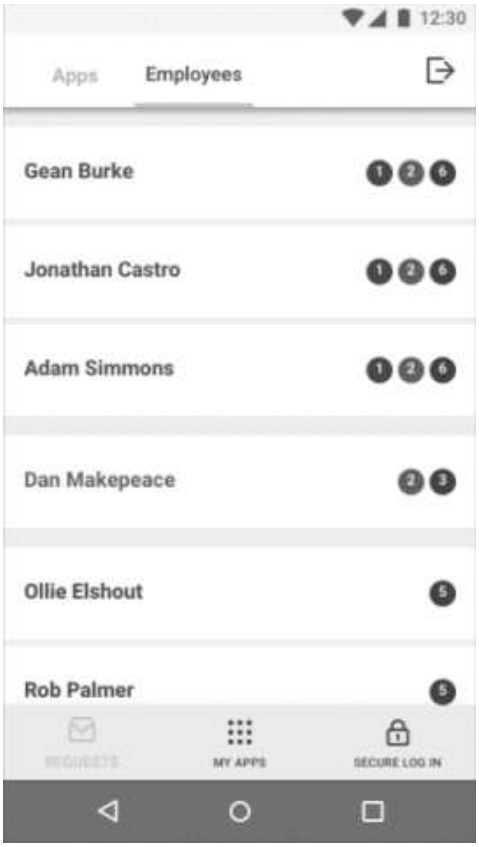
将显示对应每个受管用户的未完成审批的数目及其状态。已过期审批将显示为红色。接近到期审批将显示为黄色。未到期审批或接近过期审批显示为深灰色。

按员工搜索

按员工搜索审批。

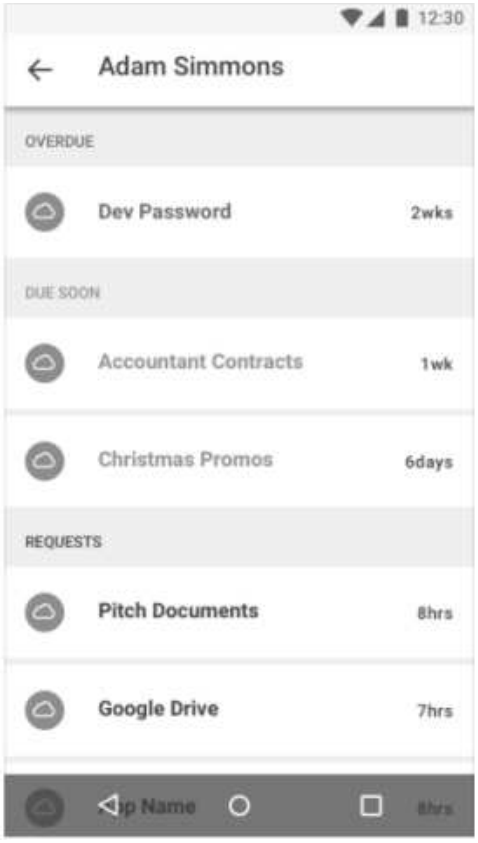
过程

1. 在您的设备上打开 IBM 移动应用，点击**请求**，然后点击**员工**。



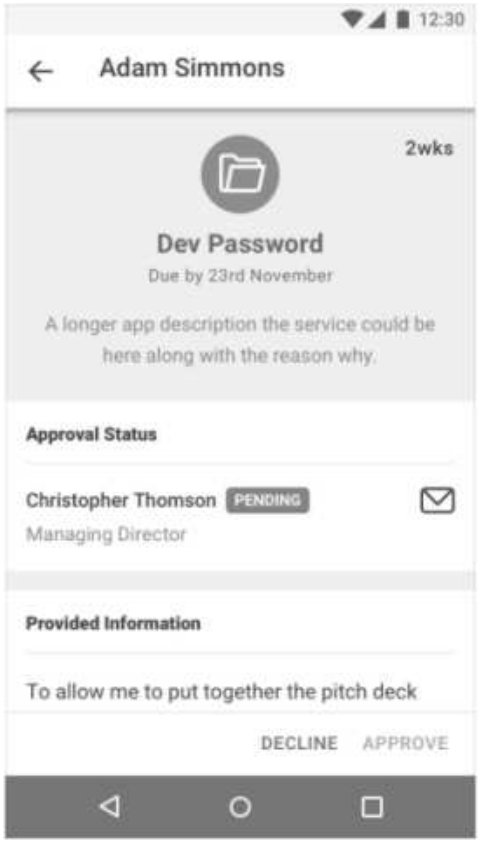
   员工请求是按审批到期日期和时间排序的。具有最多过期请求的员工显示在最前。还会显示请求数目和请求状态。

2. 点击您要管理其请求的员工。

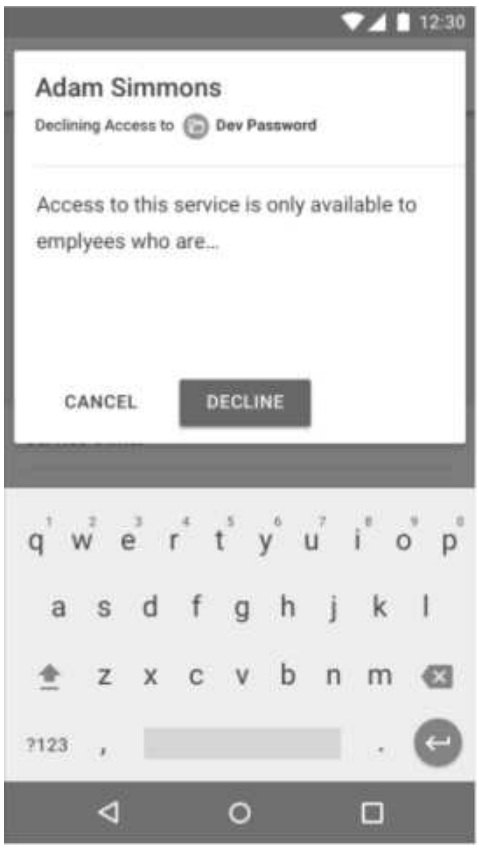


请求现在将按服务及到期日期和时间排序。

3. 点击服务以查看针对该服务的请求。



4. 批准或拒绝请求：
   - 点击**批准**以批准该请求。
   - 点击**拒绝**以拒绝该请求，必要时输入理由。

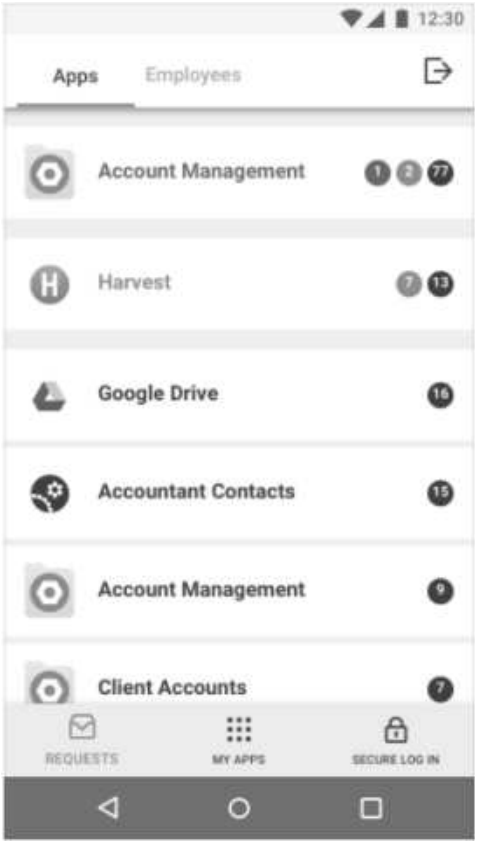


按服务搜索

按服务搜索审批。

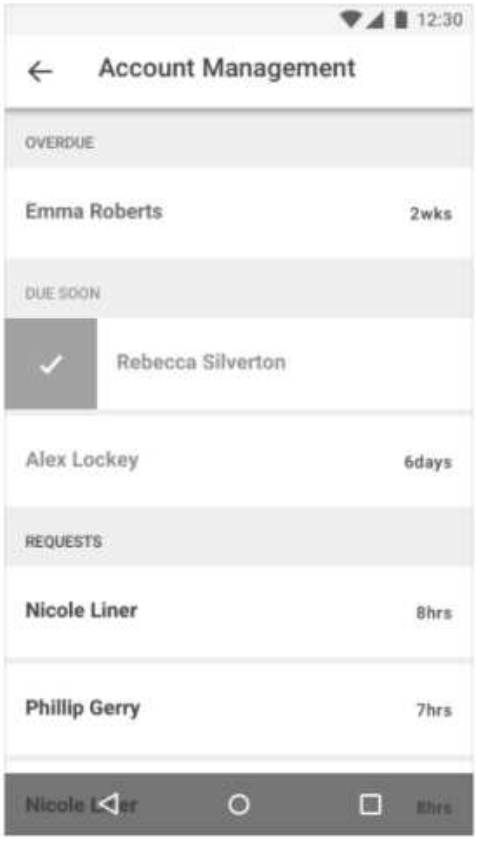
过程

1. 在您的设备上打开 IBM 移动应用，点击**请求**，然后点击**应用程序**。



   请求是按审批到期日期和时间排序的。具有最多过期请求的服务显示在最前。还会显示请求数目和请求状态。

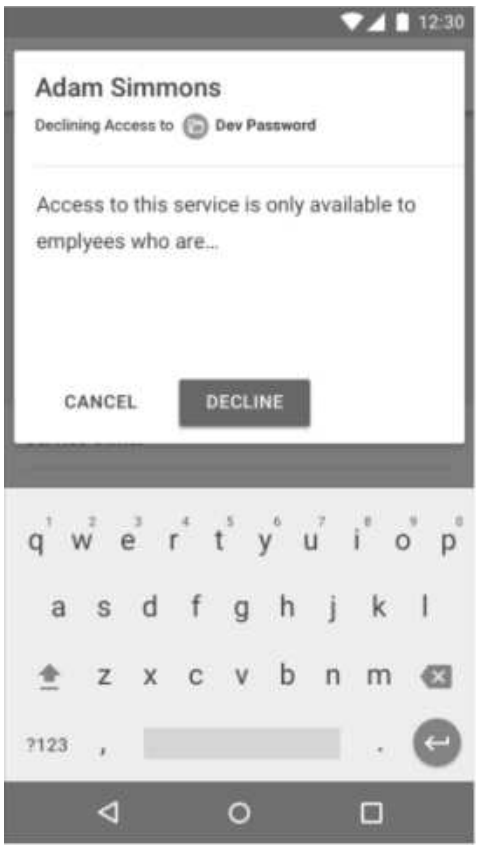
2. 点击您要管理对应请求的服务。



请求现在将按员工及到期日期和时间排序。

3. 选择您要管理其请求的员工，然后批准或拒绝请求：

   - 点击  以批准该请求。
   - 点击  以拒绝该请求，必要时输入理由。


12:30
Adam Simmons
Declining Access to Dev Password
Access to this service is only available to emplyees who are...
CANCEL
DECLINE
?123

第 9 章 策略

策略用于确定或优化用户对不同资源的访问。

创建全局用户策略

用户策略定义用户的最大登录失败次数、最长密码寿命和帐户到期日期。全局用户策略应用于所有用户。

过程

1. 在导航窗格中，单击**策略** > **全局用户策略**。
2. 设置您所需的用户策略设置。
3. 单击**保存**。

用户策略设置

表 *41.* 用户策略设置

设置	描述
最大登录失败次数	在帐户被锁定之前，用户可以尝试的最大登录失败次数。如果此选项设置为 0 或"未设置"，那么表示不限制登录失败尝试次数。 • **设置**。最大登录失败尝试次数。如果此选项设置为 0，那么表示不限制登录失败尝试次数。 • **未设置**。不限制登录失败尝试次数。
禁用时间间隔	指定超过"最大登录失败次数"计数之后是否锁定用户帐户。 • **设置**。超过"最大登录失败次数"计数之后锁定用户帐户。帐户被永久或暂时禁用。 • **未设置**。永远不会因为登录失败尝试而锁定用户帐户。"未设置"等同于将"最大登录失败次数"设置为 0 或"未设置"，用户可以进行无限次登录尝试。 • **永久禁用**。用户被永久锁定，直到 Cloud Identity Portal 管理员将该用户的用户状态设置为有效为止。 • **暂时禁用**。以秒为单位表示的时间，在此期间，用户帐户将在超过"最大登录失败次数"计数之后保持锁定状态。该帐户将在经过此时间间隔之后解锁。
最小长度	有效帐户密码所需的最少字符数。 • **设置**。密码的最少字符数。 • **未设置**。无最小密码长度。

© Copyright IBM Corp. 2015, 2017

表 41. 用户策略设置（续）

设置	描述
最少字母数	帐户密码所需的最少字母字符数。 • **设置**。密码必须包含的最少字母字符数。 • **未设置**。不限制最小值。
最少非字母数	帐户密码所需的最少非字母字符（数字或特殊字符）数。 • **设置**。密码必须包含的最少非字母字符数。如果设置为 0，那么不限制最小值。 • **未设置**。不限制最小值。
最大重复字符数	帐户密码中允许的最大连续重复字符数。 • **设置**。允许的最大重复字符数。 • **未设置**。不限制重复字符数。
允许空格?	指定帐户密码是否可以包含空格。 • **设置**。指定是否允许空格。 – **是**。允许空格。 – **否**。不允许空格。 • **未设置**。允许空格。
密码到期?	密码创建之后保持有效的最长时间，之后将到期且必须更改。 • **是**。密码有效的天、小时、分钟和秒数。如果所有值都设置为 0，那么密码永不到期。 • **否**。密码永不到期。
跟踪密码复用?	指定重置密码时是否可以使用相同密码。 • **是**。用户重置或更改其密码时，不能使用相同密码。请指定新的唯一密码的数目，必须先设置此数目，然后才能复用旧密码。 • **否**。用户重置其密码时，可以使用相同密码。
帐户到期?	指定一个到期日期，在此日期之后所有帐户都设置为无效。该设置通常仅用于个人用户策略覆盖。例如，如果某个合同商对特定资源具有有限的访问期限，那么可以使用此选项来禁用特定日期的此访问权。 • **设置**。帐户的到期日期。以 YYYY/MM/DD 格式输入日期。 • **未设置**。有效期不受限，帐户有效性永不到期。
限制访问权?	指定用户可以访问系统的一天中具体时间约束。 • **是**。用户可以访问 Cloud Identity Service 的日期和一天中的具体时间。时间可以服务的本地时间或全球标准时间表示。 • **否**。用户可以随时访问 Cloud Identity Service。

第 10 章 身份监管

通常，请求在自助服务应用程序中由指定的管理者管理。需要时，管理员可以在 Cloud Identity Portal 中管理用户请求。

如果常规核准人不可用且没有委派核准人，Cloud Identity Portal 管理员可能需要管理服务的用户请求。

搜索请求

在想要批准、重新分配或拒绝请求时搜索请求。还可以向请求核准人发送提示。

过程

1. 在导航窗格中，单击**身份监管** > **请求管理**。
2. 在**优化结果**字段中，输入搜索条件。

   您可以搜索为其发起请求的人员名字或姓氏的前 3 个或更多字符。还可以搜索核准人的名字或姓氏的前 3 个或更多字符。例如，要搜索名为 John Smith 的核准人的请求，可以输入 `smi` 或 `joh`。

   这样将列出与您的搜索条件匹配的请求。

   可以使用**全部**、**逾期**和**即将到期**复选框来过滤列表。您可以单击列标题以按该列对列表进行排序。

批准、拒绝和重新分配请求

如果核准人没有针对请求执行任何操作，您可以批准、重新分配或拒绝请求。还可以向请求核准人发送提示。

© Copyright IBM Corp. 2015, 2017

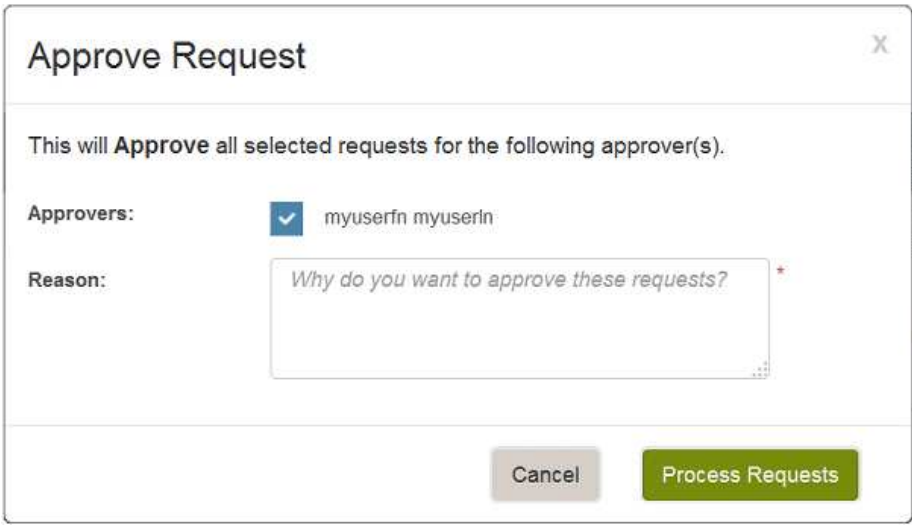
关于此任务

到期审批显示在红色行中。即将到期的审批显示在黄色行中。

过程

1. 搜索请求。
2. 选择请求，单击**操作**菜单，然后选择想要针对请求执行的操作。

- 要批准请求：

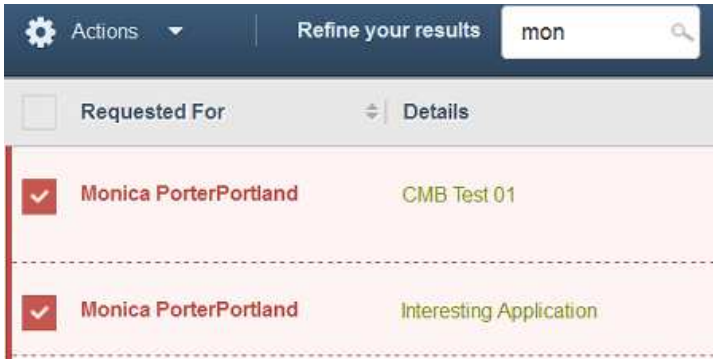


  a. 选择要以其名义批准请求的核准人。
  b. 输入批准请求的原因。
  c. 单击**过程请求**。
- 要重新分配请求：
  a. 选择要以其名义重新分配请求的核准人。
  b. 搜索并选择要将请求重新分配到的用户。

  您可以搜索管理者名字或姓氏的前 3 个或更多字符。
  c. 输入重新分配请求的原因。
  d. 单击**过程请求**。

- 要向核准人发送提示：
  a. 选择要将提示发送到的核准人。
  b. 输入发送提示的原因。
  c. 单击**过程请求**。

您还可以选择所需请求复选框针对多个请求执行操作。



您可以使用列标题中的复选框来选择所有请求。使用列标题中的**操作**菜单以针对多个请求执行操作。

声明

本信息是为在美国国内供应的产品和服务而编写的。

IBM 可能在其他国家或地区不提供本文档中讨论的产品、服务或功能特性。有关您所在区域当前可获得的产品和服务的信息，请向您当地的 IBM 代表咨询。任何对 IBM 产品、程序或服务的引用并非意在明示或暗示只能使用 IBM 的产品、程序或服务。只要不侵犯 IBM 的知识产权，任何同等功能的产品、程序或服务，都可以代替 IBM 产品、程序或服务。但是，评估和验证任何非 IBM 产品、程序或服务的操作，由用户自行负责。

IBM 可能已拥有或正在申请与本文档内容有关的各项专利。提供本文档并不意味着授予用户使用这些专利的任何许可。您可以用书面形式将许可查询寄往：

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

有关双字节字符集 (DBCS) 信息的许可查询，请与您所在国家或地区的 IBM 知识产权部门联系，或用书面方式将查询寄往：

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

以下段落对于英国和与当地法律有不同规定的其他国家或地区均不适用：INTERNATIONAL BUSINESS MACHINES CORPORATION"按现状"提供本出版物，不附有任何种类的（无论是明示的还是暗含的）保证，包括但不限于暗含的有关非侵权、适销和适用于某特定用途的保证。某些国家或地区在某些交易中不允许免除明示或暗含的保证。因此本条款可能不适用于您。

本信息可能包含技术方面不够准确的地方或印刷错误。本信息将定期更改；这些更改将编入本信息的新版本中。IBM 可以随时对本出版物中描述的产品和/或程序进行改进和/或更改，而不另行通知。

本信息中对任何非 IBM Web 站点的引用都只是为了方便起见才提供的，不以任何方式充当对那些 Web 站点的保证。那些 Web 站点中的资料不是 IBM 产品资料的一部分，使用那些 Web 站点带来的风险将由您自行承担。

IBM 可以按它认为适当的任何方式使用或分发您所提供的任何信息而无须对您承担任何责任。

本程序的被许可方如果要了解有关程序的信息以达到如下目的：(i) 使其能够在独立创建的程序和其它程序（包括本程序）之间进行信息交换，以及 (ii) 使其能够对已经交换的信息进行相互使用，请与下列地址联系：

© Copyright IBM Corp. 2015, 2017

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 79758 U.S.A

只要遵守适当的条件和条款，包括某些情形下的一定数量的付费，都可获得这方面的信息。

本资料中描述的许可程序及其所有可用的许可资料均由 IBM 依据 IBM 客户协议、IBM 国际程序许可协议或任何同等协议中的条款提供。

涉及非 IBM 产品的信息可从这些产品的供应商、其出版说明或其他可公开获得的 资料中获取。IBM 没有对这些产品进行测试，也无法确认其性能的精确性、兼容性或任何其他关于非 IBM 产品的声明。有关非 IBM 产品性能的问 题应当向这些产品的供应商提出。

所有关于 IBM 未来方向或意向的声明都可随时更改或收回，而不另行通知，它们仅仅表示了目标和意愿而已。

本信息包含在日常业务操作中使用的数据和报告的示例。为了尽可能完整地说明这些示例，示例中可能会包括个人、公司、品牌和产品的名称。所有这些名字都是虚构的，若现实生活中实际业务企业使用的名字和地址与此相似，纯属巧合。

商标

IBM、IBM 徽标和 ibm.com 是 International Business Machines Corp., 在全球许多管辖区域的商标或注册商标。其他产品和服务名称可能是 IBM 或其他公司的商标。当前的 IBM 商标列表，可从 Web 站点 www.ibm.com/legal/copytrade.shtml 上『版权和商标信息』部分获取。

Adobe、Adobe 徽标、PostScript 和 PostScript 徽标是 Adobe Systems Incorporated 在美国和/或其他国家或地区的注册商标或商标。

Java 和所有基于 Java 的商标和徽标是 Oracle 和/或其子公司的商标或注册商标。

Microsoft、Windows、Windows NT 和 Windows 徽标是 Microsoft Corporation 在美国和/或其他国家或地区的商标。

Printed in China