08 - 模块 8：保护数据安全

模块 8：保护数据安全

模块简介（模块 8）：
在此模块中，您将学习如何保护应用程序的安全性。

讲座 8.1：简介
安全性是应用程序最重要的方面之一，因为错误配置或设置安全性失败会给利益相关者带来严重的后果。Mendix 通过 Mendix 云平台级别处理基本的安全性来帮助您。虽然这一功能有帮助，但安全性的某些部分是针对应用程序的。这些部分在开发过程中必须进行配置。Mendix 安全系统通过安全配置选项使此过程变得简单。不过，不要被愚弄了；设置安全性仍然可能很复杂。幸运的是，您将在此模块中学习正确设置安全性所需的全部知识。我们将探讨：

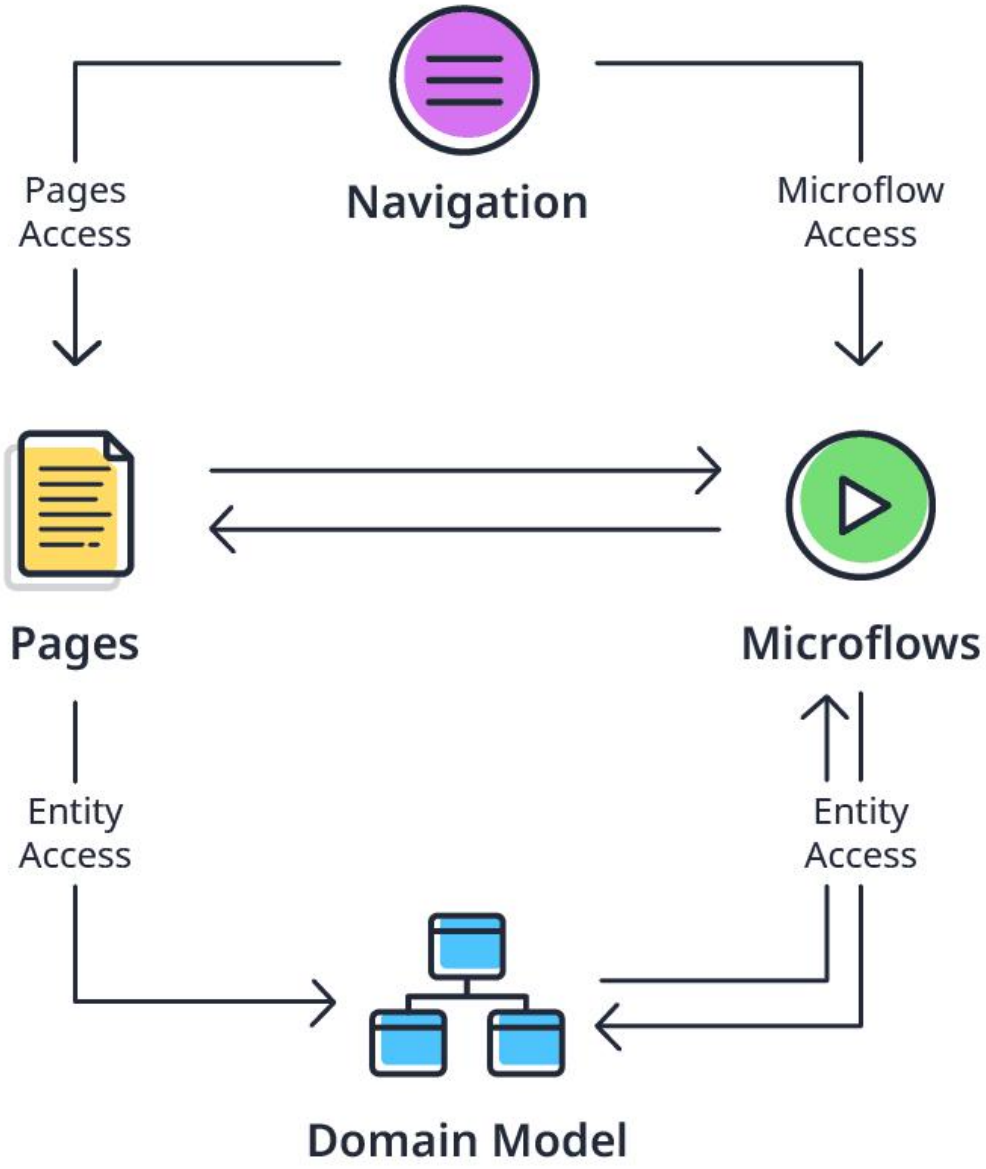
- Mendix 授权模型
- 为您自己的模块设置模块安全性
- 配置项目安全性

讲座 8.2：Mendix 安全性基础知识
在安全性方面，有两个重要概念：身份验证和授权。身份验证确定用户的身份，而授权则确定用户有权访问的内容。

身份验证
Mendix 提供开箱即用的基本密码身份验证，并通过标准协议（如 OpenID 和 SAML）提供第三方身份验证服务的集成。这样，您就可以将 Mendix 应用程序集成到现有的身份验证环境并配置单点登录 (SSO)。除此之外，您还可以使用 Mendix SSO 模块，以便用户可以使用其 Mendix 帐户登录。

授权
Mendix 授权模型已集成到平台中。这使得它成为一个跨领域的问题。为确保可以轻松将模块集成到应用程序中，Mendix 中的授权分为两部分：*项目安全性*和*模块安全性*。在项目层面，您可以配置一般的安全设置，如密码策略。在模块层面，您可以配置对页面、微流、实体等的访问。您可以通过安全配置屏幕或直接在微流、页面或实体的属性窗格配置安全性。
通过角色的概念将模块安全性与项目安全性连接在一起。当您想使用市场上的一个模块时，您所要做的就是将该模块的角色映射到您在项目中已经配置的角色上。

要了解 Mendix 的安全模型，把它分为四个主要部分是有帮助的，如下所示。用户登录后，导航菜单将只包含通向用户可以访问的页面和微流的按钮。页面上的按钮也是如此；如果它们链接到用户无法访问的页面或微流，则按钮将被隐藏。当涉及到调用其他微流的微流时，情况会发生变化。始终允许微流调用另一个微流。在这种情况下，不会检查模块角色。



在 Mendix 中，可以使用基本密码身份验证。除此之外，您可以使用市场上的 SAML 模块对身份提供者（如活动目录）进行身份验证。要查看可用的选项，请参见市场中的“身份验证”部分。

随着基础知识的掌握，您已经准备好深入了解 Mendix 的安全性。我们来看看如何使用 Mendix Studio Pro 配置安全性。

讲座 8.3：应用程序安全级别

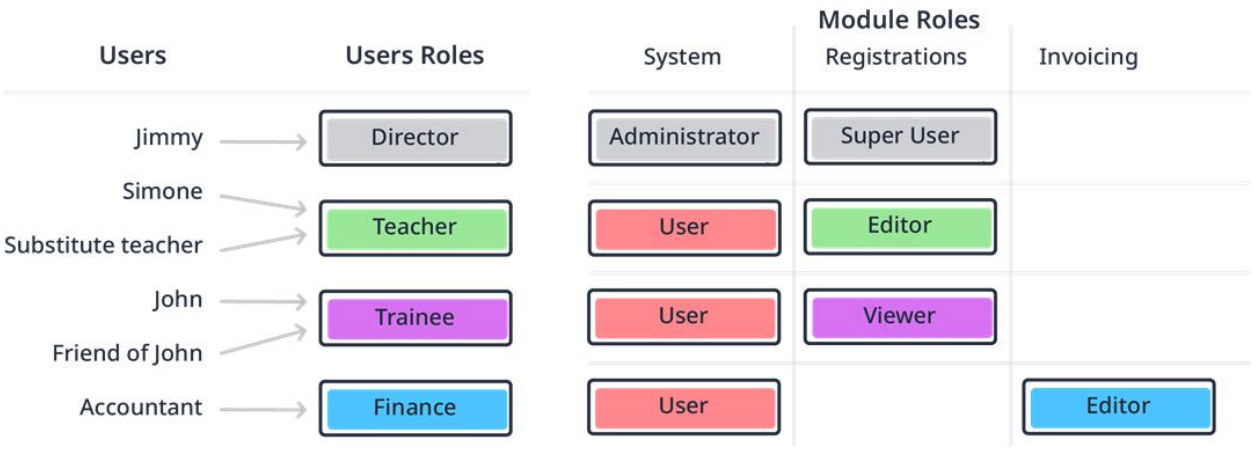
安全性始终应用于整个应用程序，而且您可以在项目层面上配置很多设置。创建一个新的 Mendix 项目时，安全性只在项目层面上可见。屏幕相当简约，提供了“关闭”、“原型/演示”和“生产”等选项。

乍一看，这给您的印象是 Mendix 的安全性非常低。但是 Mendix 安全系统相当先进。一旦您切换到其他模式之一，您会看到用户界面发生变化。在安全性方面，Mendix 只会向您展示您需要的一切。三种安全模式提供以下功能：

- **关闭：**在此模式下，Mendix 不应用任何安全性。我们一直在此模式下工作，因此它适用于初始开发，因为它的工作量比较小。但是，您希望在启动下一个项目时尽快开启安全性。这样，您就可以在开发时配置安全性。这是一个很好的节省时间的方法。
- **原型/演示：**当您具有应用程序的原型并且想要展示基本安全性时，应使用这个模式。它提供了登录功能、页面访问以及微流和纳流访问。
- **生产：**在将应用程序部署到云之前，您必须将安全性设置为生产。完成此操作后，您需要配置安全性的各个方面。如果不这样做，则不允许将应用程序部署到 Mendix 云中的已许可节点。

Mendix 的安全性分为两个部分：项目安全性和模块安全性。项目安全性主要处理常规设置，而模块安全性则处理对模块中各个元素的访问。这允许您导出模块及其安全性，并将其导入另一个项目中，促进了可重复使用性。这是使用角色概念完成的。在项目安全性中，您设置可以指派给用户的用户角色。在模块安全性中，您设置为其指派访问权限的模块角色。然后，将这些模块角色指派给用户角色。

这是安全性新图像应该如何的草图，我们可以参与设计来更新现有的图像吗？

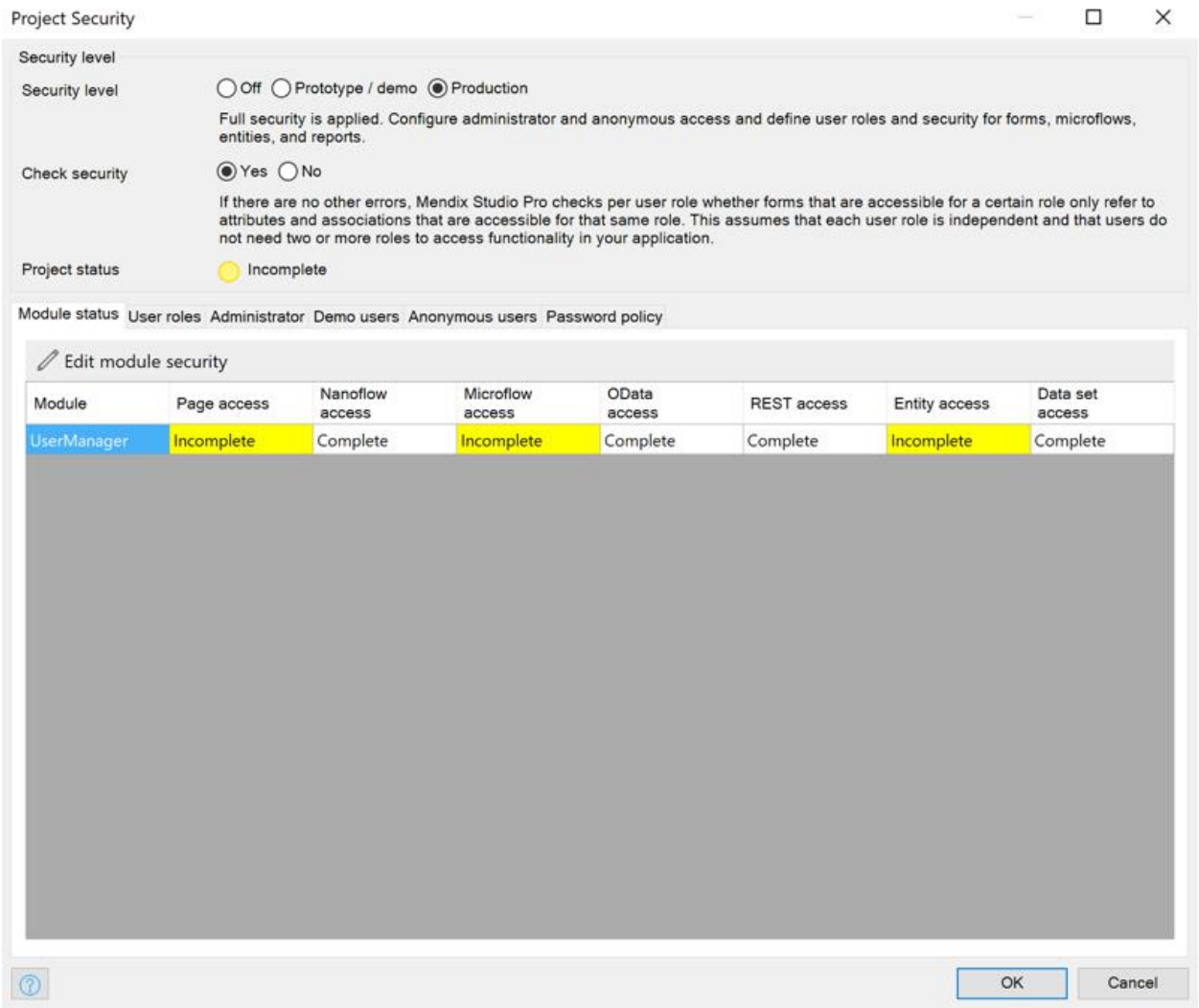


现在我们已经基本了解了三种不同的模式，可以设置应用程序的安全性。让我们开始吧！

讲座 8.3.1：将安全性设置为生产

准备好激活项目安全性后，只需执行几个步骤。激活后，会向项目添加相当多内容。我们来看一下。

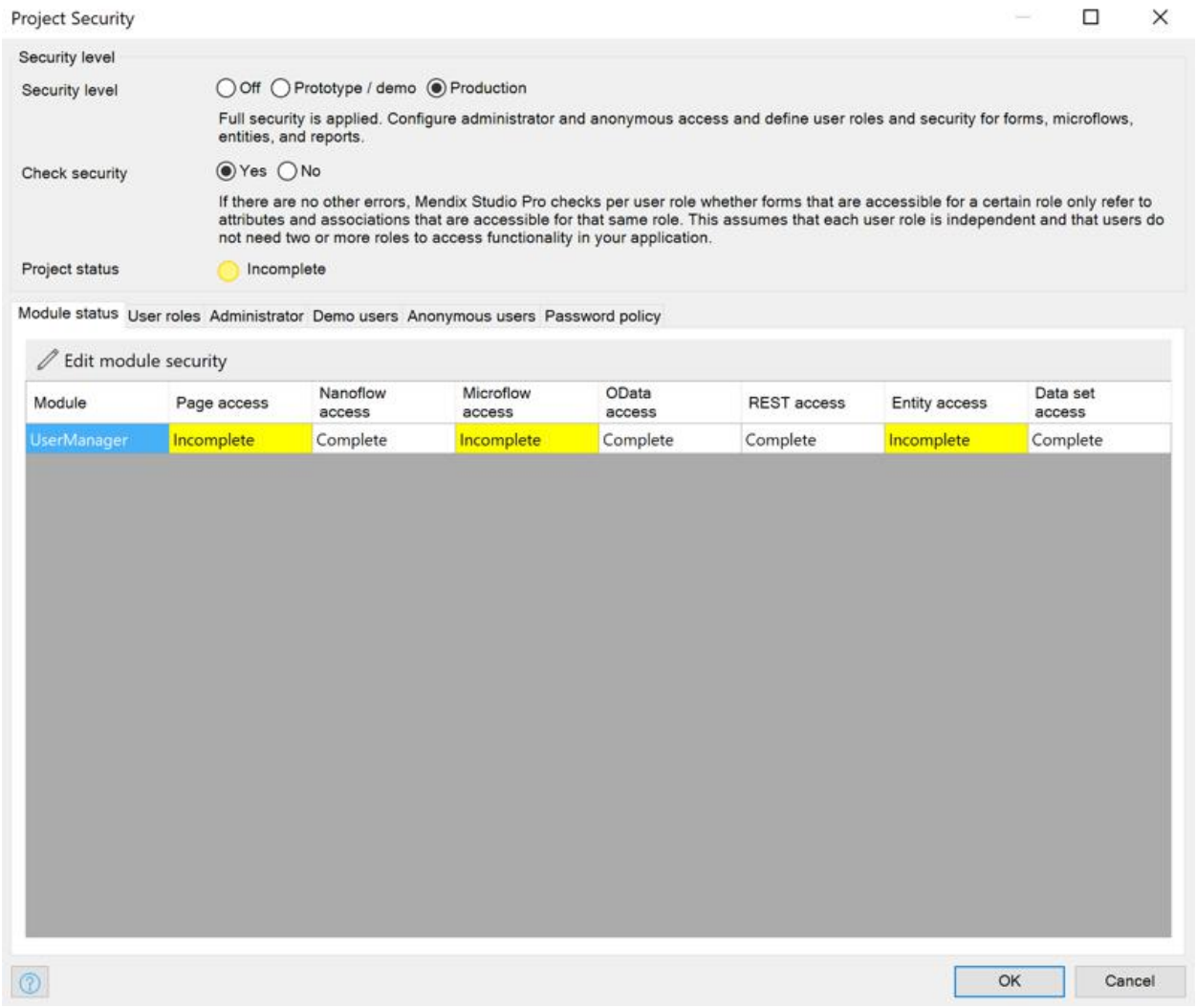
1. 在项目的项目资源管理器中，双击**安全性**。
2. 将**安全级别**从**关闭**更改为**生产**。



如您所见，现在有很多选项可用。让我们继续研究这些选项，了解它们对您的作用。

讲座 8.4：设置项目安全性

项目安全性是您在项目层面上配置应用程序安全性方面的部分。可以在屏幕中心的选项卡中找到不同的方面。每一个都配置一组不同的方面。让我们查看一下它们：



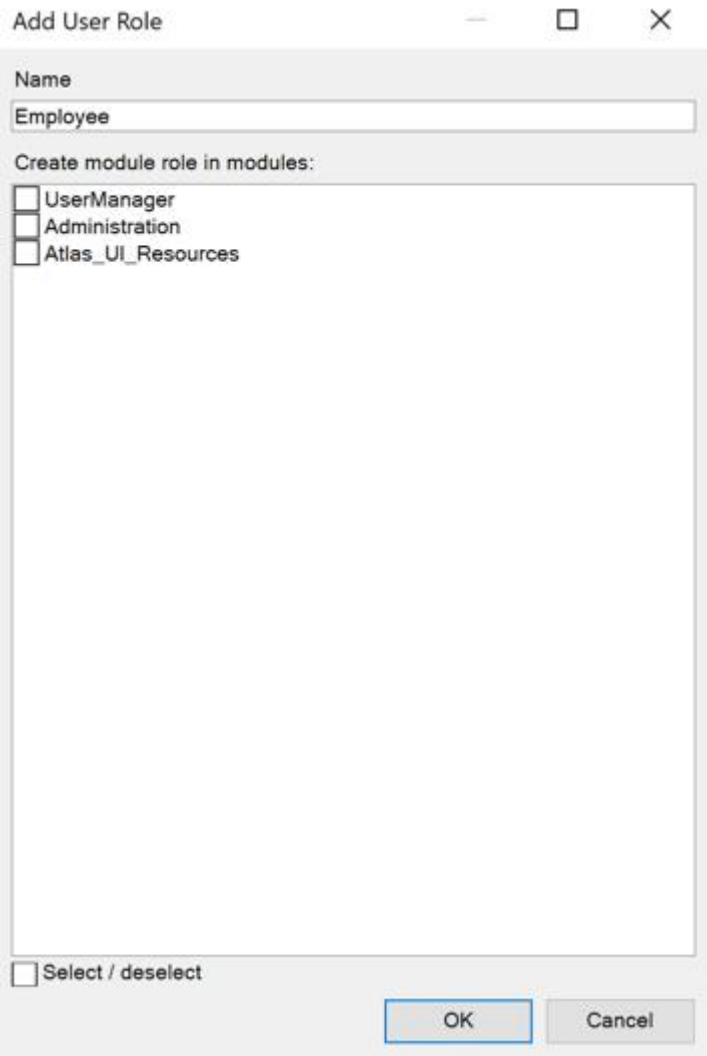
- **模块状态：**在此处，您可以看到特定模块的所有安全方面是否已正确设置。所有未完全设置安全性的模块将在此处可见。因此，当您想要查看模块中安全配置的状态时，请看一下这里。
- **用户角色：**向用户授予应用程序特定访问权限的方式为：为其指派用户角色。可以在此选项卡中创建和编辑这些用户角色。
- **管理员：**要启动应用程序，您需要初始用户才能登录。此用户应具有名称、密码和用户角色。可以在此处配置所有这些内容。
- **演示用户：**在开发应用程序时，您可能希望查看安全性设置是否如预期一样运作。在此处，您可以为每个用户角色配置演示用户，该角色可用于测试安全配置。
- **匿名用户：**有时，您需要为没有用户帐户的用户授予访问权限。要么他们永远不会拥有，要么必须创建一个。此选项卡可用于设置此帐户，并定义匿名用户将担任哪些用户角色。
- **密码策略：**Mendix 允许您设置基本密码身份验证，为此您会希望影响密码策略。此选项卡可帮助您实现这一目的。

让我们将其付诸实践，从创建用户角色开始。

讲座 8.4.1：创建用户角色

现在您已经激活了安全系统，可以添加您与 Summerhill 医院团队讨论的角色了。管理员将有权访问整个系统，关键用户将是特定部门的管理员，用户仅有权访问与其工作有关的信息。让我们开始创建一些用户角色。

1. 在**项目安全性**下，单击**用户角色**。
2. 单击名为**用户**的用户角色，然后将名称改为 **KeyUser**。单击**确定**。
3. 单击**新建**，将角色命名为**员工**。取消选中所有模块。仔细检查此处未选中任何方框。稍后，您将在此模块中配置模块安全性时创建模块角色。

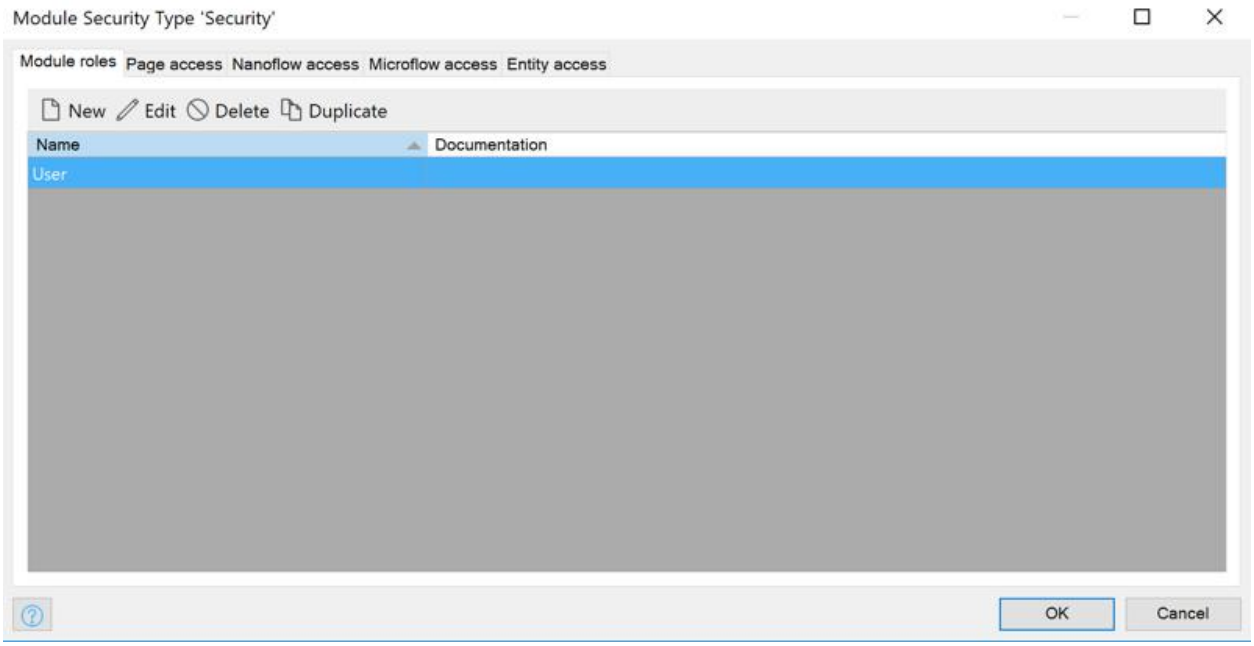


4. 单击**确定**关闭**项目安全性**窗口并保存所做的更改。您会看到一些新的错误出现。这很好。我们很快会修复它们。

非常好，用户角色在基础级别上设置。但等待一下，您没有给任何人访问任何页面的权限！如果您去听下一个讲座，您会学到如何操作，所以要抓紧时间！Summerhill 的人员正焦急地等待您的下一次更新。

讲座 8.5：设置模块安全性

在上一次任务之后，**项目资源管理器**中的 **UserManager** 增加了一个新元素：**安全**元素。这包含模块的所有安全设置。要设置的第一件事是模块角色。所有其他元素将使用这些角色来确定允许谁访问它们。然后，这些模块角色将指派给之前创建的用户角色。正如在项目安全性中一样，您会看到几个选项卡，每个选项卡负责配置模块安全性的不同部分。



- **模块角色：**您可以创建可用于为模块指派不同访问级别的模块角色
- **页面访问权限：**对于通过导航项目、链接或按钮可访问的每个页面。包含该按钮的页面本身不一定可以访问。
- **纳流访问权限：**当纳流被连接到一个按钮、一个链接或导航菜单中的一个项目时，它将显示在这个选项卡中，并且可以指派访问权限。
- **微流访问权限：**当微流被连接到一个按钮、一个链接或导航菜单中的一个项目时，它将显示在这个选项卡中，并且可以指派访问权限。
- **实体访问权限：**可以将实体配置为具有访问规则。这些规则是每个实体访问规则的一个或多个模块角色的组合。通常，每个实体访问规则只需要一个模块角色。每个规则都允许您定义是否允许该模块角色创建和/或删除对象。此外，它允许您为每个属性和关联设置访问级别，即（无）、**读取**或**读/写**。该规则允许您指定为新属性和/或关联赋予哪个访问级别。您也可以在对象层面上设置访问权限。

不是所有在 Mendix 中退出的安全性选项卡都可见。这是因为如果模块中不存在某些类型的元素，这些选项卡将隐藏。为了完整起见，现将它们列举如下。

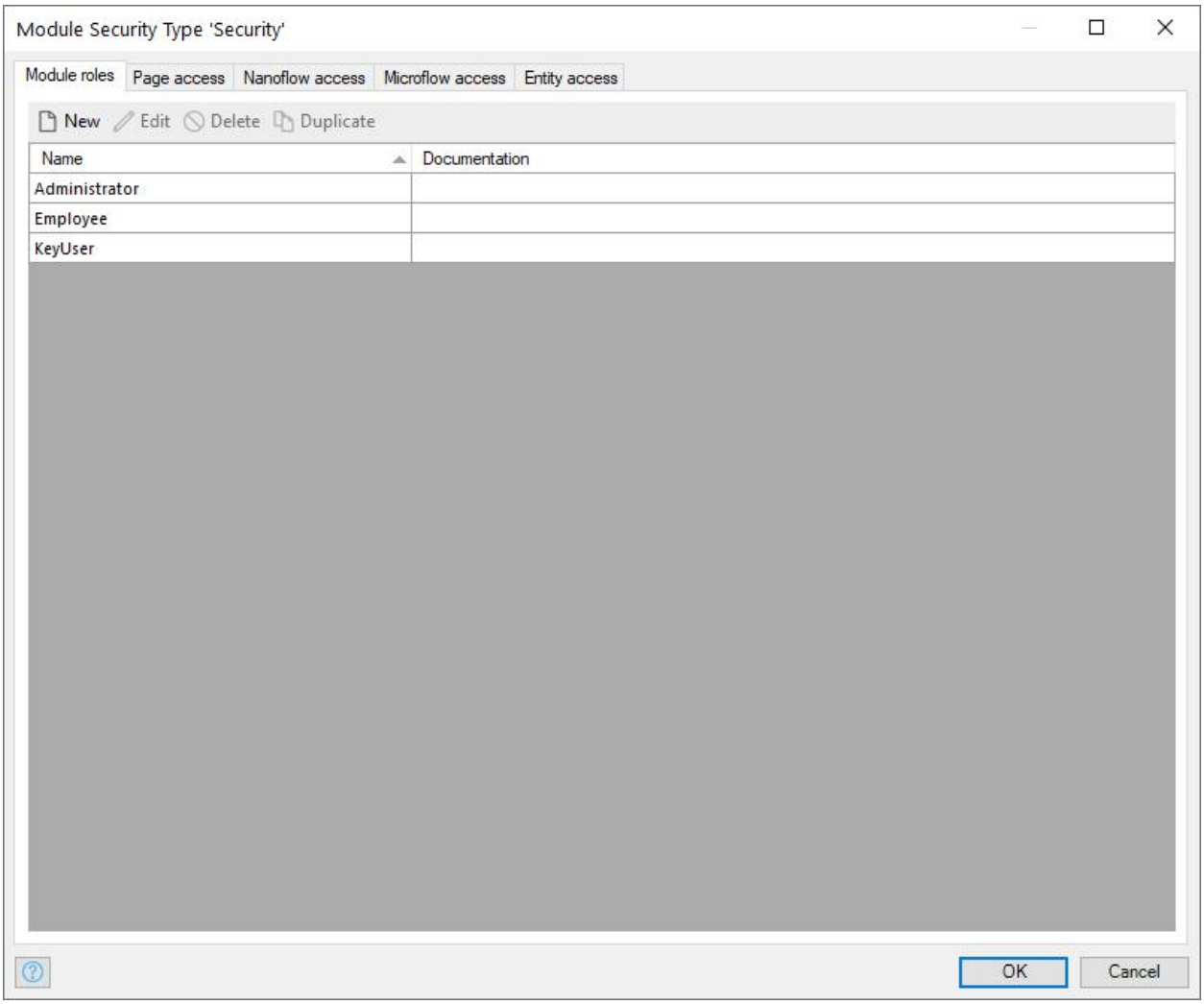
- **OData 访问权限：**您可以定义用户是否必须使用用户名/密码登录，他们是否可以使用活动会话访问 OData 服务，以及/或者使用定制微流来处理身份验证。为此，您必须指定模块角色。请注意，还将应用实体访问权限。
- **REST 访问权限：**您可以定义用户是否必须使用用户名/密码登录，他们是否可以使用活动会话访问 REST 服务，以及/或者使用定制微流来处理身份验证。为此，您必须指定模块角色。请注意，还将应用实体访问权限。
- **数据集访问权限：**您可以定义哪些模块角色有权访问为数据集定义的参数。可以单独允许或不允许每个可能的参数值。

让我们将其付诸实践，从创建模块角色开始，并配置项目中所有元素的安全性设置。

讲座 8.5.1：创建模块角色

Summerhill 医院的人已提供将登录此应用程序的用户类型列表。您甚至已经创建了所需的用户角色，因此下一步是设置模块角色。由于您只负责自己模块的角色，让我们打开 **UserManager** 模块的安全设置。

1. 在 **UserManager** 模块中，双击**安全性**。
2. 双击**用户**模块角色，将其重命名为**员工**。
3. 单击**新建**以添加名为**管理员**的新模块角色。
4. 再次单击**新建**，添加另一个名为 **KeyUser** 的模块角色。

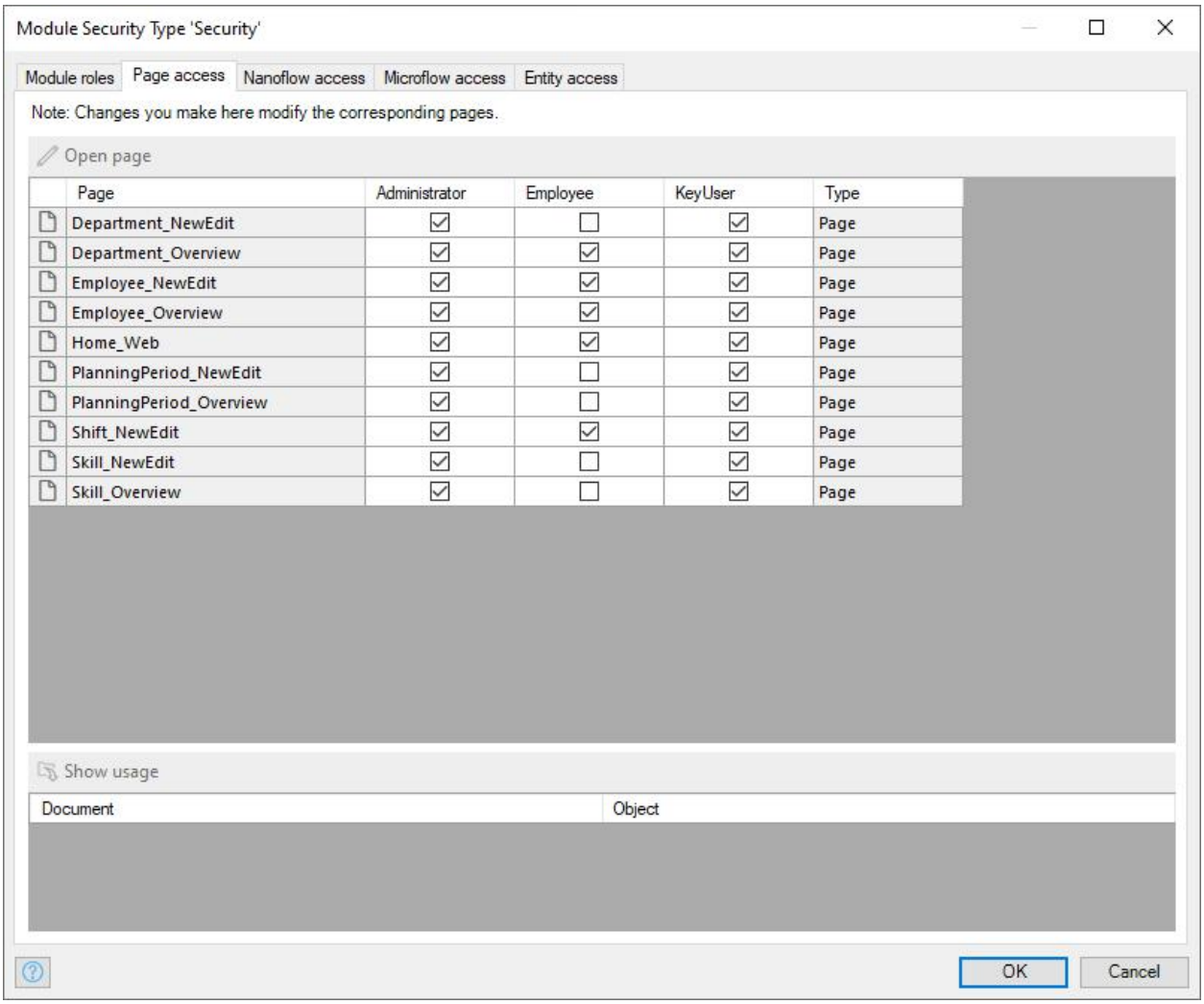


5. 操作操作完成后，单击**确定**。

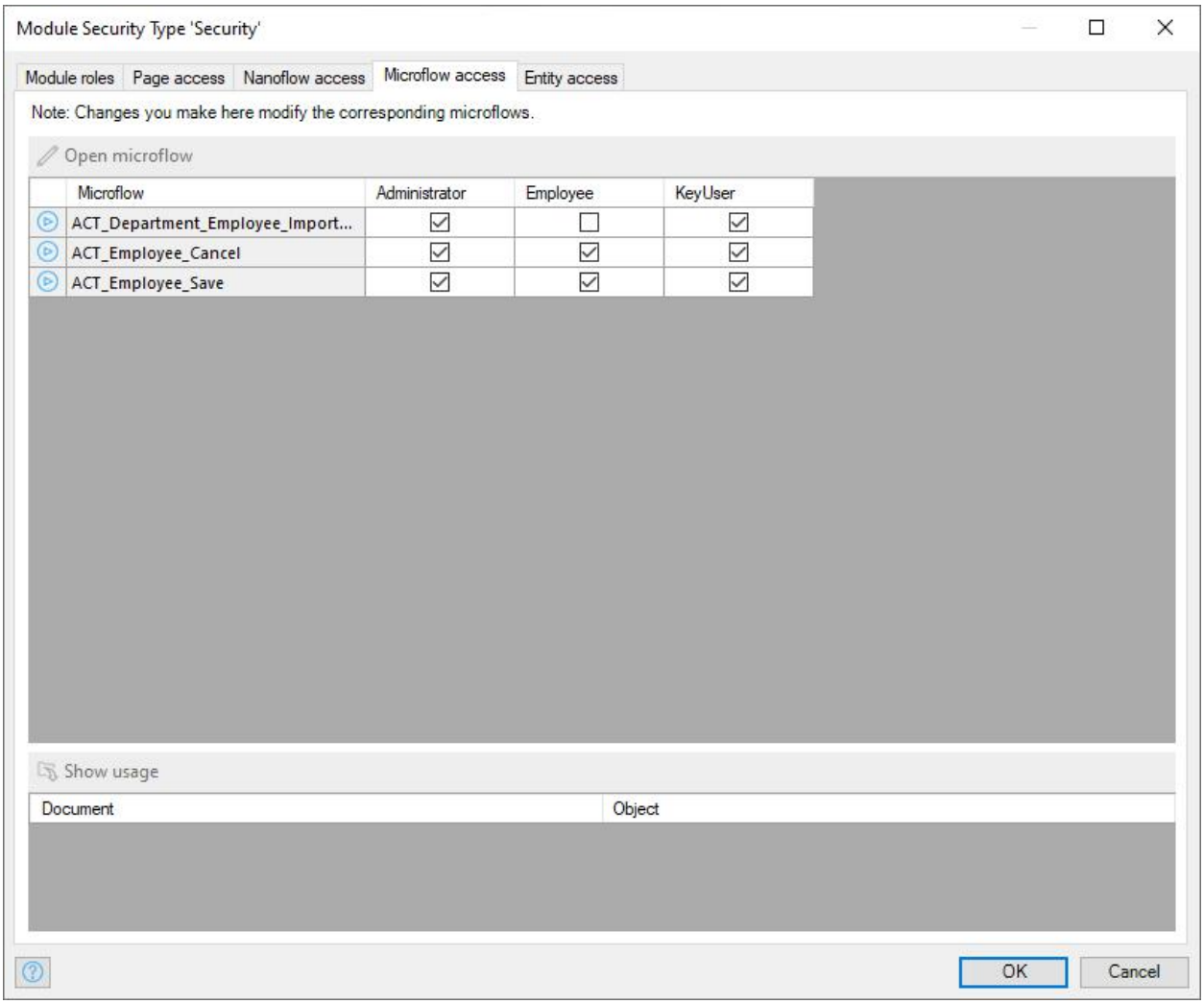
很好，您已经设置了模块角色，所以现在您可以给他们指派权限了。在接下来的练习中，您将设置页面和微流的访问权限。

讲座 8.5.2：设置页面和微流访问权限
现在您已经了解了安全性的基础知识，可以设置微流和页面的访问权限了。

1. 在 **UserManager** 模块中，双击**安全性**。
2. 单击**页面访问权限**选项卡。
3. 使用下图设置页面访问权限。



4. 单击**微流访问权限**选项卡，然后使用下图设置微流访问权限。



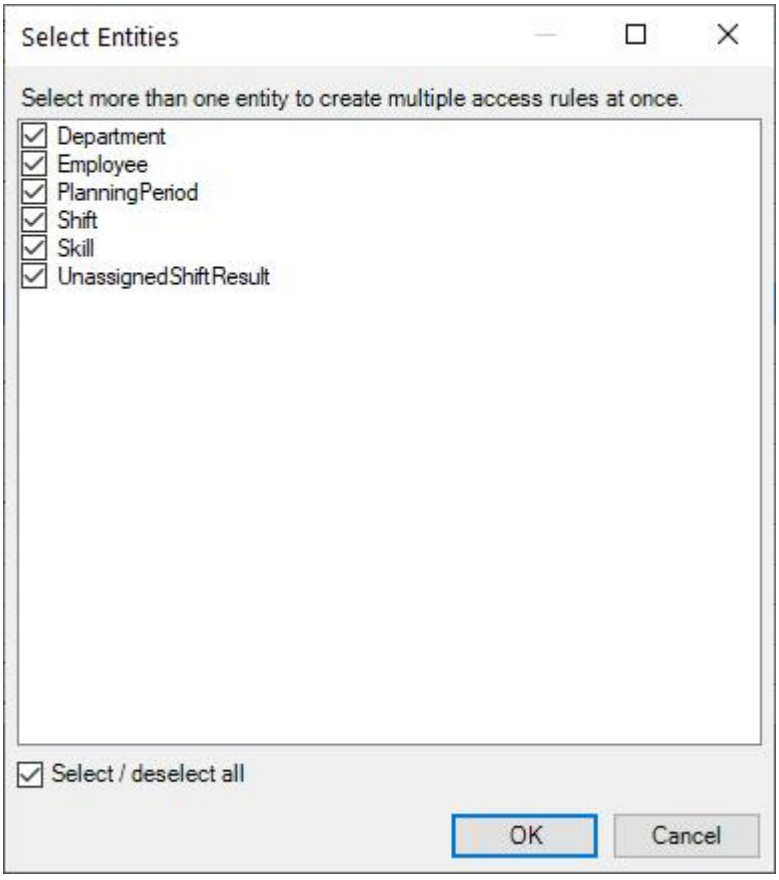
5.操作完成后，单击**确定**。

您已经配置了基本安全性，也已经为页面和逻辑定义了访问权限。是时候进入下一个任务了，您将在这里设置数据安全性。

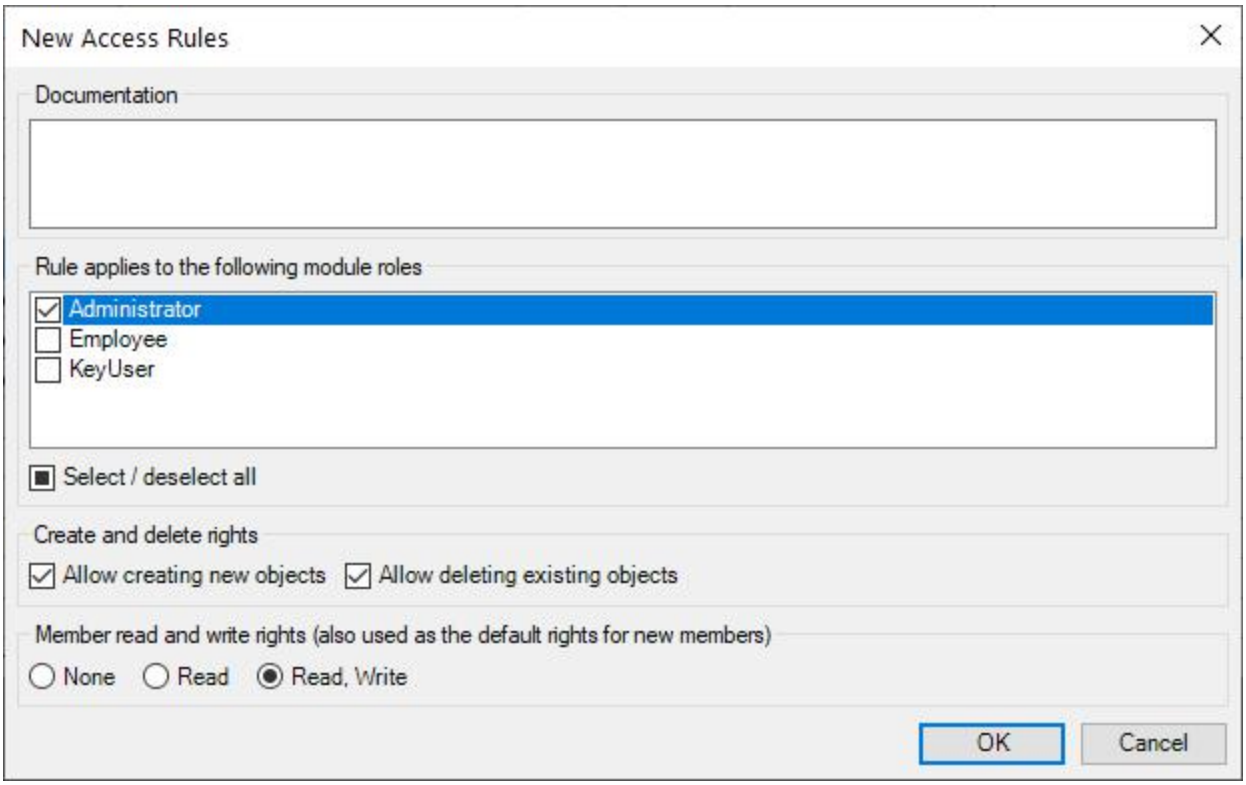
讲座 8.5.3：设置实体访问权限

我们已经设置了页面和微流访问权限，现在可以配置对数据的访问权限，以便每个角色只能看到与它们相关的数据。此外，我们将确定允许哪些人和不允许哪些人写入数据。

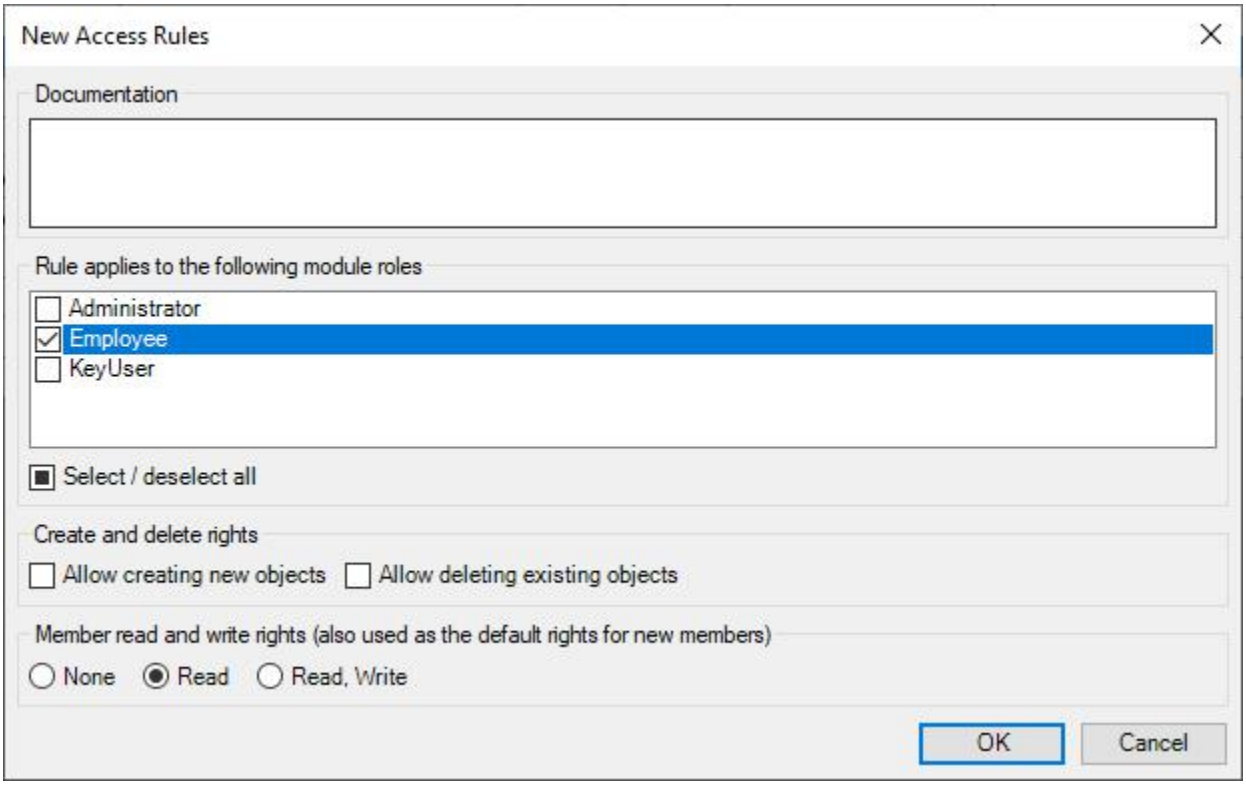
1. 在**项目资源管理器**中，在 **UserManager** 模块下，双击**安全性**。
2. 单击**实体访问权限**和**新建**以创建第一条规则。
3. 在新打开的屏幕中选择所有的实体，然后单击**确定**。



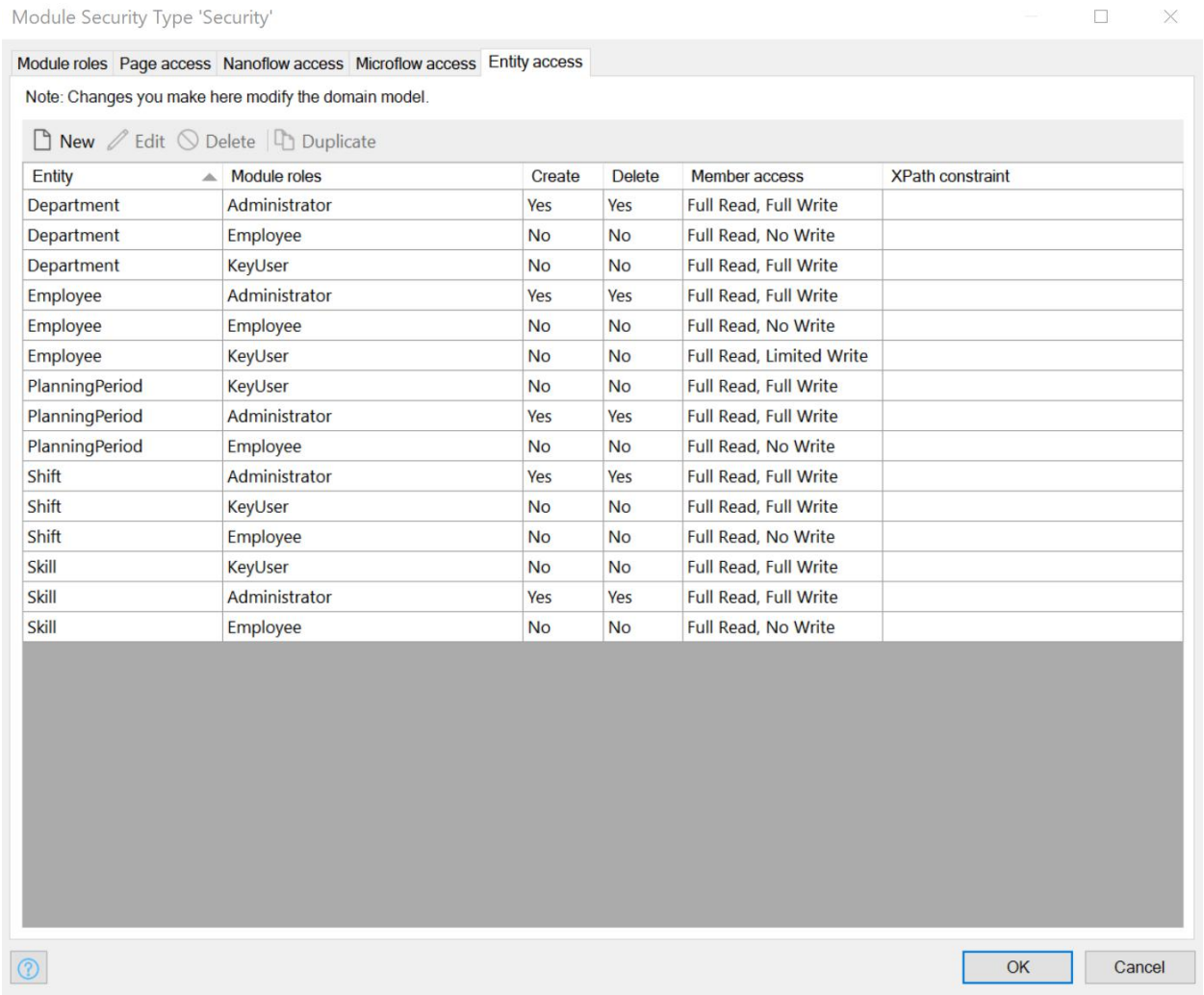
4. 选择**管理员**用户角色，然后从下图复制设置。单击**确定**。



5. 再次单击**新建**，选择所有实体并单击**确定**
6. 匹配下图中的设置。



7. 创建可在下图中查看的所有规则。此屏幕截图中的受限写入意味着至少有一个成员（属性或关联）不被允许写入访问。在这种情况下，这会是 **EmployeeId**。



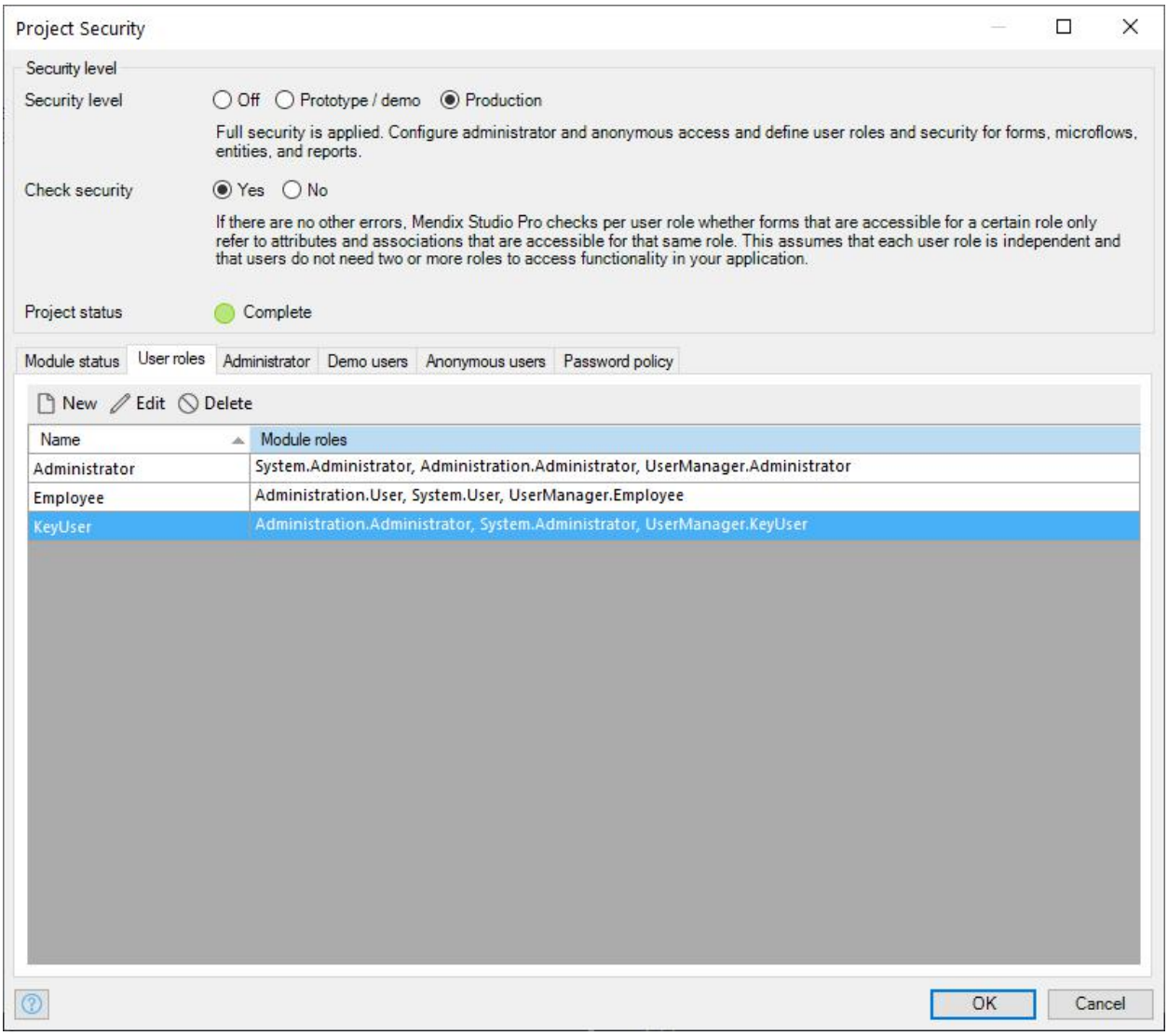
Entity	Module roles	Create	Delete	Member access	XPath constraint
Department	Administrator	Yes	Yes	Full Read, Full Write	
Department	Employee	No	No	Full Read, No Write	
Department	KeyUser	No	No	Full Read, Full Write	
Employee	Administrator	Yes	Yes	Full Read, Full Write	
Employee	Employee	No	No	Full Read, No Write	
Employee	KeyUser	No	No	Full Read, Limited Write	
PlanningPeriod	KeyUser	No	No	Full Read, Full Write	
PlanningPeriod	Administrator	Yes	Yes	Full Read, Full Write	
PlanningPeriod	Employee	No	No	Full Read, No Write	
Shift	Administrator	Yes	Yes	Full Read, Full Write	
Shift	KeyUser	No	No	Full Read, Full Write	
Shift	Employee	No	No	Full Read, No Write	
Skill	KeyUser	No	No	Full Read, Full Write	
Skill	Administrator	Yes	Yes	Full Read, Full Write	
Skill	Employee	No	No	Full Read, No Write	

8.操作完成后，单击**确定**。

讲座 8.5.4：将模块角色指派给用户角色

现在是时候把注意力转回到项目安全性上了。

1. 单击项目中**安全性**。
2. 单击**用户角色**，编辑每个用户角色，使您拥有图片中的设置。为此，您需要选择正确的模块角色。



3. 操作完成后，单击**确定**。

讲座 8.6：系统和管理模块

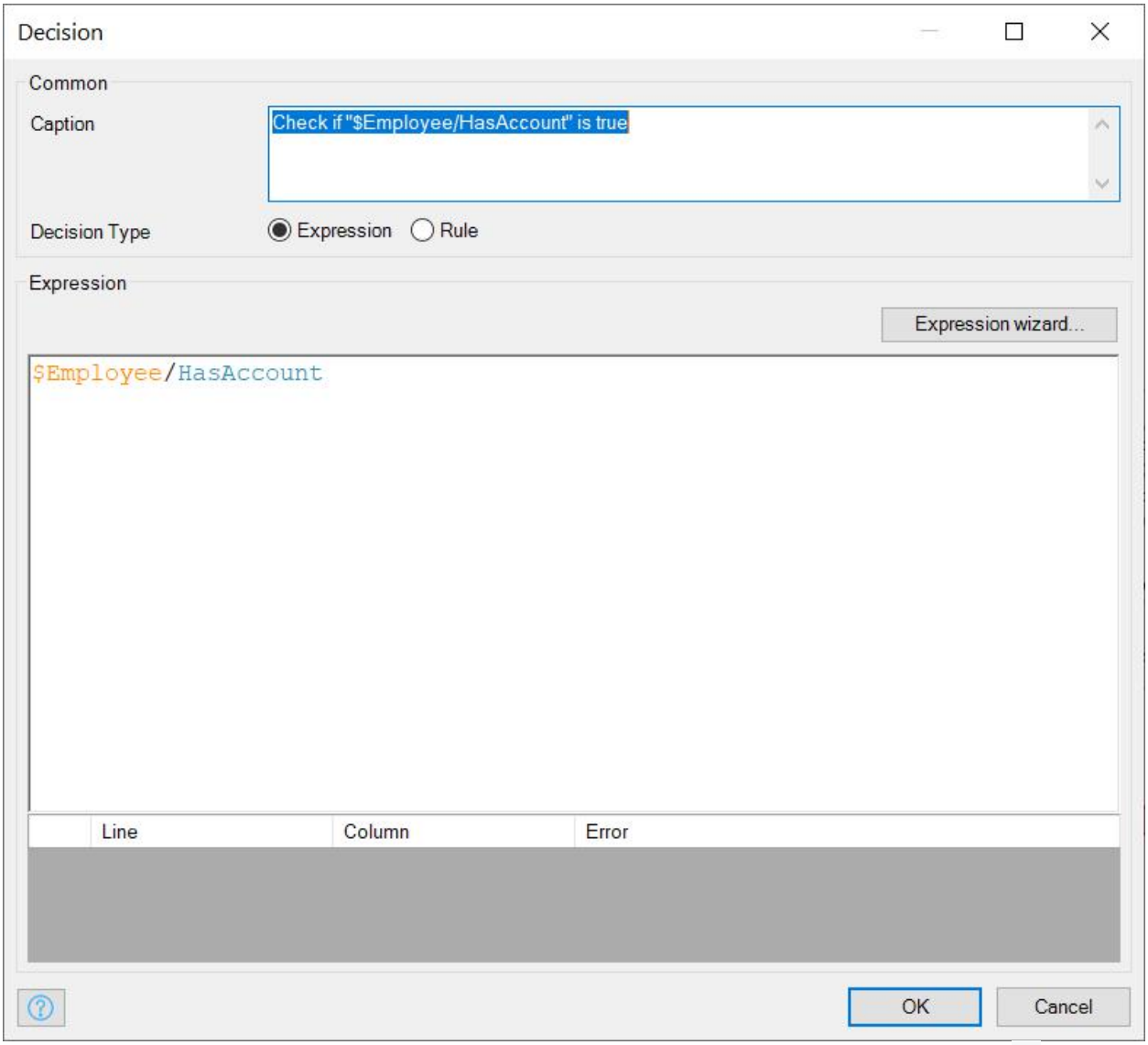
您已经看到了两个模块，但还没有讨论过，即系统模块和管理模块。系统模块是一个无法编辑的必需模块。这是 Mendix 功能的关键，允许用户登录。管理模块默认提供，可用于管理本地用户。此模块可编辑，您甚至可以将其移除（如果需要）。然而，建议让它留在原地，因为它包含管理用户的基本功能。

讲座 8.7：微流表达式编辑器

有时，您无法直观地表达某些内容。对于这些案例，Mendix 提供了表达式。表达式可以包含布尔逻辑、字符串函数和数据比较等内容。您可以在表达式编辑器中使用这些表达式，这些表达式在某些微流元素中可以找到：

- 决策
- 更改对象
- 创建对象
- 更改变量
- 更改变量

如果在表达向导中键入 Ctrl + 空格，将显示可用表达式的列表。

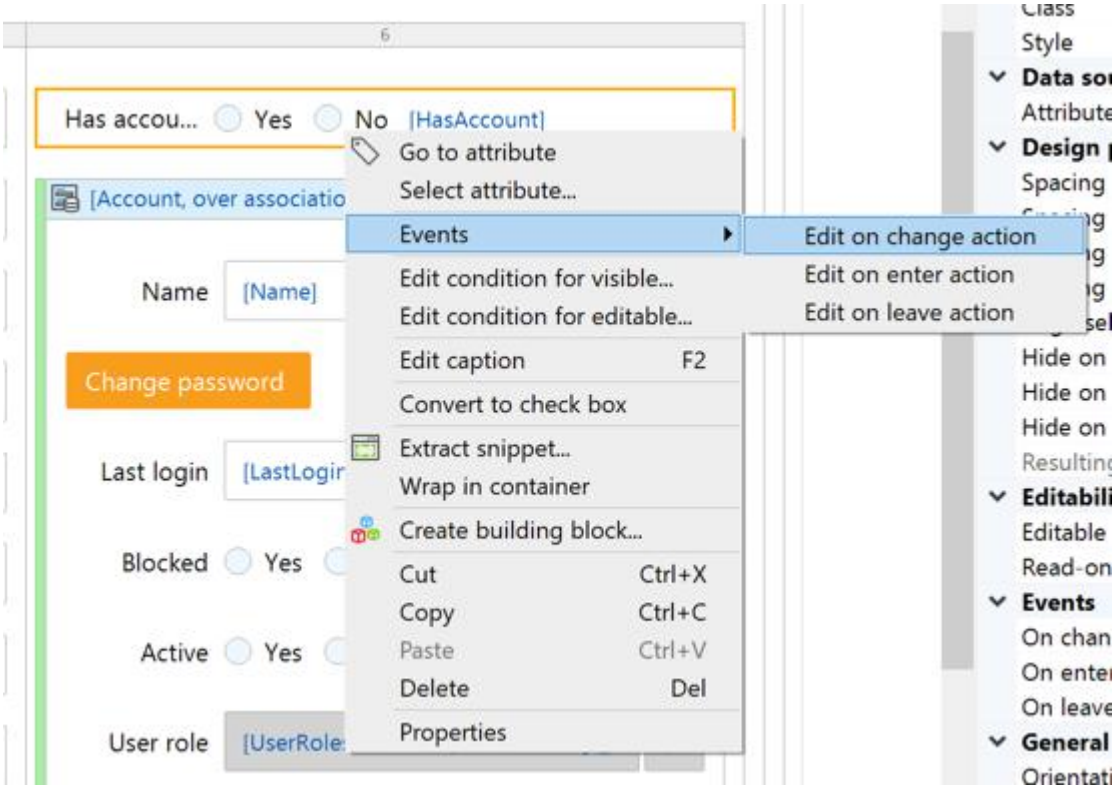


有了这些关于微流的新知识，您就可以建立一个微流，当 HasAccount 被设置为真时，该微流可为员工创建一个帐户。

讲座 8.7.1：创建帐户

现在，您将创建一个微流，将其附加到 **HasAccount** 小组件。此微流将具有一个逻辑，用于检查是否需要帐户，然后根据 **HasAccount** 决定是删除还是创建。

1. 打开 **Employee_NewEdit** 页面。
2. 右键单击 **Has Account** 单选按钮，然后打开**事件**菜单。

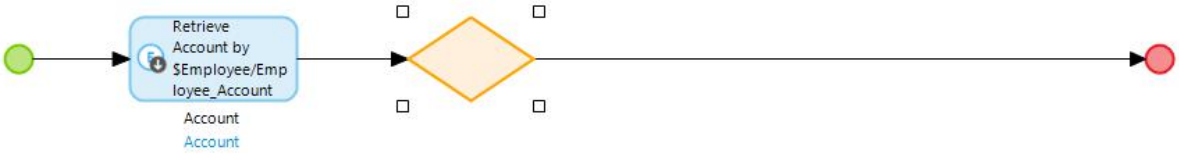


3. 从**事件**选择**编辑更改事件**，然后选择**调用微流**。
4. 在**选择微流**窗口的右下方，单击**新建**按钮，创建一个新的微流。给它起名为 **OCH_Employee_CreateDeleteAccount**。单击**确定**。

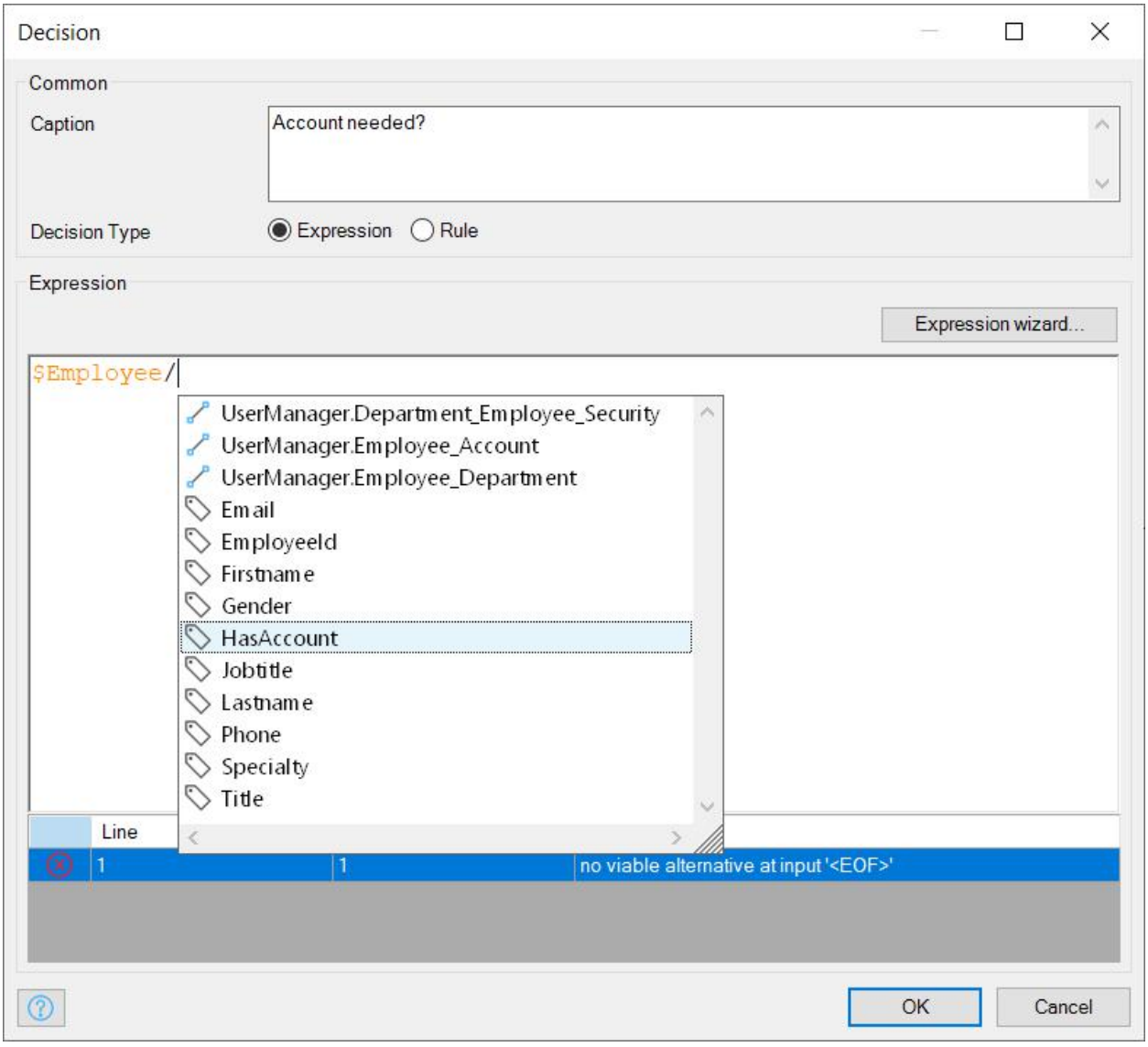
新创建的微流具有**员工**类型的参数。Mendix 添加了此参数，因为您从连接到“员工”对象的数据小组件中创建了微流。您可以检查此**员工**上 **HasAccount** 属性的状态，以确定该属性是否设置为真，表示**员工**对象需要一个帐户。此外，我们还希望检查**员工**对象是否已具有帐户。为此，您必须检索它。

5. 首先，您需要在**工具箱**中寻找**检索**活动，并将其拖到微流中。

6. 单击**检索**活动，并使用右边的**选择**按钮在 **Employee_Account** 关联上选择**帐户**对象。单击**确定**。
7. 把一个**决策**拖到您的微流上，然后双击它来打开表达式编辑器。

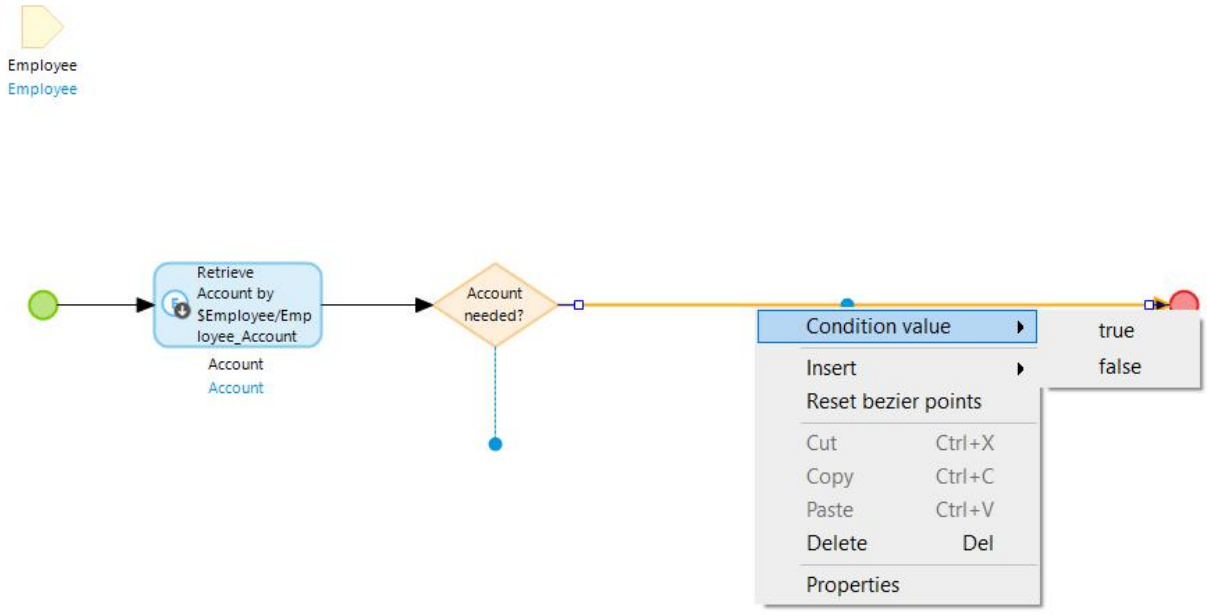


8. 当光标位于表达式编辑器中时，按 Ctrl + 空格键以查看您的选项。查找 **$Employee** 变量，并使用 / 字符查找 **HasAccount** 变量。单击**确定**。

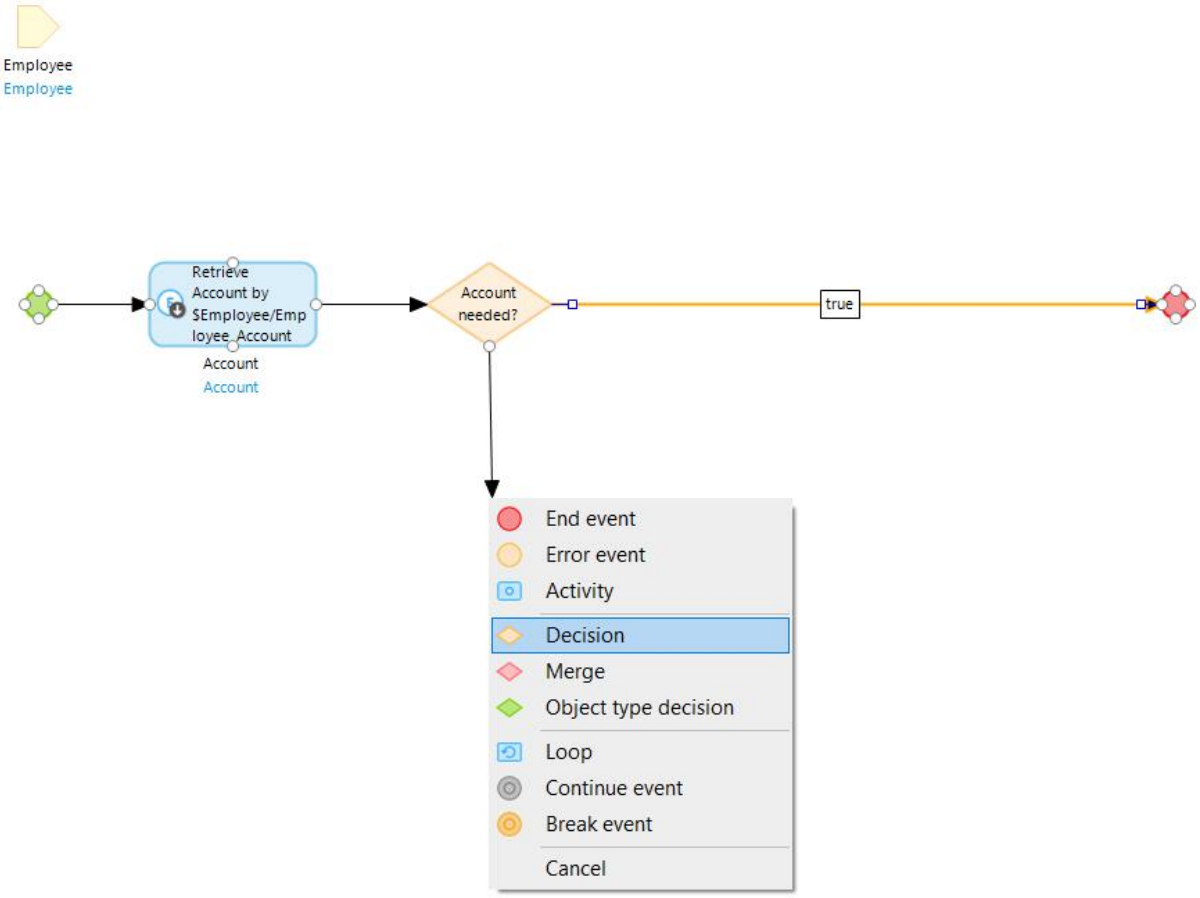


决策右侧的流程现在是红色的。这是因为 Mendix 不知道此流程是适用于 **HasAccount** 属性设为**真**还是**假**的情况。

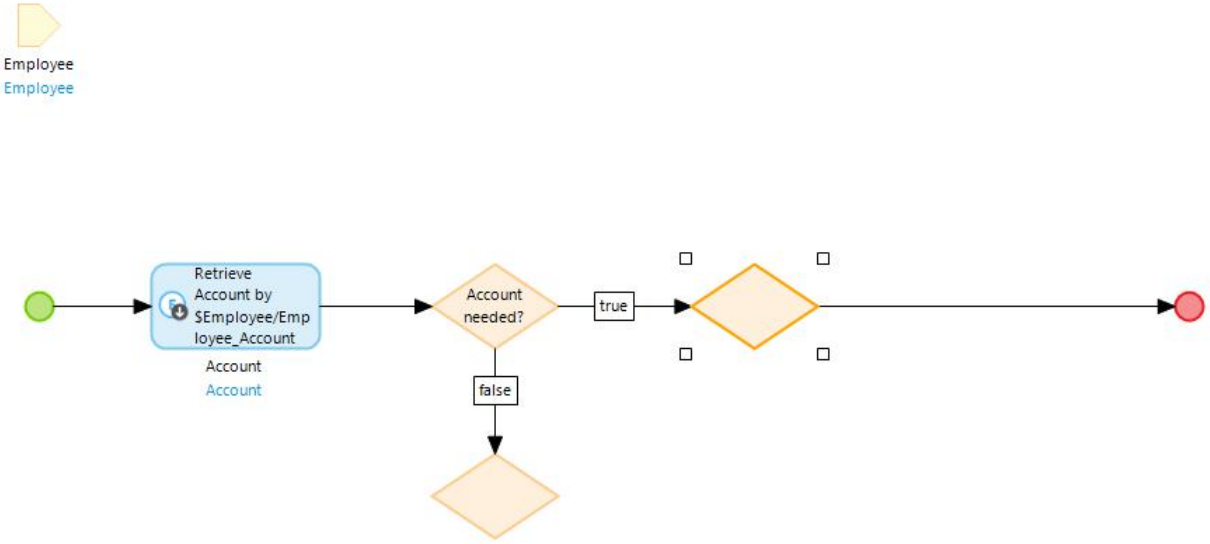
9. 右键单击**决策**右侧的流程，将**条件值**设为**真**。



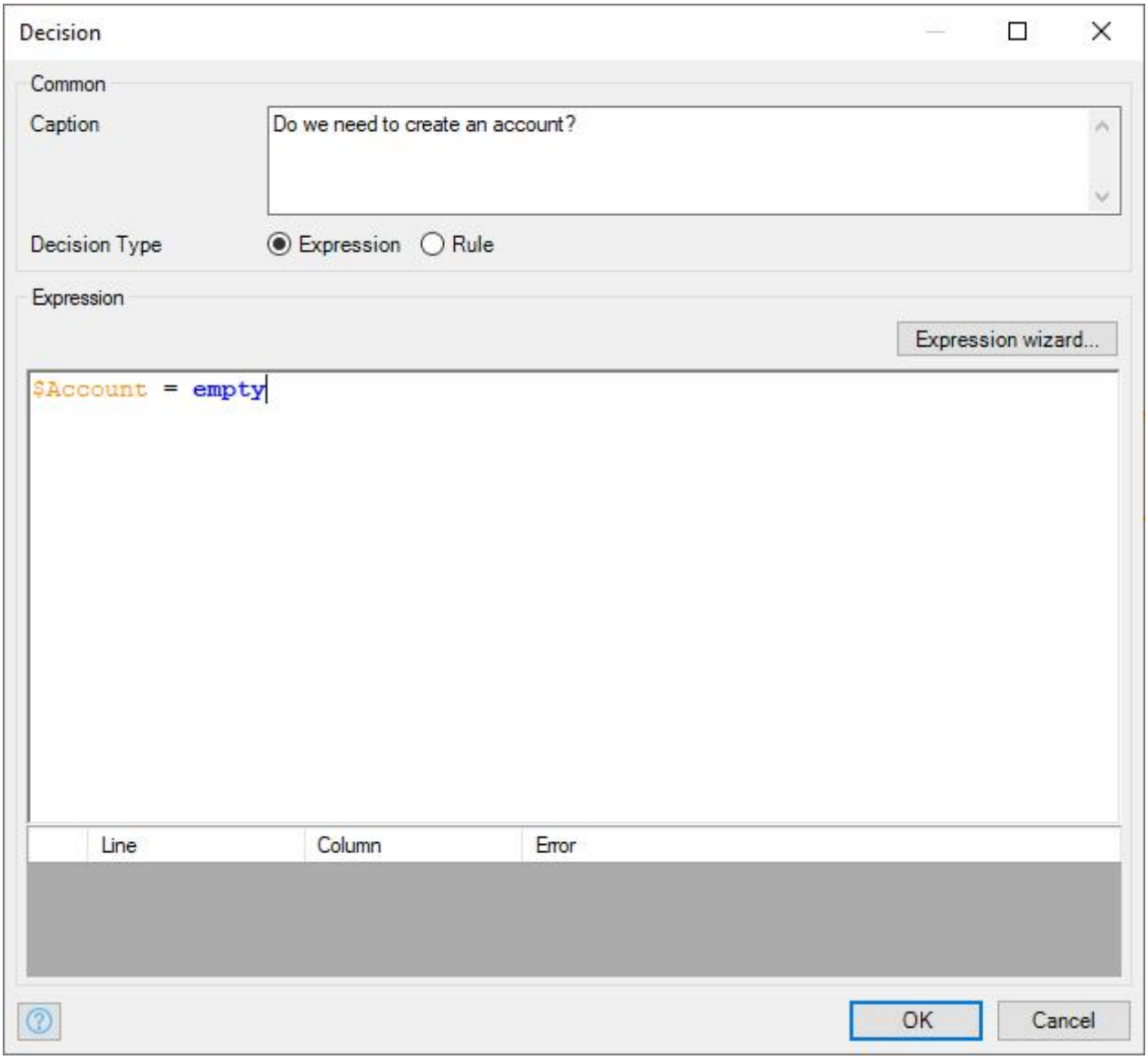
10. 将鼠标移动到**决策**，单击底部的白色圆圈，向下拖动以创建新流程。从菜单中选择**决策**。



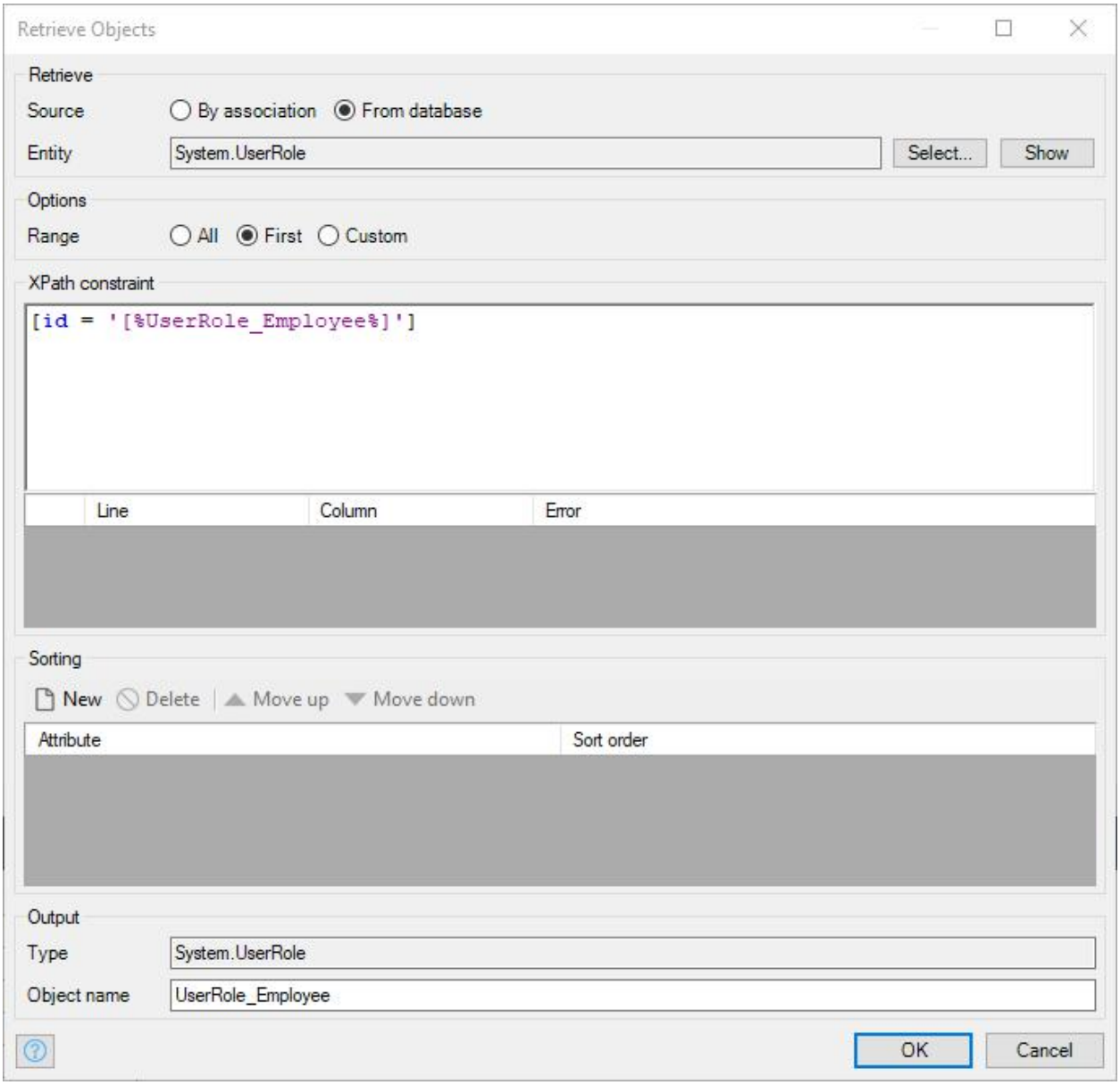
11. 将新的**决策**拖到流程上，在第一个**决策**的右边。



12. 为这两个决策设置表达式，通过与关键字 空的比较来检查**帐户**对象是否存在。单击**确定**。

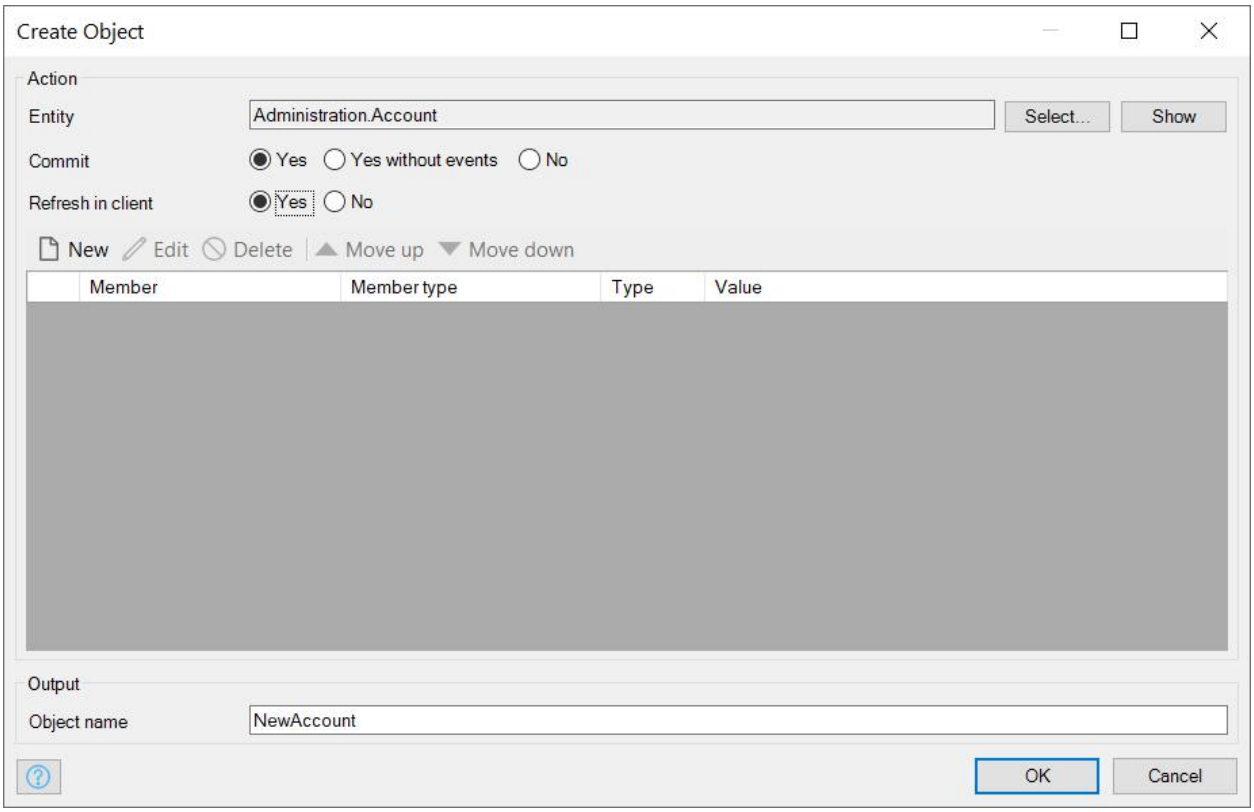


13. 将从您的最右边的决策到最终事件的红色流设置为真。
14. 在您最右边的决策的右边添加一个**检索对象**活动。您将使用这个活动来检索**用户角色**，它将被用作用户的默认角色。
    1. 将**实体**设置为 **System.UserRole**
    2. 将**范围**设置为**第一**
    3. 将对象名称改为 **UserRole_Employee**
    4. 设置 XPath 约束，如下图所示。这将从数据库中检索用户角色“员工”。稍后您可以使用此功能将用户角色指派给**帐户**对象。

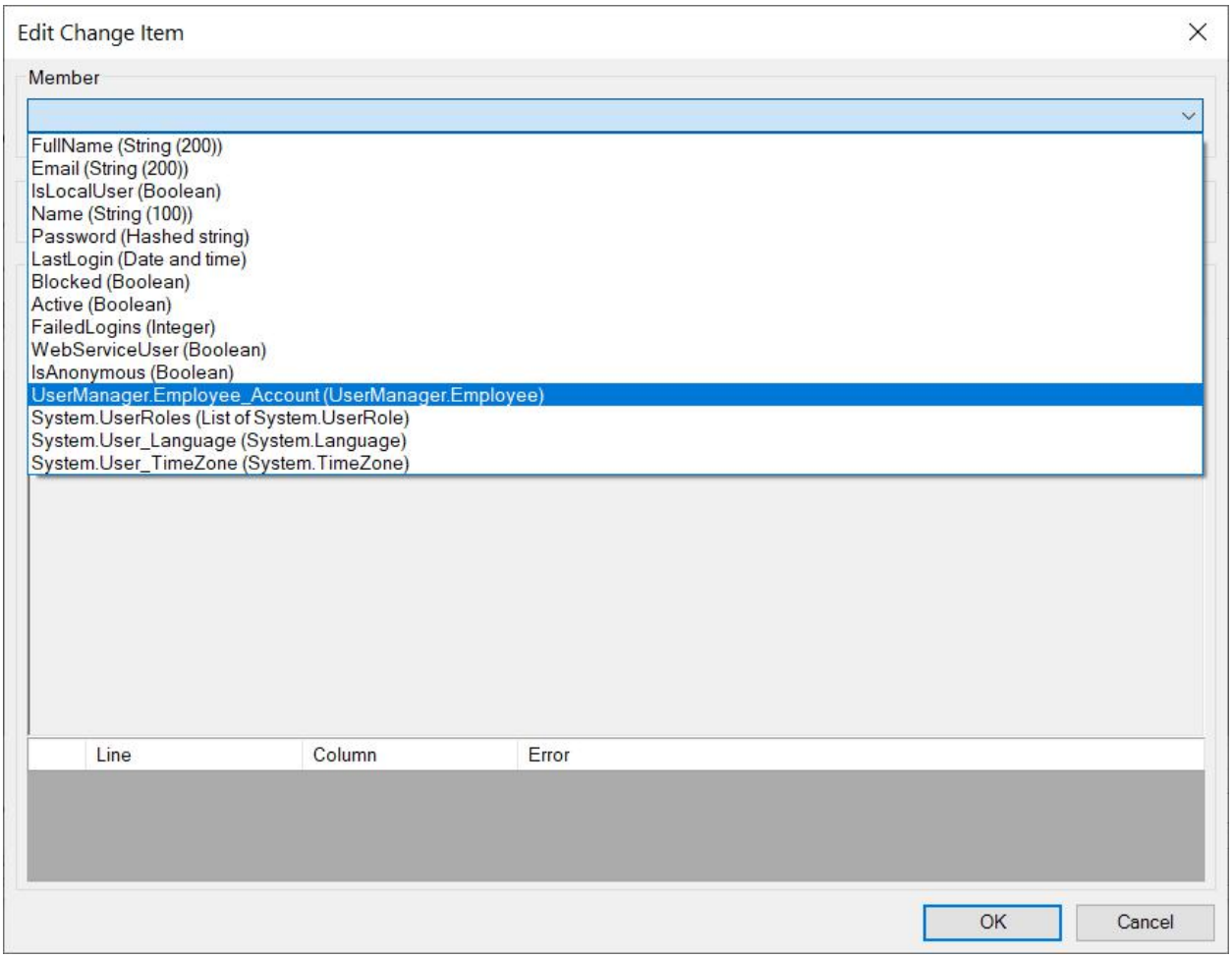


15. 在检索的右边添加一个**创建对象**活动。

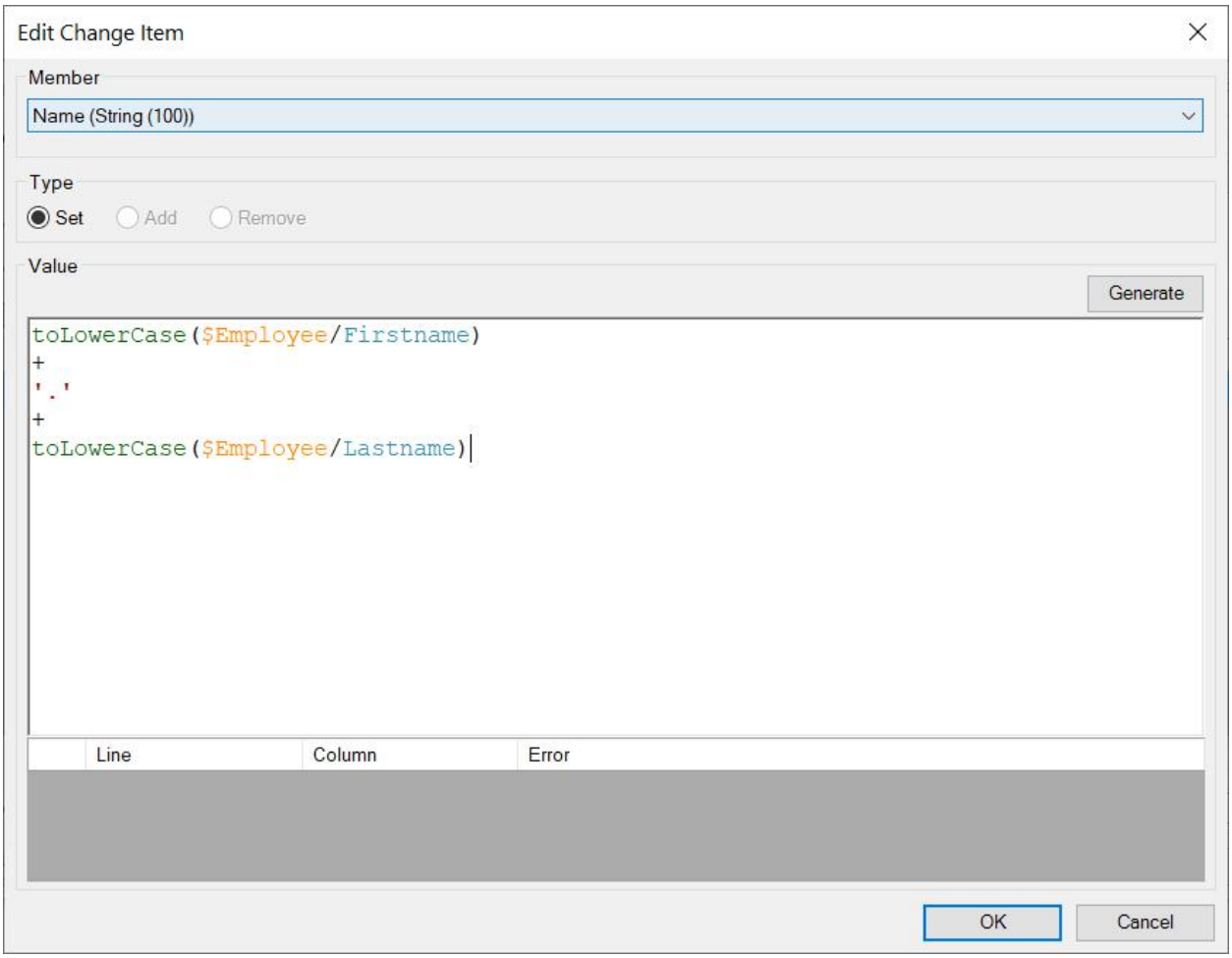
16. 双击**创建对象**事件，单击屏幕右侧的**选择**按钮。使用过滤器查找**帐户**实体，然后单击**选择**。将客户端中的**提交**和**刷新**都设置为**是**。



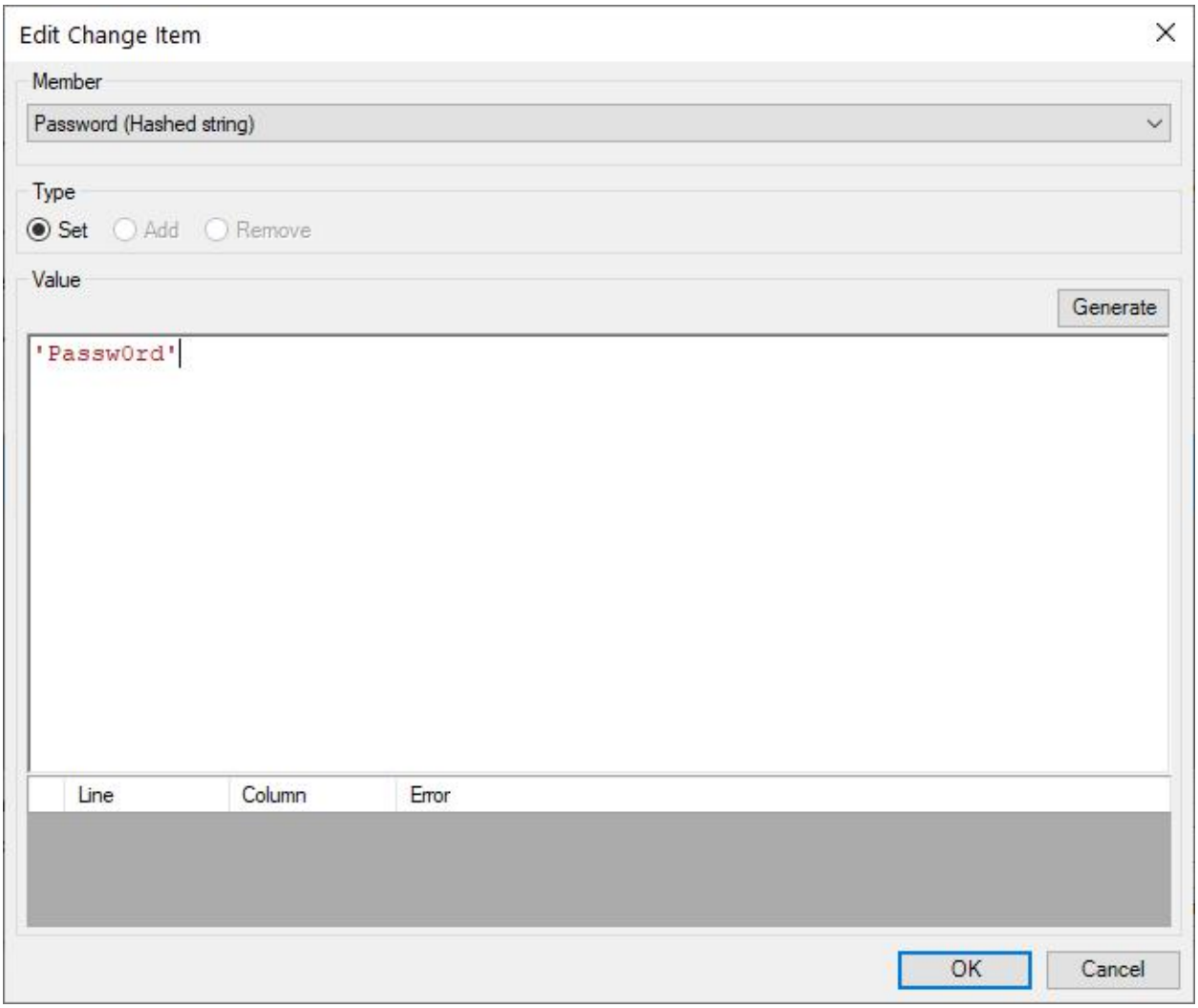
17. 单击**新建**添加新成员初始化，然后选择 **UserManager.Employee_Account**。使用表达式编辑器和 Ctrl-Space 查找 **$Employee** 对象。这将在 **$Employee** 对象和您新创建的 **$NewAccount** 对象之间建立一个关联，然后单击**确定**。



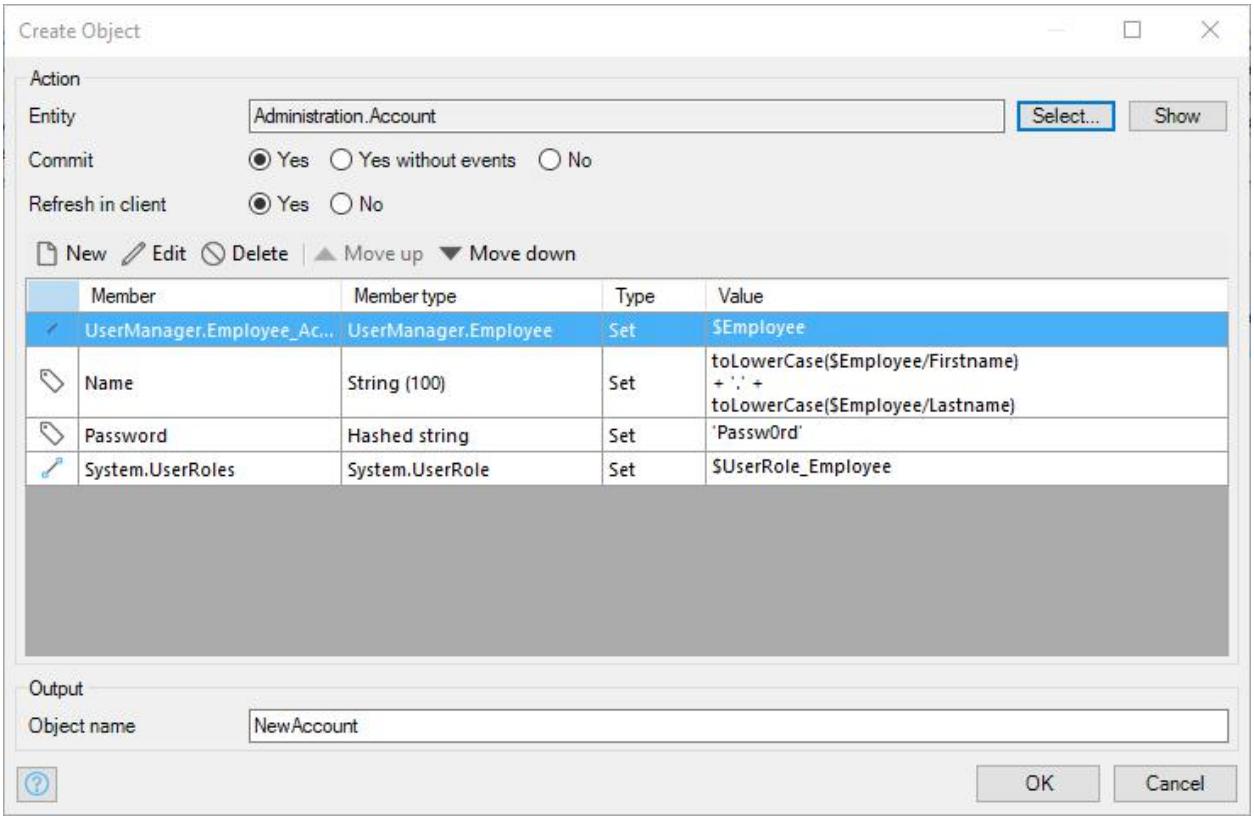
18. 接下来，您应该通过初始化**密码**和**名称**来提供密码和用户名的默认值。使用**新建**按钮为两者创建初始化条目。您可以将密码设置为*“Passw0rd”*（注意密码周围的引号）。对于用户名，您将使用**员工**实体中的名和姓。使用 **toLowerCase** 函数来确保您获得一致的用户名。



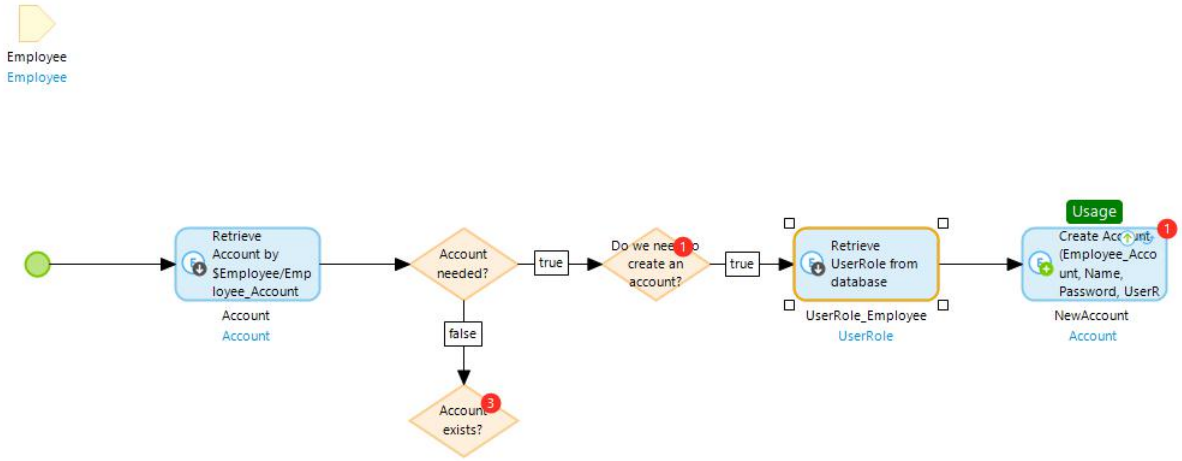
19. 要确保员工可以登录，您还应设置默认密码。由于这不是生产应用程序，因此将默认密码设置为 Passw0rd 就足够了。



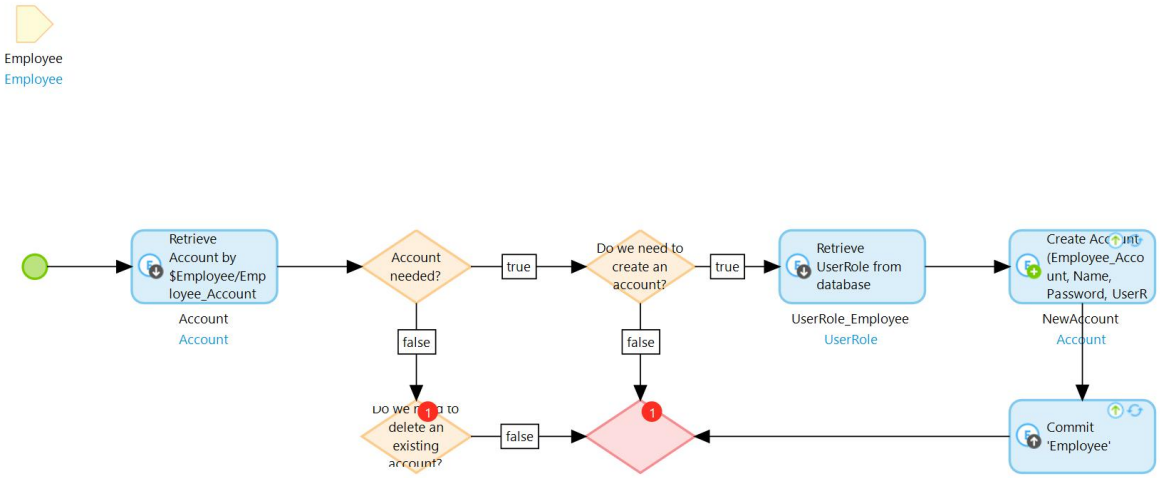
20. 将 **System.UserRoles** 关联设置为 **$UserRole_Employee**。



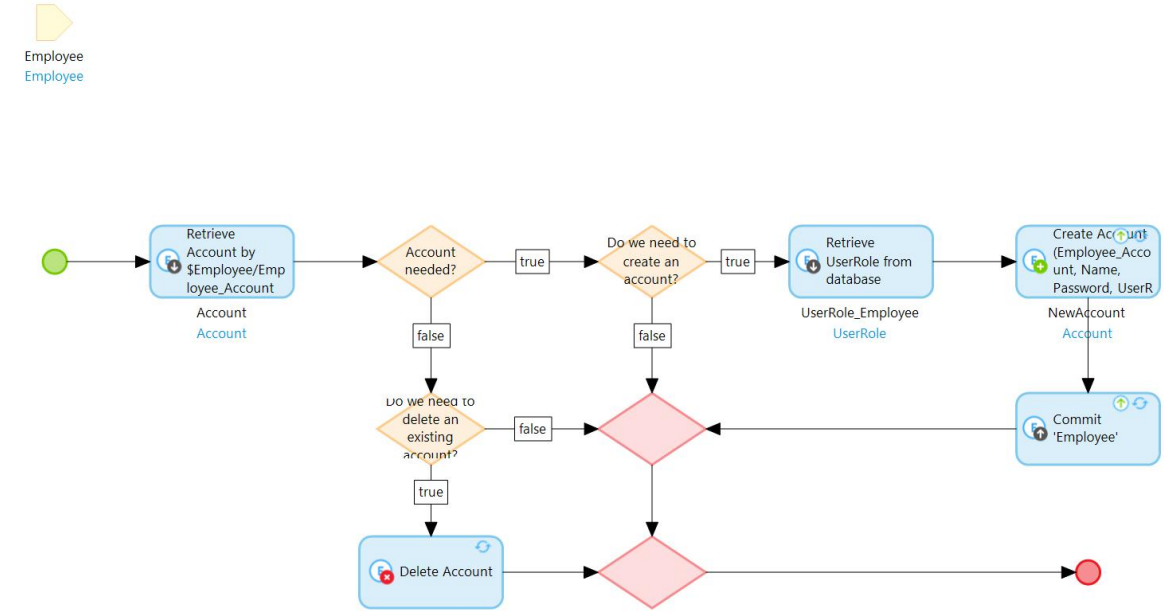
21. 从微流中移除**结束事件**，您将在以后添加它。



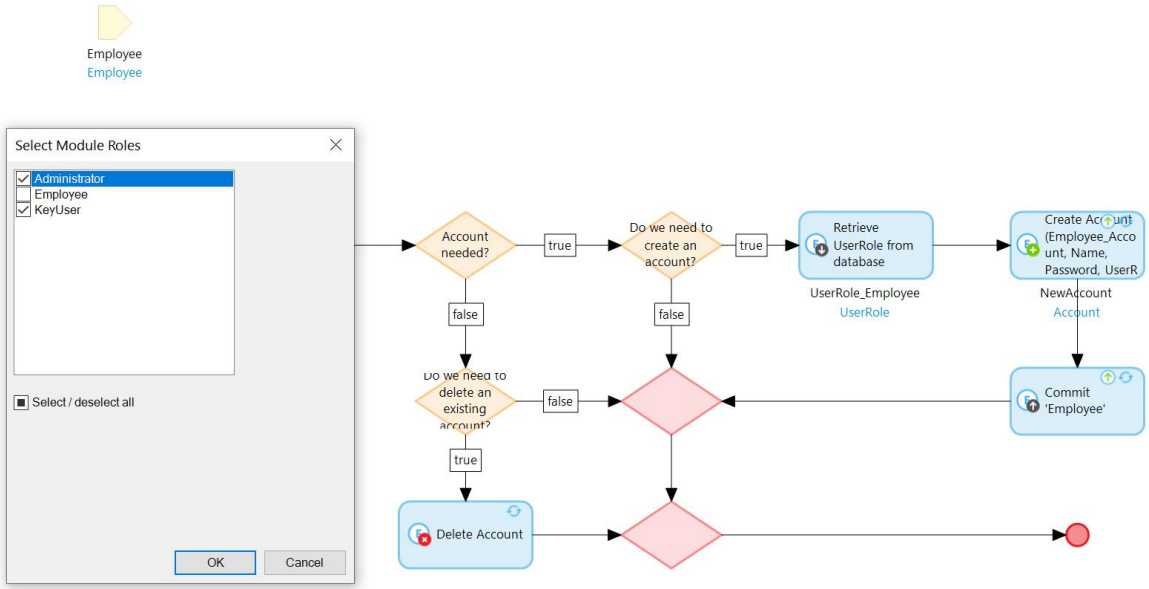
22. 要确保您的帐户和员工之间的关系被存储，使用**提交对象**活动明确地提交**员工**对象是很重要的。除此之外，您将把几个流程合并成一个，使这个微流更紧凑一些。将所有必需的元素添加到微流，以便其如下图所示。记住要启用**客户端刷新**。



23. 作为最后一步，如果您不再需要某个帐户，但它仍然存在，您需要删除该帐户。为此，您可以使用**帐户**对象上的**删除对象**活动。将所有必需的元素添加到微流，使其如下图所示。记住要启用**客户端刷新**。



24. 不要忘记为您的新微流设置安全性。您可以在属性窗格中通过单击**允许的角色**，并单击带有三个点的方框来打开**选择模块角色**窗口，以此完成这一操作。赋予**管理员**和 **KeyUser** 访问这个微流的权限。

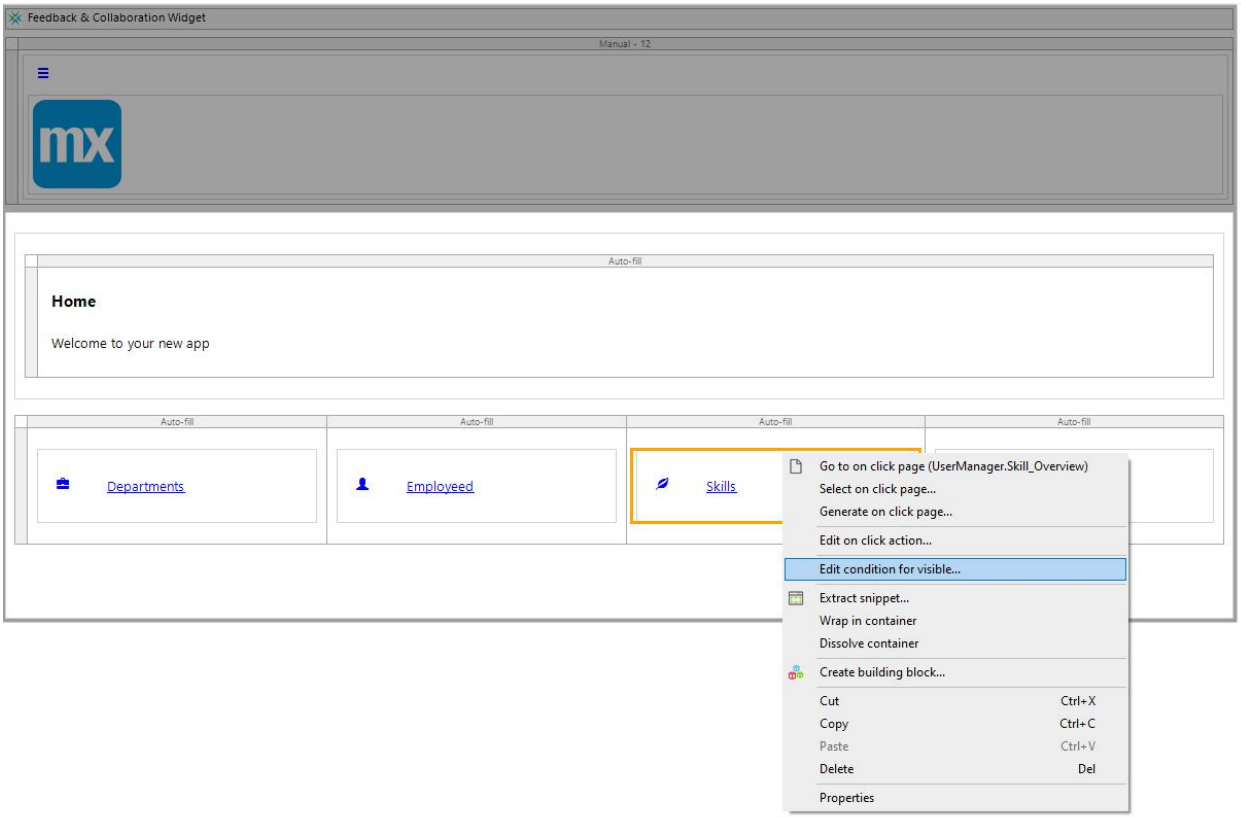


工作量相当大，而且有很多新活动。Summerhill 医院的人将会对您的辛勤工作感到非常满意。除此之外，您还学习了许多有关微流的新知识。

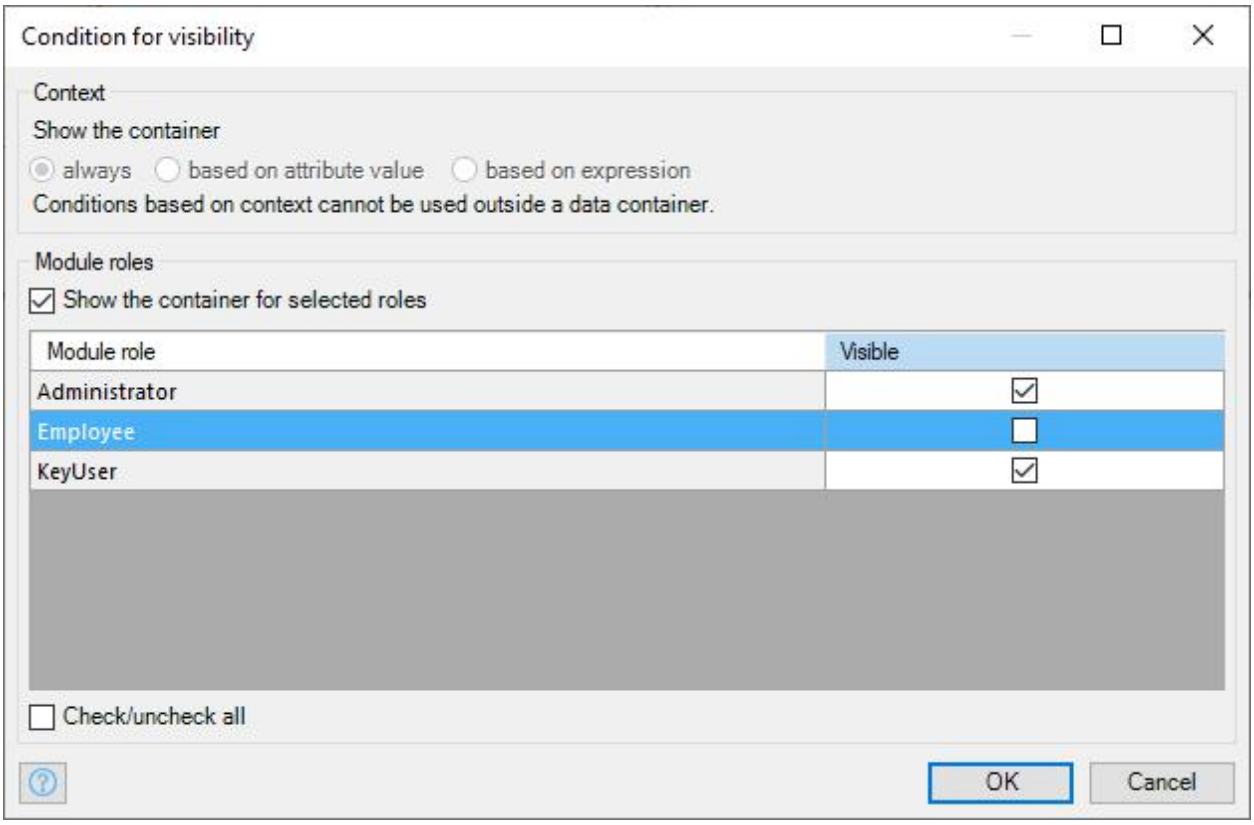
讲座 8.7.2：更新主页

现在您已经配置了安全性，可以修复主页了。虽然大多数小组件会对安全问题做出反应并隐藏自己，但对容器来说却不是这样。由于主页上的按钮基于容器，因此它们是可见的。由于有些页面对员工来说是不可访问的，您应根据**模块角色**使用**附条件的可见性**来隐藏它们。

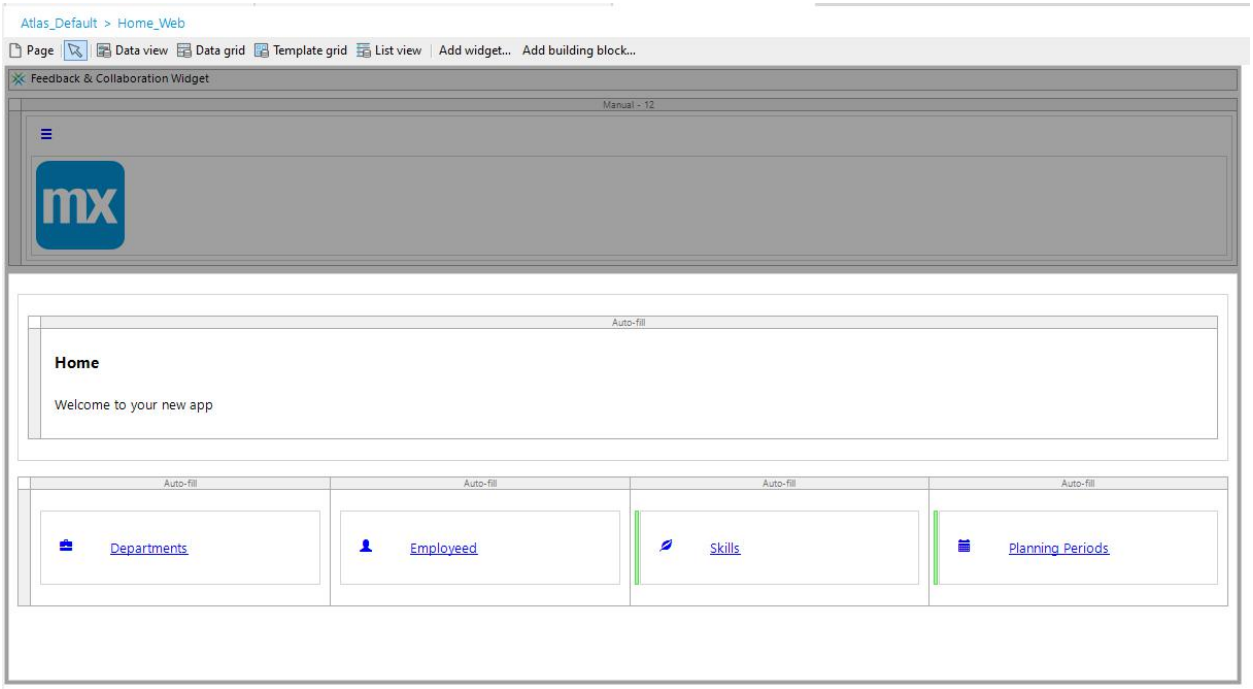
1. 打开 **Home_Web**，右键单击**技能卡操作**的容器。选择**编辑可见性条件**。



2. 在**模块角色**部分，勾选**显示所选角色的容器**，并取消勾选**员工**的复选框。



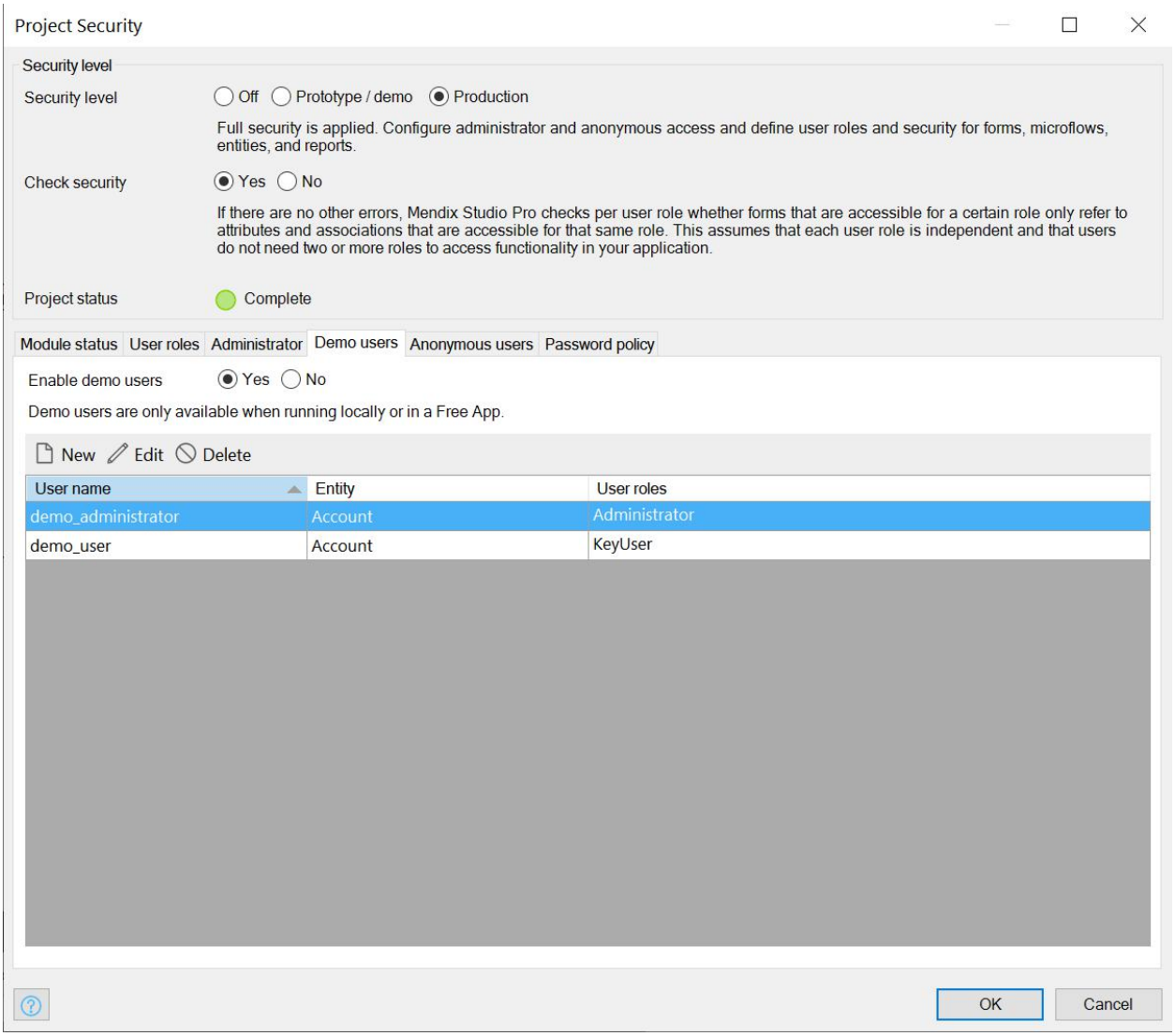
3. 对**规划期间卡操作**重复这一过程。



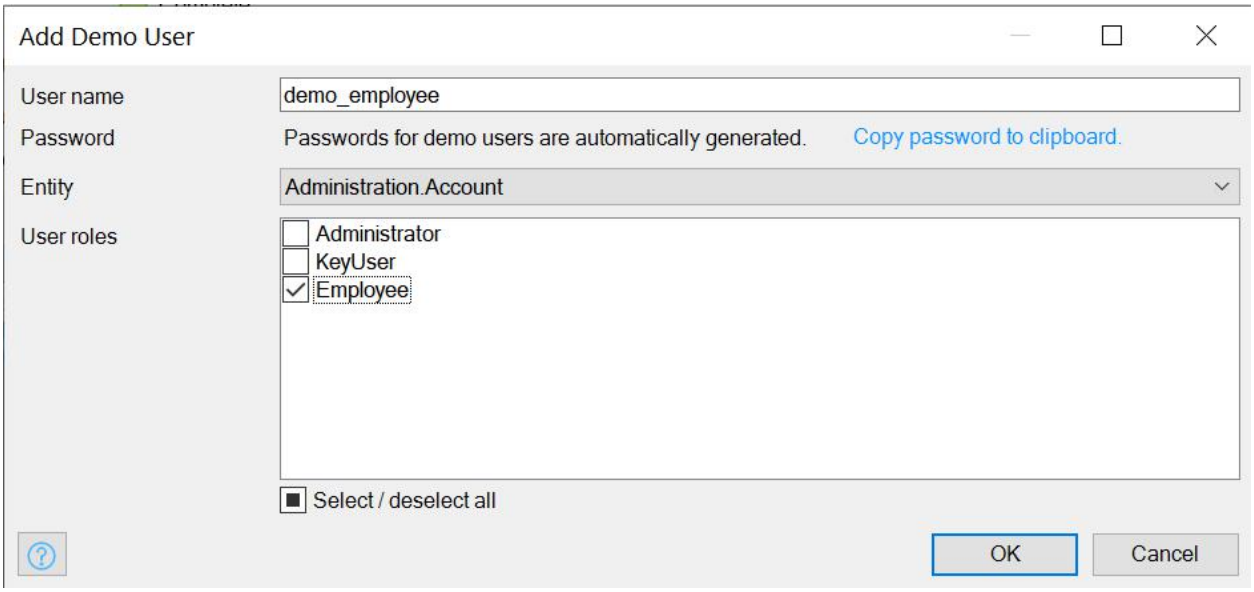
讲座 8.7.3：设置演示用户

最后一件事是帮助测试应用程序：正确配置 demo_users 应用程序。

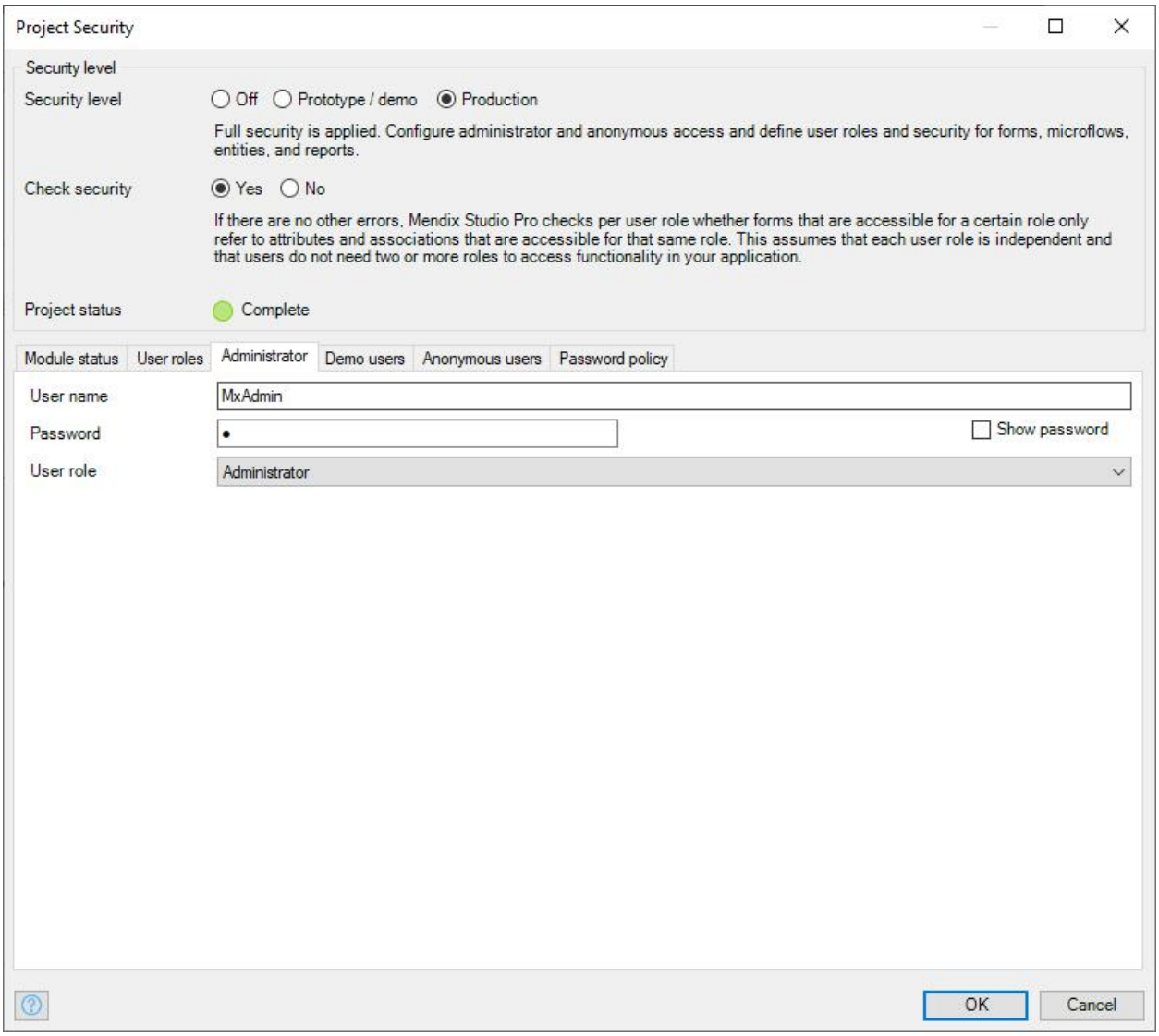
1. 进入**项目安全性**设置，然后进入**演示用户**选项卡。



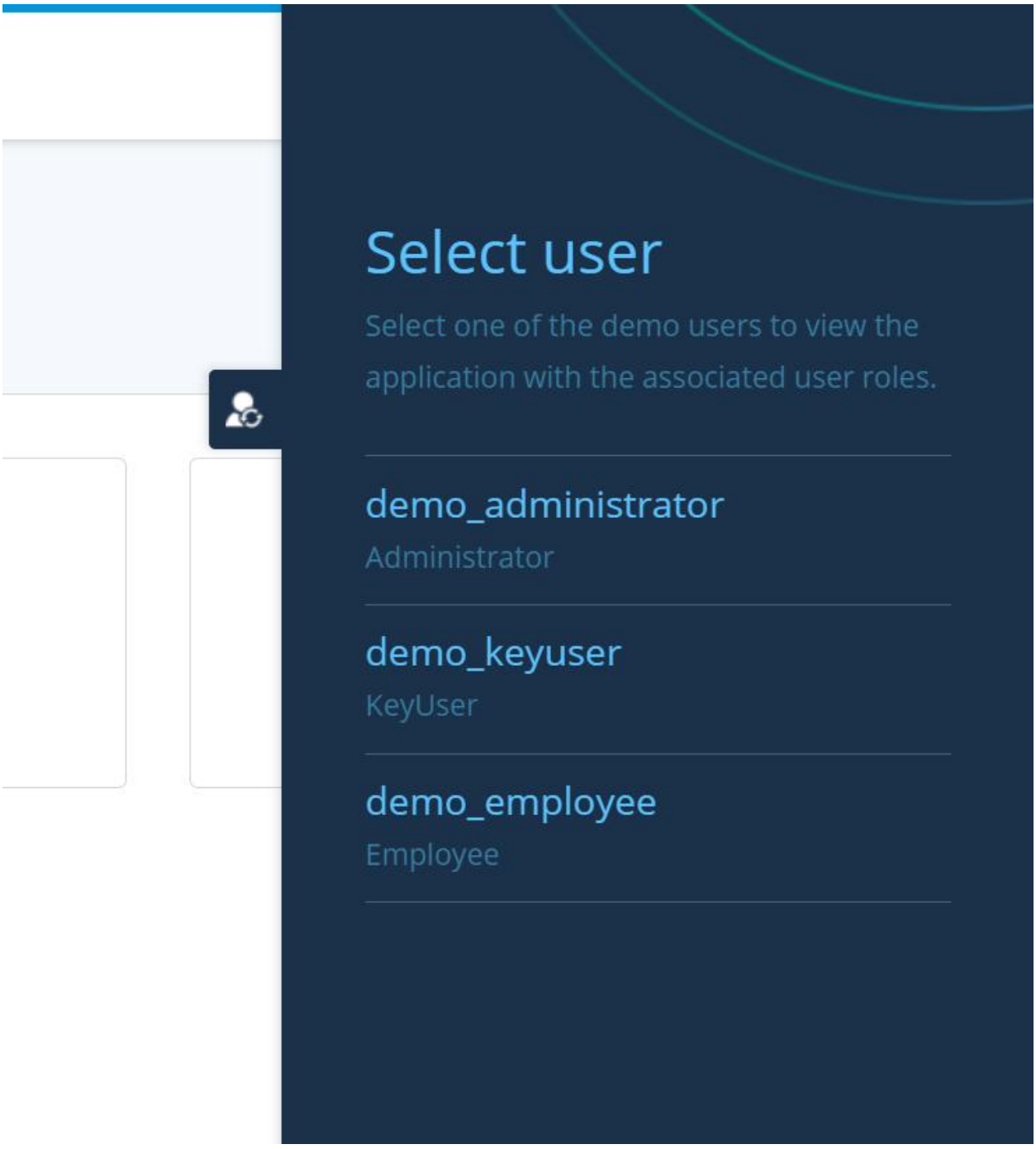
2. 默认情况下，系统给出两个实体。将 **demo_user** 重命名为 **demo_keyuser**，然后创建第三个：**demo_employee**。确保将实体设置为 **Administration.Account**。



3. 祝贺您，您的应用程序现在的状态很好。现在是时候在本地运行这个应用程序，看看一切是否如预期般运作。
4. 尝试以“**MxAdmin**”的身份和默认密码“**1**”登录。您可以在项目的**安全性**部分的**管理员**选项卡上找到该密码。默认情况下，密码处于隐藏状态，但如果选中**显示密码**复选框，您将能够看到该密码，而没有任何问题。



登录后，请注意屏幕右侧带用户图像和定向圆的小正方形选项卡。如果您单击它，您可以使用演示用户在用户角色之间即时切换，看看您的应用程序是如何表现的，这比制作一堆测试帐户要容易得多！



总结

非常好，您现在拥有保护 Mendix 应用程序安全所需的全部信息。我们涵盖了最重要的方面，如项目安全性与模块安全性的对比、角色如何在安全性的两个部分中发挥重要作用，以及您如何设置对模块中的元素的访问权限。最后，您使用微流为用户创建和删除帐户。Summerhill 的人们对您的工作非常满意，所以该进入下一个主题了。