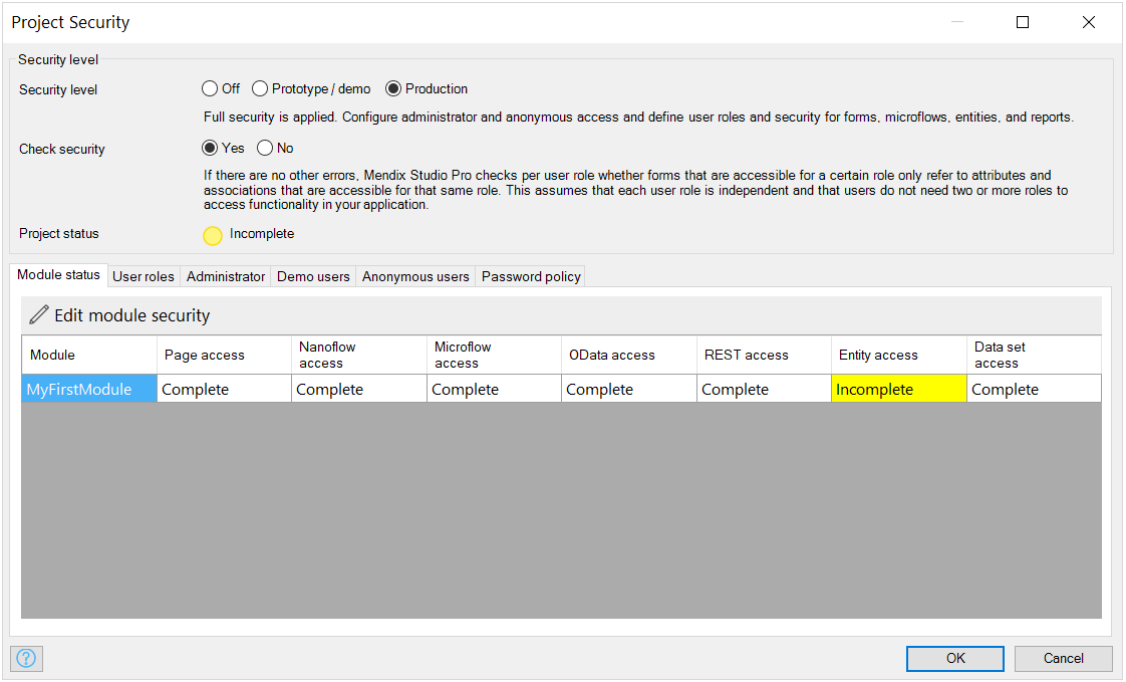
项目安全性

1 简介

在**项目安全性**中，可以开启或关闭整个项目的安全性。此外，还可配置与项目相关的安全设置，例如用户角色、管理员凭据、演示用户、匿名用户和密码策略。要能够配置每个模块的安全性或实体的访问规则，首先需要开启项目安全性。

要配置项目安全性，打开**项目资源管理器 > 项目 > 安全性**。随后将打开对话框：



关于安全性的更多常规信息，请参见安全性。

2 安全级别

安全级别定义项目的安全性是否关闭或是开启，以及需要配置哪些安全设置。

安全级别	应用安全性的方式	要配置的安全设置
关闭	未应用任何安全性。用户无需登	无

	录，即可访问所有内容。	
原型/演示	安全性应用于登录、表单和微流。用户可以访问所有数据。	管理员和匿名访问、用户角色以及表单和微流的安全性。
生产	应用完全安全性。	管理员和匿名访问、用户角色以及表单、微流、实体和报告的安全性。

对于所有已许可的 Mendix Cloud 节点，需要使用**生产**安全级别并相应配置所有安全设置。安全级别**关闭**和**原型/演示**仅允许在以下情况下使用：进行本地测试和部署免费应用程序，以及处于 Mendix Cloud 外部以**开发模式**特定设置的云环境中。

2.1 不同安全级别的设置可用性

对于不同的安全级别，可以使用不同的设置。下表给出了包含所有安全设置的列表及其每个安全级别的可用性：

设置名称	安全性关闭	原型/演示安全性	生产安全性
检查安全性	不适用	不适用	可用
项目状态	不适用	可用	可用
模块状态	不适用	可用	可用
用户角色	不适用	可用	可用
管理员	不适用	可用	可用
演示用户	不适用	可用	可用
匿名用户	不适用	可用	可用
密码策略	不适用	可用	可用

2.2 检查安全性

如果安全级别设为**生产**，可以指定是否检查安全设置的一致性。

启用**检查安全性**时，Studio Pro 将针对每个用户角色检查哪些表单可以直接在菜单栏中访问，或者可以通过下列表单和微流间接访问。对于上述每个表单，Studio Pro 将检查当前

用户角色是否可以访问引用的属性和关联。不然会将错误添加到错误列表。这些错误仅在没有其他一致性错误时显示。

2.3 项目状态

项目状态指示当前项目安全级别的安全状态。

项目状态	描述
完成	已配置当前安全级别的所有安全设置。
未完成	需要配置当前安全级别的某些安全设置。

3 模块状态

模块状态选项卡显示每个模块的安全状态。它显示需要配置安全性的项总数，以及已配置安全性的项数。

在**原型/演示**安全级别，将显示页面访问和微流访问的状态。

此外，在**生产**安全级别，将显示实体访问和数据集访问的状态（如适用）。

4 用户角色

用户角色聚合了对数据、页面和微流的多个访问权限。应用程序的最终用户由管理员指派给一个或多个用户角色，并获取这些用户角色表示的所有访问权限。

5 管理员

在**项目安全性**的**管理员**选项卡中，可以更改“管理员”用户的默认凭证和用户角色。

6 演示用户

演示用户演示应用程序中现有的每个用户角色。可以使用演示用户测试应用程序针对每个用户角色展示的外观，或向其他人演示应用程序。

7 匿名用户

匿名用户允许最终用户在无需登录的情况下访问应用程序。可为匿名用户指派特定的用户角色，以此限制其可以访问的数据。

8 密码策略

指定用户创建帐户和设置密码时的密码要求。例如，如果密码必须包含数字或大写字符，可以设置密码的最小长度。