

# 已发布 OData 服务

## 1 简介

在 Studio Pro 中，可通过添加新的已发布 OData 服务将实体作为 OData 资源公开。可在已发布的 OData 服务中公开任何数量的相关资源。默认情况下，URI 中使用实体的非限定名称作为唯一标识，但也可覆盖资源名称。

Mendix 中用于 OData 的标准是 OData 版本 3，默认表示形式设为 Atom XML。该标准的所有部分并非均已实施。如果此处未记录某些内容，则表明尚未添加该内容。

本文档介绍创建已发布 OData 服务时可用的选项，并以一些运行时注意事项作为结尾。

## 2 常规

### 2.1 服务名称

服务名称可用于为 OData 服务创建唯一 URI。因此，服务名称应遵循 RFC 3986 和 RFC 3987 采用正确格式。

### 2.2 版本

使用**版本**字段为服务指派版本号。该编号将显示在 API 文档中。

### 2.3 命名空间

在 OData 中，命名空间可用于引用数据类型。在**设置**选项卡上可自定义该命名空间。可将其更改为以字母开头，后跟字母、数字或圆点，且最大长度为 512 个字符的任意值。

### 2.4 资源

**资源**是代表实体的网络可访问数据对象，通过 URI 予以标识。

## 3 设置

### 3.1 关联

可选择希望如何表示关联。有关更多信息，请参见 *OData* 表示的[关联](#)部分。

### 3.2 安全性

启用“项目安全性”后，可为 OData 服务配置安全性。

#### 3.2.1 需要身份验证

版本 8.0.0 中引入了**无身份验证**功能。在更早版本中，身份验证方式始终是**用户名和密码**。

版本 8.0.0 中还引入了**活动会话**和**自定义身份验证**。

选择客户端是否需要**进行身份验证**。选择**否**将允许不受限制地访问资源。选择**是**可选择要支持哪些身份验证方法。

即使选择**是**，仍可向匿名用户公开 OData 资源。有关允许匿名用户的详细信息，请参见“匿名用户角色”。

#### 3.2.2 身份验证方法

如果需要身份验证，可选择想要支持的身份验证方法。

- 选择**用户名和密码**，允许客户端使用**授权**标头中的用户名和密码进行自我身份验证（这称为“基本身份验证”）
- 选择**活动会话**，允许从当前应用程序内的 JavaScript 访问
- 选择**自定义**，以使用微流进行身份验证（每当用户希望访问某个资源时，都会调用该微流）

选中多种身份验证方法，以便服务一一进行尝试。首先会尝试**自定义身份验证**，然后是**用户名和密码**，最后是**活动会话**。

### 3.2.2.1 用户名和密码

可通过在调用的 HTTP 标头中包含基本身份验证来完成身份验证。为此，需要构造名为**授权**的标头，且其内容应构造如下：

1. 用户名和密码组合成字符串“username:password”。
2. 然后，使用 Base64 的 RFC2045-MIME 变体对生成的字符串进行编码（但不限于 76 个字符/行）。
3. 授权方法和单个空格（即，随后将“Basic”放置在编码字符串之前）。

此结果是一个标头，类似于 `Authorization: Basic QWxhZGRpbjpvYVUyIHNlc2FtZQ==`。

### 3.2.2.2 活动会话

检查此身份验证方法时，应用程序中的 JavaScript 可使用当前用户的会话访问 REST 服务。

为了防止跨网站请求伪造，需要在每个请求上设置 X-Csrf-Token 标头，例如：

```
var xmlHttp = new XMLHttpRequest();
xmlHttp.open("GET", "http://mysite/odata/myservice/myresource", false);
xmlHttp.setRequestHeader("X-Csrf-Token", mx.session.getConfig("csrftoken"));
xmlHttp.send(null);
```

### 3.2.2.3 自定义

指定将哪个微流用于自定义身份验证。

微流可能采用 `HttpRequest` 作为参数，因此可检查传入的请求。

微流也可采用 `HttpResponse` 作为参数。当微流将该响应的状态代码设为除 **200** 以外的其他值时，该值将返回，且操作将不会执行。在响应上设置的任何标头都将返回（微流返回空用户时除外）。

身份验证微流应返回“用户”。

身份验证微流有三种可能的结果：

- 当 `HttpResponse` 参数的状态代码设为除 **200** 以外的其他值时，该值将被返回，且操作将不会执行
- 当生成的“用户”非空时，操作会在该用户的上下文中执行

- 当生成的“用户”为空时，会尝试下一种身份验证方法（如果没有其他身份验证方法，则结果为 **404 找不到**）

### 3.2.3 允许的角色

允许的角色定义了用户必须具备哪个模块角色才能访问服务。该选项仅在**需要身份验证**设置为**是**时可用。

Web 服务用户无法访问 OData 服务。

## 4 属性

在已发布 OData 服务的属性窗格中，可编辑一些也能在*常规*选项卡中设置的属性，例如*服务名称*、*版本*和*命名空间*。

本节介绍了可以设置的其他属性。

### 4.1 文档

可在此描述服务的用途。本文档专供处理该项目的其他人员阅读，OData 服务的用户无法使用。

### 4.2 替换非法 XML 字符

某些特殊字符无法在 XML 中使用。如果数据中包含这些字符，则客户端会收到错误消息。如果将该设置设为**是**，则这些非法字符将由 DEL 字符所替换，且客户端不会收到错误消息。但是，由于这些字符已被替换，因此客户端接收的数据不会与数据库中存储的数据完全相同。

默认值：

该属性在 Studio Pro 8.12.0 及更高版本中可用。

### 4.3 公用文档

可编写*摘要*和*描述*，以供使用服务的人员使用。

## 5 运行时注意事项

### 5.1 常规

一旦支持 OData 的应用程序处于运行状态，后跟 `/odata-doc/` 的根 URL 上就会提供公开 OData 资源的概述。例如，`http://localhost:8080/odata-doc/`。比如，可将链接复制并粘贴到 Excel 中，以在 OData 资源和 Excel 之间建立链接。

虽然 OData 资源的 API 文档在默认情况下处于启用状态，但对于在生产中运行的应用程序，管理员可能会限制对该文档的访问。

有关如何筛选 OData 响应的详细信息，请参见“OData 查询选项”。

有关如何在 OData 中表示 Mendix 属性的详细信息，请参见“OData 表示”。

通过 OData 公开实体时，会以流式传输方式从 Mendix 数据库中检索实体，以避免 Mendix 运行时出现内存不足错误。

### 5.2 本地部署

某些本地服务器（尤其是使用 Microsoft IIS 的服务器）将从请求中剥离主机标头。这意味着，OData 服务和文档将在非预期 URL 上发布。

要解决此问题，需确保服务器保留主机标头。请参见 *Microsoft Windows* 部署文档中的“保留主机标头”部分。