实施 Microsoft 身份（第二部分）

- 实施身份验证
- 实施授权

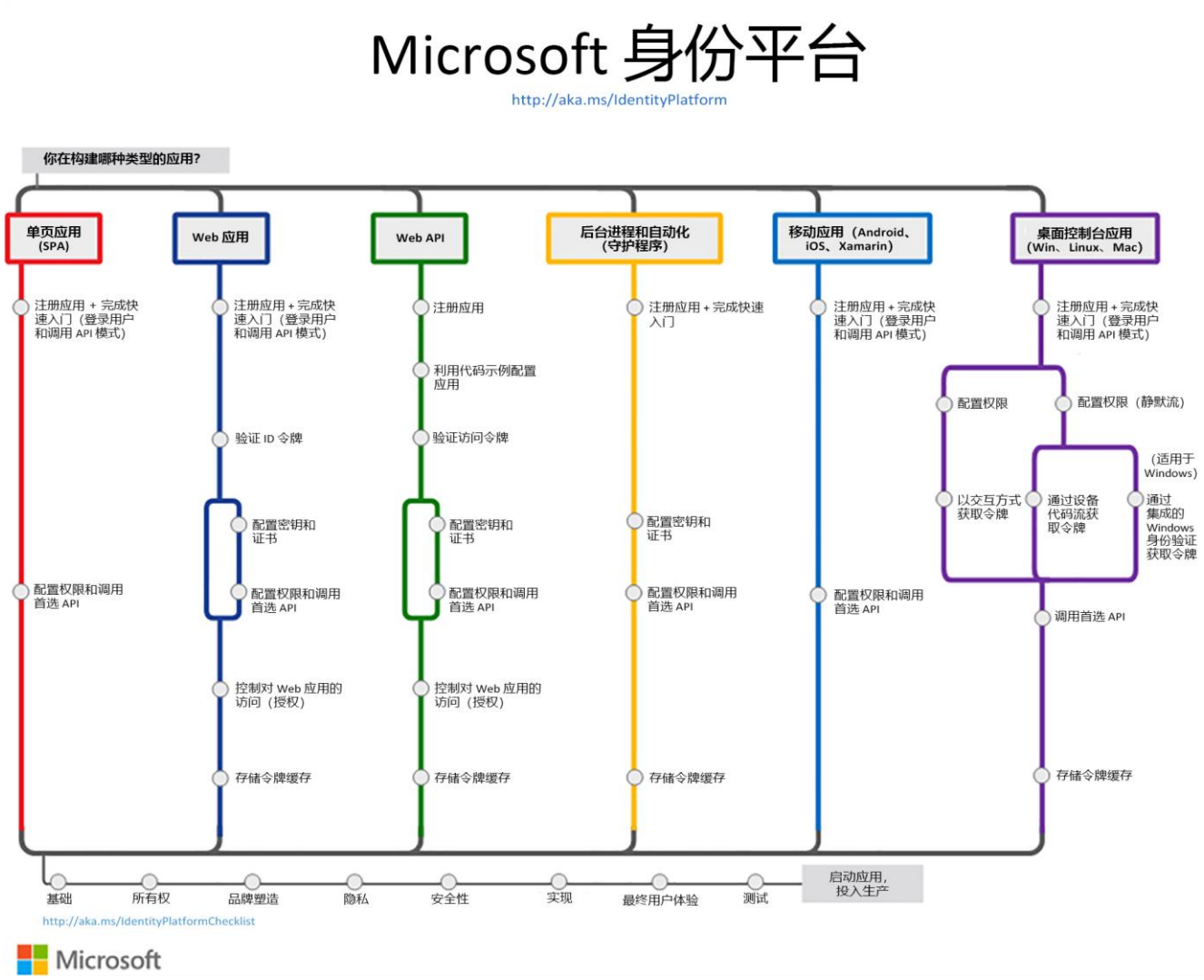
Microsoft

实施身份验证

身份验证流和应用场景

身份验证类别

- 受保护的资源与客户端应用程序
- 有用户或无用户
- 单页、公共客户端和保密客户端应用程序
- 登录受众
- 支持的 OAuth 2.0 流
- 支持的平台



Microsoft 身份验证库 (MSAL)

Microsoft 身份验证库 (MSAL) 使开发人员能够从 Microsoft 身份平台终结点获取令牌，以便访问受保护的 Web API。

- 应用程序类型和场景。
- 语言和框架。

Microsoft 身份的安全令牌

· ID 令牌

ID 令牌是一种安全令牌，支持客户端验证用户的身份。

· 访问令牌

访问令牌使客户端能够安全地调用受 Azure AD 保护的 API。访问令牌有时被称为“用户+应用”或“仅应用”

演示

实施身份验证

Microsoft

实施授权

授权模型概述

与 Microsoft 身份平台集成的应用程序遵循一种授权模型，使用户和管理员能够控制访问数据的方式。

- OAuth 2.0 授权代码流
- 范围和权限
- 委派权限与应用程序权限
  - 有效权限
- 请求整个租户的许可
- 管理员限制权限

管理员许可

- 某些权限需要管理员的许可，然后才能在租户中被授予。你还可以使用管理员许可终结点向整个租户授予权限。
- 应用注册 UI 显示授予应用的权限和管理员许可。它包含以下部分：
  - 配置的权限。
  - 授予的其他权限。
  - 管理员许可按钮。
- 向目录管理员请求权限。
- 了解应用程序授权许可。

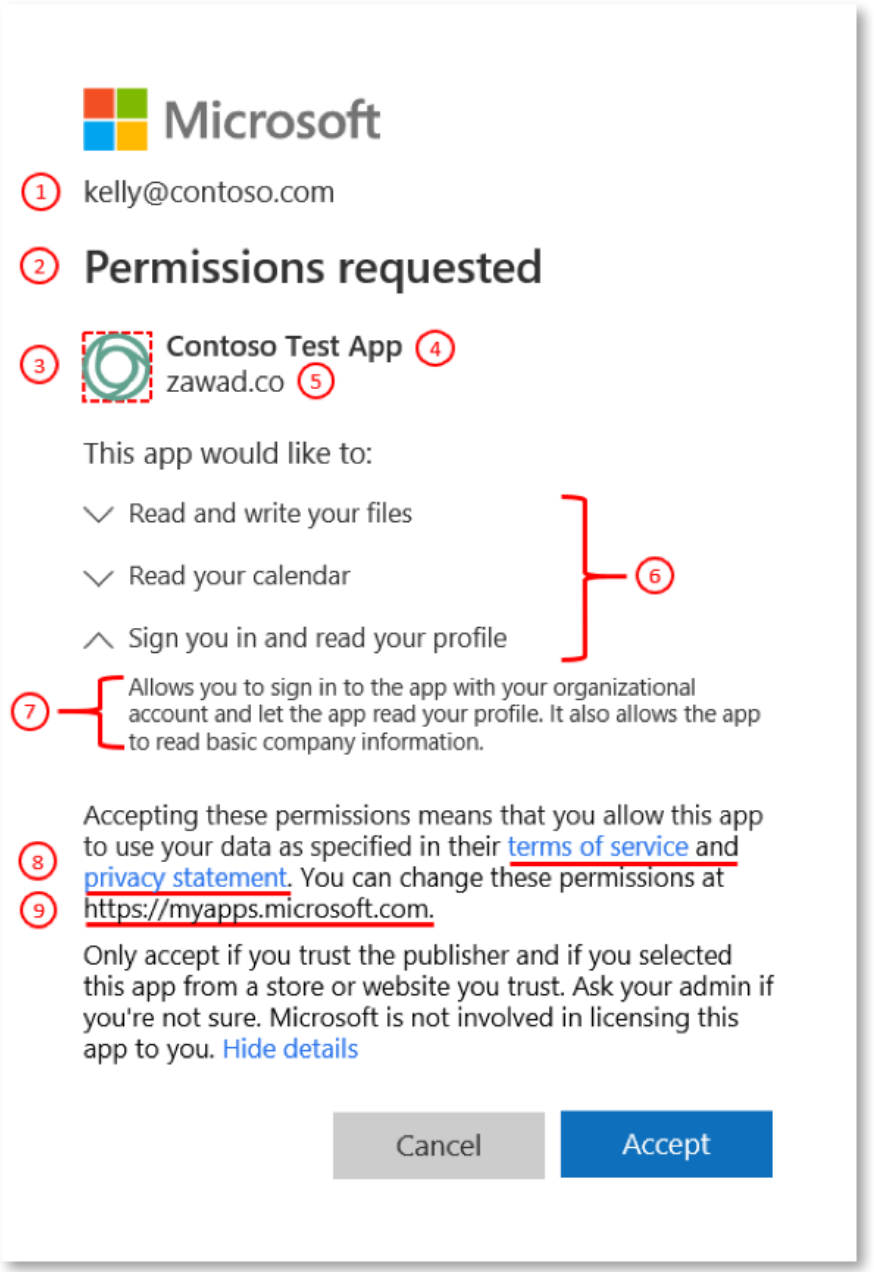
应用程序许可体验

· 用户许可流程

如果应用程序开发人员将用户定向到授权终结点，目的是仅记录当前用户的许可。

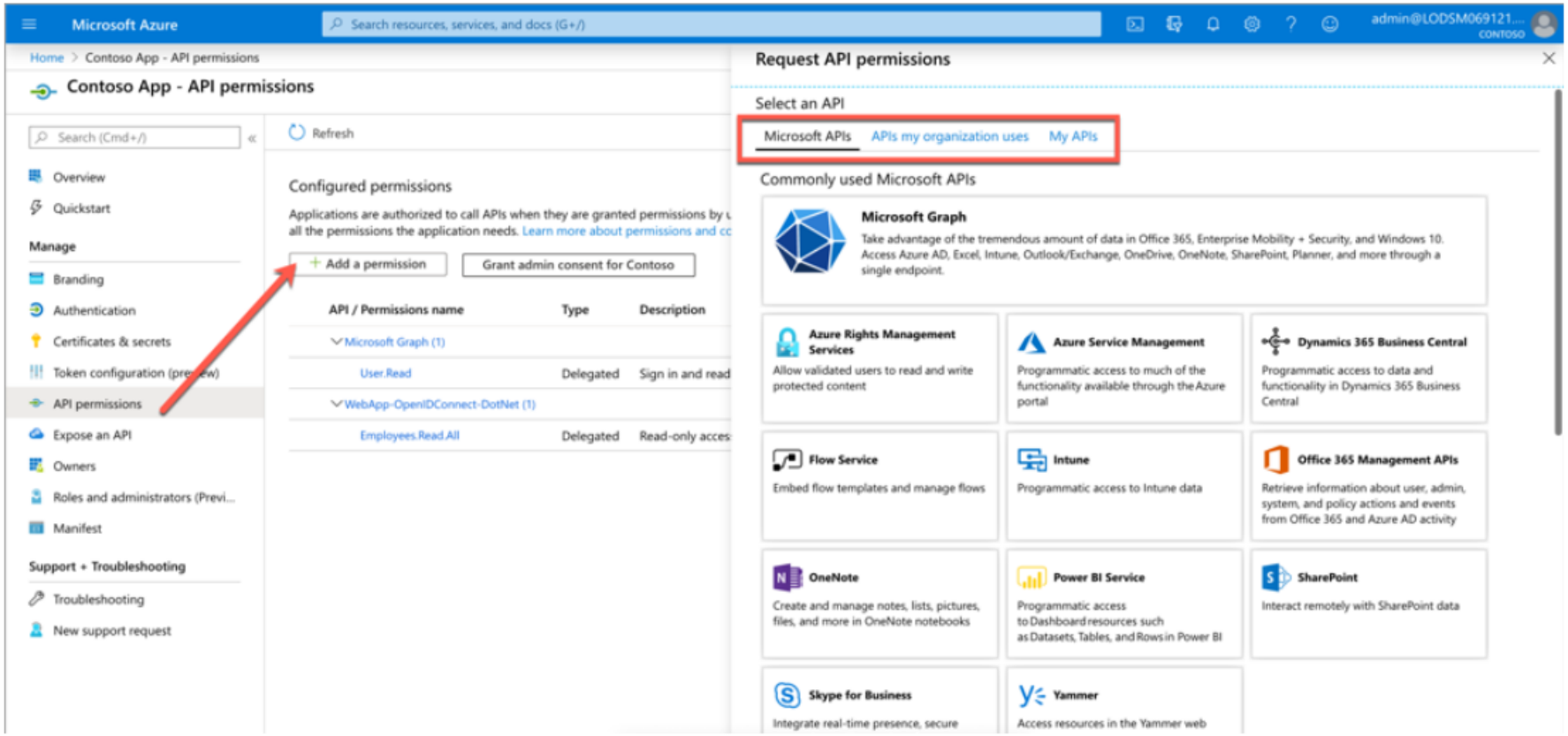
· 管理员许可流程

如果应用程序开发人员将用户定向到管理员许可终结点，目的是记录整个租户的许可。为了确保管理员许可流程正常工作，应用程序开发人员必须在应用程序清单的 RequiredResourceAccess 属性中列出所有权限。



添加访问 Web API 的权限

- Microsoft API
- 我的组织使用的 API
- 我的 API



使用 Microsoft 身份保护自定义 API

利用 Microsoft 身份保护 Web API（可由其他应用程序调用）涉及两项主要任务：

- 注册和配置 Azure AD 应用程序
  - 定义范围
- 编码 Web API 项目，配置为支持 Microsoft 身份
  - 添加支持，以验证当前请求是否具有必要的范围

调用 Microsoft Graph API

Microsoft Graph API 通过 REST API 终结点提供对 Azure AD 的编程访问。应用程序可以使用 Microsoft Graph API 对目录数据和对象执行创建、读取、更新和删除 (CRUD) 操作。

- 提供以下功能：
  - REST API 终结点。
  - 用 Azure AD 进行身份验证。
  - 基于角色的授权 (RBAC)。
  - 差异化查询。
  - 目录扩展。
  - 由权限范围保护。
- 支持应用场景，例如：
  - 业务线（单一租户）应用程序。
  - 软件即服务（多租户）应用程序。

演示

实施授权以使用 API