Application management with Azure Active Directory

Introduction to Application management

Azure Active Directory (Azure AD) provides secure and seamless access to cloud and on-premises applications. Users can sign in once to access Office 365 and other business applications from Microsoft, software as a service (SaaS) applications, on-premises applications, and line of business (LOB) apps

Key advantages

- Manage risk with conditional access policies
- Improve productivity with single sign on
- Address governance and compliance
- Manage costs

Introduction to Single sign on

Single sign-on (SSO) adds security and convenience when users sign-on to applications in Azure Active Directory (Azure AD).

Advantages of Single sign on

- One set of credentials to access domain joined devices, company resources, SaaS applications and web applications hosted on on-premise
- User can launch application from office 365 portal or Azure AD My apps panel
- Centralised user access management to applications based on group membership

Single sign on options

OpenID Connect and Oauth - When developing new applications, use modern protocols like Open ID Connect, and OAuth.

Disable SSO - Disabled mode means single sign-on isn't used for the application. When single sign-on is disabled, users might need to authenticate twice. First, users authenticate to Azure AD, and then they sign in to the application.

SAML SSO - With SAML single sign-on, Azure AD authenticates to the application by using the user's Azure AD account. Azure AD communicates the sign-on information to the application through a connection protocol

Header based SSO - Header-based single sign-on works for applications that use HTTP headers for authentication. This sign-on method uses a third-party authentication service called PingAccess. A user only needs to authenticate to Azure AD

This slide is 100% editable. Adapt it to your needs and capture your audience's attention.

Password based SSO - With password-based sign-on, users sign on to the application with a username and password the first time they access it. After the first sign-on, Azure AD supplies the username and password to the application.

Integrated Windows Authentication (IWA) SSO Application Proxy provides single sign-on (SSO) to applications that use Integrated Windows Authentication (IWA), or claims-aware applications

Linked SSO - Linked sign-on enables Azure AD to provide single sign-on to an application that is already configured for single sign-on in another service.

Decision tree for SSO option