Configuring and Customizing Software Applications in Microsoft Entra ID (Azure AD) Enterprise Applications

Overview

Microsoft Entra ID (formerly Azure Active Directory) provides a feature called **Enterprise Applications**, which allows cloud administrators to configure, customize, and manage software applications used within an organization. These applications can be **SaaS (Software as a Service)** applications from the Azure AD gallery, custom-developed applications, or third-party applications that support integration with Microsoft Entra ID.

As a **Cloud Administrator**, you can:

1. Add and configure applications from the Azure AD gallery or third-party vendors.
2. Assign roles and users to applications.
3. Configure **Single Sign-On (SSO)** to enable seamless authentication for users (only for licensed users).
4. Customize application properties based on organizational requirements.

This documentation provides a step-by-step guide to configuring and managing software applications in the **Enterprise Applications** section of Microsoft Entra ID.

Table of Contents

1. Accessing Enterprise Applications in Microsoft Entra ID

To access the **Enterprise Applications** section:

1. Log in to the **Azure Portal**: https://portal.azure.com.
2. Navigate to **Microsoft Entra ID** (Azure AD) from the left-hand menu.

3. Under **Manage**, select **Enterprise Applications**.

2. Adding an Application from the Azure AD Gallery

To add a software application from the Azure AD gallery:

1. In the **Enterprise Applications** section, click **New Application**.
2. Select **Browse Azure AD Gallery**.
3. Search for the desired application (e.g., Cisco Webex, Salesforce, Slack).
4. Click on the application and select **Create**.
5. The application will now appear in your list of enterprise applications.

3. Configuring Single Sign-On (SSO)

To configure SSO for an application:

1. Select the application from the **Enterprise Applications** list.
2. Under **Manage**, click **Single Sign-On**.
3. Choose the SSO method:
    a. **SAML**: For applications that support SAML-based authentication.
    b. **OpenID Connect**: For modern applications that support OAuth 2.0 and OpenID Connect.
    c. **Password-based**: For applications that require username and password authentication.
4. **For SAML-based SSO**:
    a. Upload the **Service Provider Metadata** file (if provided by the application vendor).
    b. Enter the **Identifier (Entity ID)**, **Reply URL**, and **Sign-on URL** manually if required.
    c. Configure **Attributes and Claims** to map user attributes (e.g., email, name) between Microsoft Entra ID and the application.
    d. Download the **Federation Metadata XML** file from Microsoft Entra ID and upload it to the application's SSO configuration page (if required).
5. **Test SSO**:
    a. Use the **Test** button to verify the SSO configuration.
    b. Sign in to the application using Microsoft Entra ID credentials to ensure the setup works correctly.

4. Assigning Users and Roles to Applications

To assign users and roles to an application:

1. Select the application from the **Enterprise Applications** list.
2. Under **Manage**, click **Users and Groups**.
3. Click **Add User/Group**.
4. Select the users or groups you want to assign to the application.
5. Assign a **Role** (if applicable):
    a. Some applications support role-based access control (RBAC). For example, you can assign roles like **User**, **Admin**, or custom roles defined by the application.
6. Click **Assign** to complete the process.

Best Practices for Managing Enterprise Applications

1. **Regularly Review Assigned Users and Roles**:
    a. Periodically audit user assignments and roles to ensure compliance with organizational policies.
2. **Enable Conditional Access**:
    a. Use conditional access policies to enforce security rules (e.g., MFA, location-based access) for sensitive applications.
3. **Monitor Sign-in Logs**:
    a. Regularly review sign-in logs to detect and respond to suspicious activities.
4. **Use Application Templates**:
    a. For custom applications, use **Azure AD Application Templates** to streamline configuration.
5. **Train End Users**:
    a. Provide training to end users on how to access and use applications via the **My Apps** portal.

Conclusion

The **Enterprise Applications** section in Microsoft Entra ID is a powerful tool for cloud administrators to configure, customize, and manage software applications based on

organizational requirements. By following the steps outlined in this documentation, you can:

- Add and configure applications from the Azure AD gallery or third-party vendors.
- Enable SSO for seamless user authentication.
- Assign users and roles to applications.
- Monitor and manage application usage effectively.

For further details, refer to the official Microsoft documentation:

Microsoft Entra ID Enterprise Applications Documentation.