Azure Active Directory Single Sign-On - Adoption Kit

Contents

Awareness

This section helps you to analyze the benefits of Azure Active Directory (Azure AD) Single Sign-On. You will learn about the ease of use, pricing and licensing model, as well as customer stories about how it helped improve their business. You will also receive up-to-date announcements and access to blogs that discuss ongoing improvements.

Business Overview

Azure AD Single Sign-On (SSO) helps you access all the apps and resources you need to do business, while signing in only once, using a single user account. After you have signed in, you can go from Microsoft Office to SalesForce to Box without being required to authenticate (for example, type a password) a second time.

- **Without single sign-on**, users must remember application-specific passwords and sign-ins for each application. IT staff needs to create and update user accounts for each application such as Office 365, Box, and Salesforce. Users need to remember their passwords, plus spend the time to sign into each application.
- **With single sign-on**, users sign in once with one account to access domain-joined devices, company resources, software as a service (SaaS) applications, and web applications. After signing in, the user can launch applications from the Office 365 portal or the Azure AD MyApps access panel. Administrators can centralize user account management, and automatically add or remove user access to applications based on group membership.

Watch this video to see how easy it is to use Windows Azure AD to configure single sign-on from your organization Overview of Single Sign-On.

Ensure your applications have the best single sign-on experiences for end users. Refer to Single sign-on best practices for Azure Active Directory and Microsoft accounts.

Pricing and Licensing Requirements

With Azure AD Free, end users who have been assigned access to SaaS apps are allowed SSO access to up to 10 apps. Admins can configure SSO and change user access to different SaaS apps, but SSO access is only allowed for 10 apps per user at a time. All Office 365 apps are counted as one app.

With Azure AD Premium P1 and Premium P2, there is no limit to the number of apps that the end users can access. However, the number of objects in your directory and the features you wish to deploy may require additional licenses. Common Azure AD scenarios include the following security features:

- Conditional Access (CA) (P1 Required)
- Azure Multi-Factor Authentication (MFA) (P1 Required)
- Group based membership (P1 required)
- Identity Protection (P2 Required)

For more information, refer to the links below:

- Azure Active Directory pricing
- See the "Licensing" section in Azure AD Single Sign-On Deployment Plan

Key Benefits

Increase Productivity
Enabling **single sign-on** across enterprise applications and Office 365 provides a superior log in experience for existing users, reducing or eliminating log on prompts. The user's environment feels more cohesive and is less distracting without multiple prompts, or the need to manage multiple passwords. Access control can be managed and approved by the business group, saving IT management costs through self-service and dynamic membership. This also improves the overall security of our identity system by ensuring the right people in the business manage access to this application.

Manage Risk
Coupling Azure AD SSO with **conditional access** policies can offer significantly improved security experiences. These include cloud-scale identity protection, risk-based access control capabilities, native multi-factor authentication support, and conditional access policies which allow for stricter control policies based on applications in use, or groups that need higher levels of security.

Address Compliance and Governance
Auditing access requests and approvals for the application, as well as understanding overall application usage, becomes easier with Azure Active Directory because it supports native audit logs for every application access request performed. Auditing includes requester identity, requested date, business justification, approval status, and approver identity. This data is also available from an API, which will enable importing this data into a Security Incident and Event Monitoring (SIEM) system of choice.

Manage Cost
Replacing current access management and provisioning process and migration to Azure Active Directory to manage self-service access to the application (as well as other SaaS applications in the future) will allow for significant cost reductions related to running, managing, and maintaining your current infrastructure. Additionally, eliminating application specific passwords eliminates costs related to password reset for that application, and lost productivity while retrieving passwords.

Customer stories/Case studies

Discover how Azure AD customers can access all the applications and resources by signing in only once using their own single user account. The following featured stories demonstrate these needs.

HEARST
Corporation

Hearst Corporation - Eight things this media giant likes about Microsoft Enterprise Mobility + Security and Azure Active Directory It could take months for the Hearst IT team to deploy the resources to run a new business app. Now, Hearst uses more than 200 applications from the Azure SaaS Apps gallery that IT can have ready to run in hours. Users get single-sign-on access managed in Azure AD, and IT can apply multifactor authentication without making any changes to the apps.

Cushman & Wakefield hybrid cloud solution eases merger, acquisition impact With Azure AD Premium, Cushman & Wakefield employees enjoy such benefits as single-sign-on access and self-service password reset, which means they can focus on their jobs, and not on how to access the resources they need.

Aramex - Global logistics and transportation company creates cloud-connected office with identity and access management solution. The IT team set up all of Aramex with Single Sign-On (SSO), so all employees could quickly access SuccessFactors, Office 365, and other third-party SaaS applications within the gallery. Employees can just go to Azure AD to access all the applications they need with the click of a button.

Lululemon - Azure AD helps lululemon enable productivity and security all at once for its employees**.** Within three months of Azure AD rollout, Lululemon users loved the SSO experience so much that the business units requested that additional apps get rolled out.

To learn more about customer and partner experiences on Azure AD SSO, visit - See the amazing things people are doing with Azure.

Announcements/Blogs

Azure AD receives improvements on an ongoing basis. To stay up to date with the most recent developments, refer to What's new in Azure Active Directory?

Blogs by the Tech Community and Microsoft Identity Division:

- March 12, 2019, Support for more apps with Azure AD Application Proxy
- January 24, 2019, Single sign-on wins over business and users at lululemon!
- December 05, 2018, Step-By-Step: Setting up AD FS and Enabling Single Sign-On to Office 365
- September 07, 2018, How to enable Single Sign-On for my Terminal Server connections
- September 07, 2018, Introducing Web Single Sign-On for RemoteApp and Desktop Connections

Training/Learning Resources

The section provides concepts, role-based guidance, online training and lists resources available on Azure AD SSO.

Level 100 Knowledge/Concepts

Learn the many ways to configure an application for single sign-on. Choosing a single sign-on method depends on how the application is configured for authentication.

- Watch these videos
  - Azure Active Directory and Single Sign On
  - What's single sign-on for SaaS applications?
  - How to deploy single sign-on for SaaS applications?
  - How to roll-out single sign-on for SaaS applications?
- Choose the right SSO method in Single sign-on to applications in Azure Active Directory.

- Read Application management with Azure Active Directory
- See “Planning Single Sign-on” section in the Azure AD Single Sign-On Deployment Plan
- Follow Single sign-on best practices for Azure Active Directory and Microsoft accounts.

Role-Based Guidance

IT Administrator Staff

The Global Administrator has access to all administrative features. By default, the person who signs up for an Azure subscription is assigned the Global Administrator role for the Azure AD. Only Global Administrators and Privileged Role Administrators can delegate administrator roles. See Administrator role permissions in Azure Active Directory.

Here are some additional links to help you get started:

- Choose Tutorials for integrating SaaS applications with Azure Active Directory.
- Visit Azure Marketplace for a list of SaaS apps that have been pre-integrated into Azure AD.
- In case application-specific tutorials are unavailable, follow the Tutorial: Configure SAML-based single sign-on for an application with Azure Active Directory
- Get a step-by-step Azure AD Single Sign-On Deployment Plan
- Follow Single sign-on best practices for Azure Active Directory and Microsoft accounts.

Help Desk Staff

- Search the Microsoft Support Knowledge Base for solutions to common technical issues.
- Search for and browse technical questions and answers from the community, or ask your own question in the Azure Active Directory forums.

Training

On-Demand Webinars

Register here – Manage your Enterprise Applications with Azure AD.

Learn the various ways Azure AD can help you achieve single sign-on to your enterprise SaaS applications as well as best practices for controlling access for these applications.

Videos

Check out the video links with their description in the table below:

Site	Video	Description
Azure videos	Overview of Single Sign-On	“See how easy it is to use Windows Azure AD to configure single sign-on from your organization to Birst analytics.”

Azure videos	Introducing Single Sign-on and Active Directory Integration	"Windows Azure Active Directory (WAAD) provides single sign on (SSO) capabilities through integration with Windows Server Active Directory."
Azure videos	Single sign-on best practices for Azure Active Directory and Microsoft accounts	"Ensure your applications have the best single sign-on (SSO) experiences for end users when integrating with Azure Active Directory or Microsoft accounts."
Azure videos	Integrating Salesforce with Azure AD: How to enable Single Sign-On	"Integrate an existing Salesforce deployment with Azure Active Directory (part 1 of 2). Follow along with the video to configure single sign-on (SSO) with Salesforce."
Channel9	Azure Active Directory and Single Sign-On	"Demo showing how to set up Azure Active Directory and build ASP.NET application to enable Single Sign-On."
Channel9	How to use Azure Access Control for Single Sign-On	"If your web application needs to support multiple user validations, you must handle different tokens with different methods, but when you try to move your application to Windows Azure, Access Control Service (ACS) can solve this problem for you."
Channel9	Deep-dive: Azure Active Directory Authentication and Single Sign-On	"Azure AD Connect is used to synchronize on-premises users to Azure AD, but how do you give your users the best possible sign-in experience?"
YouTube	What's single sign-on for SaaS applications?	"Get an overview of the single sign on capabilities of Azure Active Directory for 3rd party (non-Microsoft) applications."
YouTube	How to deploy single sign-on for SaaS applications?	"Learn how to configure single sign on in the Azure portal for 3rd party (non-Microsoft) applications."
YouTube	How to roll-out single sign-on for SaaS applications?	"Learn how to roll out single sign on for 3rd party (non-Microsoft) applications and the end-user experience."

Books

- Oreilly.com - Mastering Identity and Access Management with Microsoft Azure
  "This book is for business decision makers, IT consultants, and system and security engineers who wish to plan, design, and implement Identity and Access Management solutions with Microsoft Azure."

- Microsoft Press - Modern Authentication with Azure Active Directory for Web Applications (Developer Reference) 1st Edition. "This book will guide you through the essentials of authentication protocols, decipher the disparate terminology applied to the subject, tell you how to get started with Azure AD, and then present concrete examples of applications that use Azure AD for their authentication and authorization, including how they work in hybrid scenarios with Active Directory Federation Services (ADFS)."

Tutorials

- Refer to Tutorials for integrating SaaS applications with Azure Active Directory.
- In case application-specific tutorials are unavailable, follow the Tutorial: Configure SAML-based single sign-on for an application with Azure Active Directory.

Whitepapers

Published 2018, Migrating Application Authentication from Active Directory Federation Services to Azure Active Directory

End-user Readiness and Communication

This section provides customizable posters and email templates to roll out Azure SSO to your organization.

You can distribute the readiness material to your users during SSO rollout, educate them about the feature, and remind them to register. Refer to "Implementing Your Solution" section in the Azure AD Single Sign-On Deployment Plan.

Planning and Change Management

This section provides the resource links to Azure AD SSO deployment plan and topology to help you determine your SSO strategies and document your decisions and configurations to prepare for implementation.

Deployment Plan

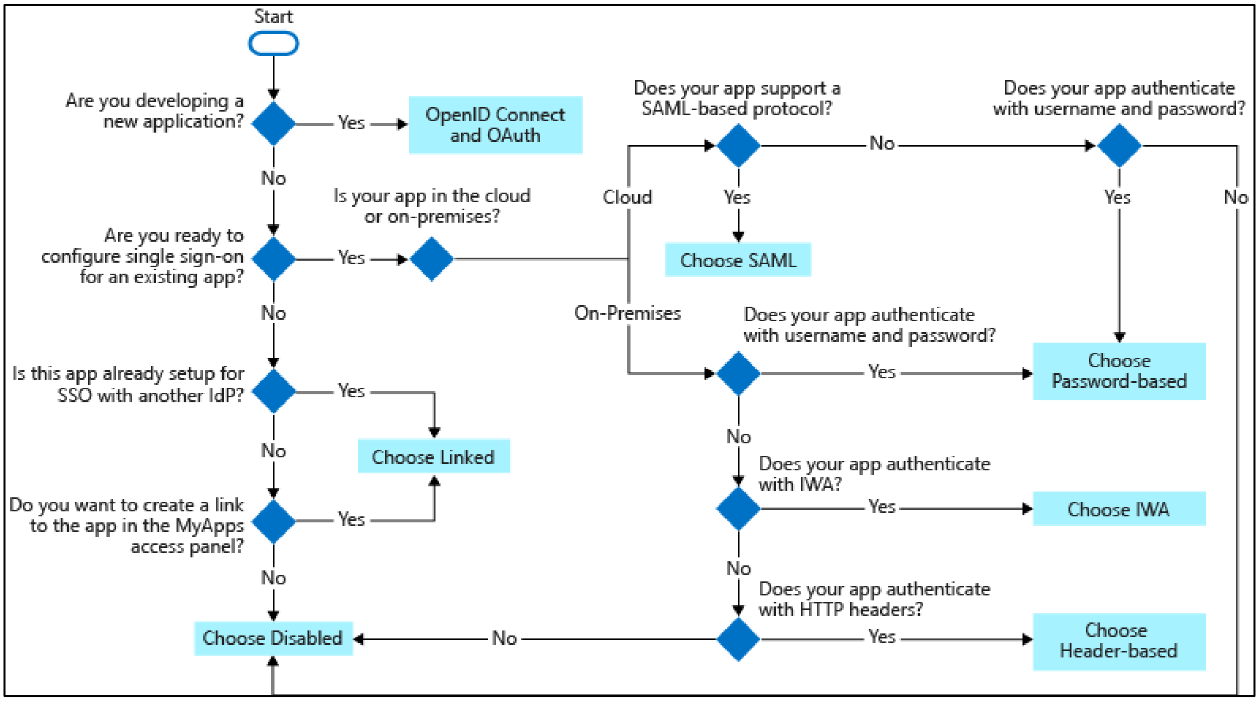
Refer to the step-by-step instructions in the "Planning Your Implementation" and "Designing Your Implementation" section, and follow the "Technical Requirements" in the Azure AD Single Sign-On Deployment Plan.

You can also refer to the Tutorials for integrating SaaS applications with Azure Active Directory.

Architecture Plan/Topology

There are several ways to configure an application for single sign-on. Choosing a single sign-on method depends on how the application is configured for authentication.

- Cloud applications can use OpenID Connect, OAuth, SAML, password-based, linked, or disabled methods for single sign-on.
- On-premises applications can use password-based, Integrated Windows Authentication, header-based, linked, or disabled methods for single sign-on. The on-premises choices work when applications are configured for Application Proxy.


Start
Are you developing a new application?
Yes
OpenID Connect and OAuth
No
Are you ready to configure single sign-on for an existing app?
Yes
Is your app in the cloud or on-premises?
Cloud
On-Premises
Does your app support a SAML-based protocol?
Yes
Choose SAML
No
Does your app authenticate with username and password?
Yes
No
Does your app authenticate with username and password?
Yes
Choose Password-based
No
Does your app authenticate with IWA?
Yes
Choose IWA
No
Does your app authenticate with HTTP headers?
Yes
Choose Header-based
No
Is this app already setup for SSO with another IdP?
Yes
Choose Linked
No
Do you want to create a link to the app in the MyApps access panel?
Yes
No
Choose Disabled

For more information:

- Refer to Single sign-on to applications in Azure Active Directory.
- Follow the “Solution Architecture Diagram and Description” chapter under “Designing Your Implementation” section in the Azure AD Single Sign-On Deployment Plan.

Testing

This section provides the plan to test the functionality of Azure AD SSO in a sandbox or test lab environment before the customer rolls it into production.

Refer to the following links:

- “Implementing Your Solution” section in the Azure AD Single Sign-On Deployment Plan.
- Tutorial: Configure SAML-based single sign-on for an application with Azure Active Directory

Deployment

How can I get Azure AD SSO deployed in my environment? This section provides the resource links to deploy, register, and configure Azure AD SSO.

Deployment

To set up and use Azure SSO, follow the guidance under “Implementing Your Solution” section in the Azure AD Single Sign-On Deployment Plan.

Refer to the following links:

- Tutorials for integrating SaaS applications with Azure Active Directory

- Tutorial: Configure SAML-based single sign-on for an application with Azure Active Directory
- Tutorial: Add an on-premises application for remote access through Application Proxy in Azure Active Directory
- Video: How to deploy single sign-on for SaaS applications?

Readiness Checklist

Follow the readiness checklist under "Implementing Your Solution" section in the Azure AD Single Sign-On Deployment Plan

Design Template

Follow the design template under "Implementing Your Solution" section in the Azure AD Single Sign-On Deployment Plan

Operations

How do I manage and maintain Azure AD SSO? This section provides troubleshooting info, Azure AD SSO operation and management details, and other important references.

Operations

Refer to "Operationalize your Implementation" section in the Azure AD Single Sign-On Deployment Plan.

You can also refer to the following links:

- Video: How to roll-out single sign-on for SaaS applications?
- How to configure federated single sign-on for an Azure AD Gallery application
- Problem configuring federated single sign-on for an Azure AD Gallery application
- How to configure federated single sign-on for a non-gallery application
- Problem configuring federated single sign-on for a non-gallery application
- How to configure password single sign-on for an Azure AD Gallery application
- Problem configuring password single sign-on for an Azure AD Gallery application
- How to configure password single sign-on for a non-gallery application
- Problem configuring password single sign-on for a non-gallery application

Monitoring

Refer to "Planning Reporting and Auditing" section in Azure AD Single Sign-On Deployment Plan.

You can also refer to the following links:

- What is guest user access in Azure Active Directory B2B? (for external users such as partners and vendors)
- What is conditional access in Azure Active Directory?
- What is Azure Active Directory Identity Protection?
- Configurable token lifetimes in Azure Active Directory (Preview)
- How to: Customize claims emitted in tokens for a specific app in a tenant (Preview)
- Audit activity reports in the Azure Active Directory portal

- Sign-in activity reports in the Azure Active Directory portal

Troubleshooting

Follow the troubleshooting guide and steps under “Operationalize your Implementation” section in the Azure AD Single Sign-On Deployment Plan.

You can also refer to the following links:

- Debug SAML-based single sign-on to applications in Azure Active Directory
- How to: Customize claims issued in the SAML token for enterprise applications
- Single Sign-On SAML protocol
- Single Sign-Out SAML protocol
- Unexpected consent prompt when signing into an application
- Unexpected error when performing consent to an application
- Problems signing into an application using a deeplink
- Problems signing into an application from the access panel
- https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/application-sign-in-problem-application-error
- Problems signing into an Azure AD Gallery application configured for password single sign-on
- Problems signing into a Microsoft application
- Problems signing into a non-gallery application configured for federated single sign-on
- Problems signing into a gallery application configured for federated single sign-on
- Problems signing into a custom-developed application

Support and Feedback

How can we improve Azure AD SSO? This section provides links to discussion forums and technical community support email IDs.

We encourage you to join our Technical Community, a platform to Microsoft Azure Active Directory users and Microsoft to interact. It is a central destination for education and thought leadership on best practices, product news, live events, and roadmap.

If you have technical questions or need help with Azure, please try StackOverflow or visit the MSDN Azure AD forums.

Tell us what you think of Azure and what you want to see in the future. If you have suggestions, please submit an idea or vote up an idea at our User Voice Channel - feedback.azure.com.