Microsoft

The role of Azure Active Directory in Windows 10 cloud subscriptions

Overview of identity management in the
Cloud Solution Provider program

January 2018

Windows 10

Copyright information

Contents

Executive summary

Making the decision to use the Cloud Solution Provider (CSP) program—either by subscribing to a Microsoft 365 solution or by choosing Windows 10 Enterprise—means your organization will benefit from the most secure and productive Windows ever and the robust management services of Azure Active Directory (Azure AD).

This document provides guidance for integrating on-premises Active Directory (AD) with Azure AD or migrating completely from on-premises AD to Azure AD. The first section of this document discusses identity management and the role of Azure AD in Windows 10 cloud subscriptions. The second section provides your internal IT staff or a certified Microsoft partner with technical guidance on Azure AD implementation paths with a CSP subscription.

Introduction

Organizations need to implement Azure AD to activate Windows 10 cloud subscriptions using a CSP. To take advantage of Azure AD, you can move from either on-premises AD to Azure AD or integrate the two environments.

These documents provide more information about related topics:

- Introduction to Windows 10 subscriptions in the Cloud Solution Provider program
- Windows 10 upgrade benefits for customers with Cloud Solution Provider subscriptions

What is Azure Active Directory?

Azure Active Directory (Azure AD) is an identity and access management service (IDaaS) for on-premises and cloud-based apps. Azure AD gives you the capability to manage users, groups, and devices while also helping secure access to on-premises and cloud applications, including Microsoft applications and many non-Microsoft software as a service (SaaS) applications.

Windows 10 in CSP subscriptions (Microsoft 365 Business, Microsoft 365 Enterprise, or Windows 10 Enterprise) require an Azure AD tenant. You can use Azure AD to manage directory services, identity governance, and application access management from the cloud. Azure AD also makes it possible for end users to sign in only once (often referred to as single sign-on or SSO) to thousands of apps, including familiar products such as Microsoft Office 365, Salesforce.com, Box, ServiceNow, and Workday.

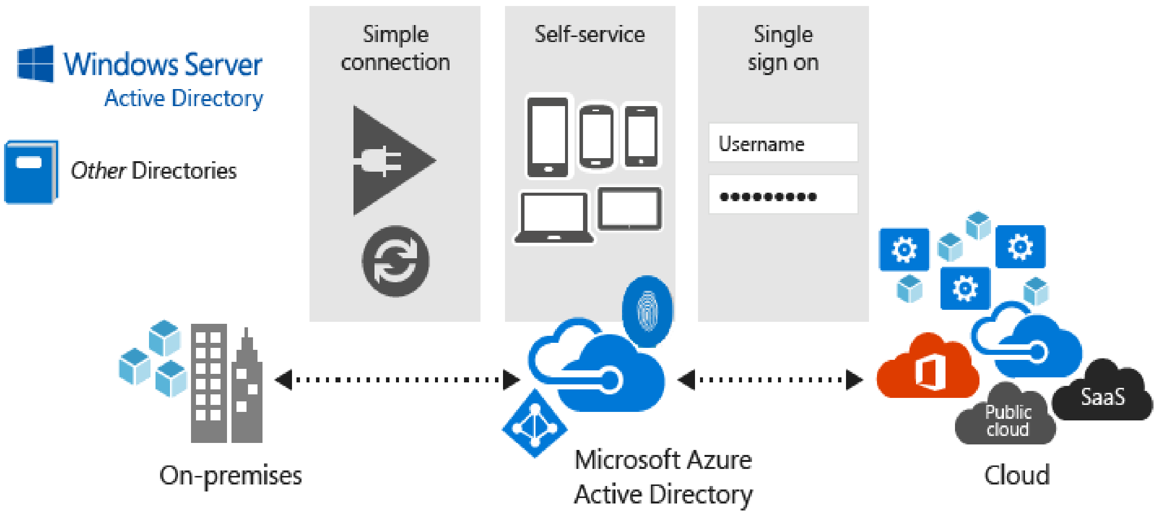
A single Azure AD tenant is automatically associated with a Microsoft Azure subscription (or an Office 365 subscription) when it is created. As the identity service in Azure, Azure AD provides all identity management and access control functions for cloud-based resources. These resources can include users, apps, groups, and devices for an individual tenant (organization).

Identity management using Azure AD

Using Azure AD for identity management makes it easy to do the following:

- Create and manage a single identity for each person across your company, keeping employees, groups, and devices in sync.
- Provide SSO access to your applications, including thousands of pre-integrated software as a service (SaaS) apps, or grant secure remote access to on-premises SaaS applications using the Azure AD Application Proxy.
- Provide secure application conditional access by enforcing rules, like requiring Multi-Factor Authentication or requiring a compliant device for both on-premises and cloud applications.
- Enable employees to reset passwords (self-service) and request group and application access using the MyApps portal.

You can choose to manage your organizational identity in the cloud or work in a hybrid environment using both Azure AD and your on-premises Windows Server Active Directory, as shown in the diagram below. The next section of this document offers guidance on different scenarios.



Technical guidance

Steps for setting up Azure Active Directory

For organizations adopting Windows 10 using a CSP subscription, the table below outlines general steps to follow when setting up Azure Active Directory, based on your identity management starting point.

Initial steps also adjust based on other Microsoft solutions you own.

- For example, if an Azure AD tenant already exists with a subscription to an online Microsoft service such as Office 365, Microsoft Dynamics 365, Azure, or Microsoft Enterprise Mobility + Security (EMS), you can skip steps 1 and 2.
- If more than one Azure AD tenant exists, Microsoft recommends consolidating all online services into a single Azure AD tenant.

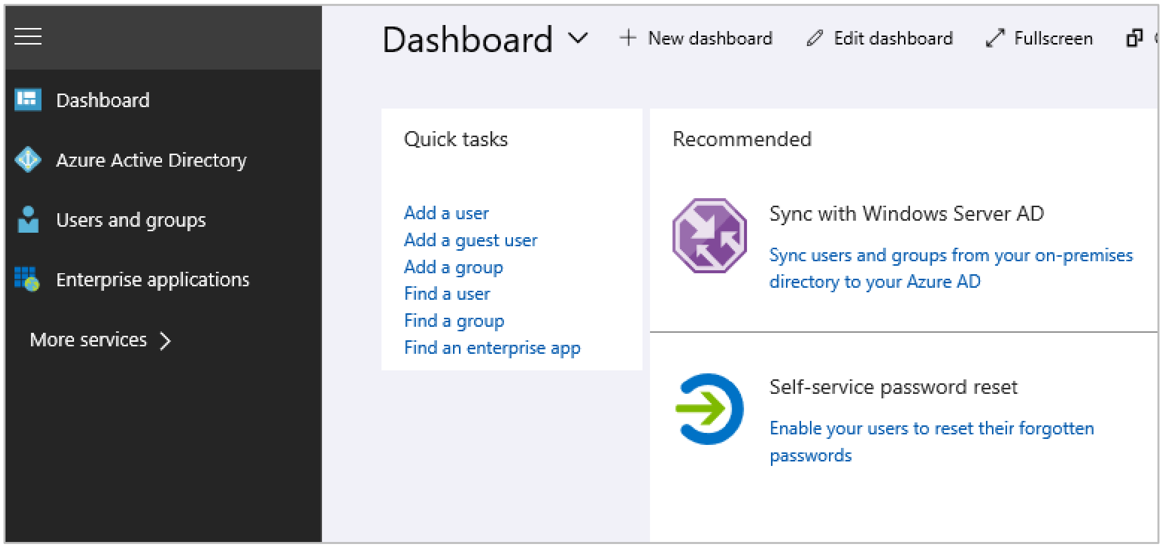
		SCENARIO OPTIONS		
Task	**Action**	**Configuring your first identity management platform**	**Integrating on-premises AD with Azure AD**	**Migrating on-premises AD to Azure AD**
1.	Create tenant.	Must complete	Must complete	Must complete
2.	Add and verify domains.	Optional	Optional	Optional
3.	Add user accounts.	Must complete	Set-up Azure AD Connect	Migrate user accounts from on-premises AD to Azure AD using Azure AD Connect
4.	Purchase products.	Must complete	Must complete	Must complete
5.	Assign licenses to users.	Must complete	Must complete	Must complete
6.	Deploy subscriptions.	Deploy Azure AD joined devices	Configure hybrid Azure AD joined devices (Auto-registration of domain joined devices with Azure AD)	Deploy Azure AD joined devices

For more information about devices in Azure AD including Azure AD join and hybrid Azure AD join, review Introduction to device management in Azure Active Directory.

Configuring your first identity management platform

If you are building a new identity management platform or migrating from a Microsoft Workgroup peer-to-peer network, most of the Azure AD setup will be completed automatically as part of your subscription purchase.

Your dashboard—shown in the following example image—is your central point for importing or adding users, purchasing products for users, and assigning licenses. You can also find guidance in the document called Introduction to Windows 10 subscriptions in the Cloud Solution Provider program. This document also explains how to determine the most appropriate Windows subscription.



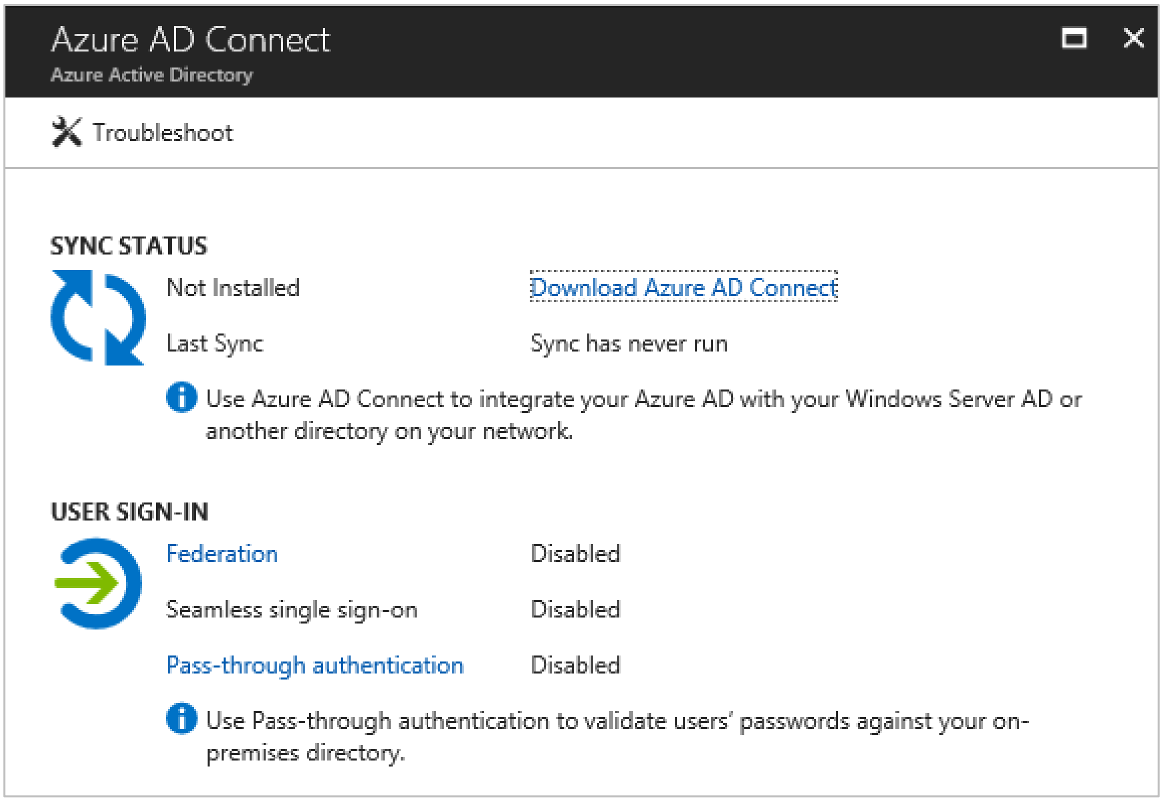
Sync users and groups from your on-premises directory to your Azure AD

Enable your users to reset their forgotten passwords

Integrating on-premises AD with Azure AD

If you have an on-premises AD infrastructure that you want to maintain and extend to Azure AD, your devices can be Azure AD joined or you can have your domain joined devices automatically registered with Azure AD (hybrid Azure AD joined). You need hybrid Azure AD joined devices if, for example, you are relying on on-premises management of devices like Group Policy or tools like System Center Configuration Manager. Customers working in a hybrid environment will synchronize Windows Server AD objects with Azure AD, while still managing users on-premises. The organization's new directory infrastructure will span on-premises and cloud-based environments, creating a single-user identity for authentication and authorization for all applications and services, regardless of location, including Office 365, Azure, and software as a service (SaaS) applications that integrate with Azure AD.

To integrate and synchronize on-premises AD with Azure AD, customers use the Azure AD Connect tool, which can be downloaded when using Azure, as shown in the image below, or from the Microsoft Download Center.



Azure AD Connect
Azure Active Directory

Troubleshoot

SYNC STATUS

Not Installed — Download Azure AD Connect

Last Sync — Sync has never run

Use Azure AD Connect to integrate your Azure AD with your Windows Server AD or another directory on your network.

USER SIGN-IN

Federation — Disabled

Seamless single sign-on — Disabled

Pass-through authentication — Disabled

Use Pass-through authentication to validate users' passwords against your on-premises directory.

The Azure AD Connect tool includes three primary components:

- Synchronization is responsible for creating users, groups, and other objects. It is also responsible for making sure identity information for your on-premises users and groups matches the information in the cloud.
- AD Federation Services (AD FS) is an optional component that you can deploy. AD FS can be used by organizations to address requirements such as enforcement of AD sign-in policy, enforcement of conditional access policy on-premises, and smart card or third-party multi-factor authentication.
- Azure AD Connect Health provides robust monitoring from a central location in the Azure portal to make sure users can reliably access resources both on premises and in the cloud from any device. It is as simple as installing an agent on each of your on-premises identity servers.

For more information about using Azure AD Connect, review Integrate your on-premises directories with Azure Active Directory.

Migrating on-premises AD to Azure AD

Customers can also use the Azure AD Connect tool to move their IT identity, single sign-on, and policy management infrastructure to the cloud. Customers use the tool to synchronize their on-premises AD with Azure AD, as if they were integrating the two solutions, and then they make the transition to Azure AD only.

Ensure you have done the proper assessment before disconnecting on-premises AD from Azure AD.

Next steps

For more information about working with Azure AD, refer to the following documents:

- Introduction to Windows 10 subscriptions in the Cloud Solution Provider program
- Windows 10 upgrade benefits for customers with Cloud Solution Provider subscriptions

We also invite you to review the following resources or contact your Microsoft partner.

Resources

- What is Azure Active Directory?
- Fundamentals of Azure Identity Management
- Microsoft hybrid identity solutions
- Azure Active Directory Hybrid Identity Design Considerations
- Hybrid identity directory integration tools comparison
- Azure Active Directory Documentation