Microsoft Cloud Identity for Enterprise Architects

What IT architects need to know about designing identity for organizations using Microsoft cloud services and platforms

This topic is 1 of 5 in a series 1 2 3 4 5

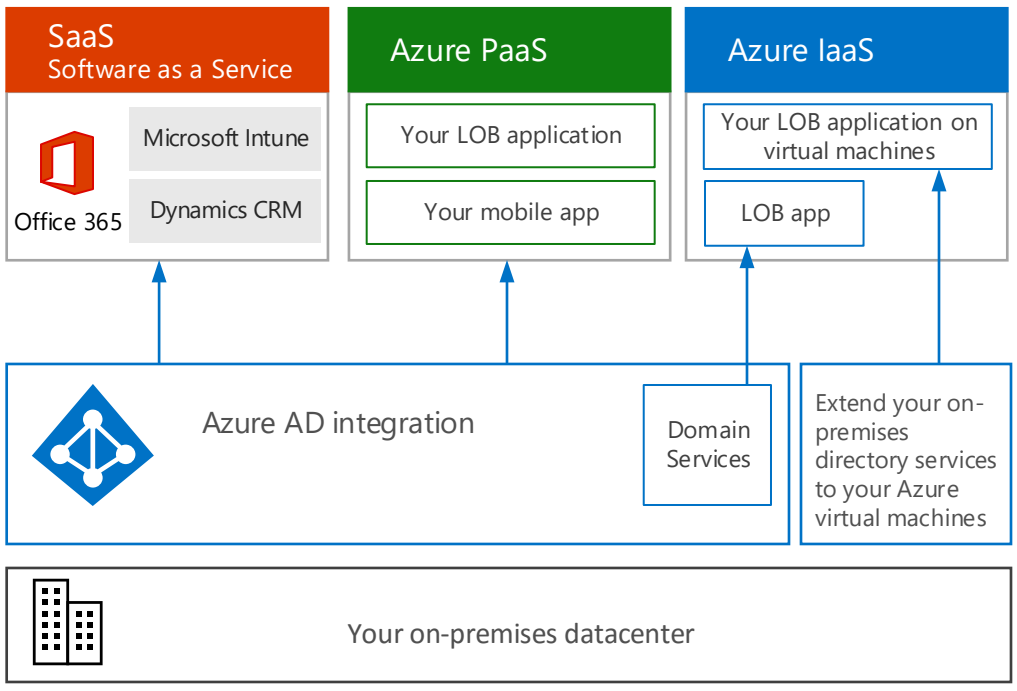
Introduction to identity with Microsoft's cloud

Integrating your identities with the Microsoft cloud provides access to a broad range of services and applications.

Azure Active Directory (Azure AD) integration provides:

- Identity management for applications across all categories of Microsoft's cloud (SaaS, PaaS, IaaS).
- Consolidated identity management for third-party cloud applications in your portfolio.
- Collaboration with partners.
- Management of customer identities.
- Integration with web-based applications located on-premises.

For line of business (LOB) applications hosted on virtual machines in Azure IaaS, you can use Domain Services in Azure AD. Or, you can extend your on-premises Windows Server Active Directory (AD) environment.



Use Azure Active Directory as your Identity as a Service (IDaaS) provider

Azure AD is a leading provider of cloud-based Identity as a Service (IDaaS) and provides a broad range of capabilities for enterprise organizations. Click each box for more information.

Azure Active Directory

On-premises infrastructure integration
- Synchronization or federation of identities
- Self-service password reset with write back to on-premises directories
- Web App Proxy for authentication against on-premises web-based applications

User accounts
- MyApps Panel
- Multi-factor authentication (MFA)
- Conditional access to resources and applications
- Behavior and risk-based access control with Azure AD Identity Protection

Devices
- Mobile device management with Intune
- Windows 10 Azure AD Join and SSO
- Device registration and management for non-Windows devices (iOS, Android, Mac)

Partner collaboration
- Secure collaboration with your business partners using Azure AD B2B collaboration

Customer account management
- Self-registration for your customers using a unique identity or an existing social identity with Azure AD B2C

Application integration
- Pre-integrated with thousands of SaaS applications
- Deep integration with Office 365 features
- Cloud App Discovery
- PaaS application integration
- Domain Services
- Integration with other cloud providers, such as Amazon Web Services

Administration
- Reporting
- Global telemetry and machine learning
- Enterprise scale
- Worldwide availability
- Connect Health

Azure Active Directory editions

Free

- Synchronization or federation with on-premises directories through Azure AD Connect (sync engine)
- Directory objects
- User/group management (add/update/delete), user-based provisioning, device registration
- Single sign-on (SSO)
- Self-service password change for cloud users
- Security and usage reports

More information: Azure Active Directory editions

Basic

All features in Free, plus:

- Group-based access management and provisioning
- Self-service password reset for cloud users
- Company branding (logon pages, Access Panel customization)
- Application Proxy
- Enterprise SLA of 99.9%

Premium

All features in Free and Basic, plus:

- Self-service group and app management, self-service application additions, dynamic groups
- Self-service password reset, change, unlock with on-premises write-back
- Multi-factor authentication (cloud and on-premises, MFA Server)
- MIM CAL + MIM Server
- Cloud App Discovery
- Connect Health
- Automatic password rollover for group accounts

See topics 2-5 for more information and resources.

More information

Video: Getting Started with Microsoft Azure Active Directory
https://mva.microsoft.com/en-US/training-courses/getting-started-with-microsoft-azure-active-directory-8448?l=hvlTSEWz_5704984382

Infographic: Cloud identity and access management
http://go.microsoft.com/fwlink/p/?LinkId=524282

Azure Hybrid Identity Design Considerations Guide
https://gallery.technet.microsoft.com/Azure-Hybrid-Identity-b06c8288

August 2016

Microsoft

Microsoft Cloud Identity for Enterprise Architects

What IT architects need to know about designing identity for organizations using Microsoft cloud services and platforms

Azure Active Directory integration capabilities

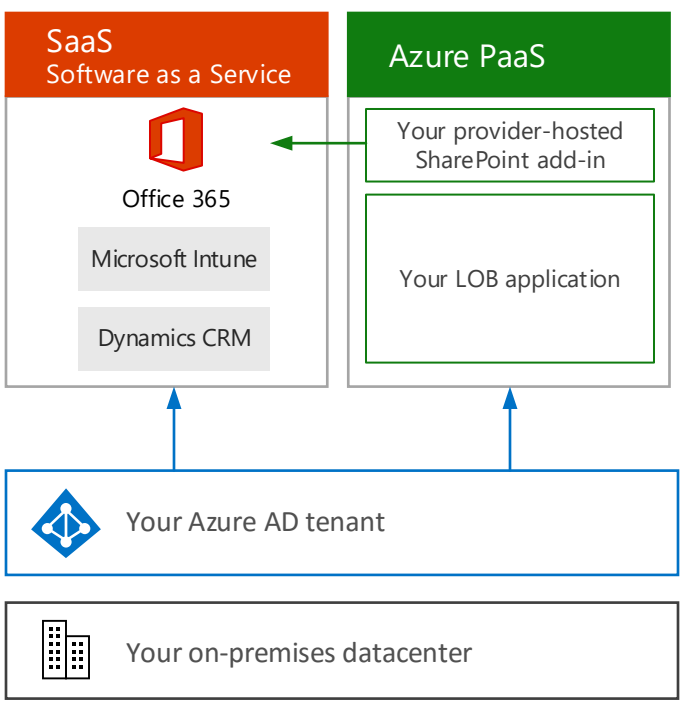
Azure Active Directory (AD) provides a broad range of capabilities that allow you to centralize and simplify identity management while integrating applications across environments and with partners and customers.

This topic provides more information about some of these capabilities.

Integration across Microsoft's cloud

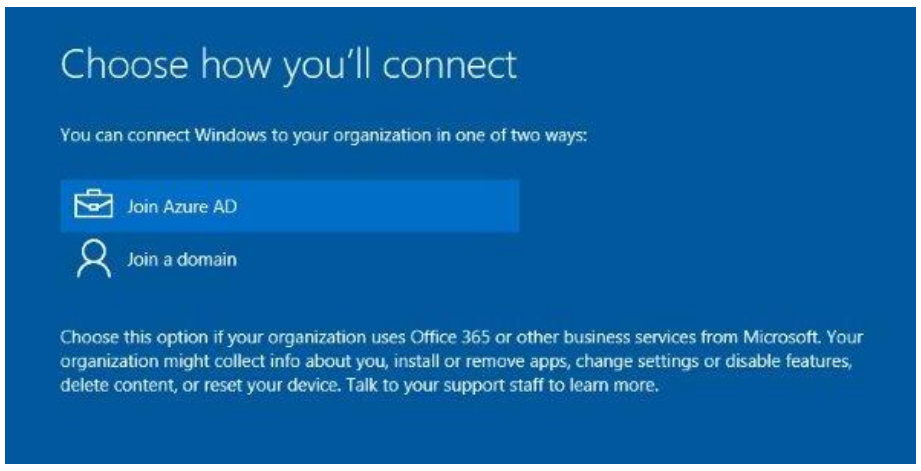
The foundational architectural steps you take with Office 365 for identity integration provide a single architecture for adoption of workloads across Microsoft's cloud, including PaaS workloads in Azure as well as other SaaS workloads, such as Dynamics CRM Online.

With this foundation, you can add other applications to Microsoft's cloud and apply the same set of authentication and identity security features for access to these apps. For example, you can develop new line of business (LOB) applications using cloud-native features in Microsoft Azure and integrate these apps with your Azure AD tenant. This includes your custom SharePoint add-ins.

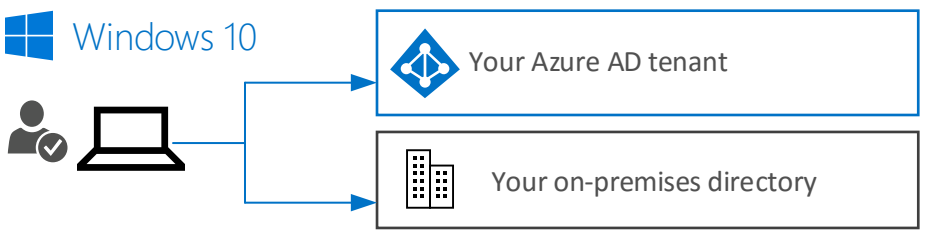


Windows 10 Azure AD Join

Join Windows 10 devices to Azure Active Directory and provision these with Office 365 services and applications within minutes when the device is configured during the out-of-box experience.

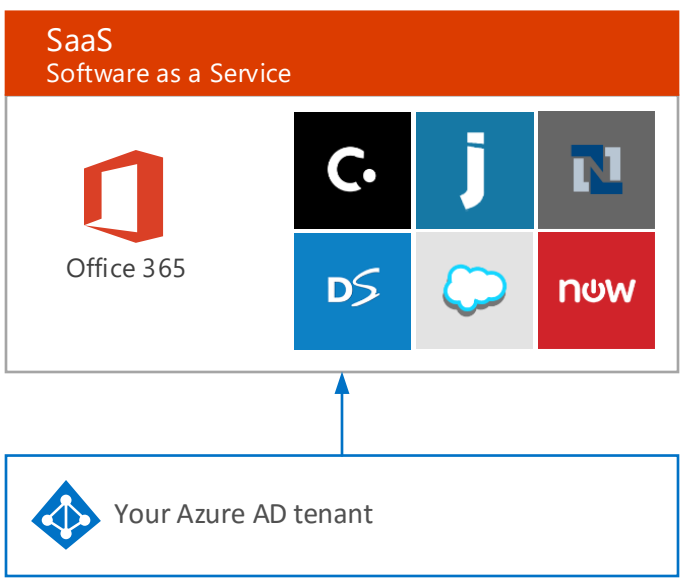


Windows 10 automatically authenticates with Azure AD and your on-premises directory, providing single-sign on without the need for AD FS.



Single sign-on to other SaaS apps in your environment

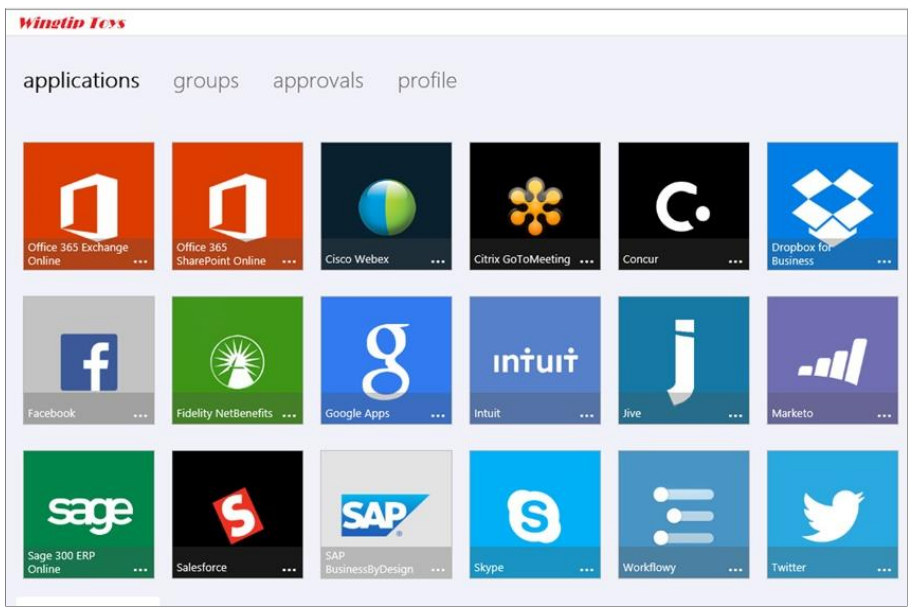
You can greatly simplify the management of identity across your organization by configuring single-sign on to other SaaS applications in your environment. See the Active Directory Marketplace for apps that are already integrated. By doing this, you can manage all identities in the same place and apply the same set of security and access policies across your organization, such as multi-factor authentication (MFA).



Azure AD MyApps panel

The Access Panel at https://myapps.microsoft.com is a web-based portal that allows users with an organizational account in Azure AD to view and launch cloud-based applications to which they have been granted access. If you are a user with Azure AD Premium, you can also use self-service group management capabilities through the Access Panel.

The Access Panel is separate from the Azure portal and does not require users to have an Azure subscription.

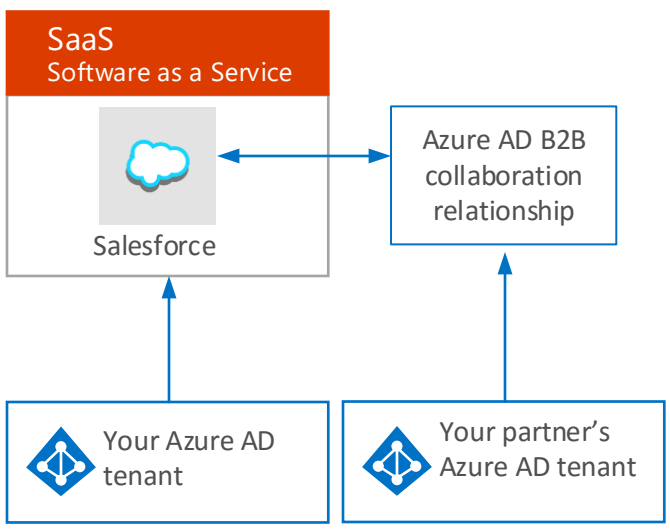


Continued on next page

Azure AD B2B collaboration

Azure AD B2B Collaboration enables secure collaborate between business-to-business partners. These new capabilities make it easy for organizations to create advanced trust relationships between Azure AD tenants so they can easily share business applications across companies without the hassle of managing additional directories or the overhead of managing partner identities.

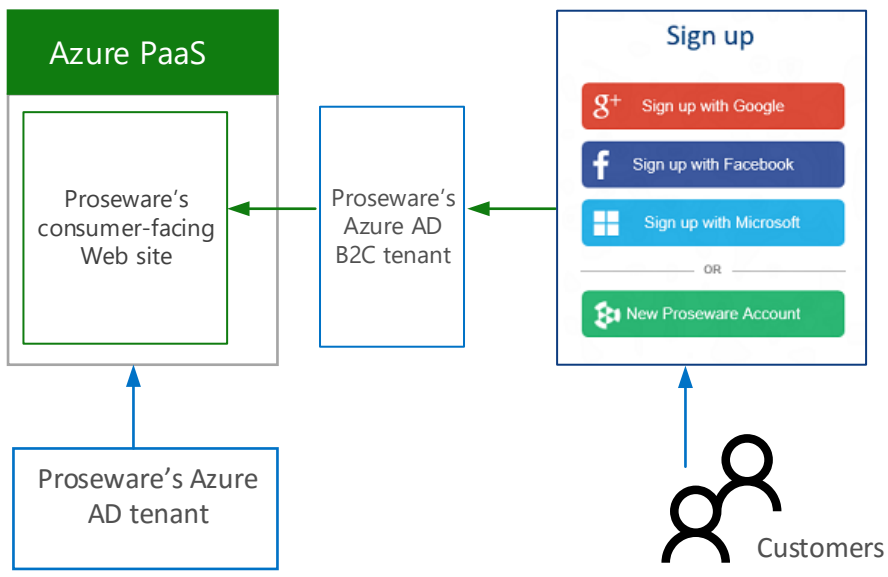
With 6 million organizations already using Azure AD, chances are good that your partner organization already has an Azure AD tenant, so you can start collaborating instantly. But even if they don't, Azure AD's B2B capabilities make it easy for you to send them an automated invitation which will get them up and running with Azure AD in a matter of minutes.



Azure AD B2C collaboration

Azure Active Directory B2C is a highly available, global, identity management service for consumer-facing applications that scales to hundreds of millions of identities. It can be easily integrated across mobile and web platforms. Your consumers can log on to all your applications through fully customizable experiences by using their existing social accounts or by creating new credentials.

Here is an example for the fictional Proseware organization.

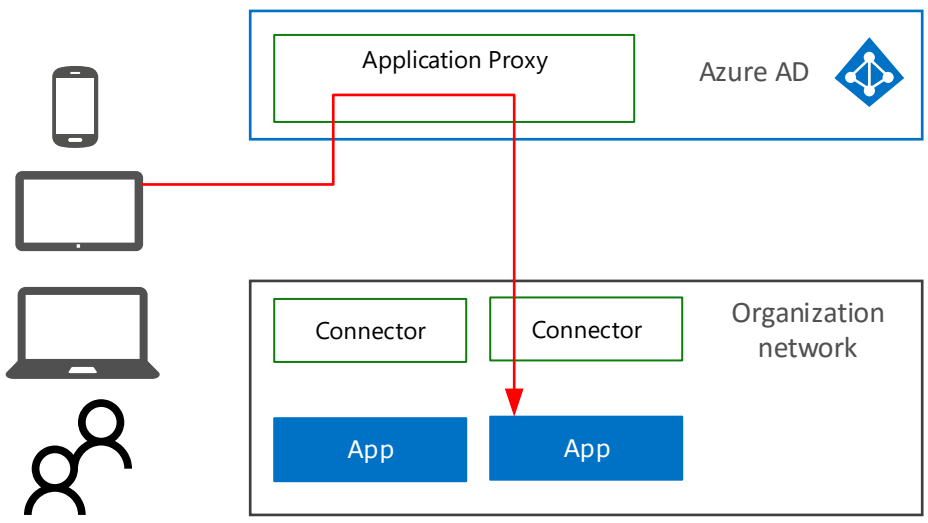


Application Proxy

Microsoft Azure Active Directory Application Proxy lets you publish applications, such as SharePoint sites, Outlook Web Access, and IIS-based apps inside your private network and provides secure access to users outside your network. Employees can log into your apps from home on their own devices and authenticate through this cloud-based proxy.

By using Azure AD Proxy you can protect on-premises applications with the same requirements as other cloud-based applications with MFA, device requirements, and other conditional access requirements. You also benefit from the built in security, usage, and administration reports.

Application Proxy works by installing a slim Windows service called a Connector inside your network. The Connector maintains an outbound connection from within your network to the proxy service. When users access a published application, the proxy uses this connection to provide access to the application.

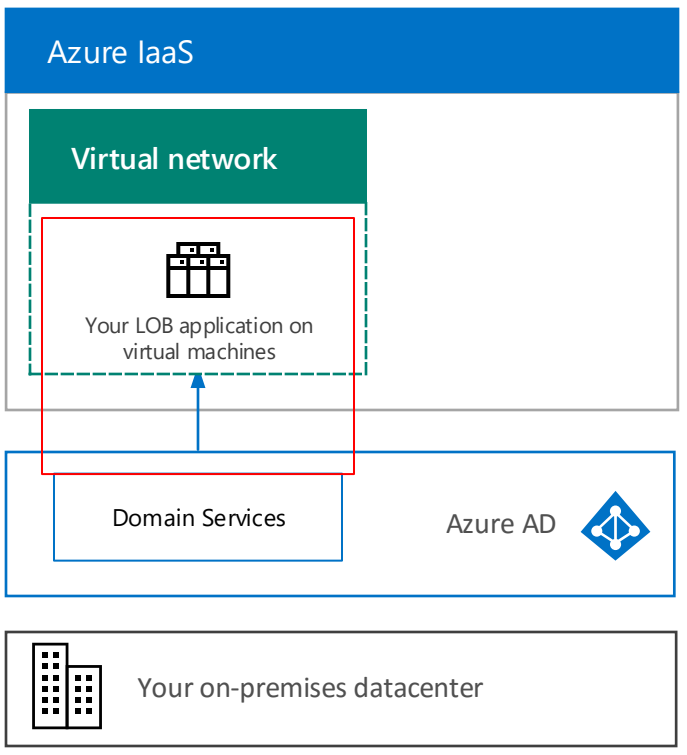


Domain services

Azure AD Domain Services provides managed cloud based domain services such as domain join, group policy, LDAP & Kerberos/NTLM authentication in Azure IaaS that are fully compatible with Windows Server AD. You can join Azure virtual machines to this domain without the need to deploy domain controllers. Because Azure AD Domain Services is part of your existing Azure AD tenant, users can login using the same credentials they use for Azure AD.

This managed domain is a standalone domain and is not an extension of an organization's on-premises domain or forest infrastructure. However, all user accounts, group memberships, and credentials from the on-premises directory are available in this managed domain.

Blog: Use Azure AD as a cloud domain controller



More Microsoft cloud IT resources

Services and Platform Options	Security	Identity	Storage
aka.ms/cloudarchoptions	aka.ms/cloudarchsecurity	aka.ms/cloudarchidentity	aka.ms/cloudarchstorage

Microsoft

Microsoft Cloud Identity for Enterprise Architects

What IT architects need to know about designing identity for organizations using Microsoft cloud services and platforms

Integrate your on-premises Windows Server AD accounts with Azure AD

- Provides access to all of the Microsoft SaaS services.
- Provides cloud-based identity options for Azure PaaS and IaaS applications.

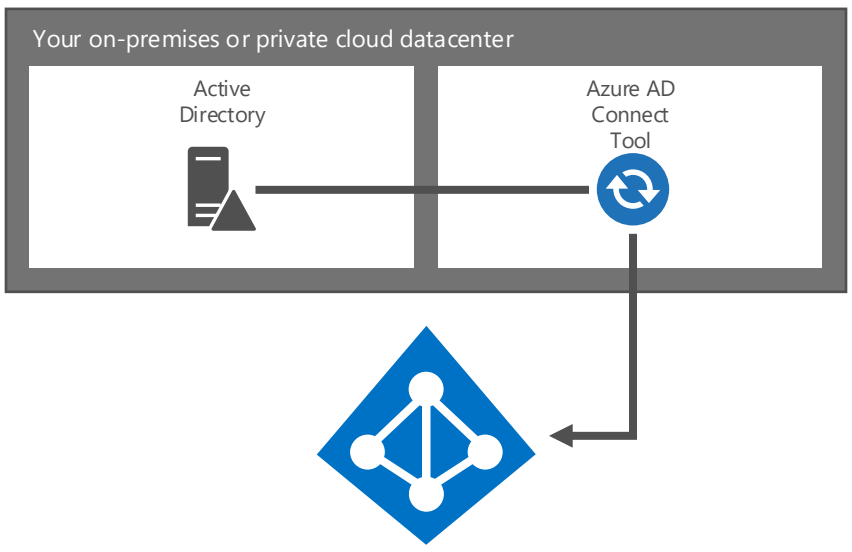
Two approaches are recommended (below).

Using cloud-only accounts is not recommended for enterprise-scale organizations unless Windows Server AD is not already used on premises.

Choose one option

Start with the simplest option that meets your needs. You can switch between these options, if needed.

Directory and password synchronization



This is the simplest option and the recommended option for most enterprise organizations.

- User accounts are synchronized from your on-premises directory to your Azure AD tenant. The on-premises directory remains the authoritative source for accounts.
- Azure AD performs all authentication for cloud-based services and applications.
- Supports multi-forest synchronization.

Password synchronization

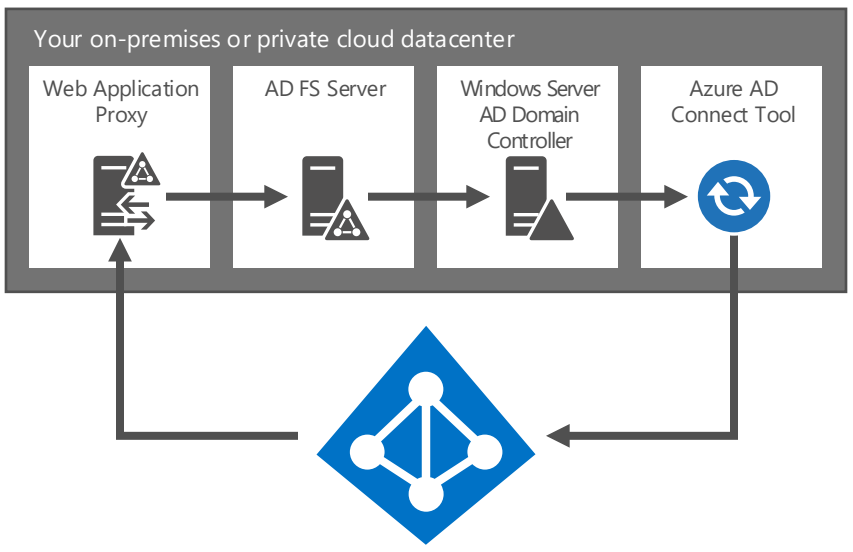
- Users enter the same password for cloud services as they do on-premises.
- User passwords are never sent to Azure AD. Instead a hash of each password is synchronized. It is not possible to decrypt or reverse-engineer a hash of a password or to obtain the password itself.

Multi-factor authentication (MFA)

- You can take advantage of basic MFA features offered with Office 365.
- Applications in Azure can take advantage of the Azure Multi-Factor Authentication service.
- Directory synchronization does not provide integration with on-premises MFA solutions.

Azure AD Connect in the Office 365 dev/test environment

Federation



Federation provides additional enterprise capabilities. It is also more complex and introduces more dependencies for access to cloud services.

- All authentication to Azure AD is performed against the on-premises directory via Active Directory Federation Services (AD FS) or another federated identity provider.
- Works with non-Microsoft identity providers.
- Password hash sync adds the capability to act as a sign-in backup for federated sign-in (if the federation solution fails).

Use federation if:

- AD FS is already deployed.
- You use a third-party identity provider.
- You have an on-premises integrated smart card or other MFA solution.
- You require sign-in audit and/or disablement of accounts.
- Compliance with Federal Information Processing Standards (FIPS).

Federated authentication requires a greater investment in infrastructure on-premises.

- The on-premises servers must be Internet-accessible through a corporate firewall. Microsoft recommends the use of Federation Proxy servers deployed in a perimeter network, screened subnet, or DMZ.
- Requires hardware, licenses, and operations for AD FS servers, AD FS proxy or Web Application Proxy servers, firewalls, and load balancers.
- Availability and performance are important to ensure users can access Office 365 and other cloud applications.

If you use federation, be sure to create online administrative accounts so you can administer Azure AD if your on-premises identity solution is not available.

More information

Synchronizing your directory with Office 365 is easy
http://go.microsoft.com/fwlink/p/?LinkId=524281

Prepare to provision users through directory synchronization to Office 365
http://go.microsoft.com/fwlink/p/?LinkId=524284

Define a hybrid identity adoption strategy
https://azure.microsoft.com/en-us/documentation/articles/active-directory-hybrid-identity-design-considerations-identity-adoption-strategy/

Ignite 2015: Extending On-Premises Directories to the Cloud Made Easy
https://channel9.msdn.com/Events/Ignite/2015/BRK3862

Multi-Factor Authentication for Office 365
http://go.microsoft.com/fwlink/p/?LinkID=392012

Azure Multi-Factor Authentication
http://go.microsoft.com/fwlink/p/?LinkId=524285

August 2016

Microsoft

Microsoft Cloud Identity for Enterprise Architects

What IT architects need to know about designing identity for organizations using Microsoft cloud services and platforms

This topic is 4 of 5 in a series 1 2 3 **4** 5

Running directory components in Azure IaaS

Deploying directory components to Azure

Consider the benefits of deploying directory components to Azure IaaS, especially if you plan to extend your on-premises Windows Server AD to Azure virtual machines for your line of business applications.

Which components can be put in Azure?

- Azure AD Connect tool
- Windows Active Directory Federation Services (AD FS) plus the Azure AD Connect tool
- Standalone Windows Server AD environments in Azure IaaS

Azure AD Connect Tool

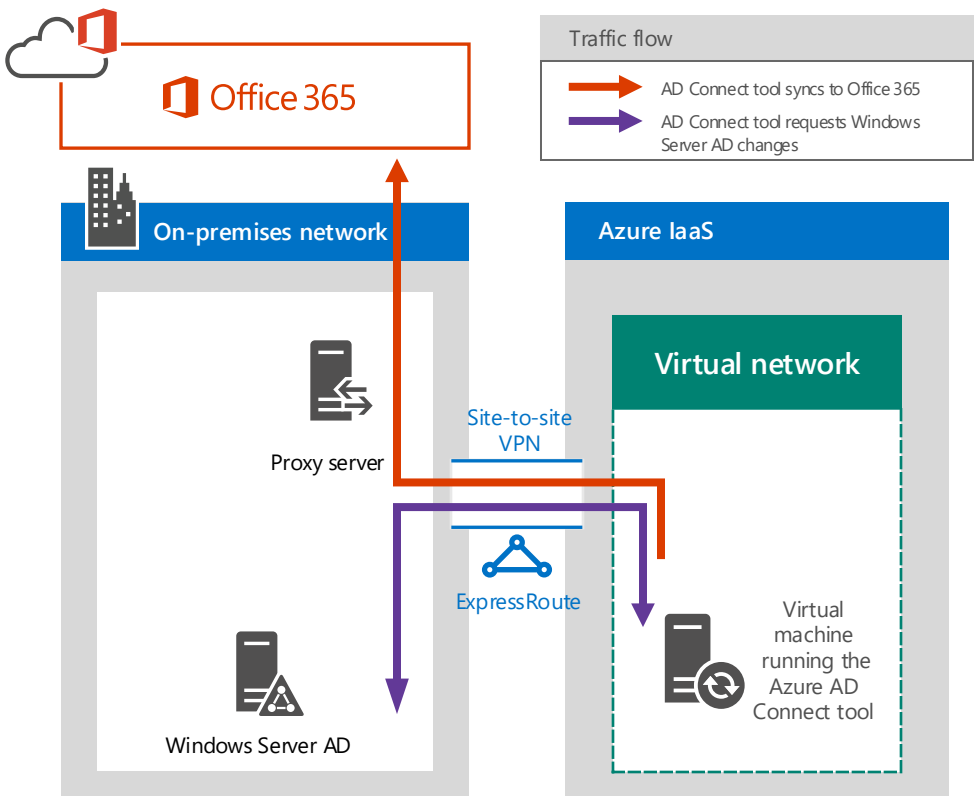
The Azure AD Connect tool can be hosted in the cloud using Azure IaaS.

- Potentially faster provisioning and lower cost of operations
- Increased availability

The architecture illustrated on the right details how you can run Azure AD Connect Tool on a virtual machine in Azure IaaS.

This solution provides a way to integrate with Azure AD without deploying additional components on premises.

For more information, see ***Deploy Office 365 Directory Synchronization in Microsoft Azure***.



AD FS + AD Connect tool

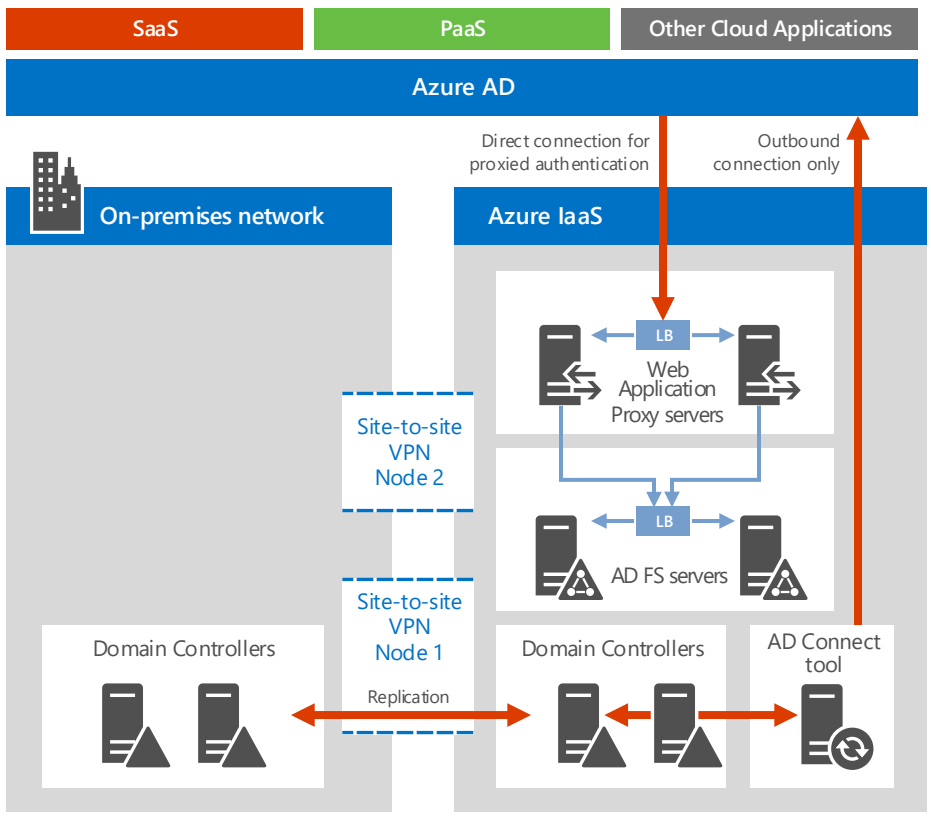
If you haven't already deployed AD FS on-premises, consider whether the benefits of deploying this workload to Azure makes sense for your organization.

- Provides autonomy for authentication to cloud services (no on-premises dependencies).
- Reduces servers and tools hosted on-premises.
- Uses a site-to-site VPN gateway on a two-node failover cluster to connect to Azure (new).
- Uses ACLs to ensure that Web Application Proxy servers can only communicate with AD FS, not domain controllers or other servers directly.

This solution works with:

- Applications that require Kerberos
- All of Microsoft's SaaS services
- Applications in Azure that are Internet-facing
- Applications in Azure IaaS or PaaS that require authentication with your organization Windows Server AD

For more information, see ***Guidelines for Deploying Windows Server Active Directory on Azure Virtual Machines.***



Standalone Windows Server AD environment in Azure IaaS

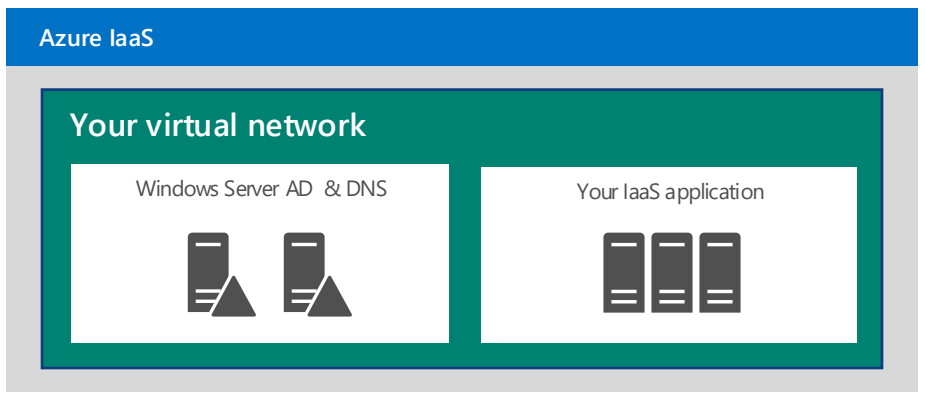
You don't always need to integrate a cloud application with your on-premises environment. A standalone Windows Server AD domain in Azure supports applications that are public-facing, such as Internet sites.

This solution works with:

- Applications that require NTLM or Kerberos authentication
- Applications that require Windows Server AD
- Test and development environments in Azure IaaS

Also consider whether Azure AD Domain Services can be used instead.

For more information, see ***Guidelines for Deploying Windows Server Active Directory on Azure Virtual Machines.***



Microsoft

Microsoft Cloud Identity for Enterprise Architects

What IT architects need to know about designing identity for organizations using Microsoft cloud services and platforms

Design domain services for workloads in Azure IaaS

Many LOB solutions that run on virtual machines require Windows Server AD for the following functionality:

- Support for NTLM, Kerberos, or LDAP-based authentication
- Domain-joined virtual machines
- Group Policy

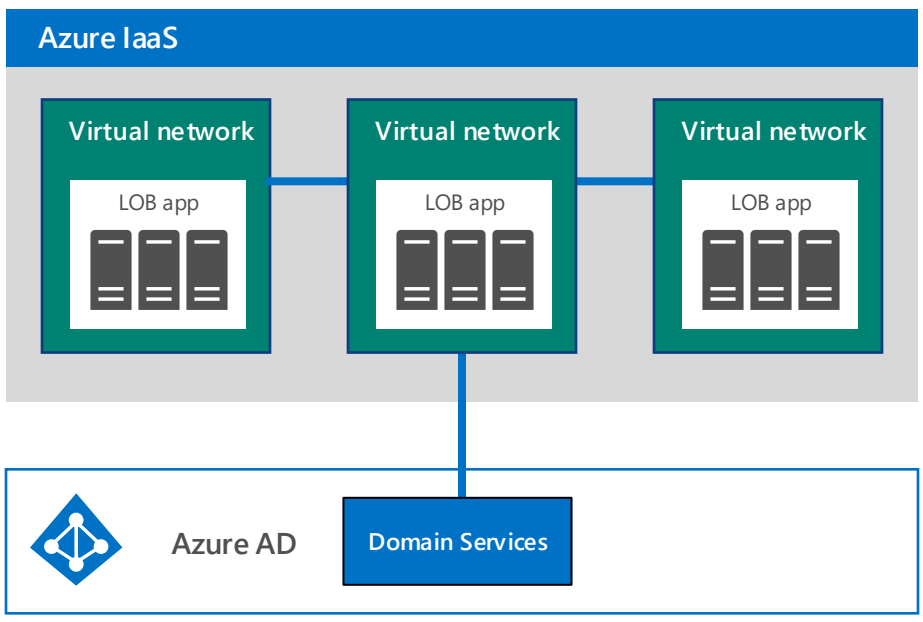
Microsoft currently recommends two solutions.

Use Azure AD Domain Services

AD Domain Services can be enabled in your existing Azure AD tenant. You do not need to deploy and manage domain controllers.

This managed domain is a standalone domain and is not an extension of an organization's on-premises domain/forest infrastructure. However, all user accounts, group memberships and credentials from the on-premises directory are available in this managed domain. Users login using the same corporate credentials they use for Azure AD.

- Domain Services is connected to a virtual network in Azure IaaS.
- This instance of Domain Services can be used by other virtual networks that are connected to the virtual network configured with Domain Services.



When to use which solution

Use Azure AD Domain Services when your applications require domain services support for:

- Server application management.
- Server login.
- User authentication over Kerberos, NTLM, or LDAP.
- Directory lookup over LDAP/LDAPS.

See: Deployment scenarios and use cases.

Extend your on-premises Windows Server AD domain to Azure when you require:

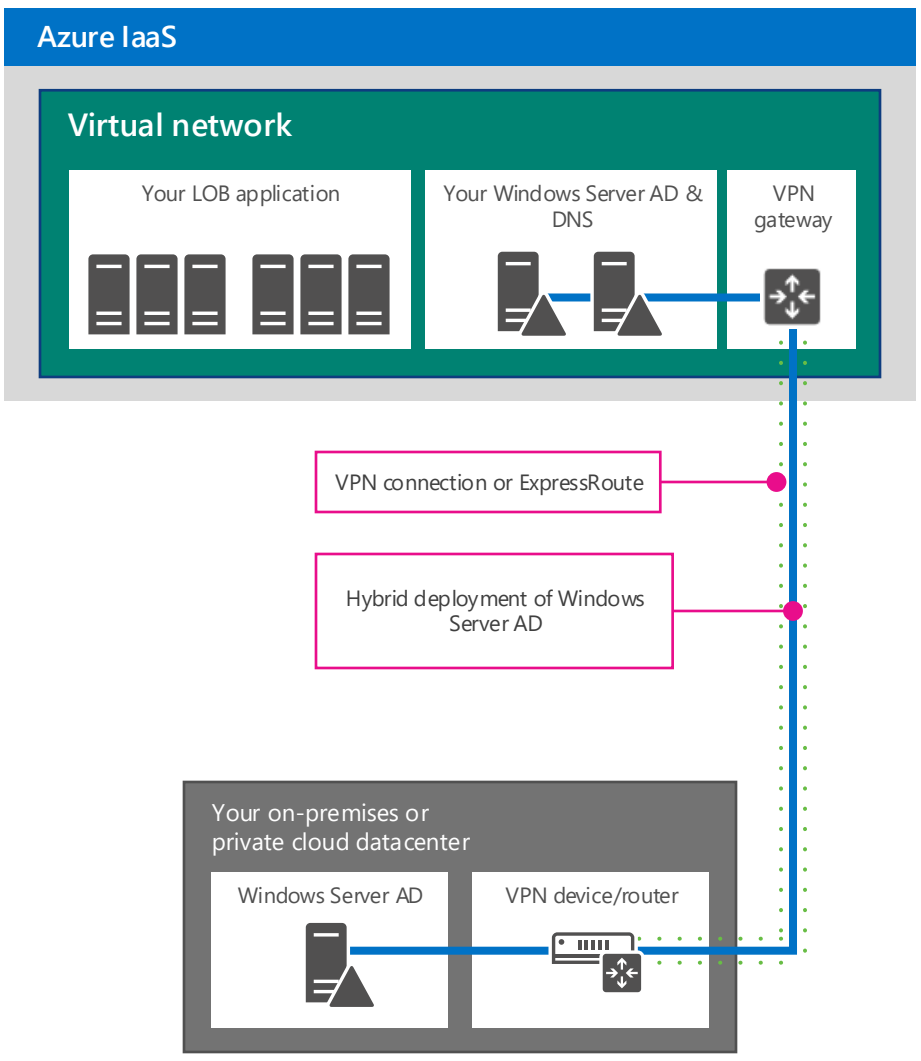
- Schema extensibility.
- Ability to write to existing directory identities.
- Support for applications in Azure virtual networks where network isolation is a requirement.
- Support across multiple Azure subscriptions.
- Certificate or smartcard-based authentication for applications.

See: Guidelines for Deploying Windows Server Active Directory on Azure Virtual Machines

Extend Windows Server AD to your Azure virtual machines

This configuration is a hybrid deployment of Windows Server AD on-premises and in Azure. It requires:

- A virtual network in Azure IaaS.
- A site-to-site VPN connection or ExpressRoute connection.
- Extending your on-premises, private IP address range to virtual machines in the virtual network.
- Deploying one or more domain controllers in the Azure virtual network designated as a global catalog server (reduces egress traffic across the VPN connection).



Connectivity options

Virtual Private Network (VPN)

Site-to-Site
Connect 1–10 sites (including other Azure virtual networks) to a single Azure virtual network.

Point-to-Site
Connect a single machine to an Azure virtual network.

ExpressRoute

A private, dedicated link to Azure IaaS via a cloud exchange, point-to-point Ethernet, or any-to-any (IP VPN) provider.

- Predictable performance
- Lower latencies

More Microsoft cloud IT resources

Services and Platform Options	Security	Identity	Storage
aka.ms/cloudarchoptions	aka.ms/cloudarchsecurity	aka.ms/cloudarchidentity	aka.ms/cloudarchstorage

August 2016

Microsoft