

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

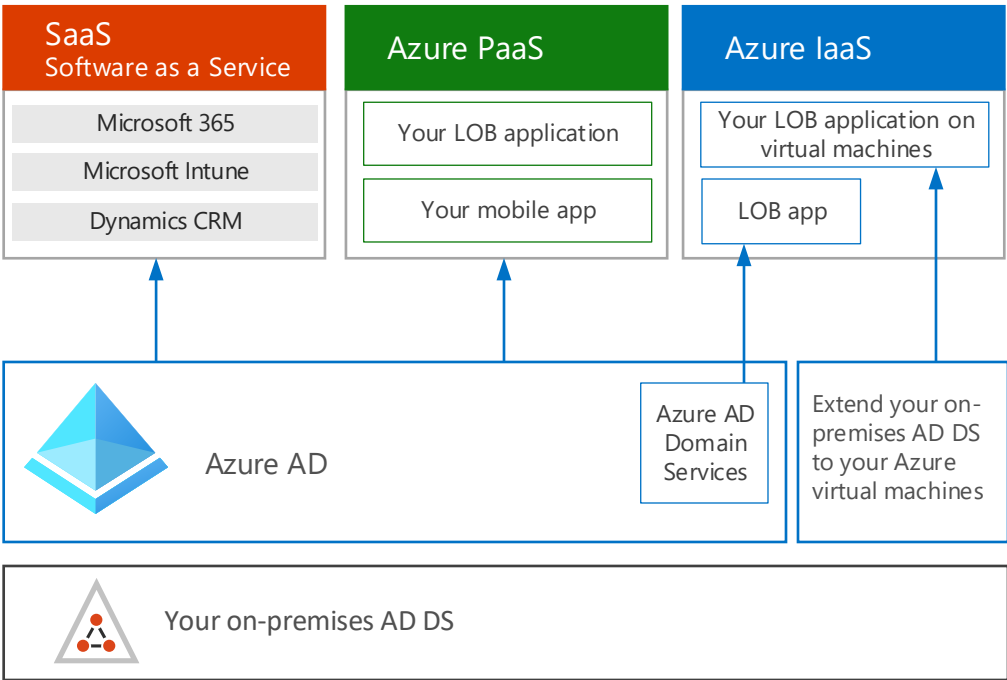
Introduction to identity with Microsoft's cloud

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

Azure Active Directory (Azure AD) integration supports:

- 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.

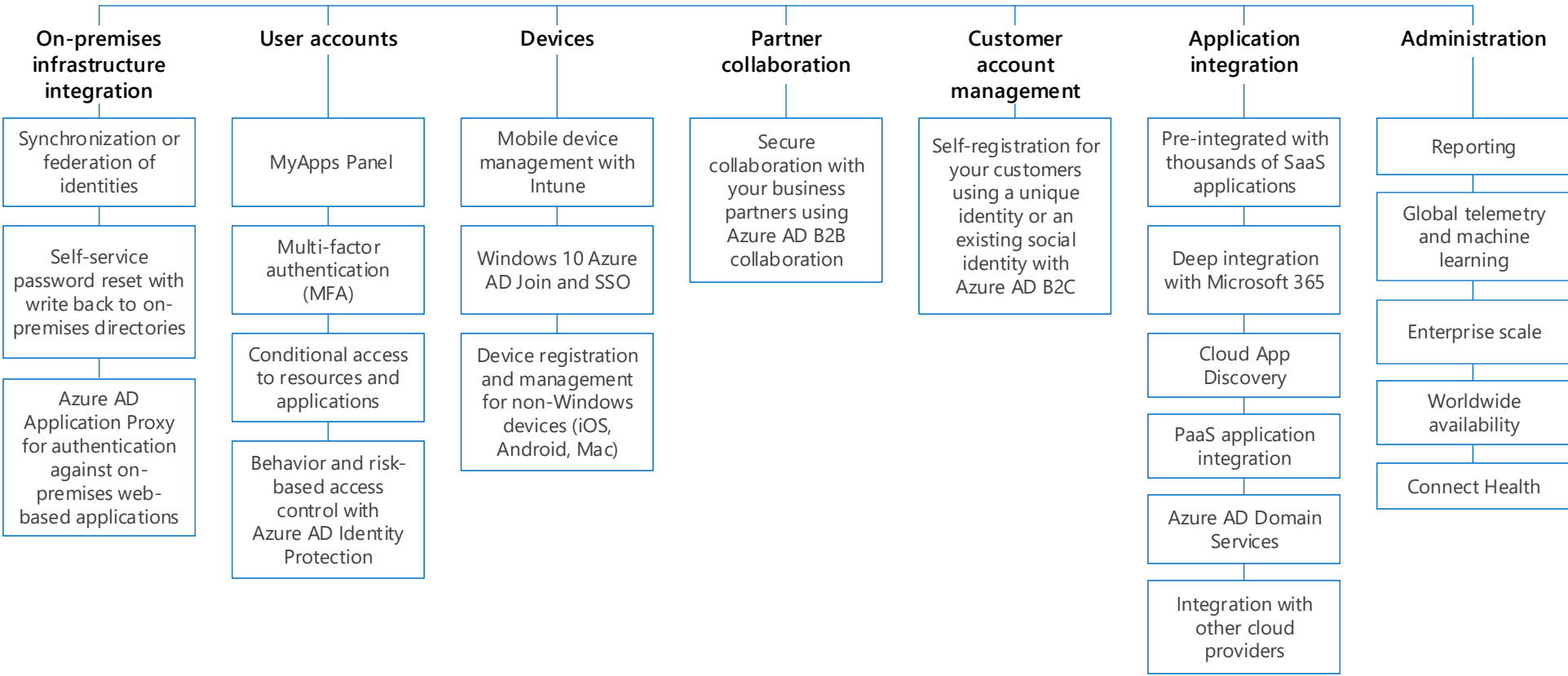
For line of business (LOB) applications hosted on virtual machines in Azure IaaS, you can use Domain Services in Azure AD or you can extend your on-premises Active Directory Domain Services (AD DS) environment.



Use Azure AD as your Identity as a Service 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 AD



Azure AD editions

Free	Office 365 apps	Premium P1	Premium P2
<p>Core identity and access management features.</p> <p>Included with Azure, Dynamics 365, Intune, and Power Platform.</p>	<p>Free edition capabilities plus features for identity and access management.</p> <p>Included with Office 365 E1, E3, E5, F1, and F3.</p>	<p>Office 365 apps edition capabilities plus advanced features for password and group access management, hybrid identities, and Conditional Access.</p> <p>Included with Microsoft 365 E3 and E5, Enterprise Mobility + Security (EMS) E3 and E5, or as separate licenses.</p>	<p>Premium P1 edition capabilities plus identity protection and governance features.</p> <p>Included with Microsoft 365 E5 and EMS E5, or as separate licenses.</p>

For more information, see [Azure AD pricing](#).

More information

Identity roadmap for Microsoft 365
<https://aka.ms/m365deployid>

Manage identity and access learning path
<https://docs.microsoft.com/learn/paths/manage-identity-and-access>

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

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 2 of 5 in a series 1 2 3 4 5

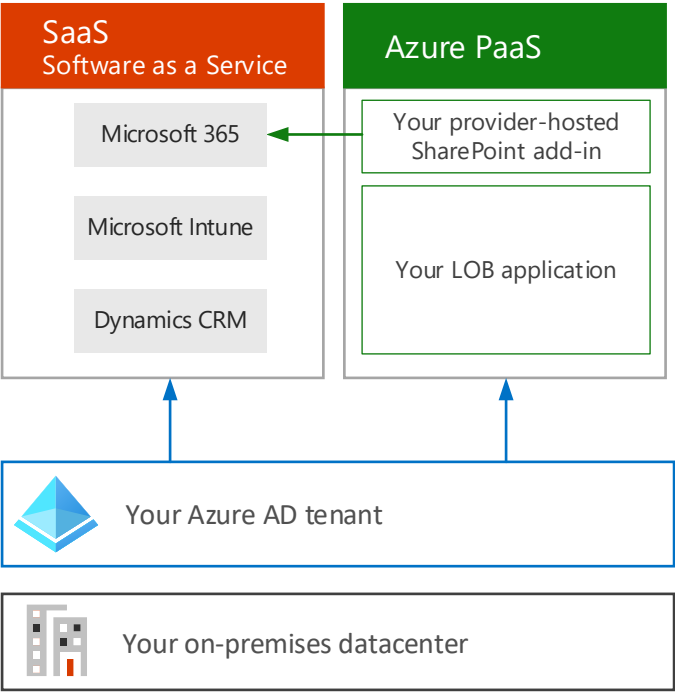
Azure AD integration capabilities

Azure 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.

Integration across Microsoft’s cloud

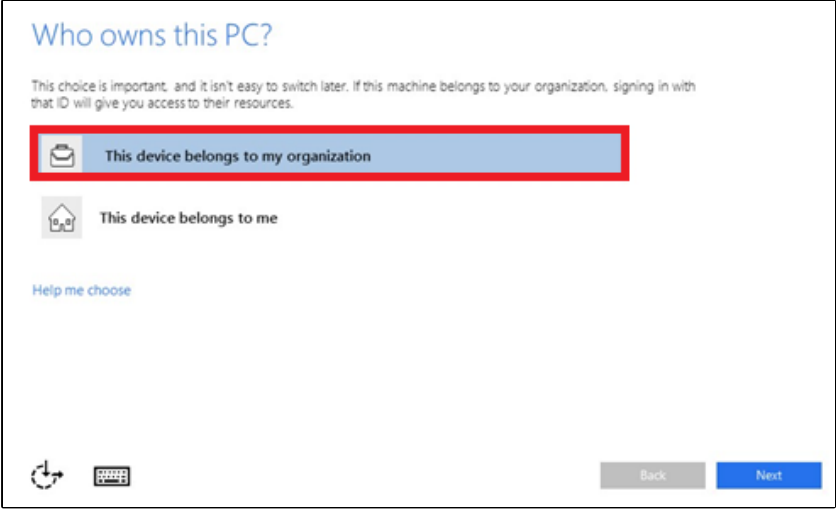
The foundational architectural steps you take with Microsoft 365 for identity integration provide a single architecture for adoption of workloads across Microsoft’s cloud, including PaaS workloads in Azure as well as other SaaS workloads, such as Dynamics CRM Online.

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](#).

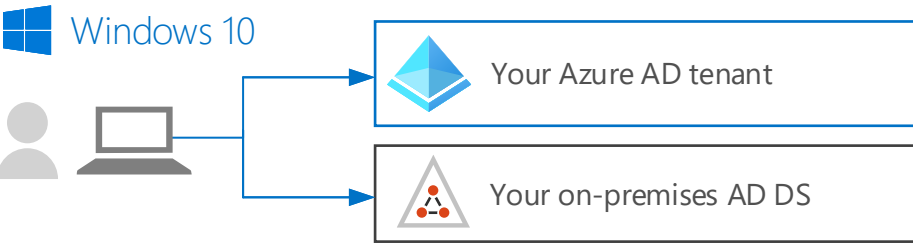


Windows 10 Azure AD Join

[Join Windows 10 devices to Azure AD](#) and provision these with Microsoft 365 services and applications within minutes when the device is configured during the out-of-box experience.

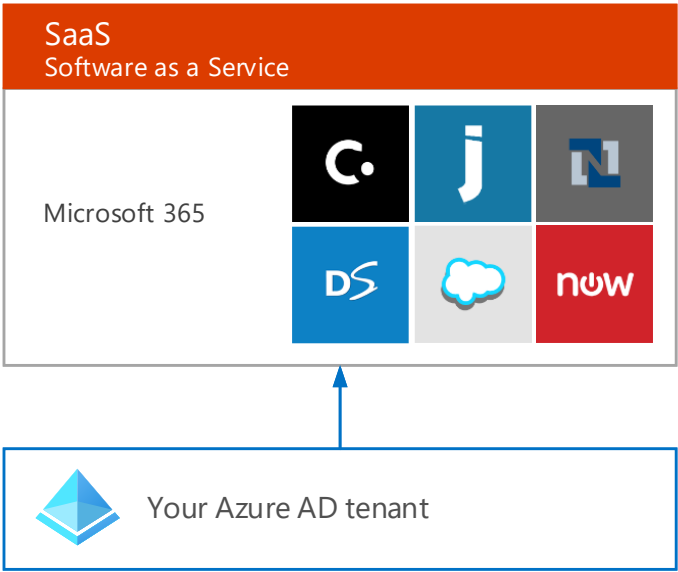


Windows 10 automatically authenticates with Azure AD and your on-premises AD DS, providing single-sign on without the need for Active Directory Federation Services (AD FS).



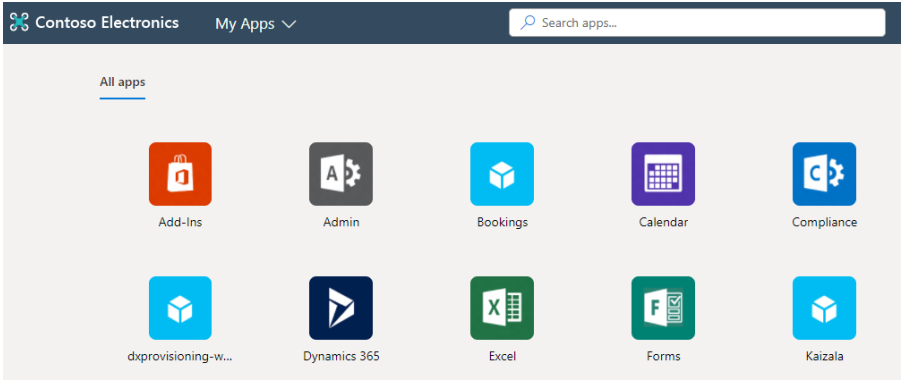
Single sign-on to other SaaS apps in your environment

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 [Azure 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 My Apps portal

The [My Apps portal](#) at <https://myapplications.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.

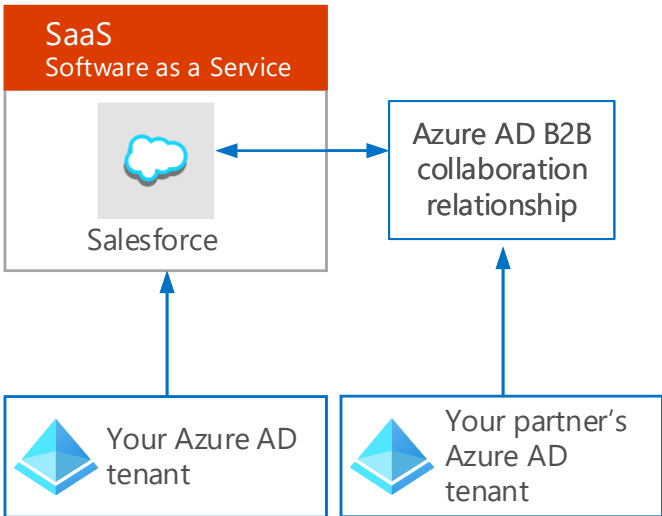


If you are a user with Azure AD Premium P1 or P2, you can also use self-service group management capabilities through the Access Panel Applications page at <https://account.activedirectory.windowsazure.com/#/>. This page is separate from the Azure portal and does not require users to have an Azure subscription.

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 having to manage additional directories or incurring the overhead of managing partner identities.

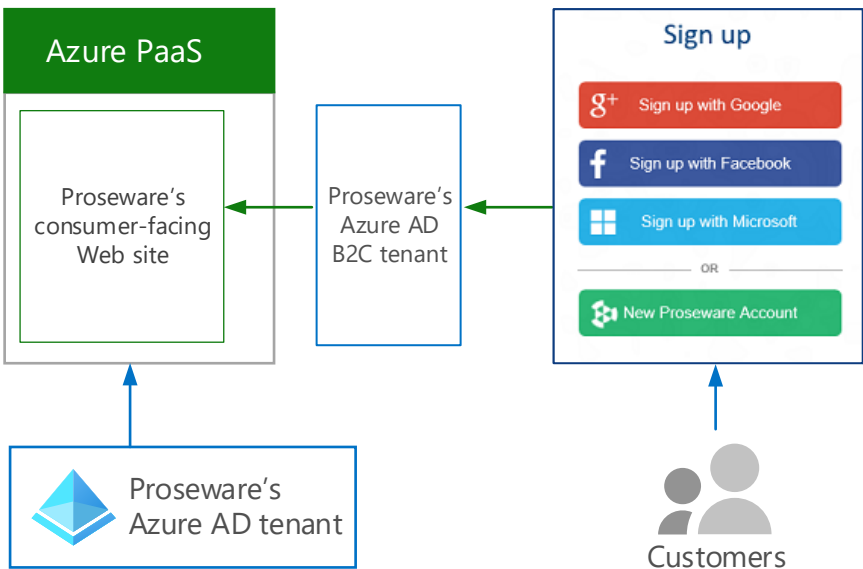
With 6 million organizations already using Azure AD, chances are good that your partner organization already has an Azure AD tenant, so you can start collaborating immediately. But even if they don't, Azure AD's B2B capabilities make it easy for you to send them an automated invitation which will get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



Azure AD B2C collaboration

[Azure AD 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 accounts or by creating new credentials.

Here is an example for the fictional Proseware organization.

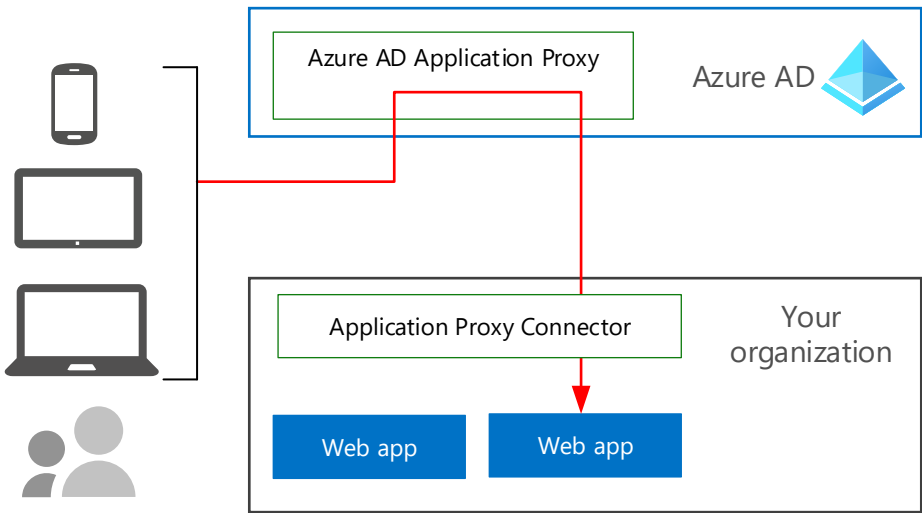


Application Proxy

Microsoft [Azure AD Application Proxy](#) lets you publish web applications inside your private network—such as SharePoint sites, Outlook Web Access, and Internet Information Services (IIS)-based apps—and provide secure access to users outside your network. Employees can log into your on-premises web apps remotely on their own devices and authenticate through this cloud-based proxy.

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

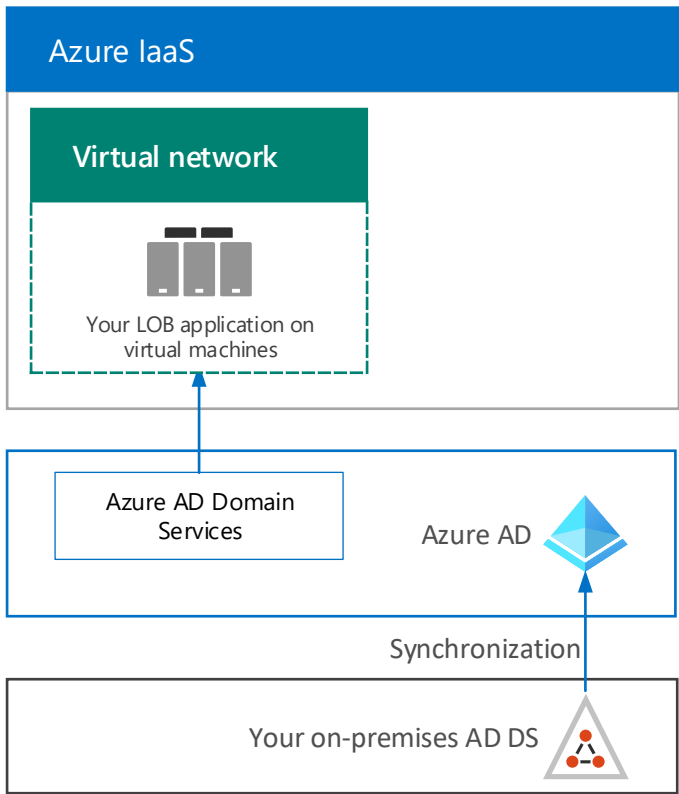
Azure AD Application Proxy works by installing a slim Windows service called an Application Proxy Connector inside your network. This Connector maintains an outbound connection from within your network to the Azure AD Application Proxy service. When users access a published web app, the proxy uses this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



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 Active Directory Domain Services (AD DS). You can join Azure virtual machines to an Azure-based AD DS 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 your organization's on-premises domain or forest infrastructure. However, all user accounts, group memberships, and credentials synchronized from the your on-premises AD DS are available in this managed domain.



More Microsoft cloud IT resources

Security
[aka.ms/cloudarchsecurity](#)

Networking
[aka.ms/cloudarchnetworking](#)

Hybrid
[aka.ms/cloudarchhybrid](#)

Identity and device access policies for baseline, sensitive, and highly regulated protection

Identity and device access policies ensure that only approved users and devices can access your critical apps and data.

Baseline protection is a minimum level of security for your identities and devices that access your apps and data.

Sensitive protection provides additional security for specific data. Identities and devices are subject to higher levels of security and device health requirements.

Highly regulated protection is for typically small amounts of data that are highly classified, contain trade secrets, or is subject to data regulations. Identities and devices are subject to much higher levels of security and device health requirements.

Protection level	Device type	Azure AD conditional access policies				Azure AD Identity Protection user risk policy	Intune device compliance policy	Intune app protection policies
Baseline	PCs	Require multi-factor authentication (MFA) when sign-in risk is <i>medium</i> or <i>high</i>		Block clients that don't support modern authentication Clients that do not use modern authentication can bypass Conditional Access policies.	Require compliant PCs	High risk users must change password This policy forces users to change their password when signing in if high risk activity is detected for their account.	Define compliance policies (one for each platform)	
	Phones and tablets		Require approved apps This policy enforces mobile app protection for phones and tablets.					Apply Level 2 App Protection Policies (APP) data protection (one for each platform)
Sensitive	PCs	Require MFA when sign-in risk is <i>low</i> , <i>medium</i> , or <i>high</i>			Require compliant PCs and mobile devices This policy enforces Intune management for PCs, phones, and tablets.			
	Phones and tablets							
Highly regulated	PCs	Require MFA <i>always</i> This is also available for all Office 365 Enterprise plans.						
	Phones and tablets							Apply Level 3 APP data protection

Start by implementing multi-factor authentication (MFA). First, use an Identity Protection MFA registration policy to register users for MFA. After users are registered you can enforce MFA for sign-in.

Using MFA is recommended before enrolling devices into Intune for assurance that the device is in the possession of the intended user.

For other SaaS apps in your environment, configure single sign-on with Azure AD and apply these policies or create new Conditional Access policies.

For all Conditional Access policies in Azure AD, configure an Azure AD exclusion group and add this group to these policies. This gives you a way to allow access to a critical user while you troubleshoot access issues for them.

Enroll devices for management with Intune before implementing device compliance policies.

Device compliance policies define the requirements devices must meet. Intune lets Azure AD know if devices are compliant. Recommended requirements include:

- Use passwords with strong parameters (alphanumeric, at least six characters, expiration of no more than 90 days).
- Be patched and have anti-virus and firewalls enabled.
- Use encryption, lock on inactivity, and wipe on multiple sign-in failures.
- Not be jailbroken or rooted.

For help implementing these policies, including policies for protecting Teams, Exchange email, and SharePoint sites, see [Identity and device access configurations](#).

App policies define which apps are allowed and what actions these apps can take with your organization content.

PCs include devices running the Windows or macOS platforms

Phones and tablets include devices running the iOS, iPadOS, or Android platforms

● Requires Microsoft 365 E5, Microsoft 365 E3 with the Identity & Threat Protection add-on, Office 365 with EMS E5, or individual Azure AD Premium P2 licenses

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 3 of 5 in a series

1

2

3

4

5

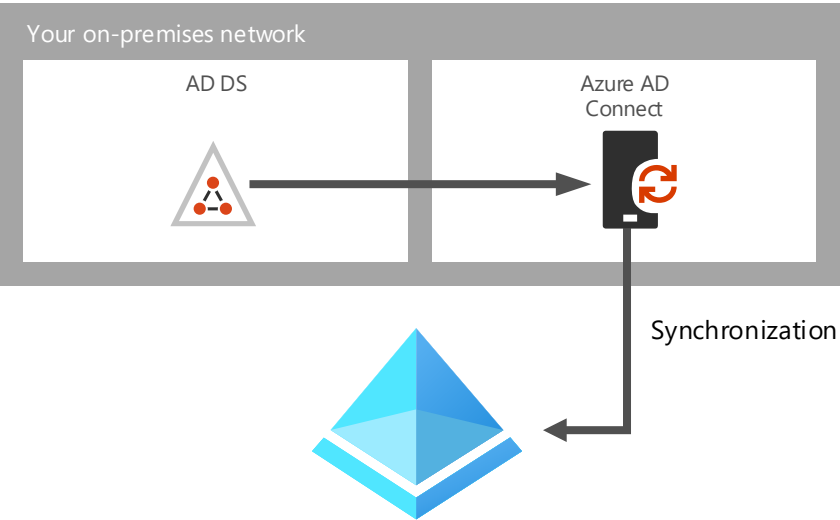
Integrate your on-premises AD DS accounts with Azure AD

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

Two identity configurations are recommended: hybrid or federated.
Using cloud-only accounts is not recommended for enterprise-scale organizations unless AD DS is not already used on premises.

Choose one option

Hybrid identity with password hash synchronization or pass-through authentication



This are the simplest and recommended options for most enterprise organizations.

- User accounts are synchronized from your on-premises AD DS to your Azure AD tenant. Your AD DS remains the authoritative source for accounts.
- Supports multi-forest synchronization.
- Users enter the same password for cloud services as they do on-premises.

Password hash synchronization (PHS)

Azure AD performs all authentication for cloud-based services and applications.

A hash of each already hashed password in AD DS is synchronized to Azure AD. It is not possible to decrypt or reverse-engineer a hash of a password or to obtain the original hashed password itself.

Pass-through authentication (PTA)

Azure AD passes all authentication for cloud-based services and applications to an AD DS domain controller through an on-premises agent. Hashed passwords are not stored in Azure AD.

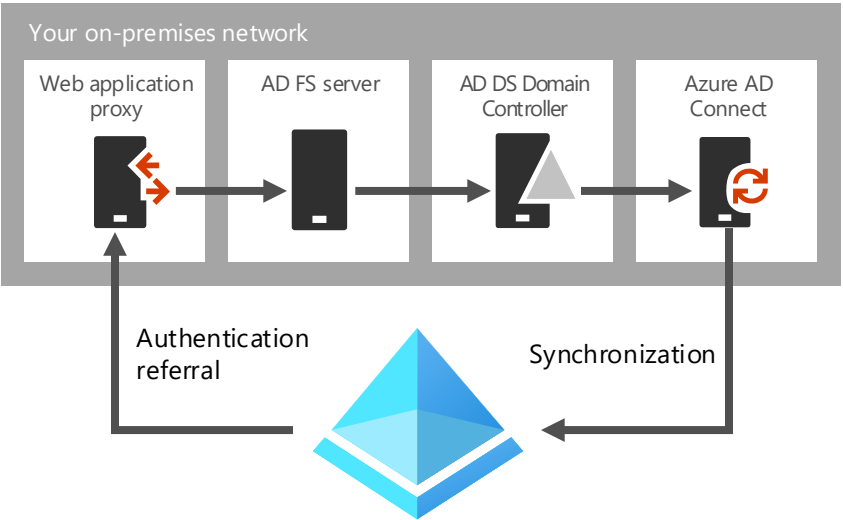
Multi-factor authentication (MFA)

User are subject to an additional verification method before completing sign-in.

Applications in Azure can take advantage of the Azure Multi-Factor Authentication service.

Directory synchronization does not provide integration with on-premises MFA solutions.

Federated identity with Active Directory Federation Services



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 Microsoft 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.



Identity configurations for your Microsoft 365 test environment



Federated identity for your Microsoft 365 test environment

More information

Prepare for directory synchronization to Microsoft 365
<http://go.microsoft.com/fwlink/p/?LinkId=524284>

Define a hybrid identity adoption strategy
<https://docs.microsoft.com/azure/active-directory/hybrid/plan-hybrid-identity-design-considerations-identity-adoption-strategy>

Set up multi-factor authentication for Microsoft 365
<https://docs.microsoft.com/microsoft-365/admin/security-and-compliance/set-up-multi-factor-authentication>

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 AD DS to Azure virtual machines for your line of business applications.

Which components can be put in Azure?

- Azure AD Connect
- Microsoft Active Directory Federation Services (AD FS) with Azure AD Connect
- Standalone AD DS environments in Azure IaaS

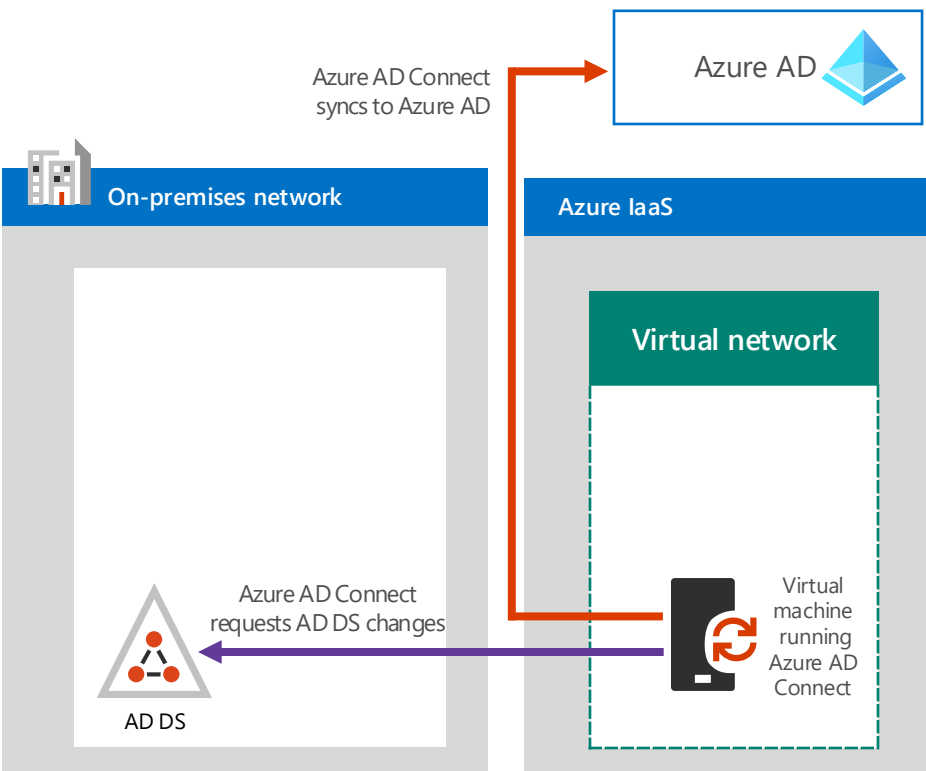
Azure AD Connect

Azure AD Connect can be hosted in the cloud using Azure IaaS virtual machines. Consider whether these benefits of deploying this workload to Azure makes sense for your organization:

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

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

For more information, see [Deploy Microsoft 365 Directory Synchronization in Microsoft Azure](#).



Azure AD Connect with federation

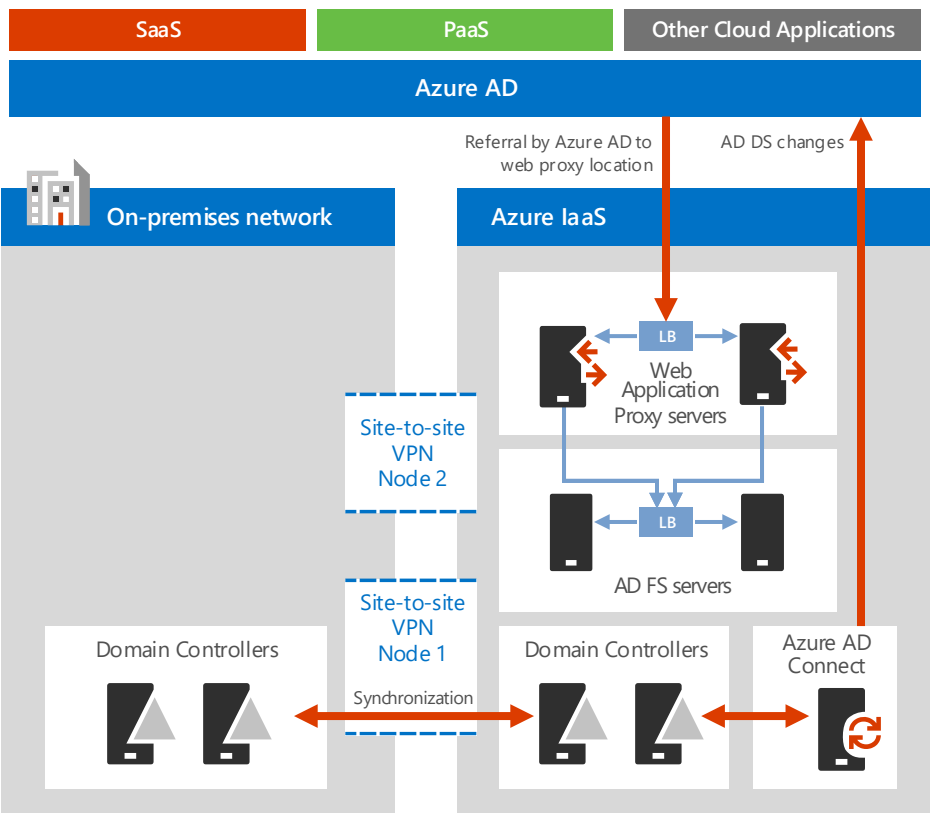
If you haven't already deployed AD FS on-premises, consider whether the benefits of deploying this workload to Azure makes sense for your organization.

- 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.
- 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 AD DS.

For more information, see [Deploy high availability federated authentication for Microsoft 365 in Azure](#).



Standalone AD DS environment in Azure IaaS

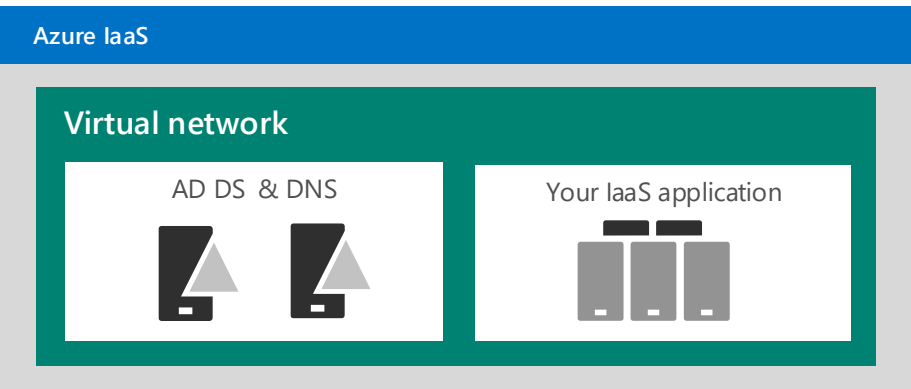
You don't always need to integrate a cloud application with your on-premises environment. A standalone AD DS domain in Azure supports applications that are public-facing, such as Internet sites.

This solution works with:

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

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

For more information, see [Active Directory Domain Services Virtualization](#).



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 5 of 5 in a series

1

2

3

4

5

Design domain services for workloads in Azure IaaS

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

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

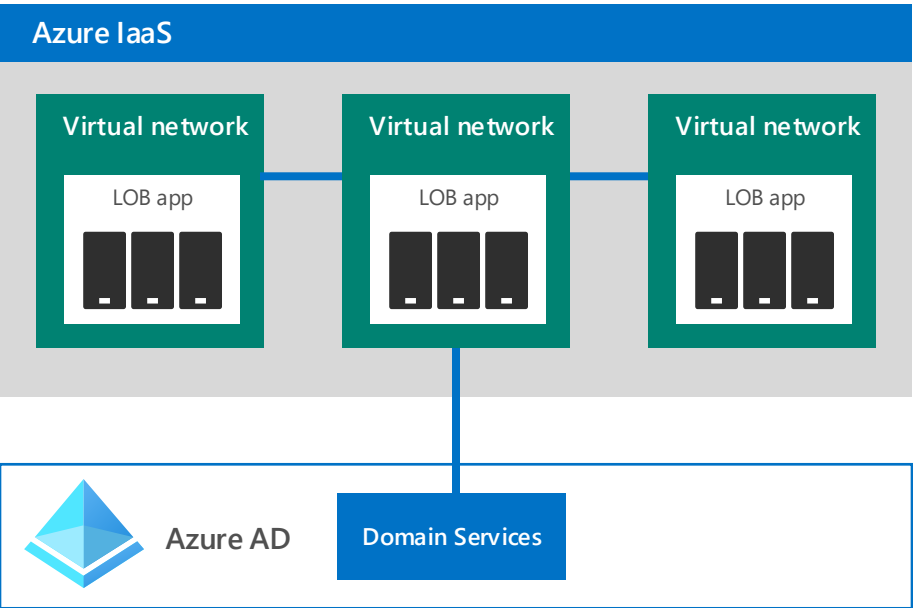
Microsoft currently recommends two solutions.

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.

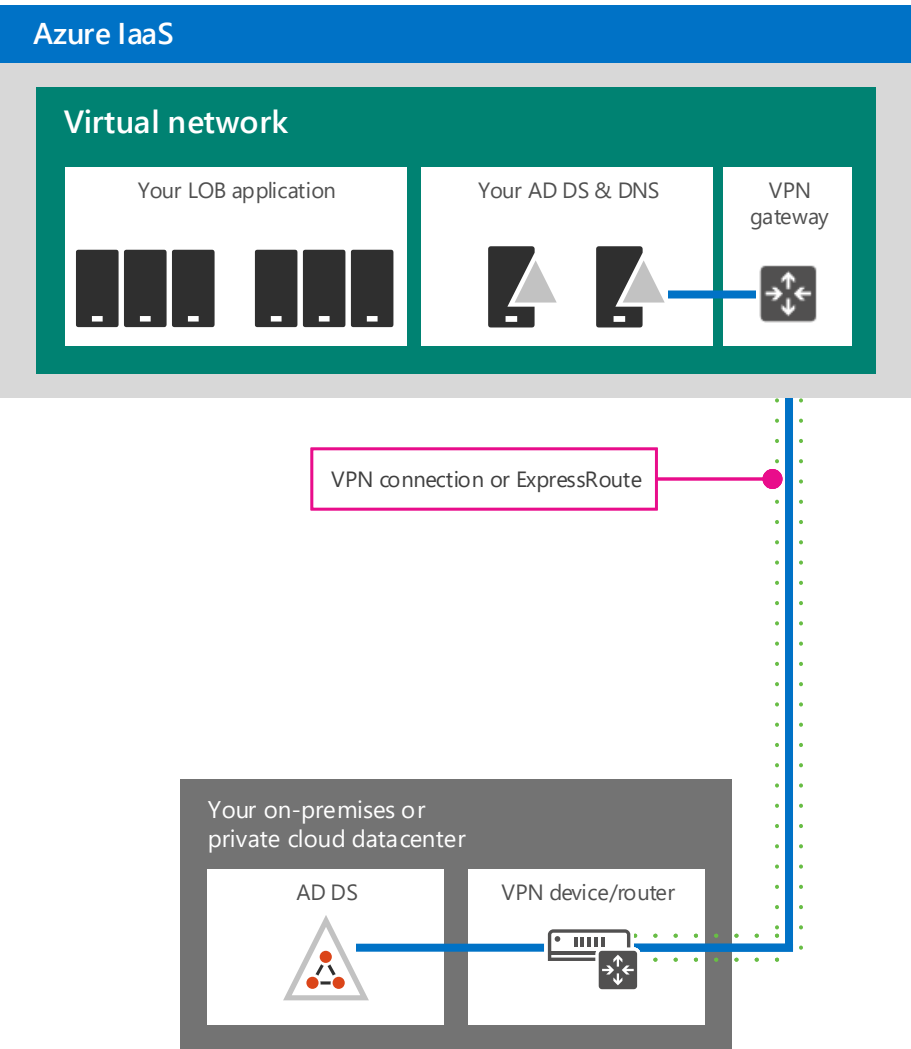
- Domain Services is connected to a virtual network in Azure IaaS. This instance of Domain Services can be used by other virtual networks that are connected to the virtual network configured with Domain Services.



Extend AD DS to your Azure virtual machines

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

- A virtual network in Azure IaaS.
- A site-to-site VPN 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, which reduces egress traffic across the VPN connection



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.

For more information, see [Common use cases and scenarios](#).

Extend your on-premises AD DS 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.

For more information, see [Safely virtualizing Active Directory Domain Services](#).

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

 Security
[aka.ms/cloudarchsecurity](#)

 Networking
[aka.ms/cloudarchnetworking](#)

 Hybrid
[aka.ms/cloudarchhybrid](#)