Microsoft

Azure Active Directory Solutions for Identity and Access Management

February 2015

Microsoft

Copyright

Microsoft

Contents

Microsoft

Introduction

Many organizations are considering the most effective and valuable way to invest in cloud services to modernize, control costs, and enable new capabilities and scenarios. Cloud-based scenarios often require new solutions to provide identity and access management capabilities.

This paper presents a collection of common scenarios and discusses the ways Azure™ Active Directory® (Azure AD) provides a comprehensive solution that addresses identity and access management requirements for on-premises and cloud applications, including Office 365 and a world of non-Microsoft SaaS applications. You can use this paper to help plan and prepare for using cloud services in your organization.

Organizations face identity challenges when doing business in new ways

Many organizations are migrating applications, data, and services to the cloud to avoid the costs of building and operating data centers. To remain competitive and relevant, organizations are retooling their business processes and workflows. As email has become a less useful means for collaboration between employees, vendors, and customers, businesses are looking towards new cloud-based collaboration solutions.

Organizations also need to meet the expectations of a mobile workforce, with device preferences, flexible schedules, and a desire to use social media. To increase productivity and agility, many businesses are enabling employees to access applications and data anywhere, anytime.

When businesses modernize, they often find shortcomings in infrastructure as well as in governance. Challenges presented by an inadequate identity infrastructure impact administration tasks, limit the types of solutions that an IT department can provide to an organization, complicate workflows, and hinder productivity.

Identity lifecycle management

IT departments burdened with identity and access management tasks have less availability to perform more high-value work, such as developing solutions at a pace that keeps up with business requirements.

Provisioning new users can be a time-consuming task, requiring a large amount of administration and configuration across several systems. Users may obtain access slowly and unreliably to the resources they need to perform their jobs. IT staff may need to access and configure several identity utilities and identity repositories when onboarding a new user for online services. Each time any employee needs to access an IT service, IT staff must manually handle the request and perform administrative tasks to enable access. With this ad hoc manual method, stringent levels of control, as well as compliance with necessary regulatory standards, is difficult to achieve.

Each LOB application at an organization can require a separate sign-in process, many maintaining their own identity stores. IT staff may need to separately provision users for each application, creating management overhead. During acquisitions of other companies, IT services can be inconsistent and

unreliable: users in new and old divisions may have difficulty accessing LOB applications, finding each other, and communicating.

Benefits of improving the management of the identity lifecycle include:

- Reduced cost and time to integrate new users
- Maximize investments of existing on-premises identities by extending them to the cloud
- Reduced time for new users to access corporate resources
- Reduced management overhead for provisioning process
- Improved security by ensuring access to systems can be controlled centrally
- Consistent application of security policies
- Reduced time to integrate acquired companies
- Reduced business interruptions
- Reduced exposure to outdated credentials
- Reduced time and cost to enable applications to accessible from the internet
- Increased capacity of IT to develop core application features
- Increased security and auditing
- Increased flexibility by delegating specific administration tasks

Communication and collaboration with employees, partners, and customers

IT staff may be unable to allow a user outside of the company to securely access only a restricted portion of the corporate network, data, and services. Opportunities are limited for employees to interact or collaborate with vendors, except through email.

Employees may be unable to locate or contact colleagues, or to schedule meetings that accommodate remote and mobile participants. Rather than using shared workspaces, meeting materials may be sent through email, limiting collaboration. Marketing campaigns may be inefficiently managed, with only limited feedback from the public.

Without a hybrid infrastructure that supports identity and access management, employees may work in relative isolation, exchanging ideas only at formal meetings or through email. Communications between team members may be erratic and unreliable. Employees may end up blocked in their work because they are unable to find or reach each other when necessary.

Benefits of improving collaboration capabilities include:

- Improved productivity for customers and partners.
- Cultivated culture of teamwork, sharing, and efficient collaboration
- Reduced operating costs
- Increased distribution of work
- Improved visibility and awareness of thought processes, team activities, tracking of tasks and commitments, external demands, and impacts
- Improved consistency in storing and managing project-related information
- Communication capabilities that scale
- Improved relationships with partners and external contributors

Mobility and device support

Employees may not be able to use LOB apps on many common personal devices and may depend on workaround solutions that create security risks. IT is unable to support mobility solutions due to existing identity and access policies. Employees struggle due to the inability of their devices to synchronize to each other. A calendar app or company address book may only sync while in on-premises, Employees can be difficult to locate because their presence information is not updated in real time. Employees cannot reliably participate in meetings, productively perform work, or collaborate with each other while out of the office.

Benefits of improving mobility and device capabilities include:

- Reduced cash outflow
- Improved productivity in accessing networks
- Improved employee satisfaction
- Reduced travel costs and lower facility costs
- Achieve efficiencies through consistent collaborative processes
- Broader contribution through attendance irrespective of type of network connection
- Improved time management
- Trustworthy data
- Improved agility

Security posture

An organization may have low confidence in its ability to avoid breaches of privacy, security, confidentiality, and data integrity. Following news reports of a breach of customer data at a market leader, many organizations examine their own policies and infrastructure for managing the identities of employees and vendors. They may find that different business units have LOB applications that perform authentication differently, and they may not all be in compliance with current policies.

Benefits of improving security posture include:

- Improved compliance with relevant regulatory requirements
- Avoiding costs of recovering from security breaches
- Avoiding costs of lost IP
- Avoiding costs of recovering from data loss
- Explicit and secure levels of access to online services

Digital identities are at the core of IT-related services

Identity is how people, devices, applications, and services access a variety of resources both within and outside an organization. Establishing an overall identity strategy involves far more than just provisioning objects and adding or removing access. It determines how an organization will manage accounts, standards in which validation occurs, and what a user, group, or service may access. A strategy will also address reporting on activities that affect identity lifecycles within the organization.

A well-formed identity infrastructure is based on guidelines, principles, and architectural designs that provide organizations interoperability and flexibility so they may adapt to ever-changing business goals

and challenges. The infrastructure should be based on standards for reasons of integration as well as manageability. In addition, it should be user friendly and simplify the end-user experience without sacrificing security.

Hybrid and cloud-based identity services provide solutions

With the advent of the cloud and the cost-effective data, storage, and processing power that it provides, organizations are seeking new solutions that support identity and access management for cloud-based resources as well as for on-premises resources. Azure AD makes hybrid solutions possible by allowing organizations to manage and control identity and access on-premises and in the cloud.

Traditionally, on-premises solutions provided the control points for identity and access management. In most organizations, there was limited external access to on-premises applications and data, and the security provided by on-premises solutions was adequate to support a limited number of mobile workers who needed access to IT resources.

Azure AD extends on-premises Active Directory to the cloud, and enables new scenarios and easy-to-use capabilities for employees, customers, vendors, and partners. The combination of Windows Server® AD, Microsoft® Identity Manager, and Azure AD produces a modern identity management system that spans the cloud and on-premises infrastructure, providing federation, identity management, device registration, user provisioning, access control for applications, and data protection.

Azure Active Directory is a comprehensive service

Azure AD is the world's largest enterprise identity and access management solution, and is the directory for Office 365, Azure, Intune and other Microsoft online solutions. It is a comprehensive identity and access management service that combines directory services, identity governance, application access management, and a standards-based platform for developers. Azure AD is also designed to work with on-premises Active Directory and other directories, allowing organizations to leverage existing on-premises infrastructure for the cloud.

Azure AD is cross-platform and based on well-defined standards that support interoperability and compliance. Azure AD supports many popular clients and server/service platforms.

Organizations that use the identity and access management features of Azure AD are able to:

- Simplify access and control of software as a service (SaaS) applications
- Reduce the IT burden with self-service identity and access management
- Improve security posture with cloud services
- Easily meet reporting requirements
- Rapidly develop and deploy new enterprise capabilities

Benefits and capabilities of Azure Active Directory

This section provides information about some of the specific capabilities and the benefits that Azure AD provides.

Improve operation, experience, and auditing of on-premises and cloud applications

Using Azure AD, users are able to access applications via a common experience whether on-premises or in the cloud, while enabling business, usage, and audit reporting across all applications.

Members of an IT department will spend less time assessing and auditing the use of cloud applications, and improve their ability to prioritize development and integration tasks, using Azure AD tools that scan an enterprise to identify cloud applications in use, and to identify those that have the biggest impact on the organization with regard to confidentiality, IP protection, or compliance. IT can then prioritize the process for integrating control of SaaS applications that use Azure AD.

One critical challenge that users and administrators face is the multitude of passwords needed to access the variety of cloud services that they use. Using Azure AD, organizations can centralize and manage access to applications, protect data from misuse, and monitor activities in order to identify potential security issues or threats.

Just as businesses use identity to control access to on-premises resources, Azure AD can additionally control access to applications in the cloud – including third-party services. Many service subscriptions held by businesses today, such as a customer relationship management (CRM) system, must have a trust relationship with an external entity or else manage a separate set of credentials for each user. Unlike those service subscriptions, Azure AD provides identity integration with hundreds of different enterprise applications.

Azure AD enables single sign-on (SSO) to many of the most popular SaaS applications (more than 2400 today and we continue to add new applications every month), regardless of where they are hosted. All the necessary parameters are preconfigured for federation within the Azure Application Gallery, a single place from which to access them. Some examples include Office 365, Microsoft Intune®, Salesforce.com, Box, Google Apps mail, Concur, and GoToMeeting. Some SaaS applications support pilot migrations, enabling organizations to first move an initial set of users; other applications require organizations to move all users within a subscription at one time. Have a conversation with Microsoft or your SaaS vendors to see if they allow pilot migrations.

Even if an organization uses cloud-based, custom line-of-business (LOB) applications that are not pre-integrated into Azure AD, an administrator can often use simple steps to add them and enable SSO.

Enterprises that have a hybrid connection between Windows Server AD and Azure AD will benefit from having SSO using their on-premises username and password. Managing access to applications and services in the cloud via Azure AD can be integrated with the current administration of on-premises Active Directory because the hybrid connection synchronizes group membership from on-premises Active Directory to Azure AD. For example, when a user joins an on-premises finance security group to gain access to printers, file shares, or older applications, the user will be granted access to the cloud applications for the finance team as well.

After organizations understand how they can use Azure AD to manage access to cloud based SaaS applications, the next natural question is "Can I use Azure AD to manage access to my on-premises apps?"

Azure AD Application Proxy lets you do exactly that. It extends Azure AD's SaaS app management capabilities to on-premises applications, giving you the ability to make internal browser based applications (SharePoint Sites, Outlook Web Access and IIS based applications) available on the internet. You can make these apps available in a secure manner to authenticated users through a cloud proxy hosted in Azure that publishes internal web applications to the Internet.

Support for on-premises and cloud-based applications in Azure AD enables organizations to securely adopt and use cloud applications while complying with audit policies for managing access, as well as provisioning and de-provisioning of users accounts.

Save time managing Office 365 for hybrid enterprises

For hybrid enterprises that incorporate the cloud in their IT infrastructure, there are several key advantages for enabling Azure AD Premium features as a part of using Office 365, including self-service group management, enhanced reporting, and automated provisioning.

Enterprises can use self-service group management to delegate user access. When a user is approved and added to a group, Azure AD will automatically license the user for Office 365[1] as well as give them access to the pre-defined applications. An administrator can create and manage these groups in the cloud or on-premises: Azure AD will ensure that the groups stay in sync even among challenging multi-forest environments.

Azure AD can provide enterprises with enhanced reporting and email notification about usage and anomalies for users accessing Office 365. This capability is critical for safeguarding documents across organizations.

To address the challenge of constant change in the employee community, Azure AD Premium supports automated provisioning from HR systems such as Workday, SAP, and Oracle eBusiness. This support enables Office 365 applications to always be up-to-date with employees, whether they are joining, changing roles, or leaving the organization. The ability to rapidly de-provision employees who leave the organization is a critical safety measure that Azure AD addresses.

Improve security though analytics and intelligence

Using Azure AD, IT administrators can more easily identify and mitigate security threats, address regulatory compliance requests, and meet the reporting requirements of business owners. Such information provides the data to address issues using cloud-hosted controls, such as multi-factor authentication. For a general discussion of security in the cloud, see the paper Azure Security, Privacy, and Compliance.

Because the identity system controls access to many of an organization's high-value business assets, the identity service should be considered a key security asset and a likely attacker target. Because of the level of sophistication of determined adversaries conducting targeted attacks, organizations need to apply

[1] The feature to allow the assignment Office 365 licenses to users using group membership is still in development.

rigor in the design, configuration, and operation of the identity system to ensure it is appropriately protected.

Support for reporting and roles

An IT administrator has a full range of efficient usage and management reporting through the Azure Portal. The administrator can monitor and report overall and specific application usage, and ensure prompt and accurate provisioning of users. The administrator can also monitor self-service capabilities such as end user profile registration, password registration, password change and reset, group creation, and join/leave actions. These details are available in an easy-to-use management report interface, available as an audit download, and programmatically accessible for integration with on-premises operational or security reporting systems.

Azure AD has a large variety of reporting capabilities, from cloud application discovery to machine learning for security reporting with actionable output. This machine learning builds on the billions of Azure AD/Office 365 authentications that Azure AD processes each week and creates security reports about anomalous sign-ins and suspicious usage patterns, as well as notifications about the potential compromising of accounts. Reports are also available that highlight users who may have been compromised by botnets, based on malware detection data. In addition, Azure AD can create audit reports of the activity of administrators and privileged users. Azure AD also enables role-based access control for management of resources in Azure itself. This control allows an organization to define the appropriate level of management to resources in Azure (such as websites and VMs) to Azure AD users, groups, and services. Users have roles based on a subscription, resource group, or individual resource level.

The assigned role defines the level of access that the users, groups, or services have on the Azure resource. Although the current preview is focused on management of Azure resources, this capability will soon be made available to application developers, enabling them to integrate precise access control checks in their own applications.

Support for authentication

Azure Multi-Factor Authentication (MFA) reduces risk to an organization and supports regulatory compliance. Multi-Factor Authentication, which can be used for both on-premises and cloud applications, provides an extra level of authentication, in addition to a user's account credentials, to secure access from employees, customers, and partners.

Azure MFA supports strong authentication via a range of easy options that users choose from, including mobile applications (push notifications and one-time password or OTP modes), phone calls, and text messages (one-way or two-way). Using the phone call, two-way text message, or mobile app push notifications provide 100% out-of-band authentication because the second-factor authentication is completed through a separate channel from the primary authentication. Azure MFA is integrated with Azure AD to secure applications that use Azure AD as an identity provider.

Organizations can also download and use the Azure Multi-Factor Authentication Server on-premises to secure remote access and other web applications. The ability to secure Active Directory Federation Services (AD FS) allows organizations with hybrid IT infrastructures to use Azure MFA in the cloud, on-

premises, or both. Developers can easily integrate Azure MFA into LOB applications using the Azure MFA SDK, which is available in a variety of development languages.

Simplify administration of identity-related tasks and improve the user experience

To decrease the time an IT department and delegated employees spend administering identity and access-related tasks, Azure AD supports user groups. To simplify identity-related tasks that require multiple steps, such as when granting access to multiple users, user groups support automating sets of actions. An administrator can put users into a group, and then add that group to the permission list of the application. If those same users need access to another resource, an administrator can easily enable them through the same process.

Azure AD provides this capability across all cloud services with group-based SaaS application access. An organization can create these groups solely in the cloud, or can use existing groups that have been synchronized from an on-premises Active Directory, using the Azure AD Sync tool – effectively extending any directory to Azure. Once the group exists, group owners can self-manage approval of requests to join and membership updates using the Azure AD Portal.

Administrators can easily delegate join and leave requests for application access to the appropriate business owner. All licensing requirements for Microsoft online services including Azure AD, Enterprise Mobility Suite, and Office 365 are supported to enable this delegated group-based assignment.

Administrators can define administrative units (partitioned groupings of users) and assign and delegate administrators for the units to manage the users, applications, and permissions associated with that unit. This capability allows even the largest and most complex enterprise to easily manage the distributed organization and enables the right owners to have the right permissions for managing and monitoring identity and access for their administrative units.

All actions taken on Azure AD are monitored and audited using a simple, self-service audit report available at all times to support compliance or forensics requirements of an organization.

To improve the end-user experience even more, an IT department can add a company logo and color schemes to an organization's Sign In and Access Panel pages. These options apply a consistent look and feel across all Azure web sites and services. Azure AD also supports the ability to create globalized versions of branded pages for different languages and locales.

For users that need browser-based access to cloud applications and services, sign-in pages enable Azure to redirect federated users to their on-premises security token service (such as an AD FS gateway), or to enter their credentials directly and authenticate to Azure AD.

Many Microsoft online services use Azure AD as an identity repository and authentication platform, including Office 365, Xbox Live®, and CRM Online. Each service has a distinct Active Directory tenant, managed independently by the respective service operators. It is not possible for one tenant to manage the properties or data of another.

Similarly, the Azure subscription owner or administrator manages the subscriber's Active Directory tenant via a single associated Organizational ID, which can create new identities and domains, change the schema, delegate administrative authority to other users, and configure the various Azure AD services

(such as synchronization and federation). Subscription administrators choose how they want to manage their Active Directory tenant based on the services or mechanisms best suited for their organization, and the mechanisms can be combined into an end-to-end identity solution.

Subscription administrators manage Azure AD tenants, using the Azure Portal to create, delete, distribute and manage user and group accounts. In addition, administrators use the portal to set up on-premises integration with the organization's directory service to manage access. Azure AD also supports a delegated management model with role-based access control (RBAC) for down-level service administrators.

For an organization, the Azure Portal points to the single instance of Azure AD tenant associated with the subscription and shared across all of the Microsoft cloud services that use Azure AD (such as Microsoft Intune and Office 365). An administrator can also view business-related attributes for every user, and see which devices, platforms, browsers, and IP addresses they are using.

Perhaps most importantly, an administrator can use the Azure Portal to assign access to the SaaS applications added from the Application Gallery or from other sources (such as custom-developed applications), as well as any integration services that are already configured. These applications will present a variety of options for identity management based on differing standards and authentication methods. For some an administrator can configure federated SSO, while others may only support password SSO (also known as password vaulting).

Improve efficiency of managing the user lifecycle

Azure AD helps IT departments ensure that accounts for individuals are maintained during the user lifecycle while following organizational policies and procedures for account creation, termination, and other events.

For small and mid-sized organizations that were "born in the cloud," Azure AD may be the primary identity repository. The administrator can use Azure AD's web interface to provision and de-provision users and to provide support for recovery, such as in cases of accidental deletion. As organizations grow they can use Windows PowerShell® for file-based upload and quickly add more users. Applications can also extend the schema of Azure AD objects to store additional attributes relevant to the application or a customer in the Azure AD directory.

Many larger organizations use an HR system such as SAP, Oracle PeopleSoft, or Dynamics AX as the system of record authority identifying employees as well as many user attributes. Azure AD Sync can be configured to automatically synchronize new users, as well as changes to users, from an on-premises HR system to Azure AD. Within Azure AD, the administrator can configure additional licenses and access rights for the users.

Azure AD provides additional management features for the identity object lifecycle, including features of Microsoft Identity Manager (MIM):

- **Self-service and dynamic rule-based groups**. Distribution groups such as "all employees" can be automatically maintained. Applications that rely on security groups for access control are automatically kept up-to-date as a user's employment status and job roles change.

- **Workflow-driven, role-based, and rule-based provisioning**. Organizations can define and manage the policies controlling which users should have accounts in federated SaaS applications, such as Salesforce or Box. Those accounts are automatically provisioned and de-provisioned based on changes to the user's attributes, roles, or other rules.
- **Provisioning to additional on-premises and private cloud directory services and databases**. Data from the system of record authority can be kept in sync with other existing directories and applications present in the enterprise.
- **Attestation**. Regularly scheduled recertification of user's access entitlements to SaaS applications with automated campaigns for ensuring reviews by line managers, application owners, or other responsible individuals.

Increase developer focus on core functionality of applications

Development resources should be able to remain focused on building core functionality on any cloud platform, rather than spending time creating plumbing for access controls and user databases. Azure AD is designed for businesses to offload many identity tasks. Developers can then help ensure more secure solutions and automatically extend scope as needed.

As a platform for developing identity-driven services, Azure AD provides APIs and libraries that support programmatic access to administrative and functional components. REST-based (REpresentational State Transfer) interfaces provide a mechanism for developers to integrate identity management into new applications using the Azure AD Authentication Library (ADAL) for .Net, which supports modern identity protocols, including OpenID connect and OAuth. ADAL advances the technology incorporated in the Windows Identity Foundation (WIF).

Using Azure AD authentication, developers can avoid building a unique identity and access management component for each application. Azure AD has support for OAuth 2.0, enabling developers to build mobile and web applications that integrate with Microsoft and third-party web APIs, and to build their own secure web APIs. Open source client libraries are available for .NET, Windows Store, iOS, and Android, with additional libraries under development. Other tools include:

- **Azure AD Authentication Library (ADAL) for .Net** enables client application developers to easily authenticate users to cloud or on-premises Active Directory (AD), and then obtain access tokens for securing API calls. ADAL for .NET has many features that make authentication easier for developers, such as asynchronous support, a configurable token cache that stores access tokens and refresh tokens, automatic token refresh when an access token expires and a refresh token is available, and more. By handling most of the complexity, ADAL can help a developer focus on business logic in their application and easily secure resources without being an expert on security.
- **Graph API**. Applications can interact with data in Azure AD using the (REST) Graph API, similar to how LOB applications might use LDAP to access data in local Active Directory stores. The Graph API supports Office 365, Exchange, and SharePoint Online, as well as third-party applications, and allows an application to query Azure AD and receive a view of the enterprise directory and the relationships among its objects. For example, if an application has a workflow that includes the manager of the user, the developer can retrieve the identity through the Graph API.
- **Azure Service Management API (SMAPI)**. SMAPI provides a comprehensive set of programming interfaces for any executable task in the service, including management of Azure AD. Administrators can use the Azure Active Directory Module for Windows PowerShell Cmdlets to accomplish many

Azure AD tenant-based administrative tasks, such as user and group management, domain management, and configuring single sign-on.

- **Multi-Factor Authentication SDK**. The MFA SDK enables direct integration with cloud services, enabling organizations to add Active Authentication with phone call and text message verification into an application's sign-in or transaction processes while using the application's existing user database.
- **Schema extensibility**. Directory Extensions for Azure AD enable developers to build more powerful, directory-aware applications without spending time on access controls, availability requirements, two phase commits, and other factors that an external user profile store often presents. Directory Extensions can also help organizations move their applications to the cloud by seamlessly synchronizing on-premises schema extensions to Azure AD, allowing them to leverage investments in on-premises applications as they move to the cloud.
- **Simplified integration**. Enterprises that use cloud-based SaaS or custom LOB applications that are not pre-integrated into Azure AD can often follow simple steps to add the applications and enable SSO. Similarly, existing on-premises web applications can be made securely available on the internet using Azure AD Application proxy.

Features of Azure Active Directory

There are three versions of Azure AD available: Free, Basic, and Premium. Azure Active Directory Premium is an advanced offering that includes identity and access management (IAM) capabilities for on-premises, hybrid, and cloud environments. The identity scenarios and solutions described in this paper use many features of Azure AD Premium. The following table shows the feature differences in the different versions of Azure AD.

Table 1. Comparing features of different versions of Azure Active Directory

Features	Azure AD (Free)	Azure AD Basic	Azure AD Premium
Directory as a Service	Up to 500k objects	No object limit	No object limit
User and group management using UI or Windows PowerShell Cmdlets	Yes	Yes	Yes
Access Panel portal for SSO-based user access to SaaS and custom applications	10 applications per user	10 applications per user	No limit
User-based application access management/provisioning	Yes	Yes	Yes
Self-service password change for cloud users	Yes	Yes	Yes
Directory synchronization tool – For syncing between on-premises Active Directory and Azure Active Directory	Yes	Yes	Yes
Standard security reports	Yes	Yes	Yes
High availability SLA uptime (99.9%)		Yes	Yes
Group-based application access management and provisioning		Yes	Yes
Company branding - customization of company logo and colors to the Sign In and Access Panel pages		Yes	Yes
Self-service password reset for cloud users		Yes	Yes

Features	Azure AD (Free)	Azure AD Basic	Azure AD Premium
Application Proxy		**Yes**	**Yes**
Self-service group management for cloud users		**Yes**	**Yes**
Self-service password reset with on-premises write-back			**Yes**
Microsoft Identity Manager (MIM) server licenses – For syncing between on-premises databases and/or directories			**Yes**
Advanced anomaly security reports (machine learning-based)			**Yes**
Advanced usage reporting			**Yes**
Multi-Factor Authentication service for cloud users			**Yes**
Multi-Factor Authentication server for on-premises users			**Yes**

Enterprise service level agreement (SLA) of 99.9%. Microsoft has financially backed guarantees for at least 99.9% availability of the Azure AD Premium service. For more information, see Active Directory Premium SLA.

Advanced anomaly security reports and alerts. Organizations can monitor and protect access to their cloud applications by viewing detailed logs that show advanced anomalies and inconsistent access pattern reports. Advanced reports are based on machine-learning algorithms and can help IT departments gain new insights for improving access security and proactively responding to potential threats. For more information, see View your access and usage reports.

Company branding. This feature enables an organization to set the look and feel of the key sign-in and end-user portal experience (Access Panel). This capability helps employees know that they are interacting with specific company resources when performing security actions such as signing in, accessing applications, and changing their passwords. An organization can add the company logo and color schemes to the sign-in and Access Panel pages, as well as localized versions of the logo for different languages and locales. For more information, see Add company branding to your Sign In and Access Panel pages.

Group-based licensing and application access. Use security groups to assign users to Azure AD Premium licenses, and also provision users and assign user access in bulk to thousands of SaaS applications. An administrator can create these groups solely in the cloud, or use existing groups that have been synced in from on-premises Active Directory. For more information, see Assign access for a group to a SaaS application.

Self-service password reset. Configure verification requirements and enable end users to easily update and change passwords securely, thereby significantly reducing the cost and increasing productivity of the employees in an organization. With Azure AD, IT departments can reduce helpdesk calls when users forget a password by giving all users in the directory the capability to reset their password, using the

same sign-in experience they have for Office 365™. For more information, see Self-service password reset for users.

Self-service password reset with write-back- self-service password resets from Azure AD, can be written back to on-premises Active Directories. This allows organizations to further reduce support costs and give users the flexibility to reset their on-premises AD User account passwords, from the Azure AD Access Panel.

Self-service group management. Azure AD Premium simplifies day-to-day administration of groups by enabling users to create groups, request access to other groups, and delegate group ownership so others can approve requests and maintain their group's memberships. Azure AD uses rules that are simple to configure to ensure that the right people are able to approve requests for access to critical resources. Group members are automatically provisioned and de-provisioned based on their current membership in the group. For more information, see Self-service group management for users.

Multi-Factor Authentication (MFA). This feature is now included with Azure AD Premium. MFA can help secure access to on-premises applications (VPN, RADIUS, and so on), Azure, Microsoft Online Services such as Office 365 and Dynamics CRM Online, and thousands of non-Microsoft cloud services pre-integrated with Azure AD. After an organization enables Multi-Factor Authentication for Azure AD identities, users will be prompted to set up additional verification the next time they sign in. For more information, see Adding Multi-Factor Authentication to Azure Active Directory.

Application Proxy. This feature enables an IT department to publish web applications inside your private network and allow users on any device to access them from outside the network, without opening your network to incoming traffic. For more information, see Using Application Proxy to publish applications for secure remote access.

Microsoft Identity Manager (MIM). Azure AD includes the option to grant rights for using a MIM server and client access licenses (CALs) in on-premises networks to support any combination of hybrid identity solutions. This is a great option if an organization has a variety of on-premises directories and databases to sync directly to Azure AD. MIM CALs are granted based on the allocation of an Azure AD Premium user license. For more information, see Deploy MIM 2010 R2.

Business scenarios and solutions

Some of the most common business scenarios that Azure AD enables are described in this section, including:

- Extend Office 365 to enable new solutions
- Enable mobile information workers to access applications
- Enable workers in many environments to access applications
- Enable partners and vendors to access applications
- Streamline mergers and acquisitions
- Support governance, risk management, and compliance

Extend Office 365 to enable new solutions

Many organizations moving to the cloud have made the decision to move to Office 365 for important workloads, having productively used Office applications over the course of many years. With Azure AD and simple configuration changes, these organizations can easily extend Office 365 services to enable new solutions, including single-sign-on (SSO) to existing on-premises applications and thousands of modern SaaS applications.

Multi-factor authentication and auditing have proved valuable when moving Office-related workloads to the cloud. Organizations can now significantly extend their security boundaries and identify and neutralize potentially fraudulent access attempts by integrating multi-factor authentication and using a variety of reports about access anomalies. IT departments in these organizations can now enable secure self-service password management for both cloud and on-premises users and easily, as well as delegate control for approving access to applications.

Enable mobile information workers to access applications

Many organizations now need to support access to organizational information, applications, and services on a large variety of devices and from almost any location. IT is being challenged to enable the modern workforce in a user-friendly way that is secure, compliant, and auditable. Microsoft enables IT departments to support mobility by providing on-premises and cloud capabilities that provide organizations with the ability to control the use of data, applications, and services by helping them ensure that only trustworthy people using trustworthy devices have access to resources.

Figure 1. Storyboard for enabling access for mobile information workers

In addition to multi-factor authentication, Azure AD supports conditional access controls. These controls allow an organization to implement access policies by evaluating user attributes and other factors, including the device in use and its level of trust, the network location of the device, the time of day, and what data or application the user is accessing.

User attributes include roles, group membership, and strength of authentication required. Devices are grouped into different levels of trust; for example, fully managed corporate devices, known and registered devices, and acceptable non-managed devices. Organizations can also classify the sensitivity of applications when building policies to control access.

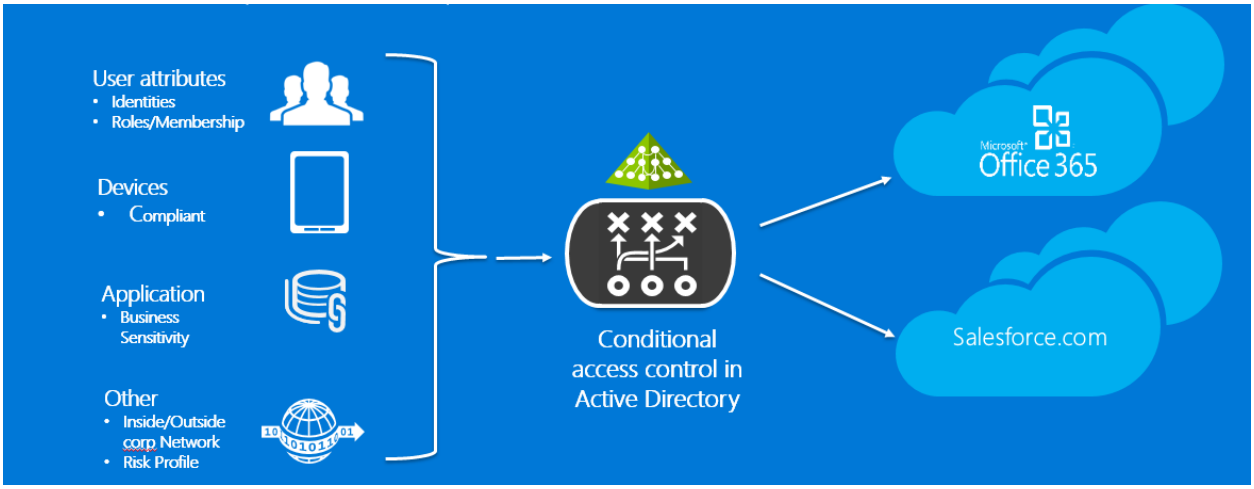

Figure 2. Conditional access control using Active Directory

There are many considerations for organizations interested in cloud-enabled mobility solutions. User profiles.

- Device choices
- Network requirements for data in transit
- Storage requirements for data used on devices
- Authentication and authorization policies
- Compliance
- Management of devices and infrastructure
- Deployment and provisioning
- Mobile user experience

Some of the questions organizations must answer, and some of the decisions they face when developing an infrastructure supporting mobility, are presented in Considerations for Mobility Solutions.

Enable workers in many environments to access applications

Organizations re-thinking how they deliver IT resources to their work force may have realized that the "one size fits all" model of the past is both cost prohibitive and many times doesn't serve the needs of their workers. Advances in the cloud and the availability of SaaS applications, are helping organizations to achieve the benefits of delivering tiers of service to meet workforce requirements, including delivering services to workers who traditionally did not have the means to access them.

Information workers are typically provided the most extensive set of IT resources, including messaging and collaboration tools, CRM/enterprise resource planning (ERP), and other LOB applications whether they are on-premises or cloud-based. Other workers may need to access fewer applications for various reasons, such as being contingent, seasonal, or highly mobile workers who do not work from dedicated offices. These workers can access applications from mobile locations or from shared kiosks or desktops. Azure AD enables organizations to meet the diverse requirements of such a workforce because it allows them to deliver IT resources quickly and cost effectively to many tiers of users.

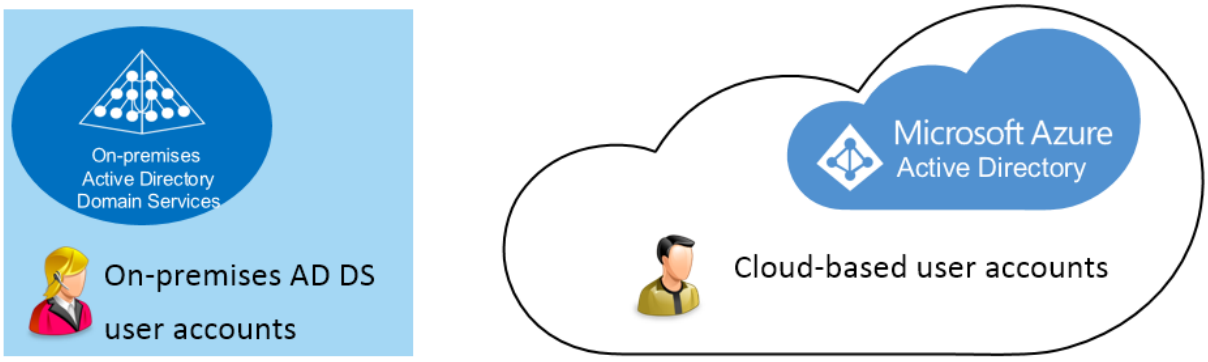

Figure 3. Supporting cloud-only and on-premises user accounts

With Azure AD, Office 365, and thousands of SaaS applications, organizations can develop a cost-effective IT strategy that meets the requirements of a workforce that consists of mobile, contingent, and seasonal workers. Workers who only need to access cloud applications and resources can be configured in Azure AD; they may not need to be configured in the on-premises Active Directory. For a workforce on the floor of a store, for example, an organization may choose to offer only Office 365 Exchange Online, Yammer for collaboration, and access to Workday for HR activities because these workers do not require any on-premises applications or resources; their identities are managed completely in the cloud and they benefit from single sign-on to Exchange Online for email, Yammer, and Workday.

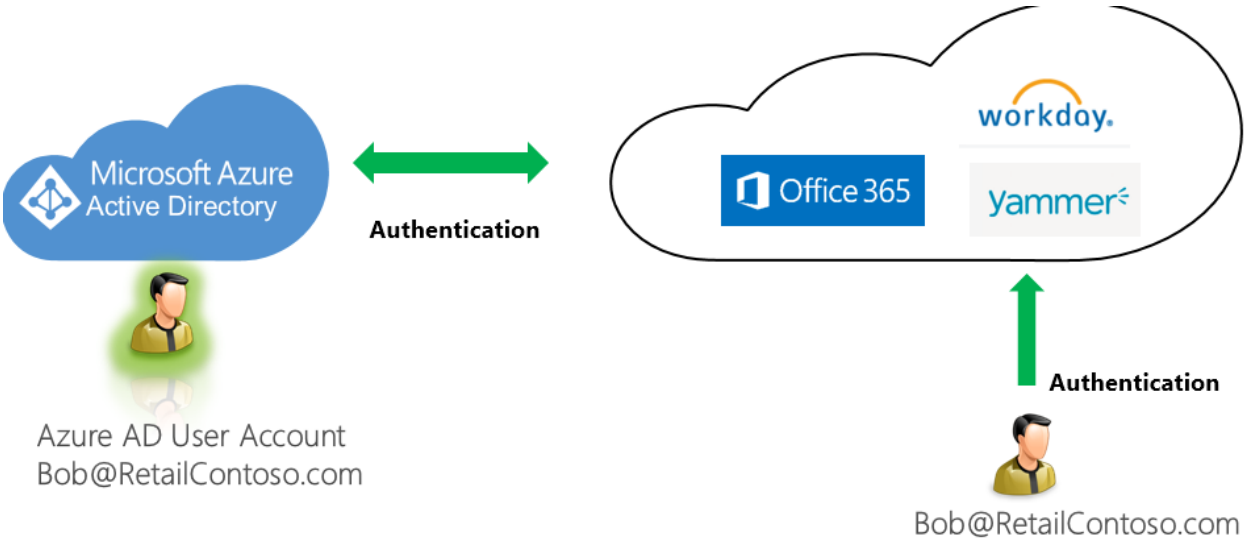

Figure 4. Accessing SaaS applications using Azure AD as the identity provider

The administrative and support costs for such workers are additionally reduced by using Azure AD features such as self-service password reset and streamlined user management using group licensing and application assignment. Administrators also have access to a rich set of reporting tools that allow them to identify anomalous sign-on activities and monitor usage of integrated SaaS applications to determine the most widely used applications.

Enable partners and vendors to access applications

Organizations often need to allow partners to access resources using the partners' own credentials. In the past this has meant establishing federation trust relationships using AD FS or, more commonly, creating external accounts for partner authentication. The cloud provides a simpler way to address business-to-business collaboration scenarios, such as:

- Sharing on-premises applications without complex configuration or proxy users
- Sharing data with external partners through SharePoint or encrypted email
- Sharing cloud applications using on-premises or cloud configurations
- Seamless onboarding of customers and partners using email-verified or social identities

In such scenarios that use the cloud without a federated relationship to provide profile data, trust is a two-way consideration. The owner of a resource trusts a partner to access the resource, and the partner trusts the resource owner to enumerate users and attributes covered by the trust.

By using a cloud-based solution instead of an on-premises one, an organization can realize many benefits of implementing business-to-business features. A cloud-based solution enables new scenarios and is easier to manage, because it enables an IT department to quickly establish access. Such a solution does not require federation configuration, is simpler and more transparent than federated trust relationships, and is simpler and more secure than creating shadow accounts.

Streamline mergers and acquisitions

When organizations evolve or change through mergers and acquisitions, the environment and requirements for IT infrastructure change. When two organizations merge, there are often multiple user directories with different trust centers. A user that logs in to the network of one organization is issued a login token that isn't trusted to access applications or services in the other organization, and vice versa.

One way to solve this problem for on-premises directories is to create trust bridges that allow login tokens from one organization to be understood and honored by the other. Solutions and architectures such as creating forest trusts, setting up federation, or even consolidating directories may solve on-premises needs, but most organizations now have to ensure that they can handle directory services in the cloud as well.

For hybrid enterprises with a variety of on-premises Active Directory forest structures and running multiple different Azure AD directory services, Microsoft and services partners provide support for a number of scenarios, including the following:

- Consolidating multiple different Active Directory forest and Azure AD tenant permutations
- Moving to and from Active Directory and Azure AD tenants, as well as between Azure AD tenants
- Providing access to users and administrators in one tenant to other tenants
- Providing access to applications and services across the cloud and different on-premises infrastructures

Support governance, risk management, and compliance

Organizations need to ensure appropriate controls are present to protect their sensitive business data, whether it is hosted on-premises or in the cloud. To ensure that data access is only provided to authorized individuals, there must be controls and visibility into how cloud providers host data.

If a department that is independent from IT oversight chooses to subscribe to SaaS applications or deploy cloud-hosted LOB applications, they could inadvertently expose their organization by inadvertently allowing access to more people than expected, including former as well as current employees.

By connecting such applications to Azure AD, the applications' access rights can be based on a centralized directory tenant whose contents are linked to a system of record authority. As employees join and leave the organization their accounts are automatically created and updated in Azure AD, which enables the organization to ensure only authorized current users have access to applications. In addition, with Azure AD administrators can delegate control for application access to business owners through groups, so that application owners across the organization can be individually responsible for ensuring appropriate access.

Azure AD also includes reports and alerts on logins and activity, which provide additional controls to enable analysis and early warning of potential problems in how users interact with directory services. In particular, Azure AD includes reports of anomalous logins, which use machine learning-based algorithms of user login behavior to identify outliers, such as users logging in from locations to which they do not normally travel, or could not have traveled to since an earlier login. Azure AD also includes reports of the updates that administrators make in the directory, to allow administrators to easily locate and review changes to users and other resources.

In addition, Azure AD includes usage rights for Microsoft Identity Manager (MIM) with the Microsoft BHOLD Suite. Microsoft Identity Manager provides additional governance control options and can be deployed on-premises, in private clouds, or as Azure-hosted cloud services. Governance control options include long-term policy, group, and permission change retention in the System Center data warehouse as well as analysis and attestation of access rights. Together, these capabilities augment Azure AD with increased visibility about the source of data, which can later be used for historical reporting or when collecting data for compliance.

Examples of organizations using Azure Active Directory

The following examples of organizations using Azure AD are drawn from Microsoft engagements and demonstrate how different enterprises use the features to meet their identity and access management requirements.

Improve management of SaaS applications

A professional services company with 4500 employees needed centralized management of employee access to SaaS applications. Employees needed to be able to use a variety of such applications, including Office 365, Workday, Salesforce, Yammer, and others.

The company took advantage of the hybrid features of Azure AD and now supports:

- Azure AD single sign-on (SSO) for SaaS applications

- Automated user provisioning and de-provisioning to SaaS applications
- Access Panel at myapps.microsoft.com
- Company-branded sign-in and user experience when accessing applications

Simplify user provisioning for users of SaaS applications
A large Fortune 500 company with more than 100,000 internationally distributed employees needed automated user provisioning and de-provisioning to SaaS applications, including ServiceNow, which also requires group objects.

Using Azure AD to support provisioning, the company enabled the following features:

- Synchronized data across on-premises sources and Azure AD
- User and group provisioning to Salesforce, ServiceNow and other SaaS applications

Enable integration of identity information using MIM Azure AD Connector
A company with multiple on-premises data sources needed to integrate sources and to provision users and groups to Azure AD for control of SaaS applications.

The Azure AD features that supported the company's requirements included:

- Synchronized data across on-premises sources and Azure AD
- Group-based application assignment in Azure AD
- Incorporating users from HR sources such as SAP, PeopleSoft, and Oracle

Support custom branding
A financial services firm with more than 200 offices wanted to improve ease of use during sign-on by providing a consistent look-and-feel across all on-premises and SaaS authentication experiences. The company was already using Office365 and Active Directory.

By integrating Azure AD, the company was able to create the following improvements to the sign-in experience:

- Sign-in page branded with company logo and illustration
- Customized help text on sign-in page
- Access Panel for end-users customized with company logo

Free up administrative resources through self-service password reset
A university with 20,000 students had a process for resetting passwords that was difficult to manage and was only available on-premises. In addition, alumni were unable to reset their passwords using the same process.

Azure AD Premium allowed the university to:

- Reset on-premises passwords from the cloud (writing passwords back to on-premises AD)
- Use phone and email verification methods
- Enable users to register their own contact information
- Customize the helpdesk URL and branding of the portal for resetting passwords, using the university's logo

Free up administrative resources through self-service group management
A large multi-national enterprise seeking a hybrid group management solution that supported self-service implemented the following features using Azure AD:

- Distributed group creation and management
- Delegated group management
- Ability for users to create groups and assign users to the groups
- Ability for group owners to delegate ownership
- Self-service group management
- Ability for users to search for groups and make requests to join
- Owner-approved and auto-approved requests

Improve security through security and usage reporting
A large multi-national enterprise found itself the frequent target of attempts to gain unauthorized access to employee accounts. The company used Azure AD to implement a range of security features, including machine learning that provides the ability to detect:

- Access anomalies
- Credential sharing
- Credential misuse/loss
- Brute force attacks
- Access from behind anonymizers

Administrators are notified when possible security issues are detected, and the company now has the ability to investigate sign-in activity and devices, and to download data as needed for offline analysis.

Improve security through Multi-Factor Authentication (MFA)
A local government agency needed to protect access to sensitive applications without locking out users while using different multi-factor authentication methods, such as a phone app SMS text to a mobile phone or alternate phone. The agency uses the following features of Azure AD:

- Targeted MFA for sensitive accounts
- Customization of MFA greetings, fraud alerts, and one-time bypass capabilities
- User self-service enrollment
- Audit reports for MFA activity
- Whitelisting IP addresses to bypass MFA from the corporate network
- "Remember this device" capability to require MFA only from untrusted devices

Evaluate application usage and access patterns
A large multi-national enterprise seeking to evaluate application usage and access patterns used the following reporting and informational features of Azure AD:

- Application dashboard
- Cross-company application usage
- Detailed usage for specific applications

Gain control of SaaS applications in use

Microsoft

A Fortune 500 company with more than 60,000 international employees had concerns about corporate data leakage, especially as departments adopted multiple subscriptions to SaaS applications without the involvement of IT. To begin gaining control and to enable single sign-on, the company needed an inventory of in-use cloud applications – previous attempts to capture SaaS application usage was very difficult. The company decided to use the Cloud App Discovery[2] feature, which enabled their IT department to easily gain visibility to their cloud SaaS app usage patterns:

- A summary view of total number of cloud applications in use and the number of users using cloud applications
- See the top cloud applications in use within the organization
- See top applications per category
- See usage graphs for applications that can be pivoted on users, requests or volume of data exchanged with the application
- Drill down into specific applications for targeted information
- Easily proceed to integrate an application with Azure Active Directory

Using Cloud App Discovery[2], the company's IT department are now enabled to make better, informed decisions on how to manage the SaaS applications that their employees are using.

Rapidly develop and deploy new enterprise capabilities

A large enterprise needed to develop applications that integrated well with Azure AD and took advantage of the Azure AD Application Proxy, Authentication, REST APIs, schema, and other details of development, including:

- Website applications, web APIs, and native client applications
- Users sign in to Active Directory-integrated applications with cloud identities; support for single sign-on with Office 365 and other services that use Azure AD
- Selectively publish internal web applications to the internet, allow web applications' http(s) endpoints to be securely available to mobile users.
- Active Directory-integrated applications can access Office 365 and other web APIs; developers can write powerful applications that access email, calendar, contacts, and files in Office 365 and other applications
- Applications can extend Azure AD schema, supporting read and write attributes which are useful to other applications in the organization
- Cross-platform support: Web applications and web APIs can run on Azure or other infrastructure; native client applications can run on iOS, Android, and Windows
- Open standards: SAML, OAuth 2.0, OpenID Connect, Odata 3.0

[2] At the time of writing this document, Cloud App Discovery is still in preview.

Architecture patterns for Azure AD identity solutions

A number of architecture patterns are used in the deployment of Azure AD, depending on the form of the organization and the core scenarios that will be supported. The patterns for Azure AD solution architecture described in this section address a large number of customer requirements.

Standard hybrid enterprise

Many organizations can use the standard enterprise deployment pattern with a single or multi-forest Active Directory Domain Services (AD DS) instantiation connected with Azure AD. In this pattern, Azure AD enables and controls all user access to business cloud applications such as Office 365, Microsoft Intune, Salesforce.com, and other company applications. This same pattern enables user access to existing applications on the corporate network. This hybrid access is enabled for mobile access from iOS, Android, and Windows devices.

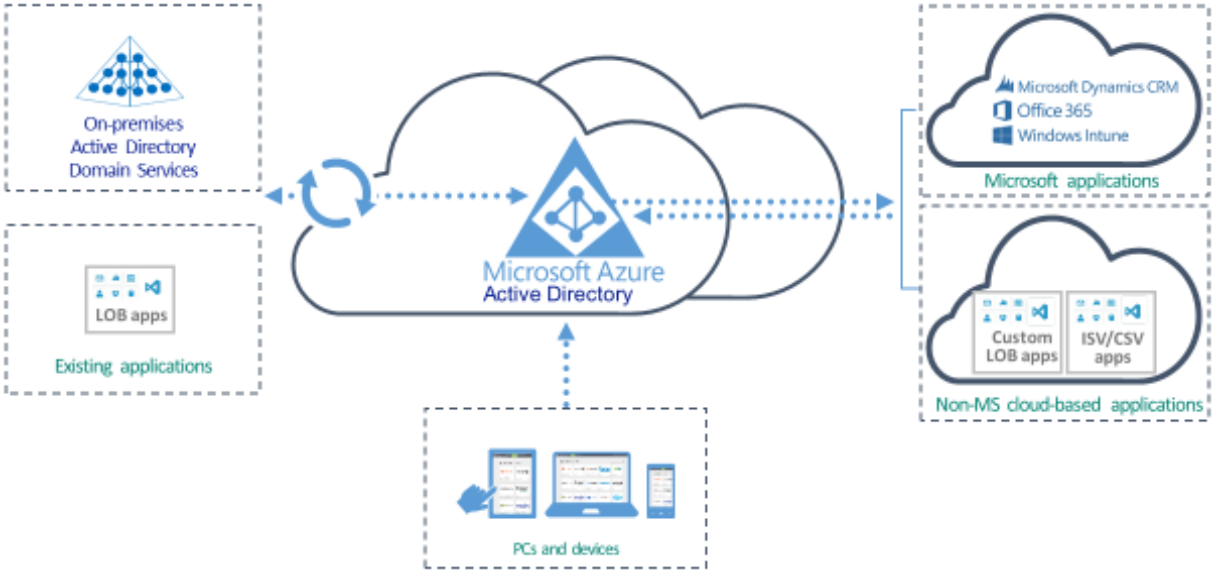

Figure 5. Standard hybrid enterprise

User provisioning for the standard hybrid enterprise

It is very simple to provision users and their attributes by connecting on-premises AD DS to Azure AD. Most enterprises can provision all users through a wizard that enables identity synchronization services, including a password hash. Authentication is completed against Azure AD.

Figure 6. Synchronization services with password hash sync

Other enterprises can gain additional advantages by provisioning users and their attributes using a wizard that enables federation as well as synchronization. Authentication is passed back through federation and is completed against AD DS.

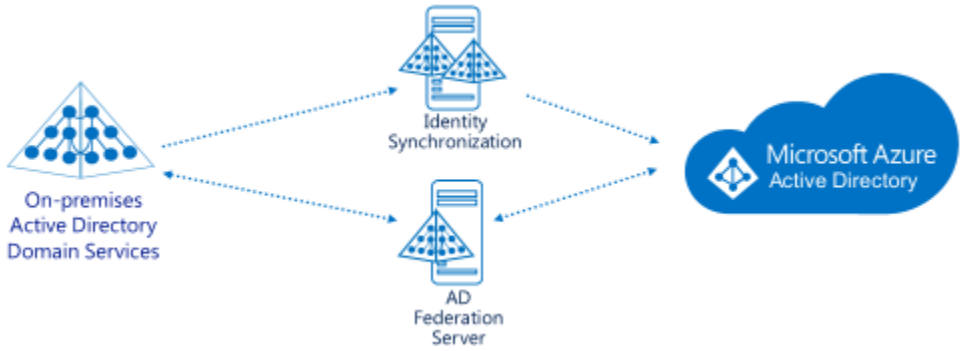

Figure 7. Enabling federation as well as synchronization

Using Azure AD as the enterprise directory

Organizations that have an extensive deployment of directory-enabled applications often have multiple directory services in place. This is especially common after mergers and acquisitions in which organizations choose to synchronize between disparate directories rather than converge to a single directory.

Multiple directory services may also be present when an organization has deployed an application that required a particular directory server technology or schema requirements.

In addition, an organization may have deployed multiple directories for different user populations, potentially using the same technology. For example, a directory of accounts for customers or trading partners may be kept distinct from a directory of accounts for employees because the applications that are connected to each directory are distinct, and the security requirements for these communities of users may be distinct.

Content from multiple directories can be brought into a single tenant directory in Azure AD, enabling cloud applications to have a unified view of users and groups.

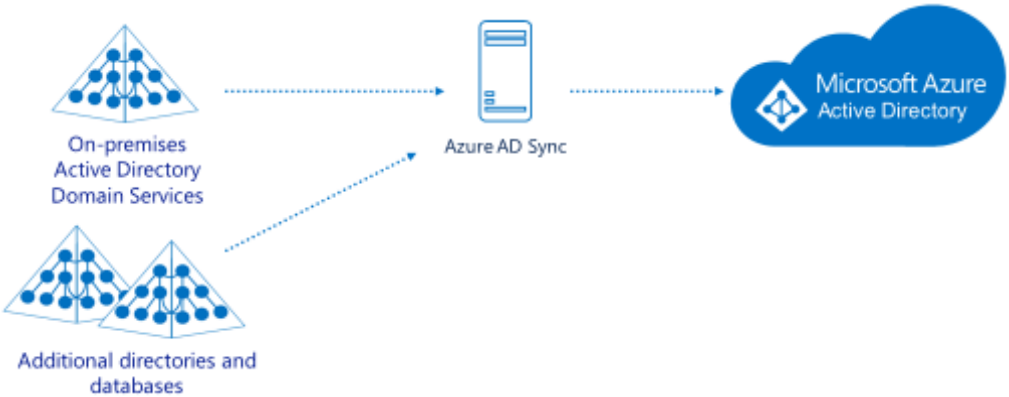

Figure 8. Consolidating content from multiple directories into a single tenant

Key considerations for deploying synchronization in these scenarios are:

- **Object and attribute selection and filtering**. In some cases, not all of the objects in the directories may be needed for cloud applications, or are subject to data protection requirements. Also, the on-premises directories may have attributes that are not necessary for cloud applications and require filtering to reduce exposure.
- **Join rules**. Objects in distinct on-premises directories may or may not represent the same user or group, depending on rules. If the objects are the same, rules must exist that identify the common attributes that indicate they represent the same object.
- **Attribute flow rules and precedence**. If multiple directories will be contributing changes for the same object's attribute, rules need to exist that indicate the authoritative source.
- **Reflecting on-premises attributes in the cloud**. Discuss with your service providers the ways in which to reflect necessary attributes from on-premises directories in the cloud.

Mostly cloud environment

Managing and provisioning users in the "mostly cloud" pattern has additional requirements beyond the standard enterprise patterns. Users who only access cloud resources need an Azure AD account, which will need to be provisioned. Smaller organizations may be able to manually manage the Azure AD accounts as users join and leave the organization – but as the user population grows, it becomes untenable to quickly keep up with the changes. And when users leave, most organizations will need to quickly revoke access.

Even when user accounts reside only in Azure AD, there is most likely another source of authority for the users' information, such as an HR or payroll database. If this source of authority resides on-premises and has an LDAP interface, the Azure AD sync tool can connect to it and be configured to provision and de-provision users.

For many organizations users will require access to both cloud and on-premises resources, which will require accounts in on-premises AD DS as well as in Azure AD. In such cases, user accounts from the on-premises directory and HR-based records can be synchronized to Azure AD using the Azure AD sync tool.

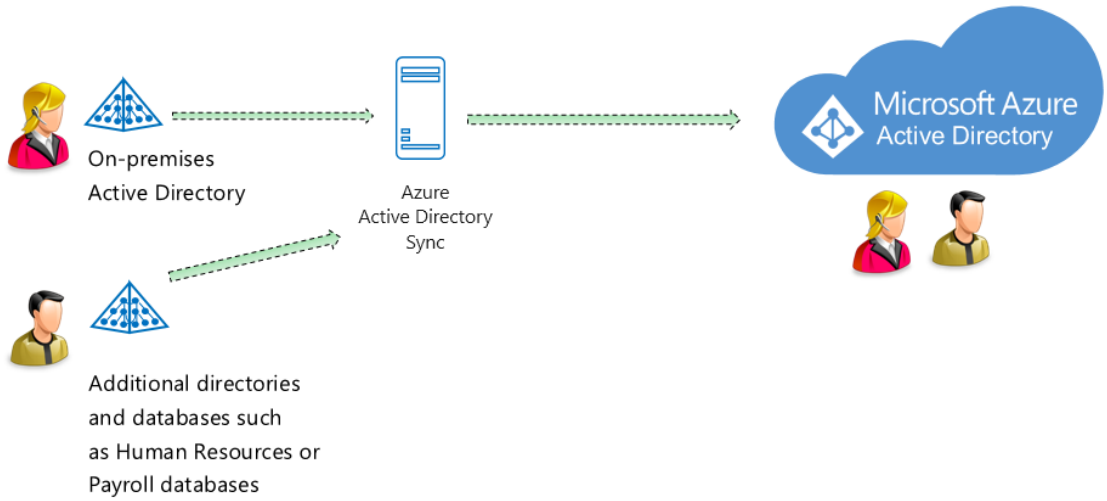

Figure 9. Active Directory and HR-based user accounts synchronized to Azure AD

In addition, Azure AD is integrated with a growing list of third-party SaaS applications, including Salesforce, Workday, ServiceNow, and many others. An organization can configure these third-party applications to support single sign-on using Azure AD as the identity provider. Information from multiple third-party applications can flow into Azure AD Sync. Azure AD can also directly connect to the programmatic interfaces of many SaaS providers, enabling Azure AD to provision and de-provision SaaS user accounts.

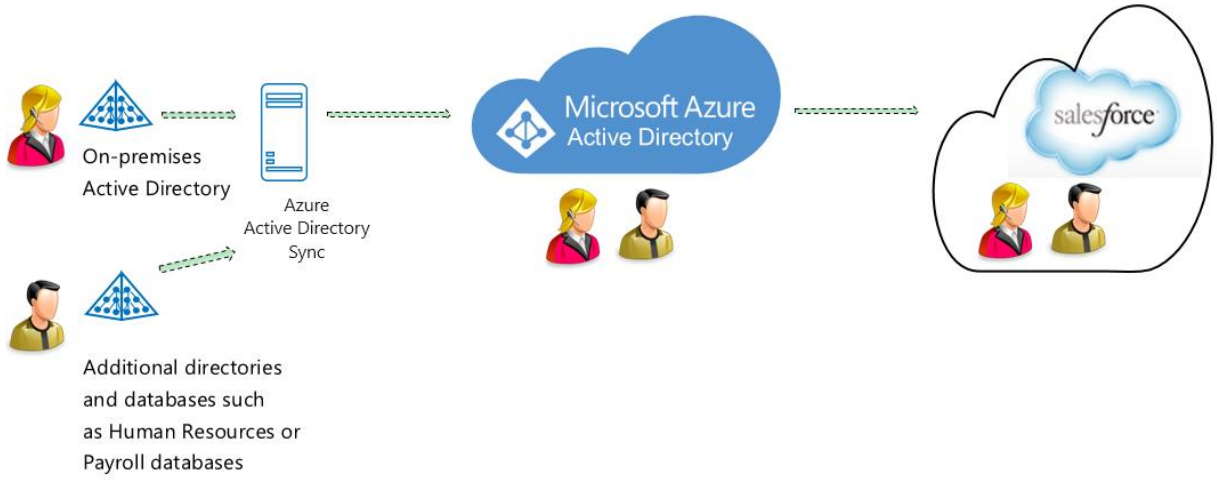

Figure 10. Azure AD accounts provisioned to Salesforce.com

As an organization moves toward using cloud services, it will find the need to have solid identity lifecycle management processes in place for updating the central directory.

The organization will also need to consider standardizing identity information in order to effectively use cloud-based identity features.

Business partner access

Azure AD enables business-to-business capabilities by using the external sharing of SharePoint Online and creating external accounts using the Azure AD portal:

- **SharePoint Online external sharing**. Allows SharePoint users to invite users with Microsoft accounts or external Azure AD accounts to access SharePoint site collections.
- **Azure Portal external accounts**. Allows Azure service administrators and co-administrators to add a Managed Service Account (MSA) user or an external account from a tenant they administer to another tenant they administer.

To enable partner and vendor access for scenarios in which the external sharing and external account creation do not support business requirements, an administrator can create new accounts in AD DS or Azure AD using one of the patterns that follows, based on the application type:

- **On-premises**. Create an account in on-premises AD DS so that the partner can authenticate against on-premises AD DS to access the application.
- **SaaS**. Create an account in Azure AD and use the Access Panel to assign the partner account to the application and be provisioned into the SaaS application.
- Using the **Graph API**, which allows applications to interact with data in Azure AD. There are two approaches:

    - **LOB**. Create a partner account in Azure AD so that the partner can authenticate against the tenant to access the LOB application.
    - **Multi-tenant**. Write the multi-tenant application to perform its own authorization checks, determining user rights from a consented tenant, to access the application.

A developer can currently use the Azure AD multi-tenant application programming model to write an application shared with partners. Azure AD will soon support creating directory constructs to make implementation (step 2 in the following process) a function of an administrator expressing policies, rather than a developer writing code.

1. Write a multi-tenant Azure AD application that accesses the resource to share.
2. Implement the AuthZ model in the application to restrict access to specific companies, groups, and users.
3. Have partners consent to the application, allowing them to use their credentials to access the application.

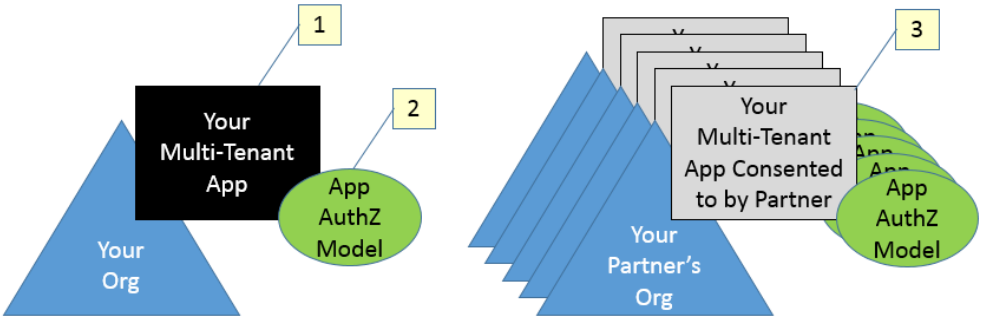

Figure 11. Steps for creating and sharing a multi-tenant application with partners

Mergers and acquisitions

Mergers and acquisitions require a variety of architectural solutions, depending on the organizations merging, the types of infrastructures currently deployed, and drivers for new capabilities. Possible scenarios include:

- An organization has multiple, non-trusted, forests on premises, and users need access to resources across the forests.
- Over the last few years, an organization has implemented multiple Azure AD's and now wants to consolidate them into one.
- An organization needs to be able to rapidly scale resources and capacity on-the-go.

For your scenarios, please consult with your Microsoft account team or partner.

Standardized identities

When moving to the cloud, an organization may need to standardize the identities in use among multiple directory services. Characteristics of a standardized identity include the following:

- Each identity is unique to an individual or is owned/assigned to a specific individual.
- The identity object contains necessary attributes about the individual to (1) know who they are and (2) to make access related decisions.
- Identity objects that are used for services, applications, or other resource specific needs must also contain information about the owner for tracking and ownership purposes.
- The identity object is managed using structured processes or tools that follow business rules.
- Data contained within the identity object must be subject to business rules and guidelines, as the identity object may be identifiable to applications outside traditional network boundaries.
- The identity object, a logical concept, is manifested differently in various systems: as a database record, object, or an account object.

As these principles are taken into consideration, the following steps should be used as a guide to define the standardized identity for an environment:

- Identify the minimum attributes required to create a new object in each destination system (such as a user, group, role, and so on).

- Go through all the identity requirements, use cases, and processes within the environment and document the attributes required to meet those needs. This list will serve as a basis for the standardized identity.
- Ensure there are standards in place for the syntax of each attribute, as well as defining what comprises uniqueness and where uniqueness is necessary.
- If necessary, determine the process that will be used to apply these standards within the central authentication and authorization repository. Plan for the impact of any changes that the new standards introduce.

User principal name (UPN) patterns

Azure AD includes authentication services for Office 365, Microsoft Intune, Dynamics CRM, and other cloud applications. Users who access cloud applications will authenticate to Azure AD, or in cases in which the user accounts have been configured for federation, users will be redirected to on-premises federation services such as Active Directory Federation Services for authentication.

Users of Office 365 and other cloud services typically authenticate using a user principal name (UPN). Most organizations standardize their UPN pattern, using the user's primary (SMTP) email address, or follow patterns such as FirstName.LastName@domainName.com, or other variations including abbreviated names or other user properties, such as partial employee IDs. Many organizations have also used non-routable domains in the UPNs for on-premises logons, for example Bob@contoso.local may work perfectly fine for on-premises' infrastructures.

It is important for an organization to consider what pattern will be adopted because users will be entering it every day for authentication.

Considerations for mobility solutions

Organizations pursuing cloud-enabled mobility solutions must consider many aspects of establishing, operating, using, and managing the solution. These considerations include:

User profiles. An organization needs to understand the users' needs and requirements for remotely performing their jobs. Not all users will have the same requirements; some users will always access data on-premises; other workers will be accessing company data from a variety of locations and circumstances. There may be different policies applied based on user profiles.

Devices. Will employees, partners, vendors, and customers be able to use any devices they want to perform their jobs, or components of their jobs? What device capabilities are necessary to support security policies? Does IT require knowledge of devices in use, or need to use only managed devices. For example, will an employee only be able to check a schedule or submit a timesheet when using a managed device?

Network. How will users access company data while using their own devices, not only remotely but on-premises? What regulatory issues apply to an organization's geopolitical alignment? For example, how can users that are physically located in a different country have personalized network access?

Storage: How will data be stored in users' devices? Data encryption must be considered, as well as scenarios in which IT must control data encryption, and for which types of data. Companies must review their policies and regulations to understand which types of data are allowed to leave on-premises or cloud storage and be at rest in remote devices' storage.

Authentication: Companies should review their current authentication and authorization policies. What are the authentication requirements for users to be able to remotely access company apps from their devices? Is the current platform able to enforce authorization per user and per app without having to rewrite the apps? Is it possible to enforce Multi-Factor Authentication according to a user's location?

Policy and compliance: Some companies might have hard requirements that will not fit into a mobility model because of business regulations. A company that is moving to a people-centric strategy must understand current policies and how these policies will be affected by enabling mobility.

Management: How will administrators monitor devices to meet compliance requirements and prevent data leakage? How will an IT department learn about the iOS versions devices are running, which corporate apps are installed on devices, and if devices are jail-broken? How will an IT department conduct application deployment and provisioning to devices?

Deployment and provisioning: How will users access apps from their own devices? How will IT provision these apps to users in a friendly and effective manner? Users should be able to securely access a centralized location from their devices and install the applications that they are authorized to use to perform their work.

Experience: Is the company willing to develop apps that will provide the same experience regardless of the platform? Will the company provide training to users to use apps on different platforms not having the same experience?

Conclusion

When an organization moves to the cloud, new scenarios are enabled and new solutions become available to solve the organization's problems. Identity and access management is one of the biggest concerns when integrating on-premises and cloud-based resources. Digital identities are at the core of all IT-related services because they control how people, devices, applications, and services access a variety of resources within and outside of the organization.

Azure AD enables workers and partners in many environments to access applications. It also provides tools to organizations for realizing maximum value from Office 365, supports compliance, and addresses many other scenarios that are now commonly required in modern enterprises. Azure AD features that support these scenarios include:

- Enterprise SLA of 99.9%
- Advanced security reports and alerts
- Company branding
- Group-based licensing and application access
- Self-service password reset and group management
- Multi-Factor authentication
- Application proxy

- Microsoft Identity Manager (MIM) for hybrid solutions

Cloud-based identity and access management solutions are especially valuable to hybrid organizations using IT architectures that combine on-premises and cloud-based resources. The many benefits that organizations realize when using Azure AD as part of their identity infrastructure enable them to:

- Simplify access and control of SaaS applications
- Reduce IT burden with self-service identity and access management
- Improve security posture with cloud services
- Easily meet reporting requirements
- Rapidly develop and deploy new enterprise capabilities

Establishing an overall identity strategy involves far more than just provisioning objects and adding or removing access. Consideration must be given to standardizing identities, establishing access policies, defining appropriate roles, specifying the identity lifecycle, and classifying security requirements for applications, data, and services. Microsoft can help plan for moving to the cloud, enable new scenarios based on cloud-based identity providers, and guide organizations in implementing a secure identity infrastructure.