Microsoft

Azure Active Directory Hybrid Identity Design Considerations Guide

Published October, 2015

Version 1.0

Consumer-based devices are proliferating the corporate world, and cloud-based software-as-a-service (SaaS) applications are easy to adopt. As a result, maintaining control of users' application access across internal datacenters and cloud platforms is challenging. Microsoft's identity solutions span on-premises and cloud-based capabilities, creating a single user identity for authentication and authorization to all resources, regardless of location. We call this *hybrid identity*. There are different design and configuration options for hybrid identity using Microsoft solutions, and in some case it might be difficult to determine which combination will best meet the needs of your organization. This Hybrid Identity Design Considerations Guide will help you to understand how to design a hybrid identity solution that best fits the business and technology needs for your organization. This guide will detail a series of steps and tasks that you can follow to help you design a hybrid identity solution that meets your organization's unique requirements. Throughout the steps and tasks, the guide will present the relevant technologies and feature options available to organizations to meet functional and service quality (such as availability, scalability, performance, manageability, and security) level requirements.

Specifically, the hybrid identity design considerations guide goals are to answer the following questions:

- What questions do I need to ask and answer, to drive a hybrid identity-specific design for a technology or problem domain that best meets my requirements?
- What sequence of activities should I complete to design a hybrid identity solution for the technology or problem domain?
- What hybrid identity technology and configuration options are available to help me meet my requirements? What are the trade-offs between those options so that I can select the best option for my business?

Copyright

This document is provided "as-is". Information and views expressed in this document, including URL and other Internet Web site references, may change without notice.

Some examples depicted herein are provided for illustration only and are fictitious. No real association or connection is intended or should be inferred.

Contents

Who is this guide intended for? CIO, CITO, Chief Identity Architects, Enterprise Architects and IT Architects responsible for designing a hybrid identity solution for medium or large organizations.

How can this guide help you? You can use this guide to understand how to design a hybrid identity solution that is able to integrate a cloud based identity management system with your current on-premises identity solution. The following graphic shows an example a hybrid identity solution that enables IT Admins to manage to integrate their current Windows Server Active Directory solution located on-premises with Microsoft Azure Active Directory to enable users to use Single Sign-On (SSO) across applications located in the cloud and on-premises.

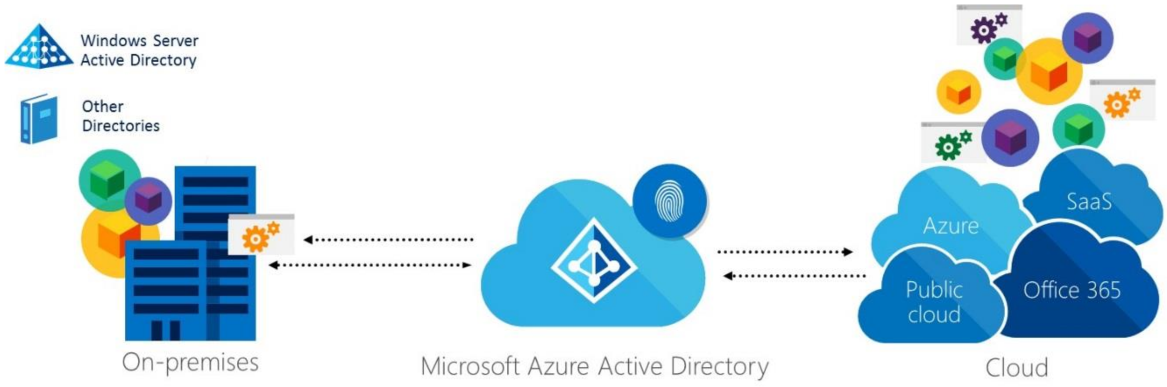


Figure 1 - Example of a hybrid identity solution using Microsoft Azure AD

Figure 1 is an example of a hybrid identity solution that is leveraging cloud services to integrate with on-premises capabilities in order to provide a single experience to the end user authentication process and to facilitate IT managing those resources. Although this can be a very common scenario, every organization's hybrid identity design is likely to be different than the example illustrated in Figure 1 due to different requirements.

This guide provides a series of steps and tasks that you can follow to design a hybrid identity solution that meets *your* organization's unique requirements. Throughout the following steps and tasks, the guide presents the relevant technologies and feature options available to you to meet functional and service quality level requirements for your organization.

Assumptions: You have some experience with Windows Server, Active Directory Domain Services and Azure Active Directory. In this document, we assume you are looking for how these solutions can meet your business needs on their own or in an integrated solution.

Design Considerations Overview

This document provides a set of steps and tasks that you can follow to design a hybrid identity solution that best meets your requirements. The steps are presented in an ordered sequence. Design considerations you learn in later steps may require you to change decisions you made in earlier steps, however, due to conflicting design choices. Every attempt is made to alert you to potential design conflicts throughout the document.

You will arrive at the design that best meets your requirements only after iterating through the steps as many times as necessary to incorporate all of the considerations within the document.

Step 1 - Determine identity requirements

Step 2 - Plan for enhancing data security through strong identity solution

Step 3 - Plan for hybrid identity lifecycle

Step 1 - Determine identity requirements

The first step in designing a hybrid identity solution is to determine the requirements for the business organization that will be leveraging this solution. Hybrid identity starts as a supporting role (it supports all other cloud solutions by providing authentication) and goes on to provide new and interesting capabilities that unlock new workloads for users. These workloads or services that you wish to adopt for your users will dictate the requirements for the hybrid identity design. These services and workloads need to leverage hybrid identity both on-premises and in the cloud.

You need to go over these key aspects of the business to understand what is a requirement now and what the company plans for the future. If you don't have the visibility of the long term strategy for hybrid identity design, chances are that your solution will not be scalable as the business needs grow and change. The diagram below shows an example of a hybrid identity architecture and the workloads that are being unlocked for users. This is just an example of all the new possibilities that can be unlocked and delivered with a solid hybrid identity strategy.

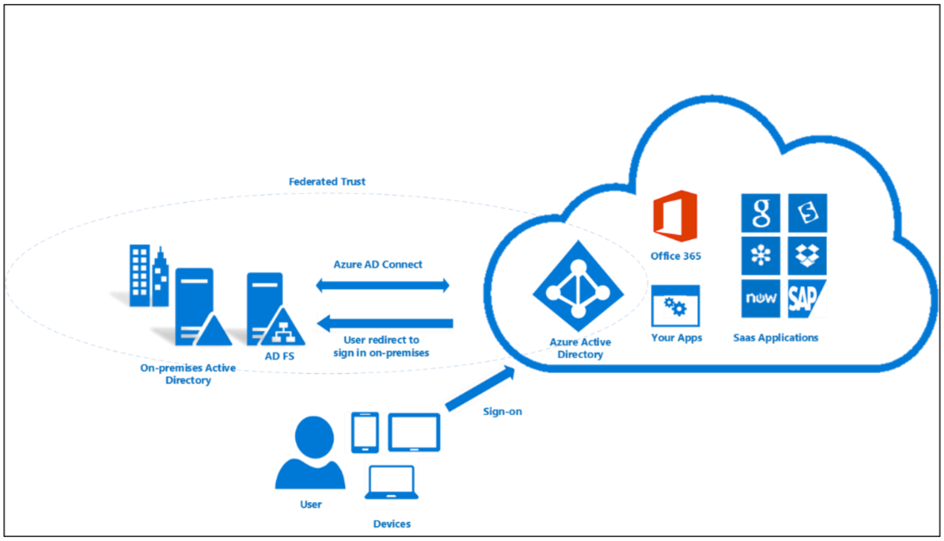


Figure 2 – Some components that are part of the hybrid identity architecture

Task 1: Determine business needs

Each company will have different requirements, even if these companies are part of the same industry, the real business requirements might vary. You can still leverage best practices from the industry, but ultimately it is the company's business needs that will lead you to define the requirements for the hybrid identity design. Make sure to answer the following questions to identity your business needs:

- Is your company looking to cut IT operational cost?
- Is your company looking to secure cloud assets (SaaS Apps, infrastructure)?
- Is your company looking to modernize your IT?
    - Are your users more mobile and demanding IT to create exceptions into your DMZ to allow different type of traffic to access different resources?
    - Does your company have legacy apps that needed to be published to these modern users but are not easy to rewrite?
    - Does your company need to accomplish all these tasks and be efficient at the same tme?
- Is your company looking to secure users' identities and reduce risk by bringing new tools that leverage the expertise of Microsoft's Azure security expertise on-premises?
- Is your company trying to get rid of the dreaded "external" accounts on premises and move them to the cloud where they are no longer a dormant threat inside your on-premises environment?

Now that you have an idea regarding your company business requirements, you need to evaluate your on-premises identity infrastructure. This evaluation is important for defining the technical requirements to integrate your current identity solution to the cloud identity management system. Make sure to answer the following questions:

- What authentication and authorization solution does your company use on-premises?
- Does your company currently have any on-premises synchronization services?
- Does your company use any third-party Identity Provider (IdP)?

You also need to be aware of the cloud services that your company might have. Performing an assessment to understand the current integration with SaaS, IaaS or PaaS models in your environment is very important. Make sure to answer the following questions during this assessment:

- Does your company have any integration with a cloud service provider?
    - If yes, which services are being used?
    - Is this integration currently in production or is it a pilot?

📝 **Note**

> If you don't have an accurate mapping of all your apps and cloud services, you can use the Cloud App Discovery tool. This tool can provide your IT department with visibility into all your organization's business and consumer cloud apps. That makes it easier than ever to discover shadow IT in your organization, including details on usage patterns and any users accessing your cloud applications. To access this tool go to https://appdiscovery.azure.com/

Next, you need to evaluate the identity integration requirements. This evaluation is important to define the technical requirements for how users will authenticate, how the organization's presence will look in the cloud, how the organization will allow authorization and what the user experience is going to be. Make sure to answer the following questions:

- Will your organization be using federation, standard authentication or both?
- Is federation a requirement because of the following:
  - Kerberos-based Single sign-on (SSO)
  - Your company has an on-premises applications (either built in-house or third-party) that uses SAML or similar federation capabilities.
  - MFA via Smart Cards. RSA SecurID, etc.
  - Client access rules that address the questions below:
    - Can I block all external access to Office 365 based on the IP address of the client?
    - Can I block all external access to Office 365, except Exchange ActiveSync?
    - Can I block all external access to Office 365, except for browser-based apps (OWA, SPO)
    - Can I block all external access to Office 365 for members of designated AD groups
  - Security/auditing concerns
  - Already existing investment in federated authentication
  - What name will our organization use for our domain in the cloud?
  - Does the organization have a custom domain?
    - Is that domain public and easily verifiable via DNS?
    - If it is not, then do you have a public domain that can be used to register an alternate UPN in AD?
  - Are the user identifiers consistent for cloud representation?
  - Does the organization have apps that require integration with cloud services?
  - Does the organization have multiple domains and will they all use standard or federated authentication?

Now that you have an idea regarding your on-premises and cloud infrastructure, you need to evaluate the applications that run in these environments. This evaluation is important to define the technical requirements to integrate these applications to the cloud identity management system. Make sure to answer the following questions:

- Where will our applications live?
- Will users be accessing on-premises applications? In the cloud? Or both?
- Are there plans to take the existing application workloads and move them to the cloud?
- Are there plans to develop new applications that will reside either on-premises or in the cloud that will use cloud authentication?

You also have to evaluate the user requirements. This evaluation is important to define the steps that will be needed for on-boarding and assisting users as they transition to the cloud. Make sure to answer the following questions:

- Will users be accessing applications on-premises?
- Will users be accessing applications in the cloud?
- How do users typically login to their on-premises environment?
- How will users sign-in to the cloud?

Note

Make sure to take notes of each answer and understand the rationale behind the answer. Task 4 will go over the options available and pros/cons of each option. By having answered those questions you will select which option best suits your business needs.

Task 2: Determine directory synchronization requirements

Synchronization is all about providing users an identity in the cloud based on their on-premises identity. Whether or not they will use synchronized account for authentication or federated authentication, the users will still need to have an identity in the cloud. This identity will need to be maintained and updated periodically. The updates can take many forms, from title changes to password changes.

Start by evaluating the organizations on-premises identity solution and user requirements. This evaluation is important to define the technical requirements for how user identities will be created and maintained in the cloud. For a majority of organizations, Active Directory is on-premises and will be the on-premises directory that users will by synchronized from, however in some cases this will not be the case. Make sure to answer the following questions:

- Do you have one AD forest, multiple, or none?
  - How many Azure AD directories will you be synchronizing to?
    - Are you using filtering?
    - Do you have multiple Azure AD Connect servers planned?
- Do you currently have a synchronization tool on-premises?
  - If yes, does your users have a virtual directory/integration of identities?

- Do you have any other directory on-premises that you want to synchronize (e.g. LDAP Directory, HR database, etc)?
- Are you going to be doing any GALSync?
- What is the current state of UPNs in your organization?
- Do you have a different directory that users authenticate against?
- Does your company use Microsoft Exchange?
    - Do they plan of having a hybrid exchange deployment?

Now that you have an idea about synchronization requirements for your company, you need to evaluate the applications that use these directory services. This evaluation is important to define the technical requirements to integrate these applications to the cloud. Make sure to answer the following questions:

- Will these applications be moved to the cloud and use the directory?
- Are there special attributes that need to be synchronized to the cloud so these applications can use them successfully?
- Will these applications need to be re-written to take advantage of cloud authentication?
- Will these applications continue to live on-premises while users access them using the cloud identity?

You also need to determine the security requirements and constraints of directory synchronization. This evaluation is important to get a list of the requirements that will be needed in order to create and maintain user's identities in the cloud. Make sure to answer the following questions:

- Where will the synchronization server be located?
- Will it be domain joined?
- Will the server be located on a restricted network behind a firewall, such as a DMZ?
    - Will you be able to open the required firewall ports to support synchronization?
- Do you have a disaster recovery plan for the synchronization server?
- Do you have an account with the correct permissions for all forests you want to synch with?
    - If your company doesn't know the answer for this question, review the section "Permissions for password synchronization" in the article Install the Azure Active Directory Sync Service and determine if you already have an account with these permissions or if you need to create one.
- If you have mutli-forest sync is the sync server able to get to each forest?

Note

Make sure to take notes of each answer and understand the rationale behind the answer. Task 4 will go over the options available. By having answered those questions you will select which option best suits your business needs.

Task 3: Determine multi-factor authentication requirement

In this world of mobility, with users accessing data and applications in the cloud and from any device, securing this information has become paramount. Every day there is a new headline about a security breach. Although, there is no guarantee against such breaches, multi-factor authentication, provides an additional layer of security to help prevent these breaches.

Start by evaluating the organizations requirements for multi-factor authentication. That is, what is the organization trying to secure. This evaluation is important to define the technical requirements for setting up and enabling the organizations users for multi-factor authentication.

Note

If you are not familiar with MFA and what it does, it is strongly recommended that you read the article What is Azure Multi-Factor Authentication? prior to continue reading this section.

Make sure to answer the following:

- Is your company trying to secure Microsoft apps?
- How these apps are published?
- Does your company provide remote access to allow employees to access on-premises apps?

If yes, what type of remote access? You also need to evaluate where the users who are accessing these applications will be located. This evaluation is another important step to define the proper multi-factor authentication strategy. Make sure to answer the following questions:

- Where are the users going to be located?
- Can they be located anywhere?
- Does your company want to establish restrictions according to the user’s location?

Once you understand these requirements, it is important to also evaluate the user’s requirements for multi-factor authentication. This evaluation is important because it will define the requirements for rolling out multi-factor authentication. Make sure to answer the following questions:

- Are the users familiar with multi-factor authentication?
- Will some uses be required to provide additional authentication?

    - If yes, all the time, when coming from external networks, or accessing specific applications, or under other conditions?
- Will the users require training on how to setup and implement multi-factor authentication?
- What are the key scenarios that your company wants to enable multi-factor authentication for their users?

After answering the previous questions, you will be able to understand if there are multi-factor authentication already implemented on-premises. This evaluation is important to define the technical requirements for setting up and enabling the organizations users for multi-factor authentication. Make sure to answer the following questions:

- Does your company need to protect privileged accounts with MFA?
- Does your company need to enable MFA for certain application for compliance reasons?
- Does your company need to enable MFA for all eligible users of these application or only administrators?
- Do you need have MFA always enabled or only when the users are logged outside of your corporate network?

Task 4: Define a hybrid identity adoption strategy

In this task, you'll define the hybrid identity adoption strategy for your hybrid identity solution to meet the business requirements that were defined in the first 3 tasks.

Task 4a: Define business needs strategy

The first task addresses determining the organizations business needs. This can be very broad and scope creep can occur if you are not careful. In the beginning keep it simple but always remember to plan for a design that will accommodate and facilitate change in the future. Regardless of whether it is a simple design or an extremely complex one, Azure Active Directory is the Microsoft Identity platform that supports Office 365, Microsoft Online Services and cloud aware applications.

Define an integration strategy

Microsoft has three main integration scenarios which are cloud identities, synchronized identities, and federated identities. You should plan on adopting one of these integration strategies. The strategy you choose can vary and the decisions in choosing one may include, what type of user experience you want to provide, do you have some of the existing infrastructure already in-place, and what is the most cost effective.

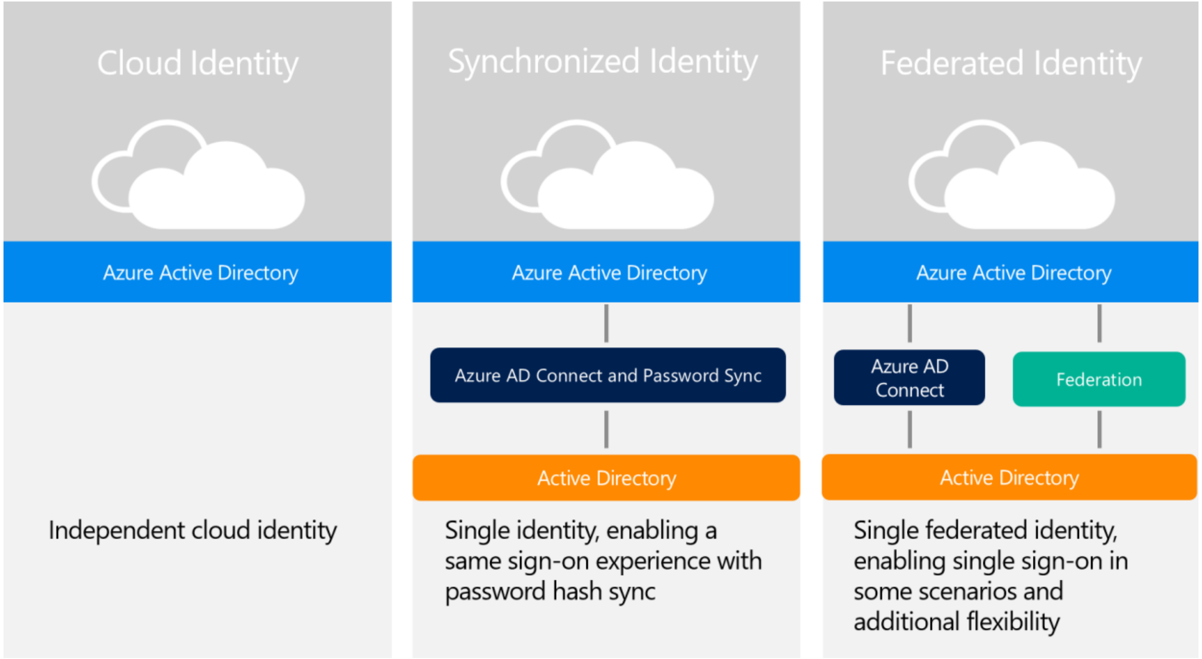

Cloud Identity
Azure Active Directory
Independent cloud identity
Synchronized Identity
Azure Active Directory
Azure AD Connect and Password Sync
Active Directory
Single identity, enabling a same sign-on experience with password hash sync
Federated Identity
Azure Active Directory
Azure AD Connect
Federation
Active Directory
Single federated identity, enabling single sign-on in some scenarios and additional flexibility

Figure 3 – Integration scenarios

The scenarios defined in Figure 3 are:

- **Cloud identities**: these are identities that exist solely in the cloud. In the case of Azure AD, they would reside specifically in your Azure AD directory.

- **Synchronized**: these are identities that exist on-premises and in the cloud. Using Azure AD Connect, these users are either created or joined with existing Azure AD accounts. The user's password hash is synchronized from the on-premises environment to the cloud in what is called a password hash. When using synchronized the one caveat is that if a user is disabled in the on-premises environment, it can take up to 3 hours for that account status to show up in Azure AD. This is due to the synchronization time interval.

- **Federated**: these identities exist both on-premises and in the cloud. Using Azure AD Connect, these users are either created or joined with existing Azure AD accounts.

Note

For more information about the Synchronization options read Integrating your on-premises identities with Azure Active Directory

Table 1 will help in determining the advantages and disadvantages of each of the following strategies:

Table 1

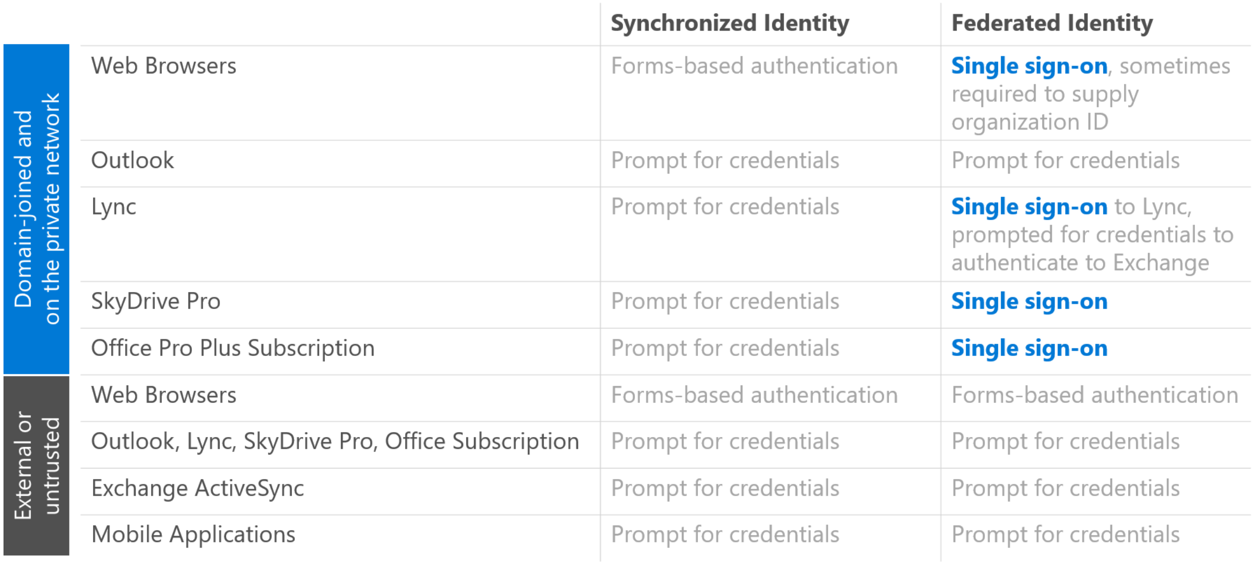
Strategy	Advantages	Disadvantages

Cloud identities	• Easier to manage for small organization. • Nothing to install on-premises • No additional hardware needed • Easily disabled if the user leaves the company	• Users will need to sign-in when accessing workloads in the cloud • Passwords may or may not be the same for cloud and on-premises identities
Synchronized	• On-premises password will authenticate both on-premises and cloud directories. • Easier to manage for small, medium or large organizations • Users can have single sign-on (SSO) for some resources • Microsoft preferred method for synchronization • Easier to manage	• Some customers may be reluctant to synchronize their directories with the cloud due specific company's police
Federated	• Users can have single sign-on (SSO) • If a user is terminated or leaves, the account can be immediately disabled and access revoked • Supports advanced scenarios that cannot be accomplished with synchronized	• More steps to setup and configure • Higher maintenance • May require additional hardware for the STS infrastructure • May require additional hardware to install the federation server. • Additional software is required if AD FS is used • Require extensive setup for SSO • Critical point of failure, if the federation server is down, users won't be able to authenticate

Client Experience

The strategy that you use will dictate the user sign-in experience. The following table will provide you with information on what the users should expect their sign-in experience to be. Please note that not all federated identity providers support SSO in all scenarios.

Table 2



		Synchronized Identity	Federated Identity
Domain-joined and on the private network	Web Browsers	Forms-based authentication	**Single sign-on**, sometimes required to supply organization ID
	Outlook	Prompt for credentials	Prompt for credentials
	Lync	Prompt for credentials	**Single sign-on** to Lync, prompted for credentials to authenticate to Exchange
	SkyDrive Pro	Prompt for credentials	**Single sign-on**
	Office Pro Plus Subscription	Prompt for credentials	**Single sign-on**
External or untrusted	Web Browsers	Forms-based authentication	Forms-based authentication
	Outlook, Lync, SkyDrive Pro, Office Subscription	Prompt for credentials	Prompt for credentials
	Exchange ActiveSync	Prompt for credentials	Prompt for credentials
	Mobile Applications	Prompt for credentials	Prompt for credentials

If you have determined from task 1 that you have a third- party IdP or are going to use one to provide federation with Azure AD, you need to be aware of the following supported capabilities:

- Any SAML 2.0 provider which is compliant for the SP-Lite profile can support authentication to Azure AD and associated applications
- Supports passive authentication, which facilitates auth to OWA, SPO, etc.
- Exchange Online clients can be supported via the SAML 2.0 Enhanced Client Profile (ECP)

You must also be aware of what capabilities will not be available:

- Without WS-Trust/Federation support, all other active clients will break
  - That means no Lync client, OneDrive client, Office Subscription, Office Mobile prior to Office 2016
- Transition of Office to passive authentication will allow them to support pure SAML 2.0 IdPs, but support will still be on a client-by-client basis

Note

For the most updated list read the article http://aka.ms/ssoproviders.

Task 4b: Define synchronization strategy

In this task you will define the tools that will be used to synchronize the organization's on-premises data to the cloud and what topology you should use. Because, most organizations use Active Directory, information on using Azure AD Connect to address the questions above is provided in some detail. For environments that do not have Active Directory, there is information about using FIM 2010 R2 or MIM 2016 to help plan this strategy. However, future releases of Azure AD Connect will support LDAP directories, so depending on your timeline, this information may be able to assist.

Synchronization Tools

Over the years, several synchronization tools have existed and used for various scenarios. Currently Azure AD Connect is the go to tool of choice for all supported scenarios. AAD Sync and DirSync are also still around and may even be present in your environment now.

> **Note**
>
> For the latest information regarding the supported capabilities of each tool, read [Directory integration tools comparison]() article.

Supported Topologies

When defining a synchronization strategy, the topology that is used must be determined. Depending on the information that was determined in step 2 you can determine which topology is the proper one to use.

The single forest, single Azure AD topology is the most common and consists of a single Active Directory forest and a single instance of Azure AD. This is going to be used in a majority of the scenarios and is the expected topology when using Azure AD Connect Express installation as shown in Figure 4.

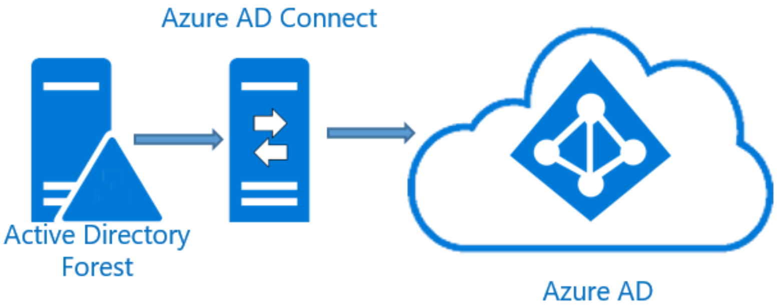


Figure 4 – Single Forest Scenario

It is very common for large and even small organizations to have multiple forests, as shown in Figure 5.

> **Note**
>
> For more information about the different on-premises and Azure AD topologies with Azure AD Connect sync read the article [Topologies for Azure AD Connect]().

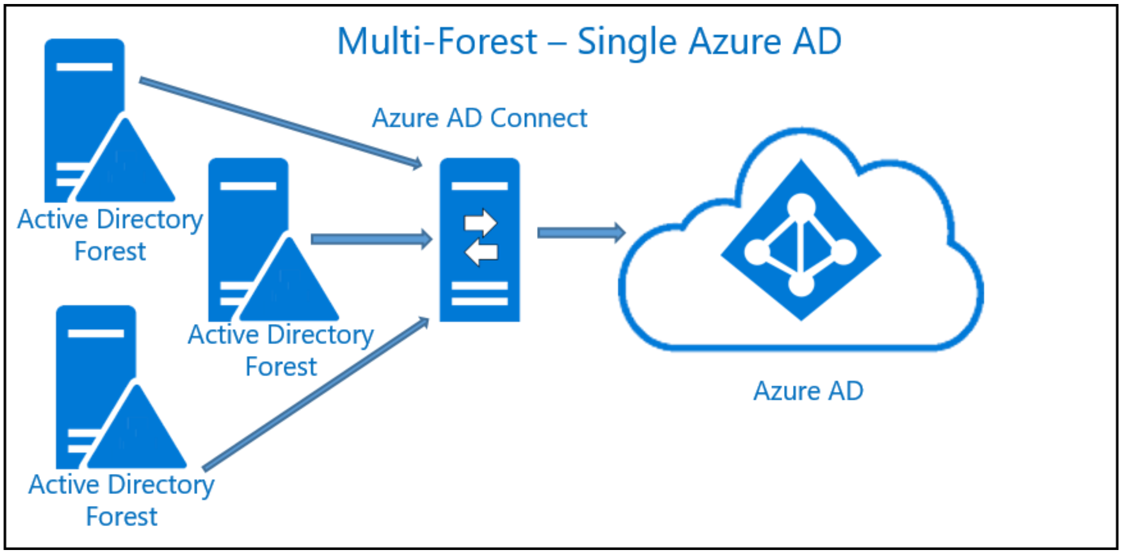


Figure 5 – Multi-Forest Scenario

If this is the case, then the multi-forest-single Azure AD topology should be considered if the following items are true:

- Users have only 1 identity across all forests – the uniquely identifying users section below describes this in more detail.
- The user authenticates to the forest in which their identity is located
- UPN and Source Anchor (immutable id) will come from this forest
- All forests are accessible by Azure AD Connect – this means it does not need to be domain joined and can be placed in a DMZ if this facilitates this.
- Users have only one mailbox
- The forest that hosts a user's mailbox has the best data quality for attributes visible in the Exchange Global Address List (GAL)
- If there is no mailbox on the user, then any forest may be used to contribute these values
- If you have a linked mailbox, then there is also another account in a different forest used to sign in.

Note

Objects that exist in both on-premises and in the cloud are "connected" via a unique identifier. In the context of Directory Synchronization, this unique identifier is referred to as the SourceAnchor. In the context of Single Sign-On, this is referred to as the ImmutableId. Design concepts for Azure AD Connect for more considerations reading the use of SourceAnchor.

If the above are not true and you have more than one active account or more than one mailbox, Azure AD Connect will pick one and ignore the other. If you have linked mailboxes but no other account, these accounts will not be exported to Azure AD and that user will not be a member of any groups. This is different from how it was in the past with DirSync and is intentional to better support these multi-forest scenarios. A multi-forest scenario is shown in Figure 6.

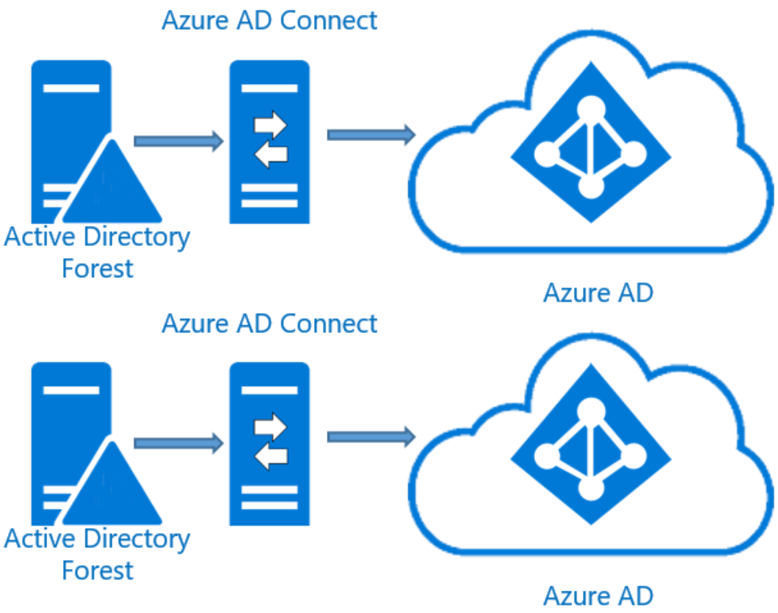


Figure 6 – Muti-forest multiple AAD scenario

It is recommended to have just a single directory in Azure AD for an organization but it is supported it a 1:1 relationship is kept between an Azure AD Connect sync server and an Azure AD directory. For each instance of Azure AD, you will need an installation of Azure AD Connect. Also, Azure AD, by design is isolated and users in one instance of Azure AD will not be able to see users in another instance.

It is possible and supported to connect one on-premises instance of Active Directory to multiple Azure AD directories as shown in Figure 7.

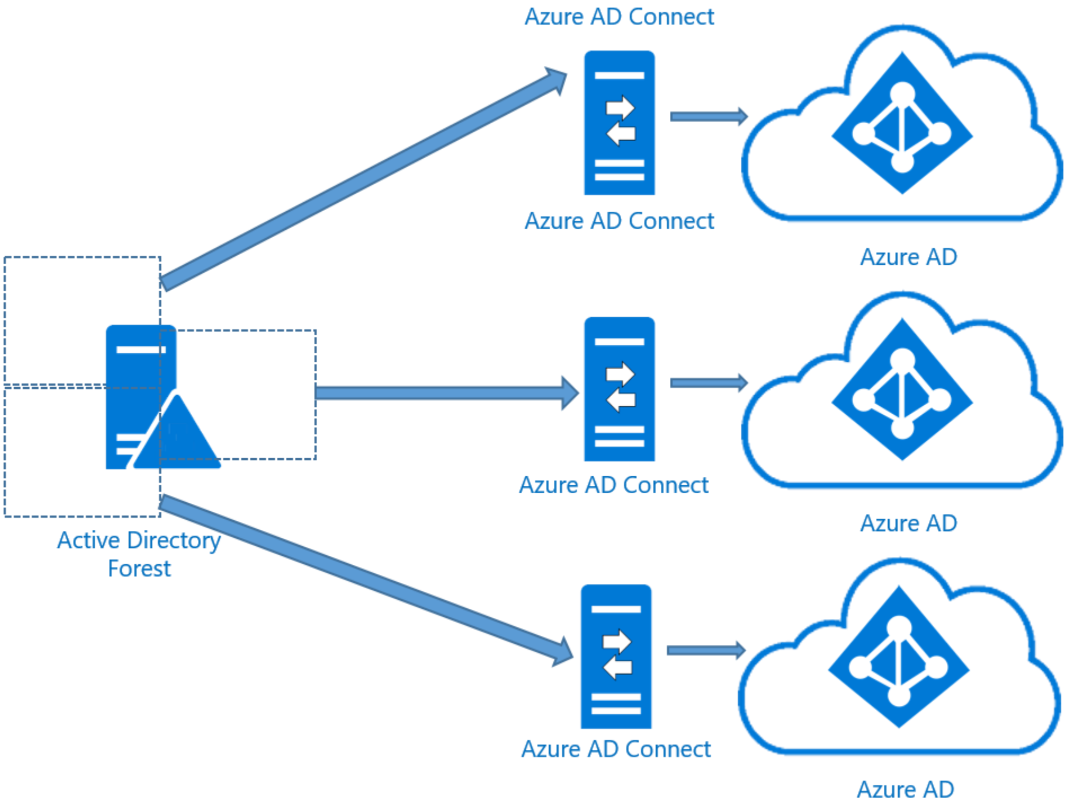


Figure 7 – Single-Forest Filtering Scenario

In order to do this the following must be true:

- Azure AD Connect sync servers must be configured for filtering so they each have a mutually exclusive set of objects. This done, for example, by scoping each server to a particular domain or OU.
- A DNS domain can only be registered in a single Azure AD directory so the UPNs of the users in the on-premises AD must use separate namespaces
- Users in one instance of Azure AD will only be able to see users from their instance. They will not be able to see users in the other instances
- Only one of the Azure AD directories can enable Exchange hybrid with the on-premises AD
- Mutual exclusivity also applies to write-back. This makes some write-back features not supported with this topology since these assume a single on-premises configuration. This includes:
    - Group write-back with default configuration
    - Device write-back

Be aware that the following is not supported and should not be chosen as an implementation:

- It is not supported to have multiple Azure AD Connect sync servers connecting to the same Azure AD directory even if they are configured to synchronize mutually exclusive set of object
- It is unsupported to sync the same user to multiple Azure AD directories.
- It is also unsupported to make a configuration change to make users in one Azure AD to appear as contacts in another Azure AD directory.
- It is also unsupported to modify Azure AD Connect sync to connect to multiple Azure AD directories.
- Azure AD directories are by design isolated. It is unsupported to change the configuration of Azure AD Connect sync to read data from another Azure AD directory in an attempt to build a common and unified GAL between the directories. It is also unsupported to export users as contacts to another on-premises AD using Azure AD Connect sync.

Note

If your organization restricts computers on your network from connecting to the Internet, this article lists the endpoints (FQDNs, IPv4, and IPv6 address ranges) that you should include in your outbound allow lists and Internet Explorer Trusted Sites Zone of client computers to ensure your computers can successfully use Office 365. For more information read Office 365 URLs and IP address ranges.

Task 4c: Define multi-factor authentication strategy

In this task you will define the multi-factor authentication strategy to use. Azure Multi-Factor Authentication comes in two different versions. One is a cloud-based and the other is on-premises based using the Azure MFA Server. Based on the evaluation you did above you can determine which solution is the correct one for your strategy. Use the table below to determine which design option best fulfill your company's security requirement:

Table 3

Asset to Secure	Design Option	
	Multi-Factor Authentication in the cloud	Multi-Factor Authentication on-premises
Microsoft apps	Yes	Yes
SaaS apps in the app gallery	Yes	Yes
IIS applications published through Azure AD App Proxy	Yes	Yes
IIS applications not published through	No	Yes

the Azure AD App Proxy		
Remote access as VPN, RDG	No	Yes

Even though you may have settled on a solution for your strategy, you still need to use the evaluation from above on where your users are located. This may cause the solution to change. Use the table 4 to assist you determining this:

Table 4

User Location	Preferred Design Option
Azure Active Directory	Multi-Factor Authentication in the cloud
Azure AD and on-premises AD using federation with AD FS	Both
Azure AD and on-premises AD using Azure AD Connect no password sync	Both
Azure AD and on-premises using Azure AD Connect with password sync	Both
On-premises AD	Multi-Factor Authentication Server

Note

You should also ensure that the multi-factor authentication design option that you selected supports the features that are required for your design. For more information read Choose the multi-factor security solution for you

Multi-Factor Auth Provider

Multi-factor authentication is available by default for global administrators who have a Azure Active Directory tenant. However, if you wish to extend multi-factor authentication to all of your users and/or want to your global administrators to be able to take advantage features such as the management portal, custom greetings, and reports, then you must purchase and configure Multi-Factor Authentication Provider.

Note

You should also ensure that the multi-factor authentication design option that you selected supports the features that are required for your design.

Step 2 - Plan for enhancing data security through strong identity solution

The first step to protect the data is identify who can access that data and as part of this process you need to have an identity solution that can integrates with your system to provide authentication and authorization capabilities. Authentication and authorization are often confused with each other and their roles misunderstood. In reality they are quite different, as shown in the figure 8.

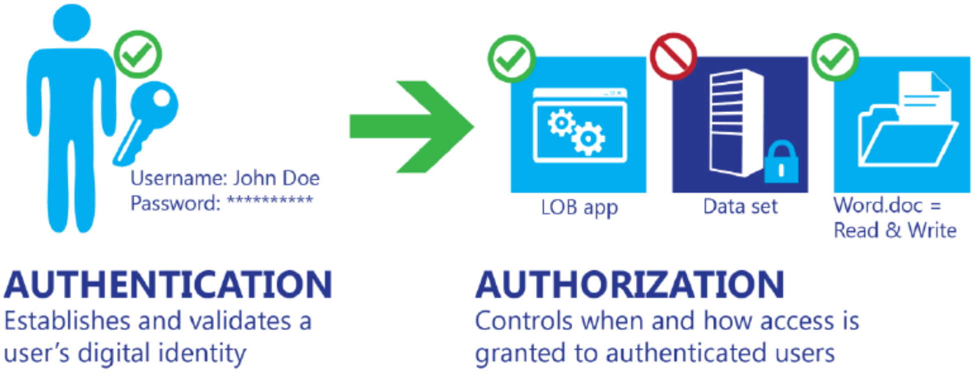

Username: John Doe
Password: **********
LOB app
Data set
Word.doc =
Read & Write
AUTHENTICATION
Establishes and validates a user's digital identity
AUTHORIZATION
Controls when and how access is granted to authenticated users

Figure 8 – Mobile device management lifecycle stages

When planning your hybrid identity solution you must understand the data protection requirements for your business and which options are available to best fulfil these requirements.

> **Note**
>
> Once you finish Step 2, review Step 1, task 3 to ensure that your selections regarding multi-factor authentication requirements were not affected by the decisions you made in this section.

Task 1: Determine data protection requirements

In the age of mobility, most companies have a common goal: *enable their users to be productive on their mobile devices while on-premises or remotely from anywhere in order to increase productivity*. While this could be a common goal, companies that have such requirement will also be concern regarding the amount of threats that must be mitigated in order to keep company's data secure and maintain user's privacy. Each company might have different requirements in this regard; different compliance rules that will vary according to which industry the company is acting will lead to different design decisions. However, there are some security aspects that should be explored and validated, regardless of the industry, which are showed in Figure 9:

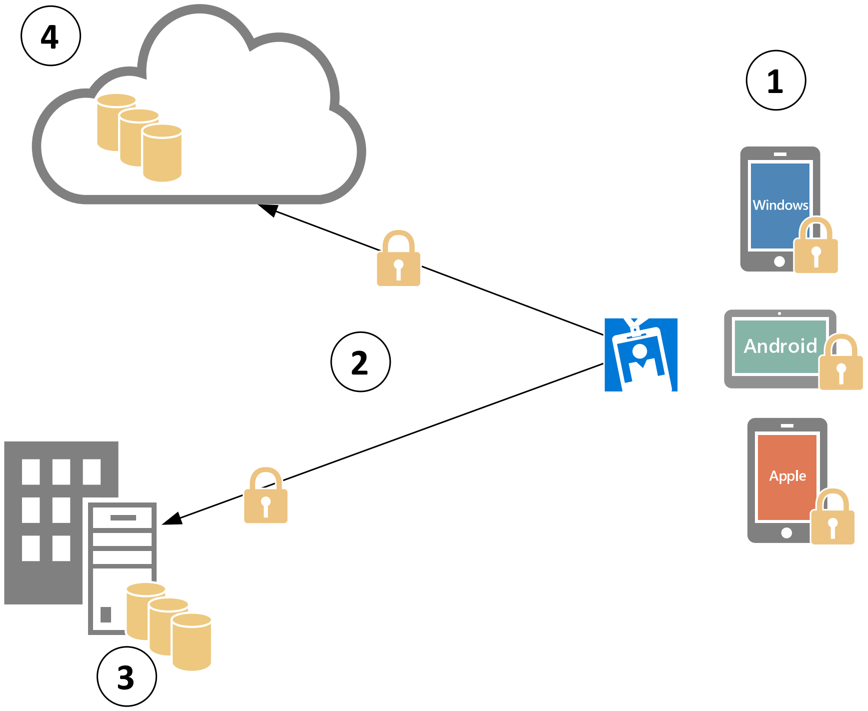


Figure 9 – Data protection paths

In the diagram showed in Figure X, the identity component will be the first one to be verified before data is accessed. However, this data can be in different states during the time it was accessed. Each number on this diagram represents a path in which data can be located at some point in time. These numbers are explained below:

1. Data protection at the device level.

2. Data protection while in transit.

3. Data protection while at rest on-premises.

4. Data protection while at rest in the cloud.

Although the technical controls that will enable IT to protect the data itself on each one of those phases are not directly offered by the hybrid identity solution, it is necessary that the hybrid identity solution is capable of leveraging both on-premises and cloud identity management resources to identify the user before grant access to the data. When planning your hybrid identity solution ensure that the following questions are answered according to your organization's requirements:

Data protection at rest: regardless of where the data is at rest (device, cloud or on-premises), it is important to perform an assessment to understand the organization needs in this regard. For this area, ensure that the following questions are asked:

- Does your company need to protect data at rest?
    - If yes, is the hybrid identity solution able to integrate with your current on-premises infrastructure?
    - If yes, is the hybrid identity solution able to integrate with your workloads located in the cloud?
- Is the cloud identity management able to protect the user's credentials and other data stored in the cloud?

Data protection in transit: data in transit between the device and the datacenter or between the device and the cloud must be protected. However, being in-transit does not necessarily mean a communications process with a component outside of your cloud service; it moves internally, also, such as between two virtual networks. For this area, ensure that the following questions are asked:

- Does your company need to protect data in transit?
    - If yes, is the hybrid identity solution able to integrate with secure controls such as SSL/TLS?
- Does the cloud identity management keep the traffic to and within the directory store (within and between datacenters) signed?

Compliance: regulations, laws and regulatory compliance requirements will vary according to the industry that your company belongs. Companies in high regulated industries must address identity-management concerns related to compliance issues. Regulations such as Sarbanes-Oxley (SOX), the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA) and the Payment Card Industry Data Security Standard (PCI DSS) are very strict regarding identity and access. The hybrid identity solution that your company will adopt must have the core capabilities that will fulfill the requirements of one or more of these regulations. For this area, ensure that the following questions are asked:

- Is the hybrid identity solution compliant with the regulatory requirements for your business?
- Does the hybrid identity solution has built in capabilities that will enable your company to be compliant regulatory requirements?

Note

Make sure to take notes of each answer and understand the rationale behind the answer. Task 5 will go over the options available and advantages/disadvantages of each option. By having answered those questions you will select which option best suits your business needs.

Task 2: Determine content management requirements

Understanding the content management requirements for your business may direct affect your decision on which hybrid identity solution to use. With the proliferation of multiple devices and the capability of users to bring their own devices ([BYOD](#)), the company must protect its own data but it also must keep user's privacy intact. Usually when a user has his own device he might have also multiple credentials that will be alternating according to the application that he uses. It is important to differentiate what content was created using *personal credentials* versus the ones created using *corporate credentials*. Your identity solution should be able to interact with cloud services to provide a seamless experience to the end user while ensure his privacy and increase the protection against data leakage. Your identity solution will be leverage by different technical controls in order to provide content management as shown in Figure 10:

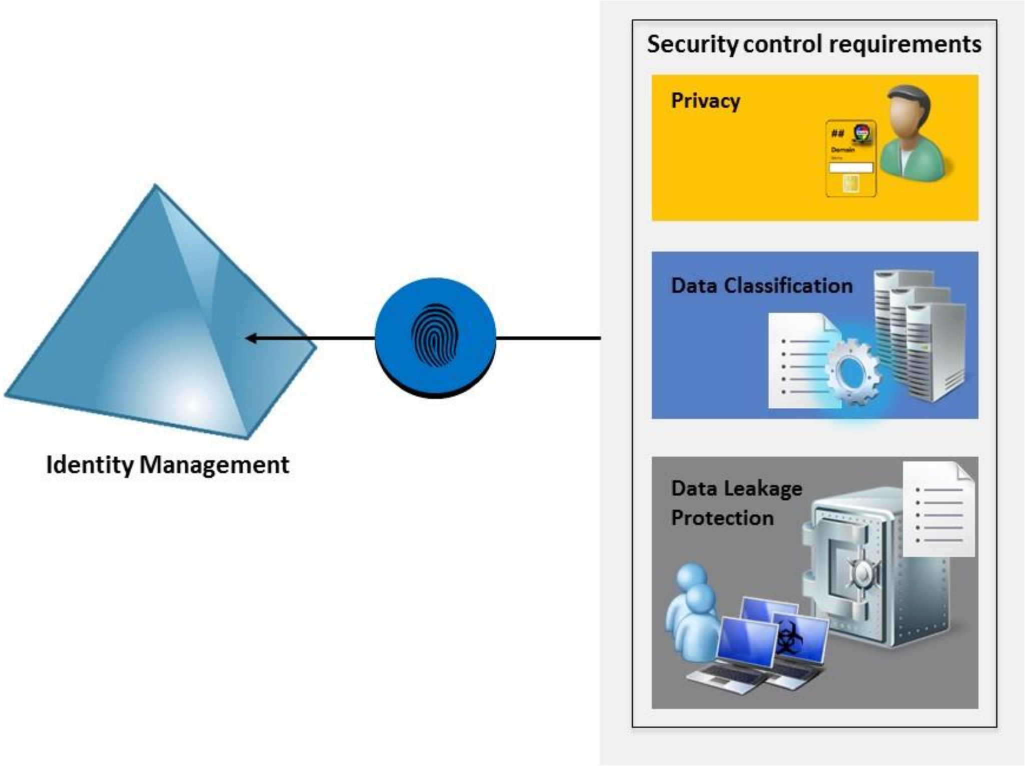


Figure 10 – Security controls that will be leveraging your identity management system

In general, content management requirements will leverage your identity management system in the following areas:

- **Privacy**: identifying the user that owns a resource and applying the appropriate controls to maintain integrity.
- **Data Classification**: identify the user or group and level of access to an object according to its classification.
- **Data Leakage Protection:** security controls responsible for protecting data to avoid leakage will need to interact with the identity system to validate the user's identity. This is also important for auditing trail purpose.

Note

Read data classification for cloud readiness for more information about best practices and guidelines for data classification.

When planning your hybrid identity solution ensure that the following questions are answered according to your organization's requirements:

- Does your company have security controls in place to enforce data privacy?
  - If yes, will those security controls be able to integrate with the hybrid identity solution that you are going to adopt?
- Does your company use data classification?
  - If yes, is the current solution able to integrate with the hybrid identity solution that you are going to adopt?
- Does your company currently have any solution for data leakage?
  - If yes, is the current solution able to integrate with the hybrid identity solution that you are going to adopt?
- Does your company need to audit access to resources?
  - If yes, what type of resources?
  - If yes, what level of information is necessary?
  - If yes, where the audit log must reside? On-premises or in the cloud?
- Does your company need to encrypt any emails that contain sensitive data (SSNs, Credit card numbers, etc)?
- Does your company need to encrypt all documents/contents shared with external business partners?
- Does your company need to enforce corporate policies on certain kinds of emails (do no reply all, do not forward)?

Note

Make sure to take notes of each answer and understand the rationale behind the answer. Task 5 will go over the options available and advantages/disadvantages of each option. By having answered those questions you will select which option best suits your business needs.

Task 3: Determine access control requirements

When an organization is designing their hybrid identity solution they can also use this opportunity to review access requirements for the resources that they are planning to make it available for users. The data access cross all four pillars of identity, which are:

- Administration
- Authentication
- Authorization
- Auditing

The sections that follows will cover authentication and authorization in more details, administration and auditing are part of the hybrid identity lifecycle. Read Step 3, task 1 for more information about these capabilities.

Note

Read The Four Pillars of Identity - Identity Management in the Age of Hybrid IT for more information about each one of those pillars.

Authentication and authorization

There are different scenarios for authentication and authorization, these scenarios will have specific requirements that must be fulfilled by the hybrid identity solution that the company is going to adopt. Scenarios involving *Business to Business* (B2B) communication can add an extra challenge for IT Admins since they will need to ensure that the authentication and authorization method used by the organization can communicate with their business partners. During the designing process for authentication and authorization requirements, ensure that the following questions are answered:

- Will your organization authenticate and authorize only users located at their identity management system?
- Is there any plans for B2B scenarios?
    - If yes, do you already know which protocols (SAML, OAuth, Kerberos, Tokens or Certificates) will be used to connect both business?
    - Does the hybrid identity solution that you are going to adopt support those protocols?

Another important point to consider is where the authentication repository that will be used by users and partners will be located and the administrative model to be used. Consider the following two core options:

- **Centralized:** in this model the user's credentials, policies and administration can be centralized on-premises or in the cloud.
- **Hybrid:** in this model the user's credentials, policies and administration will be centralized on-premises and a replicated in the cloud.

Which model will your organization adopts will vary according to their business requirements, you want to answer the following questions to identify where the identity management system will reside and the administrative mode to use:

- Does your organization currently have an identity management on-premises?
    - If yes, do they plan to keep it?
        - Is there any regulation or compliance requirements that your organization must follow that dictates where the identity management system should reside?
- Does your organization use Single Sign-On for apps located on-premises or in the cloud?
    - If yes, does the adoption of a hybrid identity model will affect this process?

Access Control

While authentication and authorization are core elements to enable access to corporate data through user's validation, it is also important to control the level of access that these users will have and the level of access administrators will have over the resources that they are managing. Your hybrid identity solution must be able to provide granular access to resources, delegation and role base access control. Ensure that the following question are answered regarding access control:

- Does your company will have more than one user with elevated privilege to manage your identity system?
  - If yes, does each user need the same access level?
- Does your company need to delegate access to users to manage specific resources?
  - If yes, how frequently this happens?
- Does your company need to integrate access control capabilities between on-premises and cloud resources?
- Does your company need to limit access to resources according to some conditions?
- Does your company have any application that needs custom control access to some resources?
  - If yes, where are those apps located (on-premises or in the cloud)?
  - If yes, where are those target resources located (on-premises or in the cloud)?

Note

Make sure to take notes of each answer and understand the rationale behind the answer. Task 5 will go over the options available and advantages/disadvantages of each option. By having answered those questions you will select which option best suits your business needs.

Task 4: Determine Incident Response Requirements

Large or medium organizations most likely will have a security incident response in place to help IT take actions accordingly to the level of incident. The identity management system is an important component in the incident response process because it can be used to help identifying who performed a specific action against the target. The hybrid identity solution must be able to provide monitoring and reporting capabilities that can be leverage by IT to take actions to identify and mitigate a potential threat. In a typical incident response plan you will have the following phases as part of the plan:

1. Initial assessment.
2. Incident communication.
3. Damage control and risk reduction.
4. Identification of what it was compromise and severity.
5. Evidence preservation.
6. Notification to appropriate parties.
7. System recovery.
8. Documentation.
9. Damage and cost assessment.

10. Process and plan revision.

During phase four it will be necessary to identify the systems that have been compromised, files that have been accessed and determine the sensitivity of those files. Your hybrid identity system should be able to fulfill these requirements to assist you identifying the user that made those changes.

Monitoring and reporting

Many times the identity system can also help in phase one, mainly if the system has built in auditing and reporting capabilities. During the initial assessment, IT Admin must be able to identify a suspicious activity, or the system should be able to trigger it automatically based on a pre-configured task. Many activities could indicate a possible attack, however in other cases, a badly configured system might lead to a number of false positives in an intrusion detection system.

The identity management system should assist IT admins to identify and report those suspicious activities. Usually these technical requirements can be fulfilled by monitoring all systems and having a reporting capability that can highlight potential threats. Use the questions below to help you design your hybrid identity solution while taking into consideration incident response requirements:

- Does your company have a security incident response in place?
    - If yes, does the current identity management system is used as part of the process?
- Does your company need to identify suspicious login attempts from users across different devices?
- Does your company need to detect potential compromised user's credentials?
- Does your company need to audit user's access and action?
- Does your company need to know when a user reset his password?

Policy enforcement

During phase 3 (Damage control and risk reduction) it is important to quickly reduce the actual and potential effects of an attack. That action that you will take at this point can make the difference between a minor and a major one. The exact response will depend on your organization and the nature of the attack that you face. If the initial assessment concluded that an account was compromised, you will need to enforce policy to block this account. That's just one example where the identity management system will be leveraged. Use the questions below to help you design your hybrid identity solution while taking into consideration how policies will be enforced to react to an ongoing incident:

- Does your company have policies in place to block users from access the network if necessary?
    - If yes, does the current solution integrates with the hybrid identity management system that you are going to adopt?
- Does your company need to enforce conditional access for users that are in quarantine?

Note

Make sure to take notes of each answer and understand the rationale behind the answer. Task 5 will go over the options available and advantages/disadvantages of each option. By having answered those questions you will select which option best suits your business needs.

Task 5: Define Data Protection Strategy

In this task, you'll define the data protection strategy for your hybrid identity solution to meet the business requirements that you defined in Tasks 1-4.

Task 5a: Define data protection options

As it was explained in Step 1, task 2, Microsoft Azure AD can synchronize with your Active Directory Domain Services (AD DS) located on-premises. This integration enables organizations to leverage Azure AD to verify user's credentials when they are trying to access corporate resources. This can be done for both scenarios: data at rest on-premises and in the cloud. Access to data in Azure AD requires user authentication via a security token service (STS). Once authenticated, the user principal name (UPN) is read from the authentication token and the replicated partition and container corresponding to the user's domain is determined. Information on the user's existence, enabled state, and role is used by the authorization system to determine whether the requested access to the target tenant is authorized for this user in this session. Certain authorized actions (i.e., create user, password reset) create an audit trail that can be used by a tenant administrator to manage compliance efforts or investigations.

Moving data from your on-premises datacenter into Azure Storage over an Internet connection may not always be feasible due to data volume, bandwidth availability, or other considerations. The Azure Storage Import/Export Service provides a hardware-based option for placing/retrieving large volumes of data in Blob storage. It allows you to send BitLocker-encrypted hard disk drives directly to an Azure datacenter where cloud operators will upload the contents to your storage account, or they can download your Azure data to your drives to return to you. Only encrypted disks are accepted for this process (using a BitLocker key generated by the service itself during the job setup). The BitLocker key is provided to Azure separately, thus providing out of band key sharing.

Since data in transit can take place in different scenarios, is also relevant to know that Microsoft Azure uses virtual networking to isolate tenants' traffic from one another, employing measures such as host- and guest-level firewalls, IP packet filtering, port blocking, and HTTPS endpoints. However, most of Azure's internal communications, including infrastructure-to-infrastructure and infrastructure-to-customer (on-premises), are also encrypted. Another important scenario is the communications within an Azure datacenter; Microsoft manages networks to assure that no VM can impersonate or eavesdrop on the IP address of another. TLS/SSL is used when accessing Azure Storage or SQL Databases, or when connecting to Cloud Services. In this case, the customer administrator is responsible for obtaining a TLS/SSL certificate and deploying it to their tenant infrastructure. Data traffic moving between Virtual Machines in the same deployment or between tenants in a single deployment via Microsoft Azure Virtual Network can be protected through encrypted communication protocols such as HTTPS, SSL/TLS, or others.

Depending on how you answered the questions in Task 1, you should be able to determine how you want to protect your data and how the hybrid identity solution will assist you on that. Table 5 shows the options supported by Azure that are available for each data protection scenario.

Table 5

Data Protection Options	Data Protection Stage		
	At Rest in the Cloud	At Rest on-premises	In Transit
BitLocker Drive Encryption	X	X	
SQL Server to encrypt databases	X	X	
VM-to-VM Encryption			X
SSL/TLS			X
VPN			X

Note

Read Compliance by Feature at Microsoft Azure Trust Center to know more about the certifications that each Azure service is compliant with.

Since the options for data protection use a multilayer approach, comparison between those options are not applicable for this task. Ensure that you are leveraging all options available for each state that the data will be.

Task 5b: Define content management options

One advantage of using Azure AD to manage a hybrid identity infrastructure is that the process is fully transparent from the end user's perspective. The user will try to access a shared resource, the resource requires authentication, the user will have to send an authentication request to Azure AD in order to obtain the token and access the resource. This entire process happens in background, without user interaction. It is also possible to grant permission to a group of users in order to allow them to perform certain common actions.

Organizations that are concern about data privacy usually require data classification for their solution. If their current on-premises infrastructure is already using data classification, it is possible to leverage Azure AD as the main repository for user's identity. A common tool that it is used on-premises for data classification is called Data Classification Toolkit for Windows Server 2012 R2. This tool can help to identify, classify, and protect data on file servers in your private cloud. It is also possible to leverage the Automatic File Classification in Windows Server 2012 to accomplish this.

If your organization doesn't have data classification in place but needs to protect sensitive files without adding new Servers on-premises, they can use Microsoft Azure Rights Management Service. Azure RMS uses encryption, identity, and authorization policies to help secure your files and email, and it works across multiple devices—phones, tablets, and PCs. Because Azure RMS is a cloud service, there's no need to explicitly configure trusts with other organizations before you can share protected content with them. If they already have an Office 365 or an Azure AD directory, collaboration across organizations is automatically supported. You can also synchronize just the directory attributes that Azure RMS needs to support a common identity for your on-premises Active Directory accounts, by using Azure Active Directory Synchronization Services (AAD Sync) or Azure AD Connect.

A vital part of content management is to understand who is accessing which resource, therefore a rich logging capability is important for the identity management solution. Azure AD provides log over 30 days including:

- Changes in role membership (ex: user added to Global Admin role)
- Credential updates (ex: password changes)
- Domain management (ex: verifying a custom domain, removing a domain)
- Adding or removing applications
- User management (ex: adding, removing, updating a user)
- Adding or removing licenses

Note

Read Microsoft Azure Security and Audit Log Management to know more about logging capabilities in Azure.

Depending on how you answered the questions in Task 2, you should be able to determine how you want the content to be managed in your hybrid identity solution. While all options exposed in Table 6 are capable of integrating with Azure AD, it is important to define which is more appropriate for your business needs.

Table 6

Content Management Options	Advantages	Disadvantages
Centralized on-premises (Active Directory Rights Management Server)	• Full control over the server infrastructure responsible for classifying the data • Built-in capability in Windows Server, no need for extra license or subscription	• Higher maintenance (keep up with updates, configuration and potential upgrades) since IT owns the Server • Require a server infrastructure on-premises • Doesn't leverage Azure capabilities natively

	• Can be integrated with Azure AD in a hybrid scenario • Supports information rights management (IRM) capabilities in Microsoft Online services such as Exchange Online and SharePoint Online, as well as Office 365. • Supports on-premises Microsoft server products, such as Exchange Server, SharePoint Server, and file servers that run Windows Server and File Classification Infrastructure (FCI).	
Centralized in the cloud (Azure RMS)	• Easier to manage compared to the on-premises solution • Can be integrated with AD DS in a hybrid scenario • Fully integrated with Azure AD • Doesn't require a server on-premises in order to deploy the service • Supports on-premises Microsoft server products such as Exchange Server, SharePoint Server, and file servers that run Windows Server and File Classification Infrastructure (FCI). • IT can have complete control over their tenant's key with BYOK capability.	• Your organization must have a cloud subscription that supports RMS • Your organization must have an Azure AD directory to support user authentication for RMS
Hybrid (Azure RMS integrated with On-Premises Active Directory Rights Management Server)	• This scenario accumulates the advantages of both, centralized on-premises and in the cloud.	• Your organization must have a cloud subscription that supports RMS • Your organization must have an Azure AD directory to support user authentication for RMS • Requires a connection between Azure cloud service

		and on-premises infrastructure

Task 5c: Define access control options

By leveraging the authentication, authorization and access control capabilities available in Azure AD you will be able to enable your company to use a central identity repository while allowing users and partners to use single sign-on (SSO) as shown in Figure 11:

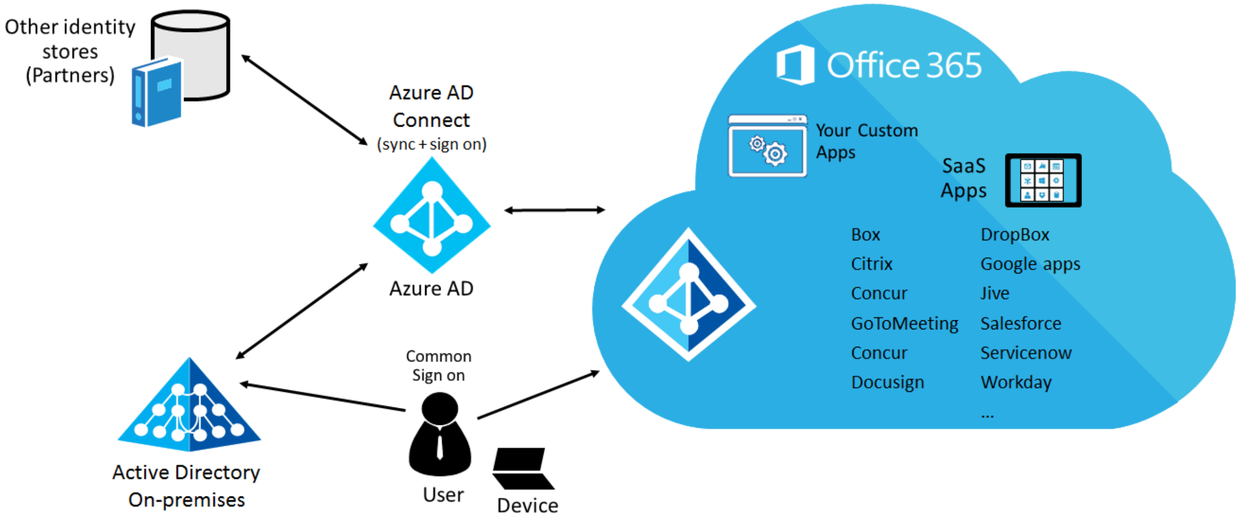


Figure 11 – Centralized management and fully integration with other directories

Azure Active Directory provides single sign-on to thousands of SaaS applications and on-premises web applications. Please read the Azure Active Directory federation compatibility list: third-party identity providers that can be used to implement single sign-on article for more details about the SSO third-party that were tested by Microsoft. This capability enable organization to implement a variety of B2B scenarios while keeping control of the identity and access management. However, during the B2B designing process is important to understand the authentication method that will be used by the partner and validate if this method is supported by Azure. Currently these are methods supported by Azure AD:

- Security Assertion Markup Language (SAML)
- OAuth
- Kerberos
- Tokens
- Certificates

Note

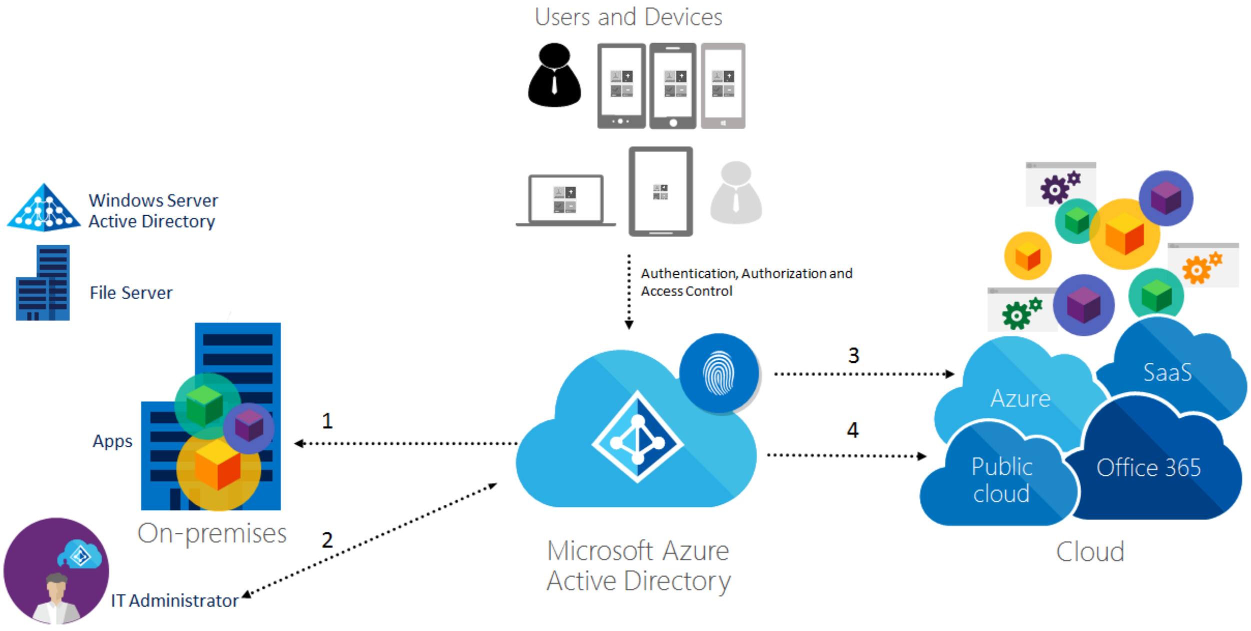
Read Azure Active Directory Authentication Protocols to know more details about each protocol and its capabilities in Azure.

Using the Azure AD support, mobile business applications can use the same easy Mobile Services authentication experience to allow employees to sign into their mobile applications with their corporate Active Directory credentials. With this feature, Azure AD is supported as an identity provider in Mobile Services alongside with the other identity providers we already support (which include Microsoft Accounts, Facebook ID, Google ID, and Twitter ID). If the on-premises apps uses the user's credential located at the company's AD DS, the access from partners and users coming from the cloud should be transparent. You can manage user's conditional access control to (cloud-based) web applications, web API, Microsoft cloud services, third- party SaaS applications, and native (mobile) client applications, and have the benefits of security, auditing, reporting all in one place. However, it is recommended to validate this in a non-production environment or with a limited amount of users.

Tip

It is important to mention that Azure AD does not have Group Policy as AD DS has. In order to enforce policy for devices you will need a mobile device management solution such as Microsoft Intune.

Once the user is authenticated using Azure AD, it is important to evaluate the level of access that the user will have it. The level of access that the user will have over a resource can vary, while Azure AD can add an additional security layer by controlling access to some resources, you must also keep in mind that the resource itself can also have its own access control list separately, such as the access control for files located in a File Server. Figure 12 summarizes the levels of access control that you can have in a hybrid scenario:



Users and Devices
Windows Server Active Directory
File Server
Apps
On-premises
IT Administrator
Authentication, Authorization and Access Control
1
2
3
4
Microsoft Azure Active Directory
Azure
SaaS
Public cloud
Office 365
Cloud

Figure 12 – Centralized management and fully integration with other directories

Each interaction in the diagram showed in Figure X represents one access control scenario that can be covered by Azure AD. Below you have a description of each scenario:

1. Conditional Access to applications that are hosted on-premises: You can use registered devices with access policies for applications that are configured to use AD FS with Windows Server 2012 R2. For more information about setting up conditional access for on-premises, see Setting up On-premises Conditional Access using Azure Active Directory Device Registration.

2. Access Control to Azure Management Portal: Azure also has the capability to control access to the Management Portal by using RBAC (Role Based Access Control). This method enables the company to restrict the amount of operations that an individual can do once he has access to Azure Management Portal. By using RBAC to control access to the portal, IT Admins ca delegate access by using the following access management approaches:

- **Group-based role assignment:** You can assign access to Azure AD groups that can be synced from your local Active Directory. This enables you to leverage the existing investments that your organization has made in tooling and processes for managing groups. You can also use the delegated group management feature of Azure AD Premium.
- **Leverage built in roles in Azure**: You can use three roles — Owner, Contributor, and Reader, to ensure that users and groups have permission to do only the tasks they need to do their jobs.
- **Granular access to resources:** You can assign roles to users and groups for a particular subscription, resource group, or an individual Azure resource such as a website or database. In this way, you can ensure that users have access to all the resources they need and no access to resources that they do not need to manage.

Note

Read Role-based access control in Azure Preview portal to know more details about this capability. For developers that are building applications and want to customize the access control for them, it is also possible to use Azure AD Application Roles for authorization. Review this WebApp-RoleClaims-DotNet example on how to build your app to use this capability.

3. Conditional Access for Office 365 applications with Microsoft Intune: IT admins can provision conditional access device policies to secure corporate resources, while at the same time allowing information workers on compliant devices to access the services. For more information, see Conditional Access Device Policies for Office 365 services.

4. Conditional Access for Saas Apps: This feature allows you to configure per-application multi-factor authentication access rules and the ability to block access for users not on a trusted network. You can apply the multi-factor authentication rules to all users that are assigned to the application, or only for users within specified security groups. Users may be excluded from the multi-factor authentication requirement if they are accessing the application from an IP address that in inside the organization's network.

Since the options for access control use a multilayer approach, comparison between those options are not applicable for this task. Ensure that you are leveraging all options available for each scenario that requires you to control access to your resources.

Task 5d: Define incident response options

Azure AD can assist IT to identity potential security risks in the environment by monitoring user's activity, IT can leverage Azure AD Access and Usage reports capability to gain visibility into the integrity and security of your organization's directory. With this information, an IT admin can better determine where possible security risks may lie so that they can adequately plan to mitigate those risks. Azure AD Premium subscription has a set of security reports that can enable IT to obtain this information. Azure AD reports are categorized as shown below:

- **Anomaly reports:** Contain sign in events that we found to be anomalous. Our goal is to make you aware of such activity and enable you to be able to make a determination about whether an event is suspicious.
- **Integrated Application report:** Provides insights into how cloud applications are being used in your organization. Azure Active Directory offers integration with thousands of cloud applications.
- **Error reports:** Indicate errors that may occur when provisioning accounts to external applications.
- **User-specific reports:** Display device/sign in activity data for a specific user.
- **Activity logs:** Contain a record of all audited events within the last 24 hours, last 7 days, or last 30 days, as well as group activity changes, and password reset and registration activity.

Tip

Another report that can also help the Incident Response team working on a case is the *user with leaked credentials* report. This report surfaces any matches between these leaked credentials list and your tenant.

Other important built in reports in Azure AD that can be used during an incident response investigation and are:

- **Password reset activity:** provide the admin with insights into how actively password reset is being used in the organization.
- **Password reset registration activity:** provides insights into which users have registered their methods for password reset, and which methods they have selected.
- **Group activity:** provides a history of changes to the group (ex: users added or removed) that were initiated in the Access Panel.

In addition to the core reporting capability available in Azure AD Premium that can be leveraged during an Incident Response investigation process, IT can also leverage Audit Report to obtain information such as:

- Changes in role membership (ex: user added to Global Admin role)
- Credential updates (ex: password changes)
- Domain management (ex: verifying a custom domain, removing a domain)
- Adding or removing applications
- User management (ex: adding, removing, updating a user)
- Adding or removing licenses

Since the options for incident response use a multilayer approach, comparison between those options are not applicable for this task. Ensure that you are leveraging all options available for each scenario that requires you to use Azure AD reporting capability as part of your company's incident response process.

Step 3 - Plan for Hybrid Identity Lifecycle

Identity is one of the foundations of your enterprise mobility and application access strategy. Whether you are logging into your mobile device or SaaS app, your identity is the key to gaining access to everything. At its highest level, an identity management solution encompasses unifying and syncing between your identity repositories which includes automating and centralizing the process of provisioning resources. The identity solution should be a centralized identity across on-premises and cloud and also use some form of identity federation to maintain centralized authentication and securely share and collaborate with external users and businesses. Resources range from operating systems and applications to people in, or affiliated with, an organization. Organizational structure can be altered to accommodate the provisioning policies and procedures.

It is also important to have an identity solution geared to empower your users by providing them with self-service experiences to keep them productive. Your identity solution is more robust if it enables single sign-on for users across all the resources they need access Administrators at all levels can use standardized procedures for managing user credentials. Some levels of administration can be reduced or eliminated, depending on the breadth of the provisioning management solution. Furthermore, you can securely distribute administration capabilities, manually or automatically, among various organizations. For example, a domain administrator can serve only the people and resources in that domain. This user can do administrative and provisioning tasks, but is not authorized to do configuration tasks, such as creating workflows.

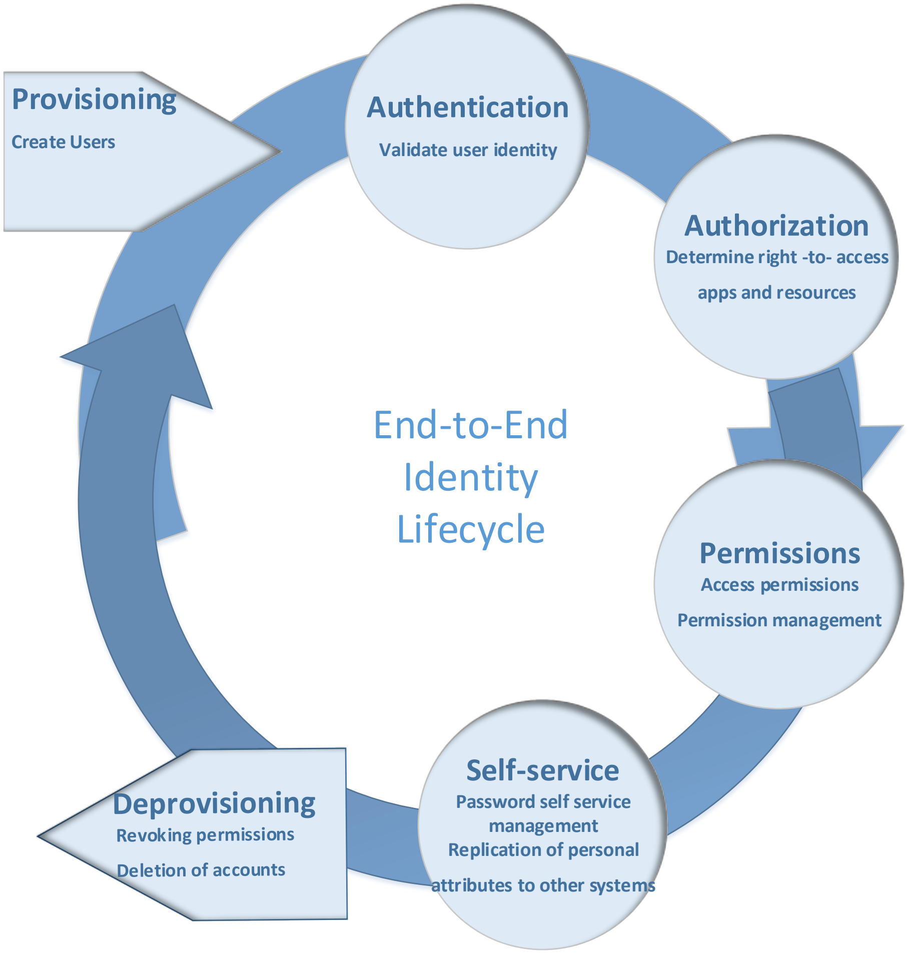


Figure 13 – Identity lifecyle

Task 1: Determine hybrid identity management tasks

Distributing administrative tasks in your organization improves the accuracy and effectiveness of administration and improves the balance of the workload of an organization. Following are the pivots that define a robust identity management system

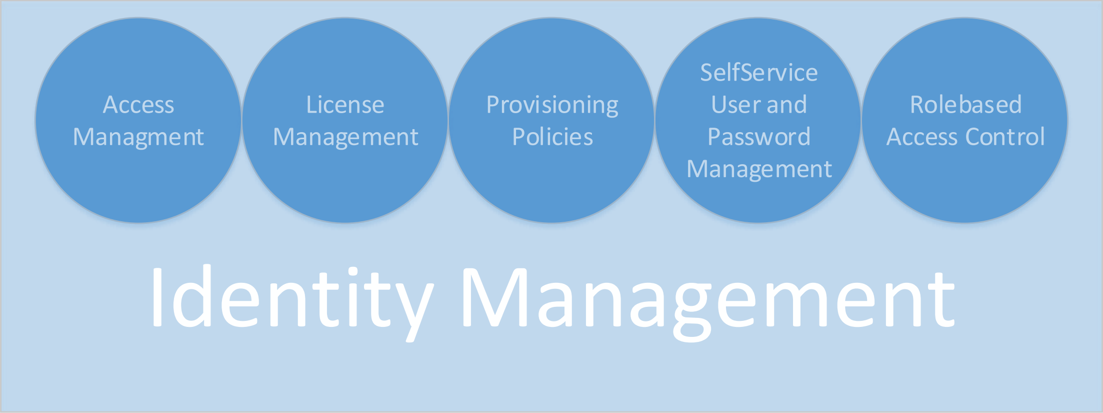


Figure 14 – Identity management considerations

In order to define hybrid identity management tasks, you must understand some essential characteristics of the organization that will be adopting hybrid identity. It is important to understand the current repositories being used for identity sources. By knowing those core elements, you will have the foundational requirements and based on that you will need to ask more granular questions that will lead you to a better design decision for your Identity solution. While defining those requirements, ensure that at least the following questions are answered

- **What are the provisioning options:**
    - Does the hybrid identity solution support a robust account access management and provisioning system?
    - How are users, groups, and passwords going to be managed?
    - Is the identity lifecycle management responsive?
        - How long does password updates account suspension take?
        - If yes, how long does it take
- **License management:**
    - Does the hybrid identity solution handles license management?
        - If yes, what capabilities are available?
    - Does the solution handles group-based license management?
        - If yes, is it possible to assign a security group to it?
            - If yes, will the cloud directory automatically assign licenses to all the members of the group?
            - What happens if a user is subsequently added to, or removed from the group, will a license be automatically assigned or removed as appropriate?
- **Integration with other third-party identity providers**:
    - Can this hybrid solution be integrated with third-party identity providers to implement single sign-on?
    - Is it possible to unify all the different identity providers into a cohesive identity system?
        - If yes, how and which are they and what capabilities are available?

Task 2: Synchronization Management

One of the goals of an identity manager, to be able to bring all the identity providers and keep them synchronized. You keep the data synchronized based on an authoritative master identity provider. In a hybrid identity scenario, with a synchronized management model, you manage all user and device identities in an on-premises server and synchronize the accounts and, optionally, passwords to the cloud. The user enters the same password on-premises as he or she does in the cloud, and at sign-in, the password is verified by the identity solution. This model uses a directory synchronization tool.

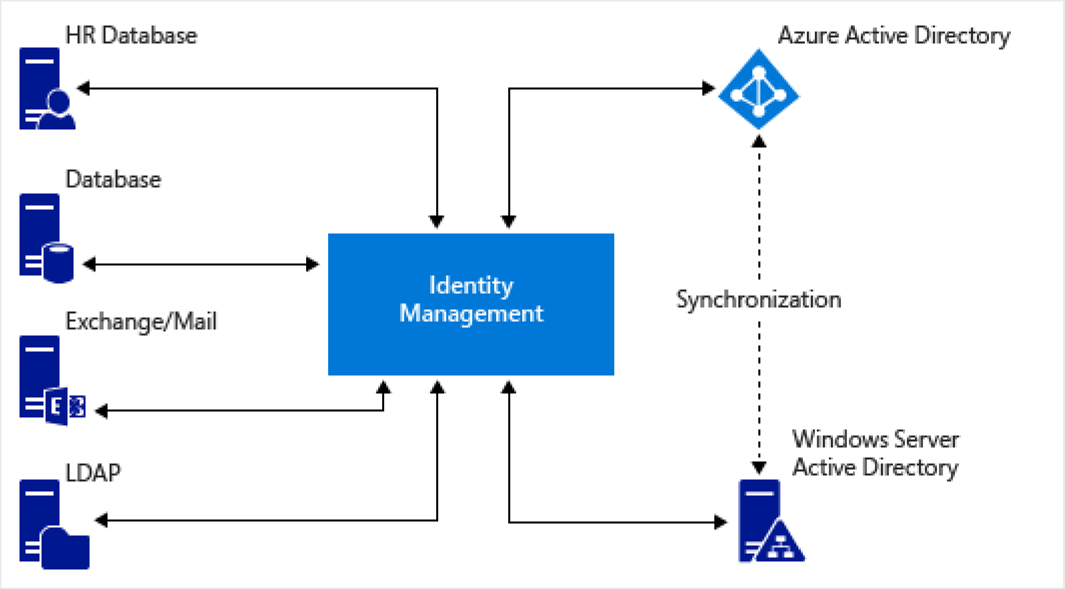


Figure 15 – Directory synchronization

To proper design the synchronization of your hybrid identity solution ensure that the following questions are answered:

- What are the sync solutions available for the hybrid identity solution?
- What are the single sign on capabilities available?
- What are the options for identity federation between B2B and B2C?

Task 3: Determine hybrid identity management adoption strategy

In this task, you'll define the identity management strategy for your hybrid identity solution to meet the business requirements that you defined in Tasks 1-2 in this step.

Task 3a: Define Hybrid Identity Management Tasks

To define the hybrid identity management tasks according to the end-to-end identity lifecycle presented earlier in this step, you will have to consider the options available for each lifecycle phase.

Account access management and the provisioning system

With an effective account access management solution, your organization can track precisely who has access to what information across the organization. Access control is a critical function of a centralized, single-point provisioning system. Besides protecting sensitive information, access controls expose existing accounts that have unapproved authorizations or are no longer necessary. *Orphan accounts* are active accounts that cannot be associated with valid users. To control orphan accounts, the provisioning system links together account information with authoritative information about the users who own the accounts. Authoritative user identity information is typically maintained in the databases and directories of human resources.

Accounts in sophisticated IT systems include hundreds of parameters that define the authorities, and these details can be controlled by your provisioning system. *New users* can be readily identified with the data feed that you establish from the human resources directory. The access request approval capability initiates the processes that approve (or reject) resource provisioning for them. The following table lists the options for user account management and provisioning compared across the three ecosystems:

Table 7

Lifecycle Management Phase	**Design Options**		
	On-Premises	**Cloud**	**Hybrid**
Account Management and Provisioning	• By using the Active Directory® Domain Services (AD DS) server role, you can create a scalable, secure, and manageable infrastructure for user and resource management, and provide support for directory-enabled applications such as Microsoft® Exchange Server. • Provisioning groups in AD DS	• You have to create an account for every user who will access a Microsoft cloud service. You can also change user accounts or delete them when they're no longer needed. By default, users do not have administrator permissions, but you can optionally assign them.	Extend Active Directory identities into the cloud through synchronization and Federation

	through an Identity manager - Provisioning users in AD DS - Administrators can use access control to manage user access to shared resources for security purposes. In Active Directory, access control is administered at the object level by setting different levels of access, or permissions, to objects, such as Full Control, Write, Read, or No Access. Access control in Active Directory defines how different users can use Active Directory objects. By default, permissions on objects in Active Directory are set to the most secure setting.	For more information, see Managing Users in Azure AD - Within Azure Active Directory, one of the major features is the ability to manage access to resources. These resources can be part of the directory, as in the case of permissions to manage objects through roles in the directory, or resources that are external to the directory, such as SaaS applications, Azure services, and SharePoint sites or on premise resources. At the center of Azure Active Directory's access management solution is the security group. The resource	

		owner (or the administrator of the directory) can assign a group to provide a certain access right to the resources they own. The members of the group will be provided the access, and the resource owner can delegate the right to manage the members list of a group to someone else – such as a department manager or a helpdesk administrator • The Managing groups in Azure AD topic provides more information on managing access through groups.	

Role-based access control

Role-based access control (RBAC) uses roles and provisioning policies to evaluate, test, and enforce your business processes and rules for granting access to users. Key administrators create provisioning policies and assign users to roles and that define sets of entitlements to resources for these roles. RBAC tasks establish role-based access control to resource. RBAC extends the identity management solution to use software-based processes and reduce user manual interaction in the provisioning process.

Azure AD RBAC (Role Based Access Control enables the company to restrict the amount of operations that an individual can do once he has access to Azure Management Portal. By using RBAC to control access to the portal, IT Admins ca delegate access by using the following access management approaches:

- **Group-based role assignment:** You can assign access to Azure AD groups that can be synced from your local Active Directory. This enables you to leverage the existing investments that your organization has made in tooling and processes for managing groups. You can also use the delegated group management feature of Azure AD Premium.
- **Leverage built in roles in Azure**: You can use three roles — Owner, Contributor, and Reader, to ensure that users and groups have permission to do only the tasks they need to do their jobs.
- **Granular access to resources:** You can assign roles to users and groups for a particular subscription, resource group, or an individual Azure resource such as a website or database. In this way, you can ensure that users have access to all the resources they need and no access to resources that they do not need to manage.

Incremental provisioning and other customization options

Your team can use business plans and requirements to decide how much to customize the identity solution. For example, a large enterprise might require a phased roll-out plan for workflows and custom adapters that is based on a time line for incrementally provisioning applications that are widely used across geographies. Another customization plan might provide for two or more applications to be provisioned across an entire organization, after successful testing. User-application interaction can be customized, and procedures for provisioning resources might be changed to accommodate automated provisioning.

You can *deprovision* to remove a service or component. For example, deprovisioning an account means that the account is deleted from a resource.

The hybrid model of provisioning resources combines request and role-based approaches, which are both supported by Azure AD. For a subset of employees or managed systems, a business might want to automate access with role-based assignment. A business might also handle all other access requests or exceptions through a request-based model. Some businesses might start with manual assignment, and evolve toward a hybrid model, with an intention of a fully role-based deployment at a future time.

Other companies might find it impractical for business reasons to achieve complete role-based provisioning, and target a hybrid approach as a wanted goal. Still other companies might be satisfied with only request-based provisioning, and not want to invest additional effort to define and manage role-based, automated provisioning policies.

License Management

Group-based license management in Azure AD lets administrators assign users to a security group and Azure AD automatically assigns licenses to all the members of the group. If a user is subsequently added to, or removed from the group, a license will be automatically assigned or removed as appropriate.

You can use groups you synchronize from on-premises AD or manage in Azure AD. Pairing this up with Azure AD premium Self-Service Group Management you can easily delegate license assignment to the appropriate decision makers. You can be assured that problems like license conflicts and missing location data are automatically sorted out.

Self-regulating user administration

When your organization starts to provision resources across all internal organizations, you implement the self-regulating user administration capability. You can realize the advantages and benefits of provisioning users across organizational boundaries. In this environment, a change in a user's status is automatically reflected in access rights across organization boundaries and geographies. You can reduce provisioning costs and streamline the access and approval processes. The implementation realizes the full potential of implementing role-based access control for end-to-end access management in your organization. You can reduce administrative costs through automated procedures for governing user provisioning. You can improve security by automating security policy enforcement, and streamline and centralize user lifecycle management and resource provisioning for large user populations.

> **Note**
>
> For more information, see Setting up Azure AD for self service application access management

License-based (Entitlement-based) Azure AD services work by activating a subscription in your Azure AD directory/service tenant. Once the subscription is active the service capabilities can be managed by directory/service administrators and used by licensed users. For more information, see How does Azure AD licensing work?

Integration with other third- party providers

Azure Active Directory provides single-sign on and enhanced application access security to thousands of SaaS applications and on-premises web applications. For a detailed list of Azure Active Directory application gallery for supported SaaS applications, see Azure Active Directory federation compatibility list: third-party identity providers that can be used to implement single sign-on

Task 3b: Define Synchronization Management

Integrating your on-premises directories with Azure AD makes your users more productive by providing a common identity for accessing both cloud and on-premises resources. With this integration users and organizations can take advantage of the following:

- Organizations can provide users with a common hybrid identity across on-premises or cloud-based services leveraging Windows Server Active Directory and then connecting to Azure Active Directory.
- Administrators can provide conditional access based on application resource, device and user identity, network location and multi-factor authentication.
- Users can leverage their common identity through accounts in Azure AD to Office 365, Intune, SaaS apps and third-party applications.
- Developers can build applications that leverage the common identity model, integrating applications into Active Directory on-premises or Azure for cloud-based applications

Figure 16 has an example of a high-level view of identity synchronization process.

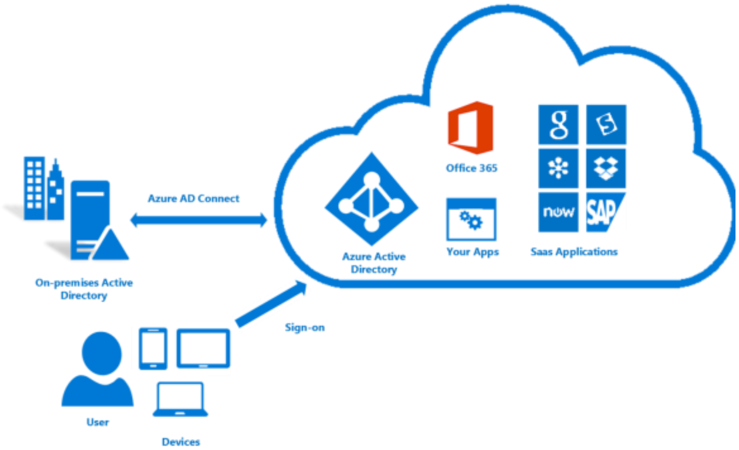


Figure 16 – Identity synchronization process

Review table 8 to compare the synchronization options:

Table 8

Synchronization Management Option	**Advantages**	**Disadvantages**
Sync-based (through DirSync or AADConnect)	• Users and groups synchronized from on-premises and cloud. • **Policy control:** Account policies can be set through Active Directory, which gives the administrator the ability to manage password policies, workstation restrictions, lock-out controls, and more, without having to perform additional tasks in the cloud. • **Access control: C**an restrict access to the cloud service so that the services can be accessed through the corporate environment, through online servers, or both. • **Reduced support calls:** If users have fewer passwords to remember, they are less likely to forget them. • **Security:** User identities and information are protected because all of the servers and services used in single sign-on are mastered and controlled on-premises. • **Support for strong authentication:** You can use strong authentication (also called two-factor	

	authentication) with the cloud service. However, if you use strong authentication, you must use single sign-on.	
Federation-based (through AD FS)	- Enabled by Security Token Service (STS). When you configure an STS to provide single sign-on access with a Microsoft cloud service, you will be creating a federated trust between your on-premises STS and the federated domain you've specified in your Azure AD tenant. - Allows end users **to use the same set of credentials** to obtain access to multiple resources. - end users do not have to maintain multiple sets of credentials. Yet, the users have to provide their credentials to each one of the participating resources. - B2B and B2C scenarios supported.	Requires specialized personnel for deployment and maintenance of dedicated on-prem AD FS servers. There are restrictions on the use of strong authentication if you plan to use AD FS for your STS. For more information, see Configuring Advanced Options for AD FS 2.0 for more information.

Note

For more information see, Integrating your on-premises identities with Azure Active Directory

Next Steps

Now that you've completed defining your requirements and examining all the options for your mobile device management solution, you're ready to take the next steps for deploying the supporting infrastructure that's right for you and your organization.

Hybrid Identity Solutions

Leveraging specific solution scenarios that fit your needs is a great way to review and plan for the details of deploying a mobile device management infrastructure. The following solutions outline several of the most common mobile device management scenarios:

- The manage mobile devices and PCs in enterprise environments solution helps you manage mobile devices by extending your on-premises System Center 2012 Configuration Manager infrastructure into the cloud with Microsoft Intune. This hybrid infrastructure helps IT Pros in medium and large environments enable BYOD and remote access while reducing administrative complexity.
- The managing mobile devices for Configuration Manager 2007 solution helps you manage mobile devices when your infrastructure rests on a System Center Configuration Manager 2007. This solution shows you how to set up a single server running System Center 2012 Configuration Manager so you can then run Microsoft Intune and take advantage of its MDM ability.
- The managing mobile devices in small environments solution is intended for small businesses that need to support MDM. It explains how to use Microsoft Intune to extend your current infrastructure to support mobile device management and BYOD. This solution describes the simplest scenario supported for using Microsoft Intune in a standalone, cloud-only configuration with no local servers.

Hybrid Identity Documentation

Conceptual and procedural planning, deployment, and administration content are useful when implementing your mobile device management solution:

- Microsoft System Center solutions can help you capture and aggregate knowledge about your infrastructure, policies, processes, and best practices so that your IT staff can build manageable systems and automate operations.
- Microsoft Intune is a cloud-based device management service that helps you to manage your computers and mobile devices and to secure your company's information.
- MDM for Office 365 allows you to manage and secure mobile devices when they're connected to your Office 365 organization. You can use MDM for Office 365 to set device security policies and access rules, and to wipe mobile devices if they're lost or stolen.

Hybrid Identity Resources

Monitoring the following resources often provides the latest news and updates on mobile device management solutions:

- Microsoft Enterprise Mobility blog
- Microsoft In The Cloud blog

- Microsoft Intune blog
- Microsoft System Center Configuration Manager blog
- Microsoft System Center Configuration Manager Team blog