National Defense ISAC

Microsoft Reference Identity Architectures for the US Defense Industrial Base

Contributing Authors & Editors

ND-ISAC Cloud Security & Architecture Working Group

MS Cloud Services Subgroup

Richard Wakeman, Microsoft

Mark Gonzalez, Lockheed Martin

Paul Meacham, Microsoft

Will Jimenez, National Defense ISAC

Renee Stegman, National Defense ISAC

TLP: CLEAR

About this paper

The National Defense Information Sharing and Analysis Center (ND-ISAC) is a non-profit, non-federal entity established and funded by its member companies to support their collective cybersecurity and resilience against all hazards through multiple lines of effort. Traditional defense contractors form approximately two-thirds of ND-ISAC's member companies. The remaining third are companies with whom traditional defense contractors have key interdependencies but have predominant lines of business in other sectors such as Finance, Health/Pharma, Comms/IT, Chem, and Energy, plus DoD university affiliated research centers and DoD federally funded research and development centers. Among the ND-ISAC lines of effort, Working Groups enable members to engage in knowledge exchanges on threats, technology, and other relevant topics to improve cybersecurity across each member organization.

Last year during our annual executive summit, Chief Information and Security Officers (CIO/CISO) representing defense sector companies examined challenges with operating multi-tenant environments in Microsoft Cloud Services. The executives made a call to action for ND-ISAC to formulate a working group to tackle the issue and produce a best practice guide for the Defense Industrial Base (DIB) sector.

The MS Cloud Services Working Group brought ND-ISAC members together with Microsoft subject matter experts to further elaborate common challenges, understand features, and provide updates on Microsoft's Cloud Services roadmap. This Working Group regularly provides a forum to discuss best-practices and use cases among member companies. It also provides a venue for the Microsoft team to update participants on their services roadmap, provide guidance on current technical challenges, and answer general how-to's based on ND-ISAC member interest and feedback. The group has been focused on the Microsoft US Government cloud service offerings, including the US sovereign cloud with Microsoft 365 US Government (GCC & GCC High), Microsoft Azure Government, and additional highly regulated solutions.

This white paper is the result of months of collaboration among the MS Cloud Services Working Group. This Microsoft Reference Architecture for the DIB Sector provides the group's consensus on common challenges coupled with guidance on potential ways to overcome those challenges. It is worth noting however that it is not intended to cover every organization's unique technology environment. The white paper focuses on the candidate reference architectures for identity to accommodate multiple tenant organizations, and specifically those that have a deployment in the US Sovereign Cloud with Microsoft 365 US Government (GCC High) and Azure Government. It addresses external collaboration in highly regulated environments, inclusive of organizations that are homed in either Commercial or in the US Sovereign Cloud. Multiple levels of trust within the Microsoft Collaboration Framework are used to define the level of security required for collaboration at each trust level. Thus, each organization can determine the reference architecture that best supports their environment and security requirements.

Contents

Microsoft Collaboration Framework

Microsoft 365 (M365) was released as a public hyperscale cloud collaboration suite of products in 2010, including hosted services such as Exchange Online, SharePoint Online and has evolved to include Teams, Planner and many more. From the beginning, the best collaboration experience for a single organization (legal entity) is within a single Microsoft Office 365 tenant and single underlying Entra ID (formerly Azure Active Directory) tenant where you have the highest level of trust across a user population. For most organizations, managing users in a single tenant provides them with a unified view of resources and single set of policies and controls that enable a consistent user experience. Microsoft recommends a single tenant model when possible, and many of the cloud services are designed for a single tenant. However, a single tenant is not always possible. Multiple tenant organizations may span two or more M365 and Entra ID tenants – resulting in unique cross-tenant collaboration and management requirements. In addition, external collaboration extends beyond the tenant to partners and other parties that are not under organizational control.

This white paper focuses on the candidate reference architectures for identity to accommodate multiple tenant organizations, and specifically those that have a deployment in the US Sovereign Cloud with Microsoft 365 US Government (GCC High) and Azure Government. It will also address external collaboration in highly regulated environments, inclusive of organizations that are homed in either Commercial or in the US Sovereign Cloud.

As Office 365 has matured to become Microsoft 365 and with the introduction of Microsoft Azure, new and innovative means of collaboration have been introduced to accommodate multi-tenant organizations and highly regulated environments. However, not all the features have been available to organizations that deploy into the US Sovereign Cloud when introduced in 2016. The US Sovereign cloud was designed to protect US Government data from ending up in foreign adversary hands. Simple and ubiquitous sharing solutions were not acceptable to either the US Government nor for Microsoft. As such, this cloud environment was designed to necessarily impede unauthorized collaboration and the unintended release of controlled data outside its boundaries. Technically speaking, the US Sovereign Cloud aligns with the higher watermark of compliance with the US Department of Defense (DoD) Cloud Computing Security Requirements Guide (SRG) Impact Level 5 (IL5). In addition, it was purpose-built to protect Controlled Unclassified Information (CUI) such as export-controlled data including the International Traffic in Arms Regulations (ITAR). This highly regulated and heavily restricted cloud environment has not been conducive to collaboration beyond its boundaries.

Once the Defense Industrial Base (DIB) began deploying into the US Sovereign Cloud, it became abundantly clear that controls on collaboration outside of the tenant boundary were too restrictive. Most DIB straddle commercial clouds alongside the government clouds. In other words, the DIB are multi-tenant organizations that have deployments in both commercial and in government. The DIB desperately needs a solution and reference architectures to collaborate “cross cloud” between cloud environments.

The need for cross cloud collaboration is not unique to the DIB. Once the DoD got settled into the US Sovereign Cloud, they realized new scenarios of collaboration existed. For example, in late 2017, Hurricane Harvey wreaked havoc across Texas. During the hurricane relief, the US Coast Guard wanted to collaborate with the FBI and local law enforcement. In addition, they were all working in concert with the American Red Cross. However, they could not collaborate effectively as each were in different cloud environments:

- US Coast Guard in the US Sovereign Cloud (DoD)
- FBI in the US Sovereign Cloud (GCC High)
- Local law enforcement in GCC
- American Red Cross in Commercial
- Organizations not hosted in the Microsoft cloud

The DoD has now validated use-cases for cross-cloud and gave Microsoft the green light to introduce new solutions to solve the dilemma. This was further amplified by the ultimate challenges imposed by the COVID pandemic where people were forced to work from home. Microsoft has been working with the DoD to enable cross-cloud collaboration with default security, such as with zero-trust architectures. In many use-cases, the collaboration is bi-directional in nature. Many had previously assumed collaboration from the US Sovereign Cloud would only be in one direction (browse down to Commercial) but proved to be wrong. For example, the Army National Guard may host a meeting out of their US Sovereign Cloud (DoD) tenant and invite the FBI, local law enforcement and Red Cross in. Not only is this an example of cross-cloud, but it is also an example of four cloud collaboration into Teams hosted from the DoD tenant.

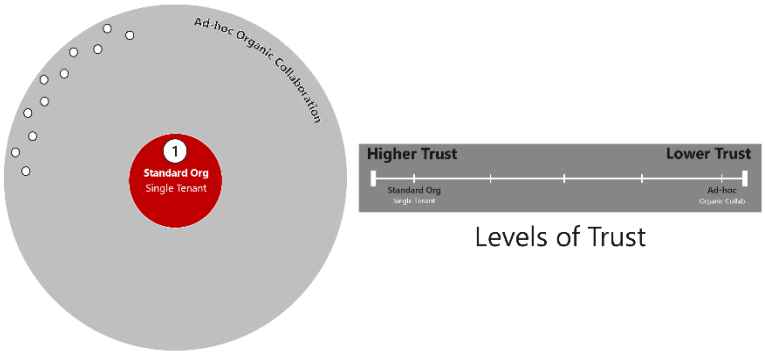
Before Microsoft could enable ad-hoc organic collaboration in cross-cloud scenarios, it was determined that a model for higher level of security is required for collaboration based on levels of trust. Thus, the Microsoft Collaboration Framework was born.

Levels of Trust

The Microsoft Collaboration Framework considers multiple levels of trust, extending from the highest level of trust achieved within a single Entra ID tenant, to the lowest level of trust afforded to ad-hoc collaboration that is organic by nature.

1: Standard Organization Collaboration

As mentioned above, the best collaboration experience for a single organization is within a single Entra ID tenant where you have the highest level of trust and control across a user population. For most organizations, managing users in a single tenant provides them with a unified view of resources and single set of policies and controls enabling a consistent user experience. Microsoft recommends a single tenant when possible, and many of the cloud services are designed for a single tenant. For example, there are services that do not yet support external identities. For these use-cases a single tenant is required to consume these services.



Levels of Trust

The vast majority of the millions of tenants deployed worldwide are standard organizations with a single Entra ID tenant for Microsoft 365 and Azure cloud services. With the 80/20 rule, when Microsoft solves for collaboration within a single tenant, it applies to 80% of the organizations on the planet. However, organizations that deploy into the US Sovereign Cloud, especially the DIB, fall into the more complicated 20%. This is why it has taken longer to solve for the additional complexity described below.

2: Complex Organization Collaboration

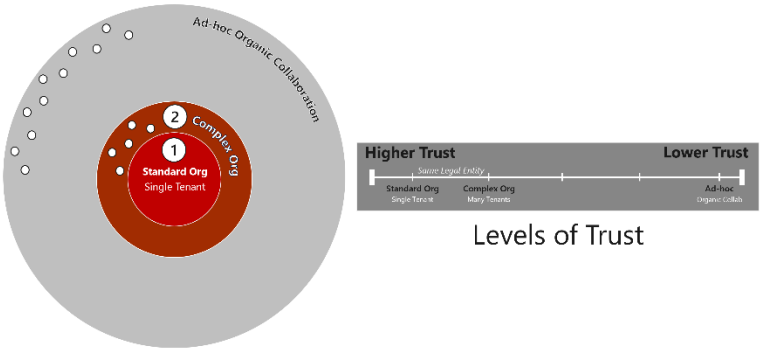
Complex organizations include multi-tenant deployments spanning two or more Entra ID tenants – resulting in unique cross-tenant collaboration and management requirements.

Complex organizations may have requirements that are complicated by:

- Collaboration across public, sovereign, and regional clouds
- Competing jurisdictions for compliance, such as data sovereignty in the U.S. versus Canada
- Political or organizational structures prohibiting consolidation to a single Entra ID tenant
- Mergers, acquisitions, and divestitures
- Partner and supply chain compliance, such as requiring CMMC certification for sub-contractors

Complex organizations often have a higher level of trust as compared to what is offered by ad-hoc collaboration but may be a lower level of trust than a single tenant architecture. Many complex organizations would like to appear as one, even though they are deployed to many. Given a single legal entity manages the user populations in all tenants belonging to the complex organization, they may configure standing policies that honor the higher level of trust, including:

- Unified Global Address List
- E-Mail domains shared between tenants
- Chat and calling with Teams
- Presence indicators
- Authenticated meeting join
- Calendar Free/Busy availability
- Ubiquitous document sharing
- Application access and single sign-on
- And more…



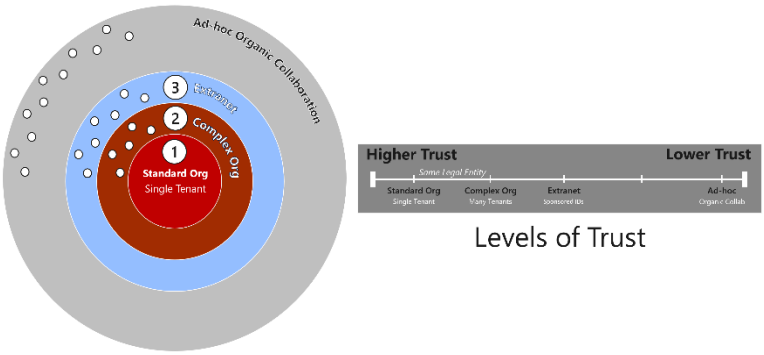
Levels of Trust

You may consider these features as having an established "trust" between two or more tenants. These trusts may be configured using Microsoft's Cross Tenant Access Settings.

This white paper proposes a reference architecture for complex multi-tenant organizations in future sections.

3: Extranet Collaboration

An extranet is a centralized repository of shared applications and content made available to authorized members of cross-organization work groups, including partners, subcontractors, vendors, suppliers, and potentially customers. This access is given to a subset of the content accessible from within an organization's private network or intranet. An extranet is similar to a DMZ in that it provides access to services for authorized parties, without granting access to an organization's entire network.



Levels of Trust

In traditional implementations of an extranet, the organization owns and manages the identity for the external parties, including the credentials used to sign-in to the extranet. These "Sponsored IDs" have a higher level of trust as the host organization has full authority over how the credentials are used. Historically, this sponsored ID credential may have been stored in an extranet directory, such as within Active Directory Domain Services hosted within a DMZ. That is no longer a requirement. With new cloud-native capabilities including Entra ID external identities, it's now possible to invite in external "Guest" user accounts that are not employees of the organization. With external identities, the organization no longer needs to manage the credentials. However, most organizations cannot simply pivot from traditional extranet to Entra ID external identities overnight. The two may co-exist in harmony for some period, or possibly in perpetuity.

Extranets may stay relevant into the future for many reasons. Most notably, CMMC compliance must be pervasive across all sub-contractors for a specified DoD contract. In some cases, these contracts and programs may include tens or hundreds of contractors in the supply chain. In the near-term, the expectation is that many of these contractors will take an extended period to get CMMC certified. Thus, any non-compliant subcontractors are either eliminated from performance on a contract, or they must be invited into a CMMC compliant enclave or extranet to work with CUI. In the

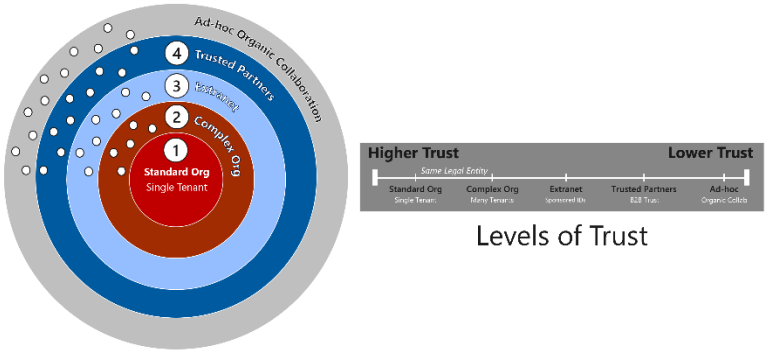
spirit of the extranet, the non-compliant subcontractor user may access relevant contract and program content without granting access to an organization's entire enterprise tenant.

Another related scenario for the extranet, is where you either lift up or shift down on the level of compliance. For example, if the enterprise tenant is certified for CMMC Level 2, but a contract requires Level 3, an enclave or extranet may be certified for Level 3 to lift up compliance. Or conversely, if the enterprise tenant is super restrictive such as having a tenant-wide US persons policy, an enclave or extranet may be designated for collaboration with non-US persons.

This white paper proposes reference architectures for the Extranet, including Extranet Entra ID tenants and "Meet Me" tenants described in future sections.

4: Trusted Partners Collaboration

Trusted partners include subcontractors, vendors, suppliers, and customers for which there is a long-term established relationship with. To build a higher level of trust with the partner, an agreement may be founded on the security and compliance posture of the partnership. For example, an agreement may include users and endpoints that are compliant with CMMC Level 2 to access CUI. Many companies within the DIB may create a Memorandum of Understanding (MOU) to solidify an agreement for CMMC compliance to enable bi-directional sharing of content between the companies. Ultimately, a trusted partner will have a higher level of trust as compared to ad-hoc organic collaboration but may be a lower level of trust than between tenants owned by a single organization.

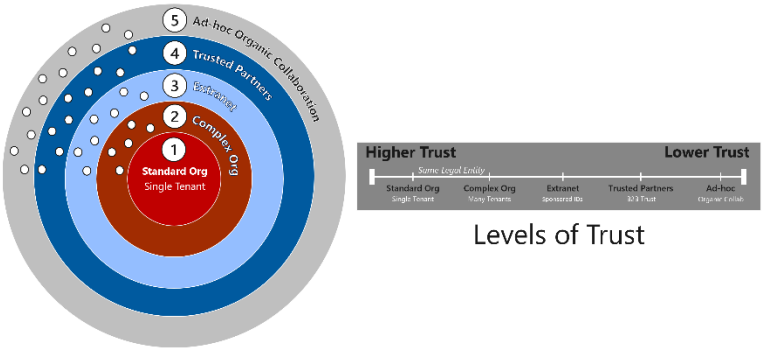


Levels of Trust

Trusted partners collaboration may include bi-directional sharing between tenants managed by multiple organizations. A primary difference between extranet as compared to trusted partners is 'who' owns and manages the credentials for external users. In the case of trusted partners, the partner will own the credentials.

5: Ad-hoc Organic Collaboration

Ad-hoc organic collaboration is the ability for an end-user to share a document, document library, Team, app, etc. with anyone that has an email address. The recipient of the sharing invitation may be hosted on the Microsoft cloud, or virtually anywhere else.



Levels of Trust

The first introduction of collaboration beyond the tenant boundary was ad-hoc and organic. For example, in the early days of SharePoint Online and OneDrive for Business Online, document sharing was enabled by default in an ad-hoc fashion. A user could organically generate a URL link to share a document on a one-on-one basis. The URL could be accessed from anywhere, with no controls or restrictions beyond having possession of the URL. If activated by the person sharing the document, it would require authentication with a One-Time Passcode (OTP) via E-Mail. While an effective tool, many highly regulated organizations would limit the use of ad-hoc sharing. Regardless, it remains a very popular feature in commercial tenants with its ease of use. This is especially compelling in comparison to other cloud products like Google and Box. Ah-hoc sharing is even relevant in US Sovereign Cloud tenants with a strong governance policy. For example, ad-hoc sharing may be enabled for document

libraries to share general content while restricting CUI and highly sensitive information. This is due to the fact there is the lowest level of trust with ad-hoc organic collaboration.

Entra ID External Identities

Entra ID external identities (*also known as 'B2B'*) enables organizations to securely share applications, services and content with external 'Guest' users from any other organization or tenant, while maintaining control of what is being shared. The Entra ID external identities feature permits organizations to invite external users to collaborate within a tenant. An invitation and redemption process lets partners use their own credentials to access the organization's tenant resources, such as accessing shared documents. Once the external user has redeemed their invitation, they're represented in the Entra ID tenant directory as a user object. Entra ID external identity user objects are typically given a user type of 'Guest' and can be typically identified by the #EXT# extension in their UserPrincipalName (UPN).

For more information, please see Entra ID External Identities and B2B collaboration overview

The concept for Entra ID external identities is simple.

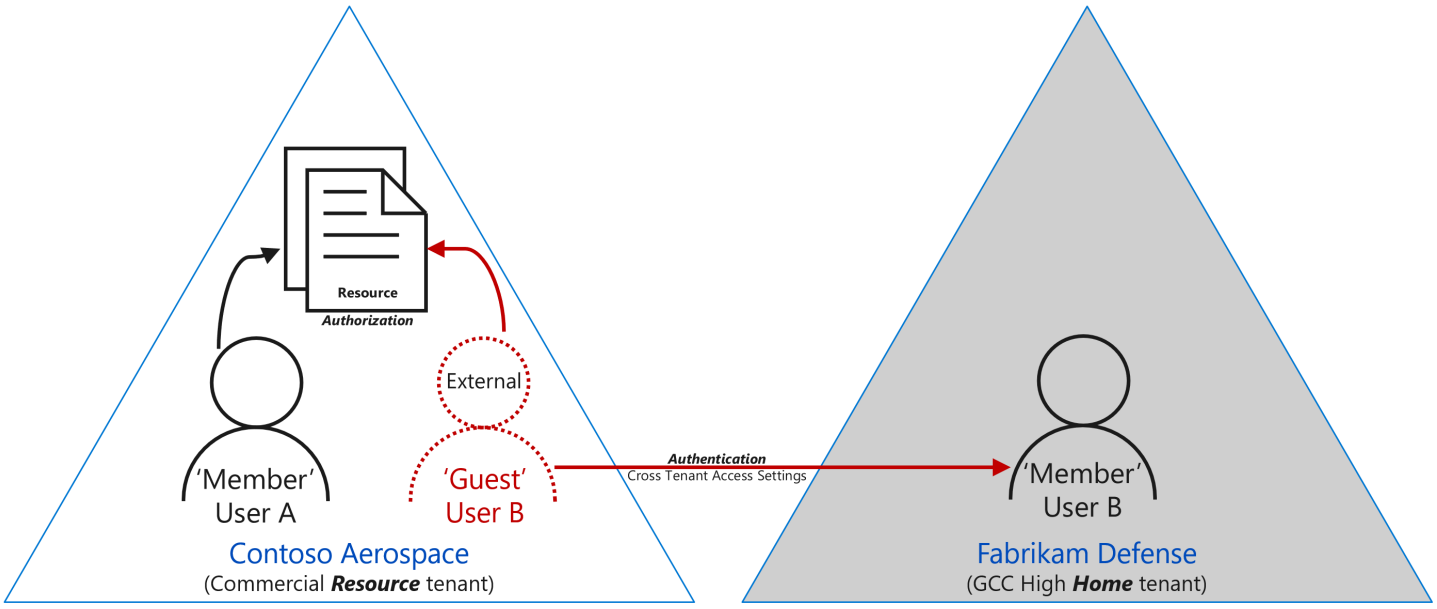


Illustration A: External Guest User Resource Authorization

When an external user is invited into the tenant and redeems the invitation, an external 'Guest' User is established. The external user is a persistent identity within the organization's tenant directory, serving as a shadow account with a security principal that may be assigned permissions to resources with Access Control Lists (ACLs), group membership, entitlement management, etc. Essentially, the external 'Guest' user can access resources in the tenant like any other internal 'Member' user, subject to limited default permissions as described in the following sections.

In Illustration A, external Guest User B lives within the Contoso Aerospace commercial "Resource" tenant. The Resource tenant contains the applications, services and content to be shared with User B. External Guest User B has a linkage back to the real internal 'Member' User B that resides in their 'Home' tenant. In this case, the Home tenant for Fabrikam Defense is in GCC High. Any time User B accesses a resource in Contoso Aerospace, it will redirect back to the home for Fabrikam Defense to authenticate. In other words, User B will always authenticate in their home tenant, no matter

where the resource resides. As such, external identities enable authorization within the resource tenant while authentication happens in the home tenant.

> *For more information on the authentication process, see* Appendix B: Cross Cloud external identities authentication flow

Internal versus External and Member versus Guest

An area of confusion with Entra ID external identities surrounds the properties of a B2B guest user. This includes the difference between 'internal' versus 'external' user accounts, and 'Member' versus 'Guest' user types. An internal user is one that is homed and authenticates to the tenant. This may be an account created with credentials directly within Entra ID, or may be sourced from traditional Windows Server Active Directory Domain Services known as Hybrid Identity. Initially, all 'internal' users are of type 'Member'. A user with a UserType attribute set to 'Member' is a user with default member-level permissions in the tenant and will likely require licensing to access resources. These Member users are generally considered employees of your organization.

		UserType property	
		Guest	**Member**
How the user authenticates	**External**	**External guest** Uses an external Azure AD account, social identity, or other external identity provider to sign in. Most external users fall into this category.	**External member** Uses an external account to authenticate but has member-level access in your organization. Common scenario in multi-tenant organizations.
	Internal	**Internal guest** Has an account in your Azure AD directory but only guest-level access in your organization. This is often a legacy guest user created before the availability of Azure AD B2B.	**Internal member** Has an account in your Azure AD directory and member-level access in your organization. Generally considered employees of your organization.

An internal user of one tenant may be invited into another tenant as an 'external' user. An external user has an external Entra ID account, social identity, or other external identity provider to sign in. In other words, an external user will authenticate somewhere outside the tenant where the external user is invited into. When external identities 'B2B' was first released, all external users were of UserType 'Guest'. A user of type 'Guest' has restricted permissions in the tenant. For example, Guest users cannot enumerate the list of all users nor groups in the tenant directory.

Several years ago, B2B was updated to flip the UserType property on users. It also began to support flipping the bit on users from internal to external. This is where the confusion sets in.

An internal user may be changed from type 'Member' to 'Guest'. In other words, you may have an internal Guest user that is likely unlicensed with guest-level permissions in the tenant. This is useful for scenarios where you provide a user account and credentials to a person that is not considered an employee of your organization (e.g. Sponsored IDs).

An external user may be changed from type 'Guest' to 'Member', giving the external user member-level permissions. This is useful for scenarios where you manage multiple tenants for your organization and need to give a user member-level permissions across all the tenants regardless of whether the user is internal or external in any given tenant. Note, there are licensing considerations for any user of type 'Member'. You can expect any Member user will require additional licenses.

Note: For scenarios where an internal user is converted into an external user, there are several considerations captured in user management section of this white paper. For example, the UPN of the user may not have the hallmark #EXT# qualifier by default (unless you change it).

Note: Most documentation for B2B will refer to an external user as a 'Guest' user. It conflates the UserType property, in a way that assumes all Guest users are external. Just keep in mind that when documentation calls out a 'Guest' user, it's assuming it's an external Guest user. This white paper will specifically use external versus internal and Member versus Guest intentionally.

Entra ID User Permissions

Guest users do not have default permissions to resources with the exception of restricted directory permissions. In other words, internal or external users of type 'Guest' have little access until entitled with permissions to resources. For example, Guest users may not enumerate the GAL. It is recommended that a strong governance policy is adopted for guests. This may include Entra ID Entitlement Management that may grant or revoke permissions intentionally.

As mentioned above, it is technically possible to change the user type to and from 'Member' <-> 'Guest' on both internal and external user accounts. This is helpful for a couple of reasons. If extranet accounts are provisioned into the Home tenant as user type 'Member', they will have default permissions above and beyond what is permissible for extranet accounts. In this case, the user type may be switched to 'Guest' to restrict default permissions within the tenant. On the other hand, complex organizations may want to have 'Member' permissions regardless of which tenant they are accessing (Home or Resource). In other words, an internal 'Member' user in a GCC High home tenant may be provisioned as an external 'Member' user in a Commercial resource tenant. In the example, Member users may enumerate the GAL facilitating collaboration with discoverability of people. This is also helpful to differentiate accounts that are truly external to the organization, as opposed to employees of the organization that has multiple tenants.

External User Attributes

By default, an external user is only stamped with a few attributes, including the PrimarySMTPAddress (E-Mail), UserPrincipalName (UPN), DisplayName and the linkage (*what's called an altSecID*) to the real internal user in another tenant. Most ad-hoc external users will only have these limited sets of attributes. However, the external users may be marked up to include any additional user attributes.

Additional attributes may include address book attributes (e.g. FirstName, LastName, Company, Title, Department, Location, etc.) and may be made visible (ShowInAddressList = True) in the Global Address List (GAL). This may be helpful in identifying the external users and putting governance and identity lifecycle management in place to handle them. This technique is popular with what is called the GALSync Solution described below.

Both external and internal users may be decorated with security-driven attributes as well. For example, it is common to define the affiliation of the user with a combination of attributes, such as the Company, that may be used with security policies. For example, a user stamped with {Company = 'Fabrikam Defense'} may be used to dynamically calculate group membership for a security group in Entra ID called 'Fabrikam Defense Users'. That security group may in turn be used to provide access to applications, Entitlement Management Access Packages, and other resources. Another example may in stamping a user with a 'US Person' extension attribute used to calculate if they are a US Person or a Non-US Person. The combination of attribute declarations may be unlimited and aligned with what's called Attribute-Based Access Control (ABAC).

Guest User Screening and Creation

While many organizations allow for ad-hoc creation and management of external Guest users, most highly regulated organizations will not. For the DIB, many will disable ad-hoc creation of external Guest user accounts and require workflows to manage the identity lifecycle. This added oversight may be burdensome, but may enforce governance policies such as stamping required attributes, Entitlement Management, security group assignment, approval chain, etc. With such discipline in place, it enables use-cases where external Guest users may access highly sensitive information, such as CUI.

Many highly regulated organizations will choose to adopt a user screening workflow to create external Guest users. This may include proofing citizenship, personnel screening, and collecting required attributes for the account. The screening may also be used to determine entitlement assignment and issuance of security policies, such as issuing virtual desktops to access extranet resources.

The workflows to screen and create external Guest users may be automated. Several organizations have developed proprietary workflows using Power Apps, Power Automate, and Azure Logic Apps. There are also third-party solutions available from Microsoft partners.

External User Licensing

Entra ID external user pricing is based on Monthly Active Users (MAU) where the first 50,000 MAUs per month are no additional cost for both Entra ID Premium Plan 1 and Plan 2 features. Technically, there is an additional cost for unlicensed external users when more than 50K access resources in a given month. However, that is very specific for Entra ID features. Most notably, Entra ID Premium Plan 1 will be used for enforcement of Conditional Access Policies, such as requiring MFA to access resources.

Note: The MAU may change. Please refer to Pricing for Entra ID External Identities for validation.

There is a huge area of confusion on Entra ID licensing for complex organizations that leverage B2B technology to access multiple organization-owned tenants. According to the Commercial Licensing Terms, employees of the organization are not considered external, and are not eligible for MAU. In other words, according to the FAQ, organization employees are always effectively internal (*even when configured as an external user*). This was instituted to prevent gaming the system by giving employees Guest user access without paying for a license (*in any tenant*). This honor system policy is intended to prohibit employees from getting tenant-wide Entra ID Premium features (e.g. Conditional Access Policies) without paying for them. But there is an oversight in the terms where the employee is in fact licensed for Entra ID Premium in their Home tenant. There should be a transitive lookup of the license in the Home tenant (*reciprocal licensing*), but there is not at the time of this writing. Ultimately, complex organizations should not have to dual-license a single employee for Entra ID Premium. That said, enterprise customers of Microsoft may need to square off on this concept during license negotiations.

Office 365 access by external users is not based on MAU. By default, any internal or external user of type 'Guest' does not have an additional cost for the collaboration suite. However, Guest users are also limited in features of Office 365. For example, external users nor users of type 'Guest' may be entitled with individual storage. This translates to these users cannot be provisioned with Exchange Online mailboxes, nor OneDrive for Business, nor a Team's SIP account for hosting meetings or originating chat or calling. Guest Users are also limited in administrative capabilities, such as the inability to create nor own Team's collaboration groups or belong to privileged administrative groups within Microsoft 365.

The exception is if the bit is flipped on external accounts to change the user type to 'Member'. External Member users still should not be provisioned with individual storage, but they may gain default permissions and pick up certain administrative functions to include creating or owning Team's collaboration groups (when properly licensed). However, there is a catch on External Member users. For certain use cases, Office 365 will begin performing a license check. Most notably, Member users that access the Teams client will require a license. The intention is for Teams to honor a license and perform a transitive lookup in the home tenant (*reciprocal licensing*). However, at the time of this writing, the cross-tenant license check only works in Commercial.

Individual Storage versus Shared data

Individual storage is per-user data for which the user is an owner of the storage container. Individual storage examples include, but not limited to:

- My Documents or OneDrive for Business site collections
- Exchange User Mailboxes
- Teams or Skype for Business SIP Accounts for 1:1 Chat, VOIP and hosting meetings

As mentioned in the previous section, external users nor any user of type 'Guest' should be entitled with individual storage. While it is technically possible to assign an M365 license with individual storage entitlements, it is not recommended and not supportable by Microsoft.

Shared data includes all content that is not kept within Individual storage. Shared data examples include, but not limited to:

- Unstructured File Storage on a File Share
- SharePoint Team Site or Document Library
- Teams or Microsoft 365 Group Files or Shared Calendar
- Exchange Shared Mailbox or Public Folder
- Published application (e.g. ERP, DevOps)

Generally speaking, all users within the Entra ID directory, including external users and users of type 'Guest' may be entitled access to shared data.

Cross Cloud External identities

To say that cross cloud external identities has been a long time in the making, is an understatement. The need for cross cloud external identities has been the number one blocker for adoption of GCC High for years. The good news is that cross cloud is here! The capabilities will roll out in phases through 2023 as it becomes generally available.

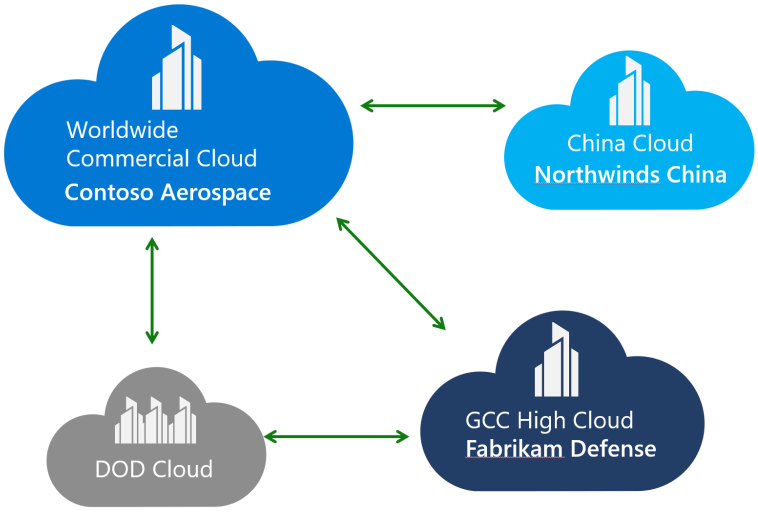


Illustration B: Cross cloud external identities

As seen in Illustration B, cross cloud external identities enable collaboration bi-directionally between Commercial and the US Sovereign Cloud with both GCC High and DOD. It also supports collaboration between Commercial and the China Sovereign Cloud. The major exception is between Sovereign Clouds. The China Sovereign Cloud may not collaborate with the US Sovereign Cloud (*for obvious reasons*).

Unlike same cloud collaboration, cross cloud must be enabled on a tenant-by-tenant basis leveraging Cross Tenant Access Settings.

For instructions, please see Configure B2B collaboration Microsoft cloud settings

Cross Tenant Access Settings

Entra ID tenants can use Cross Tenant Access Settings (CTAS) to manage how they collaborate with other Entra ID tenants. CTAS provides granular control over how external tenants collaborate coming in (*inbound access*) and how home tenant users collaborate externally (*outbound access*). CTAS also enables trusts for multi-factor authentication (MFA) and device claims (compliant claims and hybrid Entra ID joined claims) from other tenants.

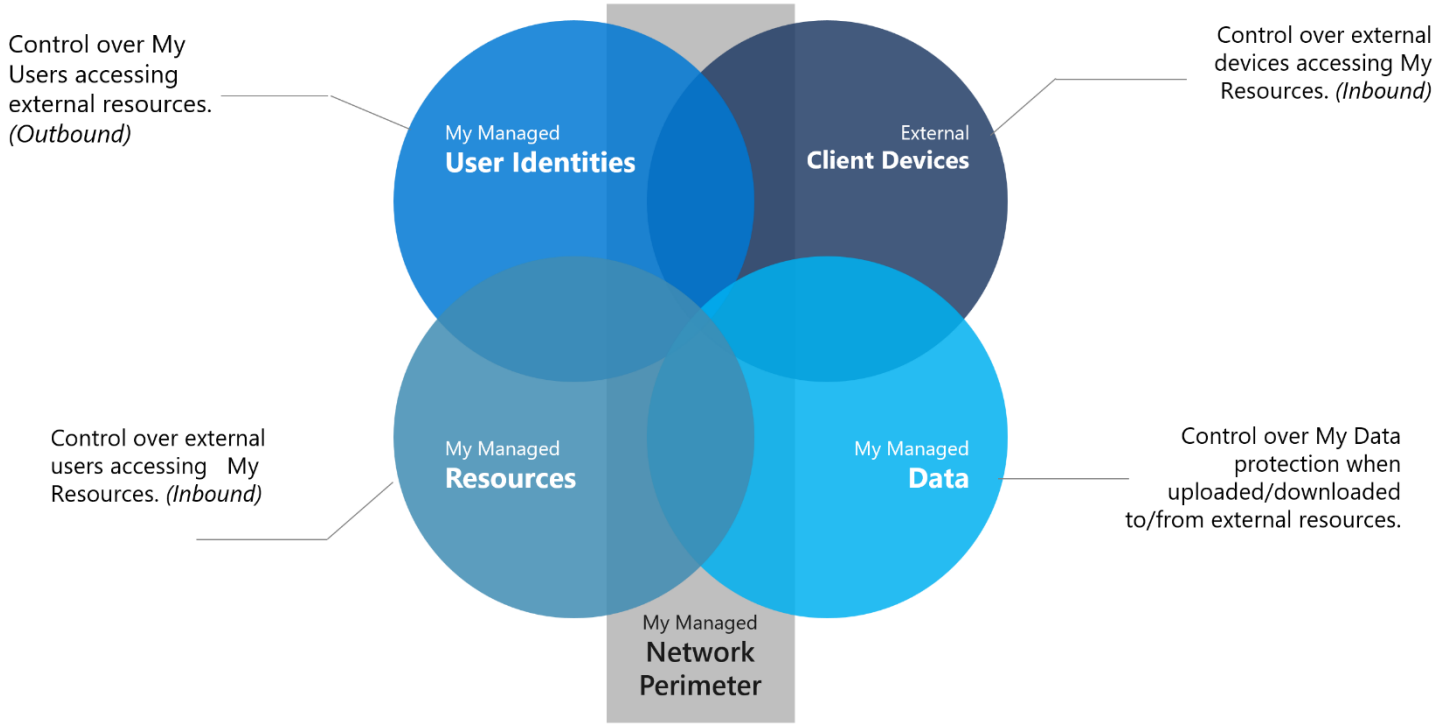


Illustration C: Cross Tenant Access Settings

Cross Tenant Access Settings govern all tenant-to-tenant interactions to and from a tenant, including:

- Allow or block access to applications and content.
- Allow native authentication between tenants and globally.
- Accept Multi-Factor Authentication (MFA).
- Accept compliant devices across tenant boundaries.
- Manage external access with inbound and outbound settings.

The following diagram shows the cross-tenant access inbound and outbound settings. The resource tenant is the tenant containing the resources to be shared. The home tenant is the tenant where the external users are managed.

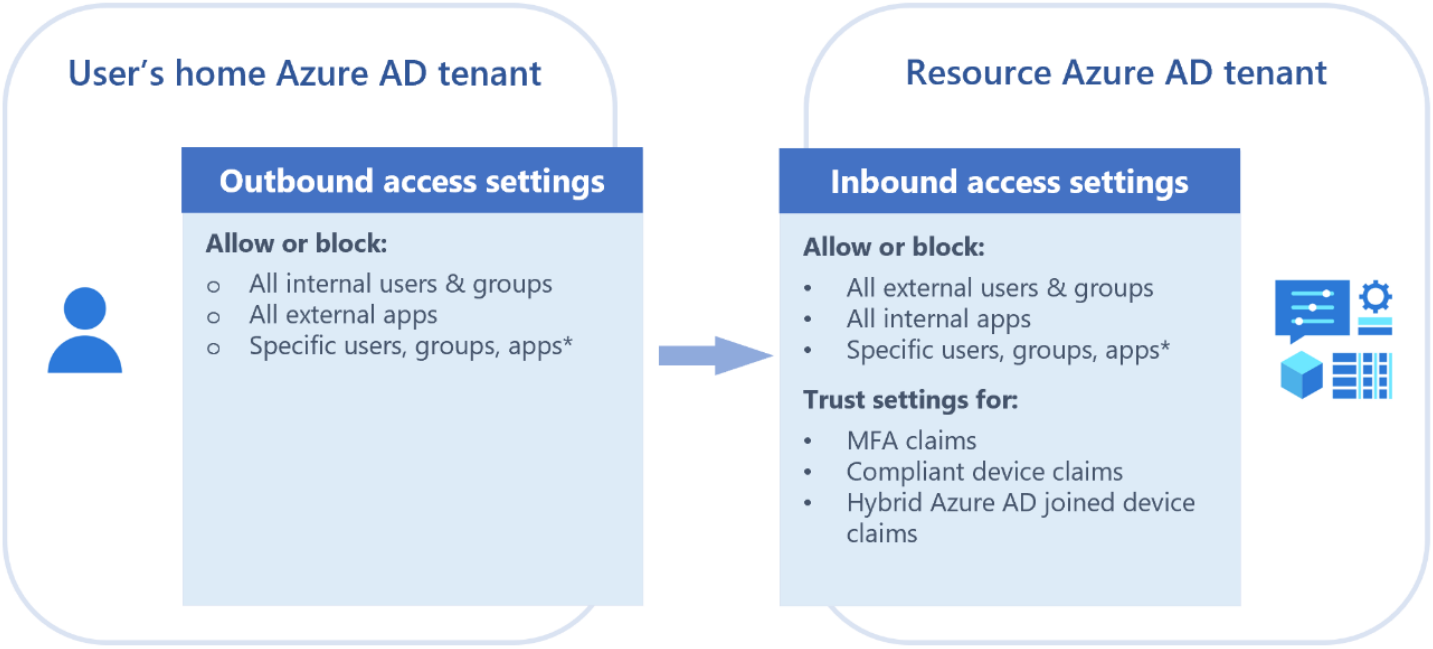


Illustration D: Cross Tenant Inbound and Outbound Settings

By default, Entra ID external identity collaboration with other tenants is enabled in the same cloud (e.g. Commercial to Commercial or Government to Government), and B2B direct connect is blocked. You must update the Inbound and Outbound settings to override the default behavior.

As mentioned above, CTAS is also required for cross cloud external identities.

For more information, please see Cross-tenant access overview

Hybrid Identity with Multiple tenants

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. This concept is known as Hybrid Identity. The most common topology for Hybrid Identity includes the pairing of Windows Server Active Directory Domain Services (AD DS) on-premises with Entra ID in the cloud.

AD DS on-premises may be set up in a hybrid configuration with multiple tenants in the cloud.

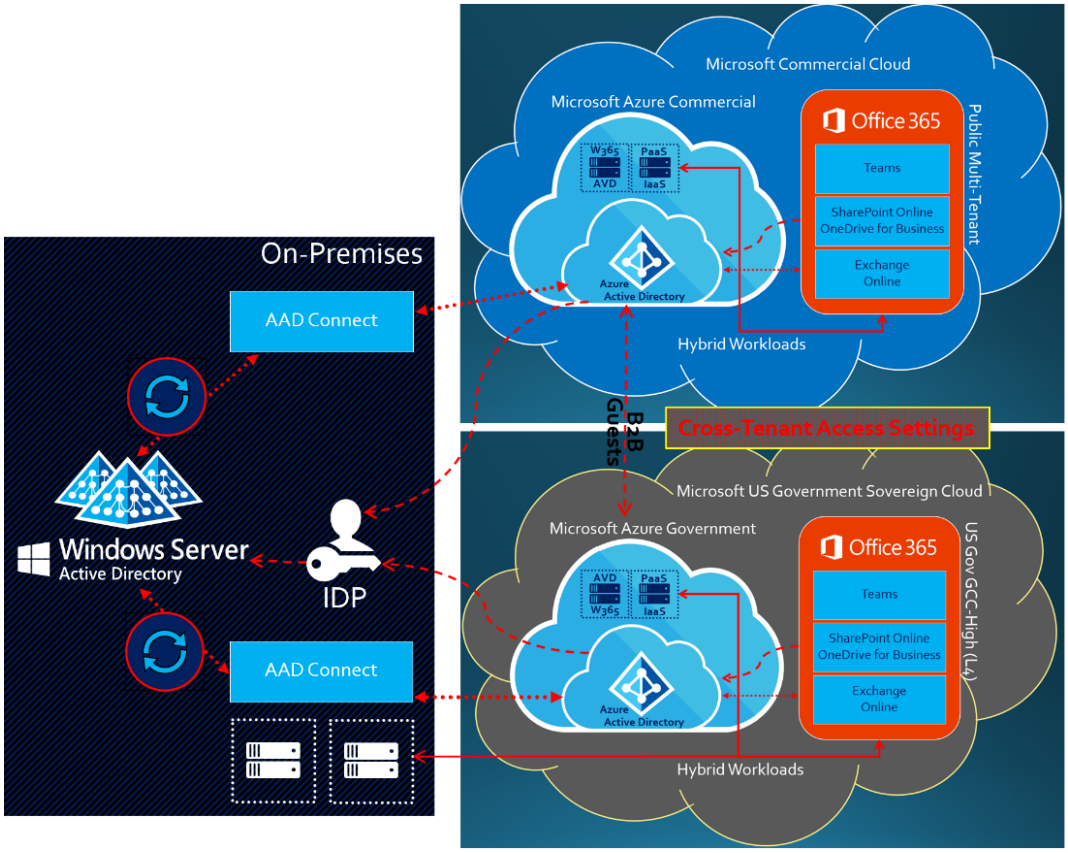


Illustration E: Microsoft Hybrid Identity with Two Tenants

In Illustration E, the on-premises environment may be a single AD Forest with a single AD Domain, or multiple forests with multiple domains. In this two-tenant topology, the single on-premises AD DS is set up in a Hybrid Identity configuration with *both tenants at the same time*. You will also observe there is a 1:1 mapping of Microsoft Entra Connect (*formerly AAD Connect*) per tenant. Each tenant must have its own instance of Entra Connect, as a single Entra Connect will not support multiple tenants.

You may find this documented in [Topologies for Entra Connect (formerly AAD Connect)]

The inherent challenge with this approach is a single identity object (User, Contact or Group) should only synchronize to a single tenant at a time. In other words, if an internal Member user (e.g. CommercialUser@ContosoAerospace.com) synchronizes to the commercial tenant, that user should be filtered from synchronizing to the government tenant as an internal user at the same time. If the User is not synchronizing to the government tenant, then it will not be visible in the GAL of the government tenant. The same applies in both directions. If an internal Member user (e.g. GCCHighUser@FabrikamDefense.us) synchronizes to the government tenant, that user should be filtered from synchronizing to the commercial tenant. The result is each tenant will have a GAL consisting of only the Users in scope for the tenant.

The GALSync Solution

The first formal Global Address List Synchronization (GALSync) solution offered by Microsoft was back in 2003 with Microsoft Identity Integration Server (MIIS). MIIS has evolved through several branding changes (e.g. ILM & FIM) and is now called Microsoft Identity Manager (MIM).

The GALSync concept is simple. For every User that appears in one tenant, that same User will appear in other tenants as either an Exchange Mail-Enabled Contact or an external user made visible in the GAL.

The traditional GALSync with Contacts is an on-premises solution. Historically, it is leveraged to support GALSync with multiple on-premises Exchange Server Organizations. The same concept applies when extending Exchange Server to the cloud with Exchange Online.

Illustration F: On-Premises GALSync with Contacts

In Illustration F, there are a few concepts to explain. First, the Users, Contacts and Groups that are in scope for the tenant are represented in the Red color scheme. For example, a Commercial User (e.g. CommercialUser@ContosoAerospace.com) may synchronize directly from AD DS on-premises mapped to a User in the cloud (*aka a Hybrid Identity enabled User*). This is the out-of-the-box behavior of Entra Connect (*formerly AAD Connect*). However, the GCC High identity is filtered from synchronizing directly. The GCC High User (e.g. GCCHighUser@FabrikamDefense.us) does not synchronize to the Commercial tenant. Alternatively, a GALSync solution will copy the GCC High User into another AD Forest and separate Exchange Organization as an Exchange Mail-Enabled Contact with the same Email address. Entra Connect will in turn import those Contacts and synchronize them to the Commercial tenant represented in the Yellow color scheme. The result is a GAL in the Commercial tenant counting the GCC High User transformed as a Contact. This GALSync solution essentially converts the User in another tenant into a Contact in this tenant.

There is one limitation to Address Book visibility when using Contacts. GALSync with Contacts will only appear in the Exchange GAL, but not elsewhere. In other words, you can see the contacts in the Outlook address list, but not in the SharePoint people picker, nor in OneDrive for Business or in Teams.

GALSync with External User Accounts

The GALSync solution with external user accounts is a cloud-based solution. The result is similar; this GALSync solution essentially converts the internal user from one tenant into a Contact in another tenant. Except in this case the Contact is an external user. The benefit of using external users as opposed to Exchange Mail-Enabled Contacts is two-fold. Like Contacts, the external user may be updated to appear in the Exchange Online GAL. Only this time, the external user is visible everywhere allowed, including in Outlook, SharePoint Online, OneDrive for Business, Teams, etc. In the Exchange world, an external user is a Mail-Enabled User that is a security principle (*aka a real user account*). Unlike Contacts, an external user may take advantage of collaboration as described earlier in this white paper.

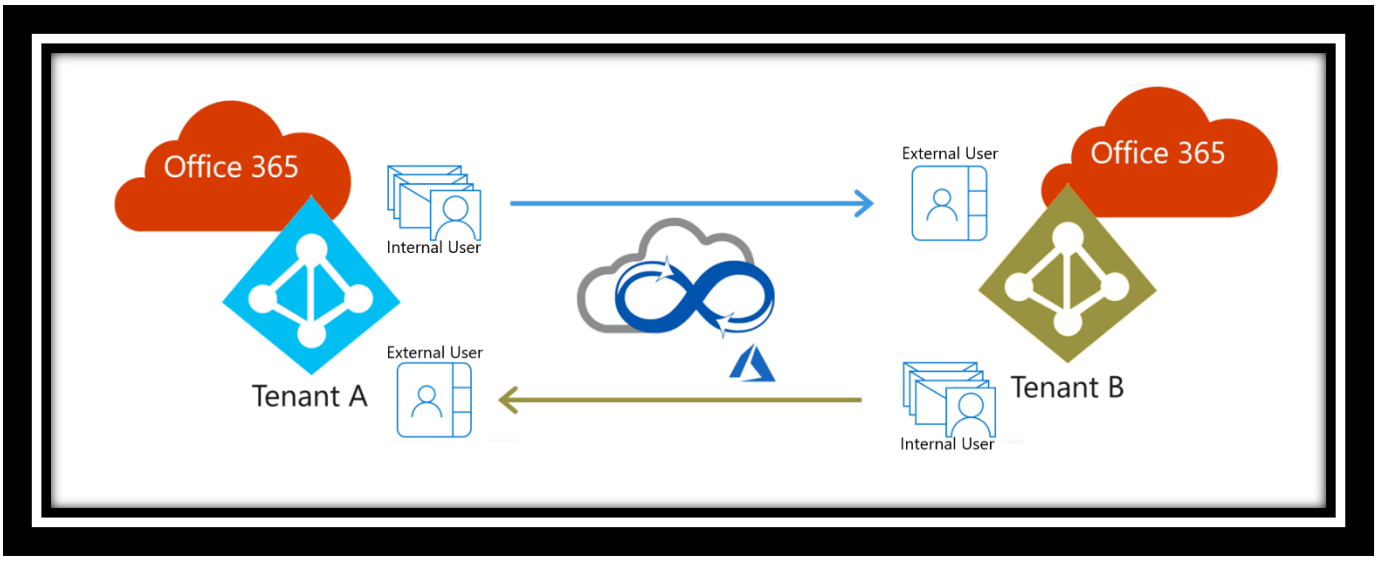


Illustration G: GALSync with external user accounts

Illustration G is a simplified view of the solution describing the tenant-to-tenant synchronization of internal users to external users.

There are multiple technical implementations for GALSync, several of which as discussed later in this white paper.

Domains in AD DS versus domains in Entra ID

There is often confusion about the difference between a domain in on-premises AD DS compared to domains registered in Entra ID. A domain in AD DS is both a physically segmented and hierarchical concept. An AD forest may have one or more AD domains. Each AD domain will have one or more domain controllers (DCs). User, group, and computer identities may be segmented between each AD domain. This is common where organizations have an AD forest for the enterprise, and another AD forest for the government environment. Or in many cases, organizations may have multiple forests or domains for autonomous business units, subsidiaries, departments, etc. Each AD forest may have one or more UserPrincipalName (UPN) suffixes registered that must be unique to the forest. The default is to align the UPN suffixes with the fully qualified domain name (FQDN) of the domains in the forest (e.g. ContosoAerospace.com or FabrikamDefense.us).

Entra ID has a virtually segmented and flat concept that is not hierarchical by nature. Entra ID does not support a concept of a domain in relation to AD DS. Alternatively, a domain in Entra ID is a registered custom domain routable in DNS that may be used for UPN suffixes, SMTP (email) address accepted domains, and SIP address resolution. For hybrid identity scenarios, the Entra ID registered custom domains align with the UPN suffixes registered in on-premises AD DS. In fact, the Entra Connect deployment wizard will check that all UPN suffixes are properly registered in Entra ID before beginning synchronization of identities.

People often conflate the definition of a domain. Keep this in mind. A user located in an on-premises AD DS domain may have a UPN suffix different than the FQDN of that domain. In fact, a user may have an arbitrary UPN suffix of any name registered in the AD forest. The only requirement is that it must be routable on DNS (e.g. no *.local UPN suffixes). An example is where the AD Domain FQDN is contoso.local, but the UPN suffix on user accounts is ContosoAerospace.com. In addition, the UPN suffix may be deployed across multiple AD domains in the same forest. As such, you can theoretically have all ContosoAerospace.com UPNs sourced from a single container in a single domain, or you can source ContosoAerospace.com UPNs from multiple containers or domains in the same forest. It's inconsequential in terms of how you source identities synchronized to Entra ID (that is flat).

Note: the blog article Microsoft US Sovereign Cloud Myth Busters - Active Directory Does Not Require Restructuring has additional information on AD domains versus Entra ID registered custom domains.

One of the largest challenges every customer large and small has encountered since Office 365 was introduced is aligning the proper UPN in on-premises AD DS with the UPN synchronized to Entra ID. It often requires you to change the AD DS UPN to match. If the UPN does not match a registered custom domain in Entra ID, it will automagically change the UPN to something arbitrary and unknown to the user (e.g. @tenantname.onmicrosoft.com). It is also highly recommended that the UPN matches the user's primary SMTP address to facilitate collaboration.

Another stumbling block is the restriction of registering DNS custom domains in Entra ID. A discrete domain (e.g. ContosoAerospace.com) may only be registered in a single tenant for cross cloud scenarios. If the domain is registered in commercial, it may not be registered in government, and vice versa. There are no exceptions. This often leads to complex organizations in the Split Tenant approach changing the UPN to match the domain registered to the government tenant (e.g. FabrikamDefense.us). See the blog article Microsoft US Sovereign Cloud Myth Busters - A Single Domain Should Not Span Multiple Tenants for more information. Many organizations that have spent years of effort consolidating domains for branding purposes tend to make this a blocker to deployment in the split tenant approach. However, the reality of what is discussed in this blog article prevails.

Entitlement Management

Entitlement Management is an identity governance feature that enables organizations to manage identity and access lifecycle at scale, by automating access request workflows, access assignments, reviews, and expiration.

Employees in organizations need access to various groups, applications, SharePoint Online sites, and Teams to perform their job. Managing this access is challenging, especially as requirements change (e.g. applications are added or users need more access rights). This scenario gets more complicated when you collaborate with outside organizations. You may not know who in the other organization needs access to your organization's resources, and they won't know what applications, groups, sites or Teams your organization is using.

Entitlement management can help you more efficiently manage access to these resources, along with support for users outside your organization.

Here are some of the capabilities of Entitlement Management:

- Control who can get access to applications, groups, SharePoint sites, and Teams with multi-stage approval, and ensure users don't retain access indefinitely through time-limited assignments and recurring access reviews.
- Give users access automatically to those resources, based on the user's properties like Company, Department and/or cost center, and remove a user's access when those properties change.
- Delegate to non-administrators the ability to create Access Packages. Access Packages contain resources that users can request, and the delegated access package managers can define policies with rules for which users can request, who must approve their access, and when access expires.
- Select connected organizations whose users can request access. When a user who isn't yet in your directory requests access, and is approved, they're automatically invited into your directory and assigned access. When their access expires, if they have no other access package assignments, their external user account in your directory can be automatically removed.
- Entitlement Management may be used to intentionally provide Guest users with permissions to resources in your tenant so that you know exactly what they have permissions to beyond the default restricted permissions in the tenant. This is an alternative to allowing for ad-hoc sharing of content virally across your tenant.

Access Packages

Entitlement Management introduces the concept of an Access Package. An Access Package is a bundle of all the resources with the access a user needs to work on a project or perform their task. Access packages are used to govern access for your employees and users external to your organization.

Here are the types of resources you can manage user's access to, with entitlement management:

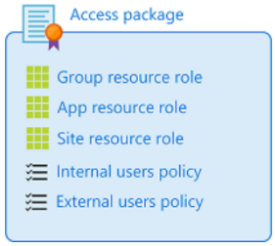
- Membership of Entra ID security groups.
- Membership of Microsoft 365 Groups and Teams.
- Assignment to Entra ID enterprise applications, including SaaS applications and custom-integrated applications that support federation/single sign-on and/or provisioning.
- Membership of SharePoint Online sites.

You can also control access to other resources that rely upon Entra ID security groups or Microsoft 365 Groups. For example:

- You can give users licenses for Microsoft 365 by using an Entra ID security group in an access package and configuring group-based licensing for that group.

- You can give users access to manage Azure resources by using an Entra ID security group in an access package and creating an Azure role assignment for that group.
- You can give users access to manage Entra ID roles by using groups assignable to Entra ID roles in an access package and assigning an Entra ID role to that group.

With an Access Package, an administrator or delegated access package manager lists the resources (groups, apps, sites, and Teams), and the roles the users need for those resources.



Access Packages also include one or more *policies*. A policy defines the rules or guardrails for assignment to the Access Package. Each policy can be used to ensure that only the appropriate users are able to have access assignments, and the access is time-limited and will expire if not renewed.

You can have policies for users to request access. In these kinds of policies, an administrator or access package manager defines:

- Either the already-existing users (typically employees or already-invited external users), or the partner organizations of external users that are eligible to request access.
- The approval process and the users that can approve or deny access.
- The duration of a user's access assignment, once approved, before the assignment expires.

You can also have policies for users to be assigned access, either by an administrator or automatically.

The following Illustration H shows an example of the different elements in entitlement management. It shows one catalog with two example access packages.

- **Access package 1** includes a single group as a resource. Access is defined with a policy that enables a set of users in the directory to request access.
- **Access package 2** includes a group, an application, and a SharePoint Online site as resources. Access is defined with two different policies. The first policy enables a set of users in the directory to request access. The second policy enables users in an external directory to request access.

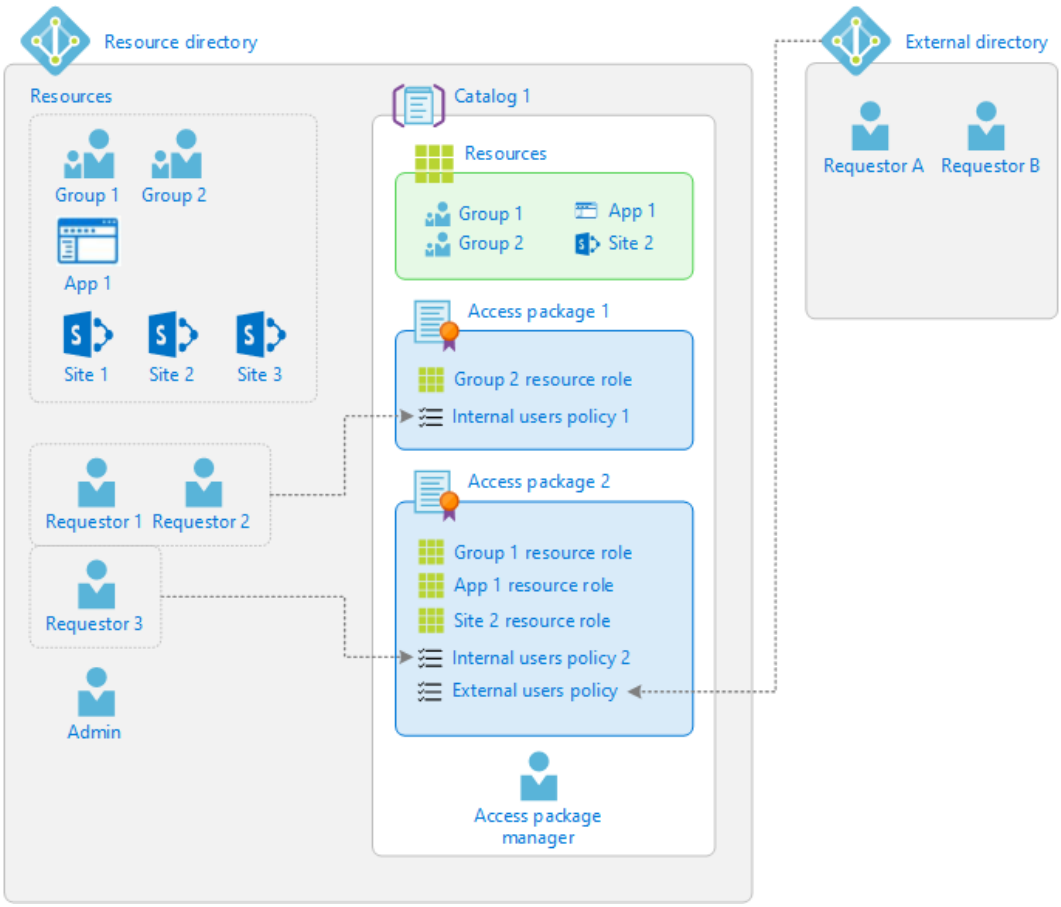
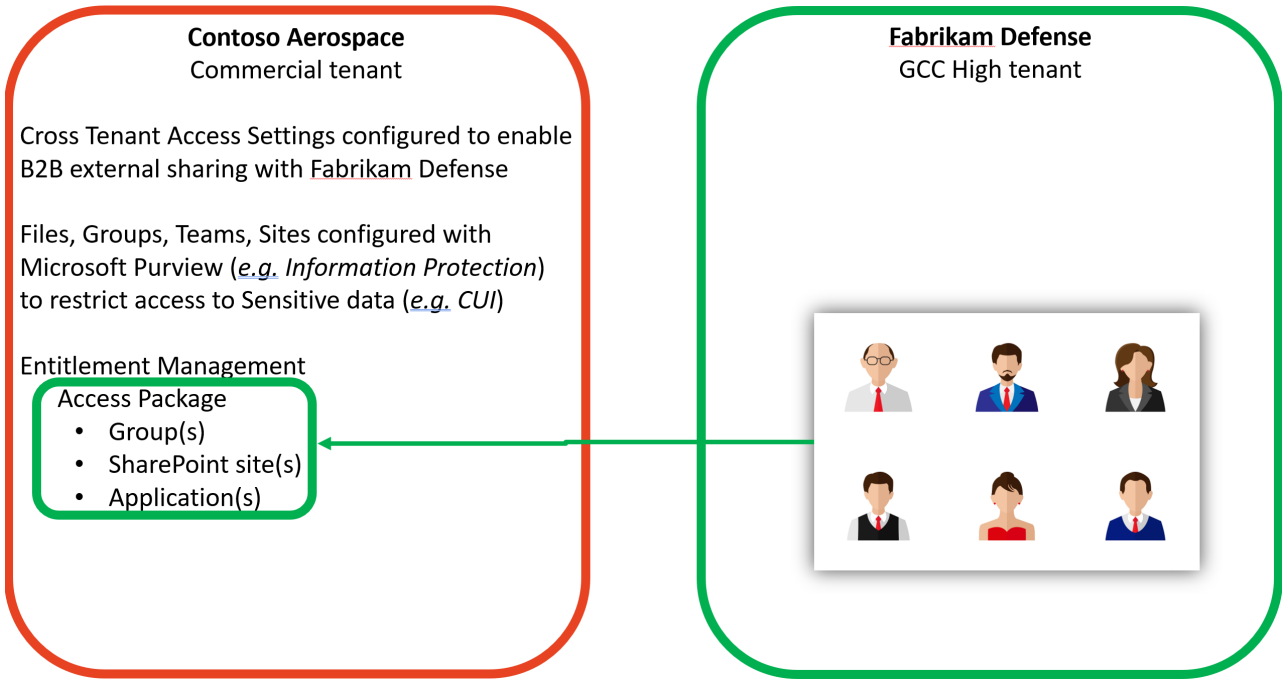


Illustration H: Entitlement Management Access Packages

In the case of managing entitlements for external user accounts, the following Illustration I demonstrates how users from a GCC High tenant may be invited into a Commercial tenant as an external user and entitled permissions with an Access Package.



For more information, please see What is Entitlement Management Access Packages?

Access Reviews

Access Reviews enable organizations to efficiently manage group memberships, access to enterprise applications, and role assignments. Users' access can be reviewed regularly to make sure only the right people have continued access.

Entra ID enables you to collaborate with users from inside your organization and with external users. Users can join groups, invite external users, connect to cloud apps, and work remotely from their work or personal burden s. The convenience of using self-service has led to a need for better access management capabilities.

- As new employees join, how do you ensure they have the access they need to be productive?
- As people move teams or leave the company, how do you make sure that their old access is removed?
- Excessive access rights can lead to compromises.
- Excessive access rights may also lead to audit findings as they indicate a lack of control over access.
- You have to proactively engage with resource owners to ensure they regularly review who has access to their resources.

Access Reviews help to mitigate these scenarios by allowing you to perform periodic reviews and remove entitlements that are no longer valid. This includes the ability to:

- Govern access to Microsoft Teams and Microsoft 365 groups.
- Govern access to critical applications.
- Reduce access risk of external users.
- Ensure that your users in privileged roles still require permissions.
- Review excessive access held by your machine accounts.
- Manage exception lists of your Conditional Access policies.

For more information, please see What are Entitlement Management Access Reviews?

Identity Reference Architecture Review

Now that you have the foundation of the Microsoft Collaboration Framework, this white paper will focus on identity reference architectures and will be broken down into two sections.

First, we will review Complex Organization Collaboration with a single organization managing multiple tenants. This includes the data enclave approach with a swivel seat scenario. We will also cover the split tenant approach where a single organization straddles multiple tenants.

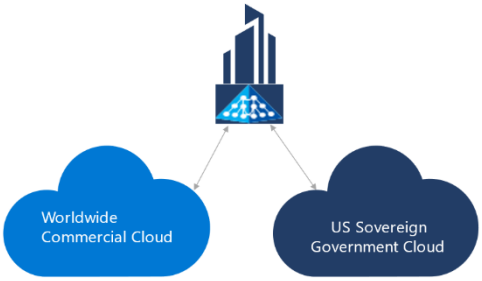
Second, we will review Trusted Partners and Extranet scenarios with external user access leveraging Entra ID external identities. This organization-to-organization sharing is in the true spirit of B2B, including:

- External sharing directly within your tenant
- Identity-only extranet
- "Meet Me" extranet enclave

- Cloud-broker managed extranet enclave

Single Organization in Multiple Clouds

As described in the section Complex Organization Collaboration, complex organizations include multi-tenant deployments spanning two or more Entra ID tenants – resulting in unique cross-tenant collaboration and management requirements. Once the DIB began deploying into the US Sovereign Cloud, it became abundantly clear collaboration was too restrictive. Many DIB straddle commercial clouds alongside government clouds. In other words, the DIB are multi-tenant organizations that have deployments straddling both commercial and government clouds. This section proposes a solution and reference architectures to collaborate "cross cloud" between cloud environments. This includes support for organizations that are either homed in commercial or in government.



Data Enclave Approach (Swivel Seat)

Virtually every complex organization starts off with a data enclave approach. Also referred to as a 'Swivel Seat', the data enclave requires individuals to work with discrete user accounts in each cloud environment. In other words, an individual has an internal Member user account in their home tenant, and another internal Member user account in the enclave tenant. The individual will have two mailboxes, two OneDrives, and two SIP accounts for Teams, referred to as individual storage. With separate user accounts, an individual may conduct enterprise business with the home tenant user account while separating duties of the enclave tenant.

The home tenant may be either commercial or government. For purposes of this section, we will assume the individual's home tenant is in commercial with an enclave in government (*the most common scenario*). By having a user account with individual storage in the government enclave, the user may isolate collaboration for the government business to include sending and receiving email with a CMMC compliant Exchange Online mailbox, hosting meetings in Teams that may include collaboration on CUI, or accessing applications that fall within the compliance boundary.

Cloud-only Data Enclave

The data enclave approach may include several architectures. Most commonly a data enclave is a cloud-only tenant with identity managed exclusively in the cloud. This contrasts with the home tenant that may be configured with hybrid identity as depicted in Illustration J below. In the commercial tenant, users are sourced from AD DS and synchronized with Entra Connect. The authentication with hybrid identity may include federation with an Identity Provider (IDP) such as Active Directory Federation Services (AD FS) or another third-party IDP. However, identity federation is not required. You may alternatively synchronize credentials to Entra ID with Entra Connect, leverage Entra Connect Pass-through Authentication, or embrace passwordless authentication with FIDO2 or Certificate-Based Authentication (CBA). CBA is also known as 'derived credentials' associated with PIV/CAC smartcards. Conversely, the cloud-only tenant for the government enclave has credentials stored exclusively in Entra ID. This may include passwords and/or passwordless authentication.

Illustration J also depicts a 'Hybrid Data Center' architecture, where hybrid workloads may be deployed both on-premises and in the cloud. An example of this may be AD DS domain controllers replicated to Virtual Machines (VMs) running in the cloud. By hosting AD DS in the cloud, it's possible to support domain services such as domain join, group policy, lightweight directory access protocol (LDAP), and Kerberos/NTLM authentication. This is especially useful to support applications that require legacy authentication (e.g. Kerberos, NTLM, LDAP, etc.) deployed to the cloud, such as in Azure Infrastructure-as-a-Service (IaaS).

Note: Entra ID may also support legacy authentication for both Hybrid Identity and cloud-only identity with Azure Active Directory Domain Services (AAD DS). You can use AAD DS without the need to deploy, manage, and patch AD DS domain controllers in the cloud.

The hybrid data center also supports Office 365 hybrid workloads, such as Exchange Online Hybrid, Hybrid OneDrive / SharePoint Online federated search, and Skype for Business Hybrid. Office 365 hybrid workloads enable users to be split between on-premises and the cloud, such as during a migration. However, with the cloud-only enclave, all Office 365 workloads are ultimately green field with users provisioned new accounts.

For both hybrid data center and for the could-only enclave, application workloads and infrastructure may be deployed to Azure. Likely the most common is Azure Virtual Desktop (AVD) and Windows 365 in support of virtual desktop environments (VDI). It is also popular to deploy Product Lifecycle Management (PLM) solutions on IaaS, including CAD & CAM products for modeling and simulation. The list goes on to include Enterprise Resource Planning (ERP), and Customer Relationship Management (CRM), security solutions deployed within the compliance boundary, and more.

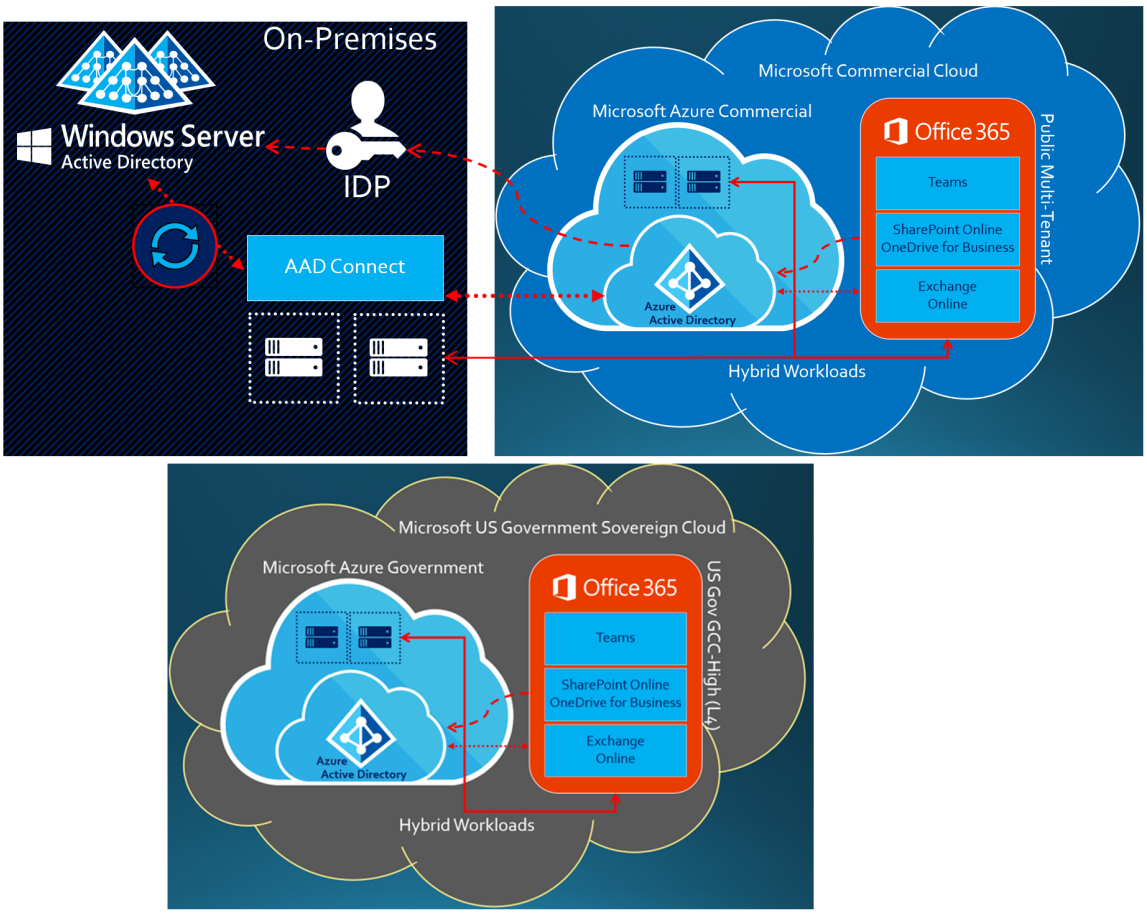


Illustration J: Data enclave with cloud-only identity

Hybrid Data Enclave

The data enclave approach may also support hybrid configurations for both commercial and government. This is common for organizations that already operate data enclaves on-premises. In Illustration K below, the government environment is virtually segmented from the commercial environment. This includes separate AD DS forests each setup in a hybrid identity configuration with their respective tenants.

For organizations that start off deploying a data enclave with hybrid identity commonly migrate the enclave to cloud-only over time, or switch to a split tenant approach discussed in the next section.

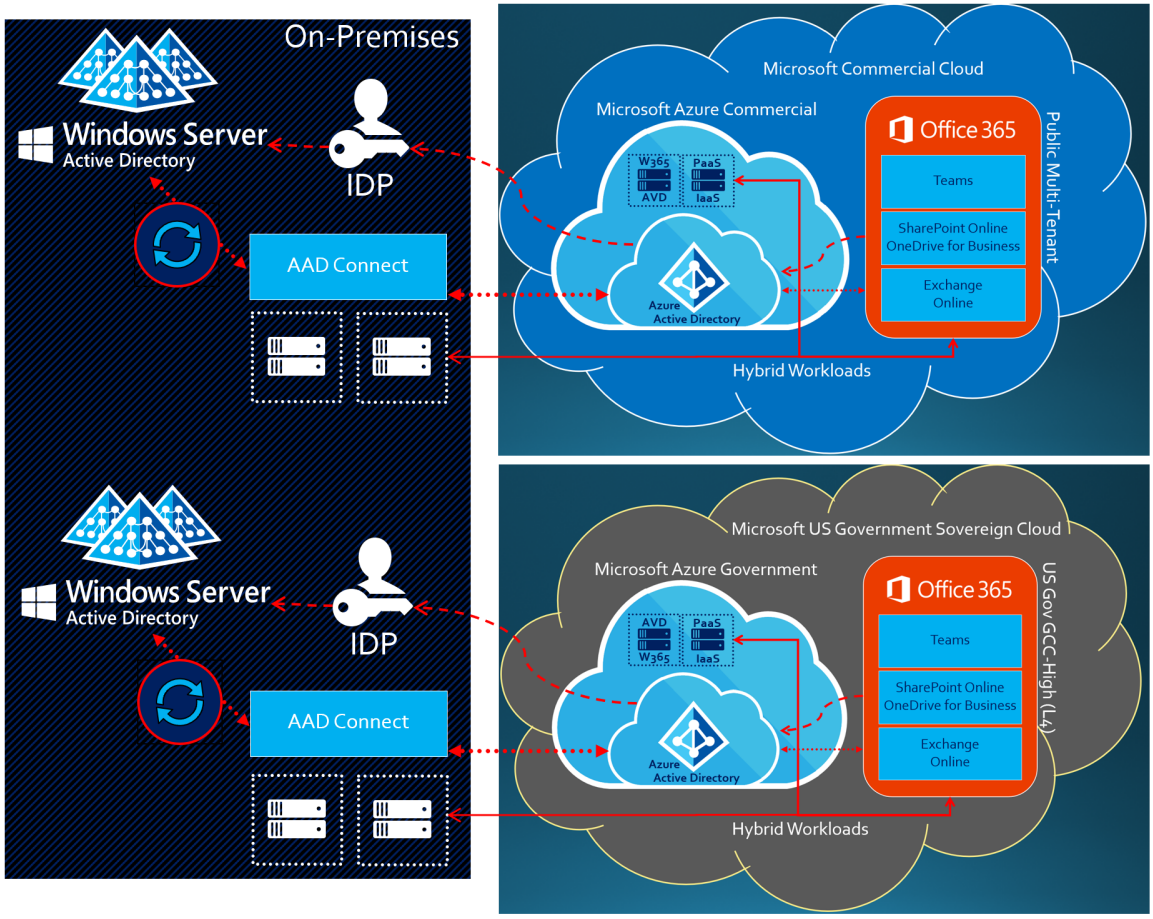


Illustration K: Data enclave with hybrid identity

Considerations for the data enclave approach

Many complex organizations contemplate the implementation of a data enclave approach where employees of the organization are deployed to an enclave tenant with shared data only. The idea is the user will only have individual storage (e.g. Mailbox, OneDrive, SIP) in the home tenant, while enabling access to shared data in the enclave tenant with an external user account. In cases where the home tenant resides in commercial and the enclave is in government, this is ill-advised and not recommended as a reference architecture for complex organizations. By having individual data exclusively in commercial, it is too high risk for data spillage of CUI into the non-compliant environment. Many organizations may demand that their users do not put CUI in their individual storage, such as not sending email that contains CUI. The truth is people make mistakes, or error for sake of convenience. But most notably, people outside your organization may send you CUI assuming you are compliant to handle it. For this reason, organizations that started off with enclaves with shared data only end up reactively responding to incidents with data spillage remediation in commercial to the point they change over to a swivel seat or split tenant approach. We will re-approach this topic in the next section on organization-to-organization sharing.

An additional rationale for leveraging a swivel seat is to control the compliance boundary and facilitate assessments, such as for Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) or for the Cybersecurity Maturity Model Certification (CMMC). As of the time of this white paper, there are multiple precedents set for organizations scoring a

110 on DIBCAC High assessments and joint-surveillance assessments with CMMC Third-Party Assessment Organizations (C3PAO) leveraging the data enclave swivel seat approach. Many of the C3PAOs themselves passed their DIBCAC High assessments using this architecture.

For more information on considerations for the compliance boundaries, see Compliance boundaries later in this white paper.

Several of the advantages of the data enclave approach include:

- **Quickest to deploy**. Greenfields tenants are always the fastest path to production. In addition, Microsoft boutique partners specializing in the DIB and CMMC have reference implementations to deploy data enclaves. This may also include managed services (MSP).
- **Less complexity**. This is especially true for cloud-only data enclaves.
- **Potentially Less cost**. Debatable, but it may be less cost than for split tenant depending on the level of complexity.
- **Enablement for migration**. Organizations that intend to deploy a split tenant approach typically begin with a swivel seat and subsequently migrate users into the data enclave (*effectively becoming split tenant*).
- **Clean Compliance boundaries**. Virtually segmenting the government data enclave to isolate CUI may assist in demonstrating compliance and passing DIBCAC/CMMC assessments.

Now for the detractors of the data enclave approach:

- **Potentially more cost / dual licensing**. Individuals that have multiple internal user accounts in multiple tenants require a license for each account. Most DIB underestimate how many users will need access to the data enclave, causing the duplication of licenses to burden the organization. No organization desires to pay for two or more licenses for any given individual.
- **Operational overhead of managing multiple tenants**. This cost is often underestimated, especially for the cost of labor and/or managed services. For this reason, organizations may choose to "go all in" to a single tenant model in government to reduce complexity and improve collaboration.
- **Potential for spill into the non-compliant commercial tenant**. Users will always prefer and gravitate to their commercial user account where it's easier to perform their work. This is especially true when their physical endpoints are paired with the commercial environment. Not to mention, the government data enclave is much more restrictive, resulting in users bypassing data protection controls by using their commercial user account.
- **Poor end-user experience**. This is often the death of the data enclave. Users absolutely loathe having to swivel seat. This is especially true if the user is forced to access the data enclave via a virtual desktop or separate set of endpoint devices. Regardless, end-users must be trained to use the data enclave appropriately and to promote the use of the proper account in collaboration with their co-workers and partners. If their collaborators continue to use the commercial account, it defeats the purpose of having the enclave account.
- **Multiple endpoints required**. See Protecting the boundary with multiple endpoints.

DIB often ask the question, "*Do data enclaves really work*?" Short answer is, yes for the specific purpose intended. However, mileage may vary in the grand scheme depending on whom you talk to, and what evolution they are in with their deployment. An observation reviewing over six years of deployments for data enclaves in government concludes that many DIB ultimately gravitate towards the split tenant approach over time, or simply "*go all in*" to a single tenant in government.

Split Tenant Approach (Migrate)

As mentioned in the previous section, complex organizations that deploy into both commercial and government clouds often gravitate to a split tenant approach. This architecture accommodates organizations that straddle multiple tenants where users are deployed exclusively in one tenant or the other. In other words, employee user populations are bifurcated and split between the tenants in such a manner that an individual has a single internal Member user in only one tenant. Microsoft highly recommends the split tenant approach, especially for organizations that cannot consolidate into a single government tenant.

Split Tenant with Hybrid Identity

There are several core concepts with the split tenant approach, beginning with hybrid identity. Hybrid identity sources users, groups, and computer identities from the on-premises AD DS. In Illustration L below, the AD DS is depicted as "Windows Server Active Directory". The topology for AD DS is extremely flexible. It may be a single forest with a single domain, or it may be multiple forests with multiple domains. For cases where there are multiple forests in scope, it may not require forest trusts. An example includes having an AD forest for the enterprise, and another independent AD forest for the government environment. Or in many cases, organizations may have multiple forests or domains for autonomous business units, subsidiaries, departments, etc. It's inconsequential, as the hybrid identity may aggregate identities from all AD DS forests and domains in scope of the solution. See Domains in AD DS verses domains in Entra ID earlier in this white paper for more information.

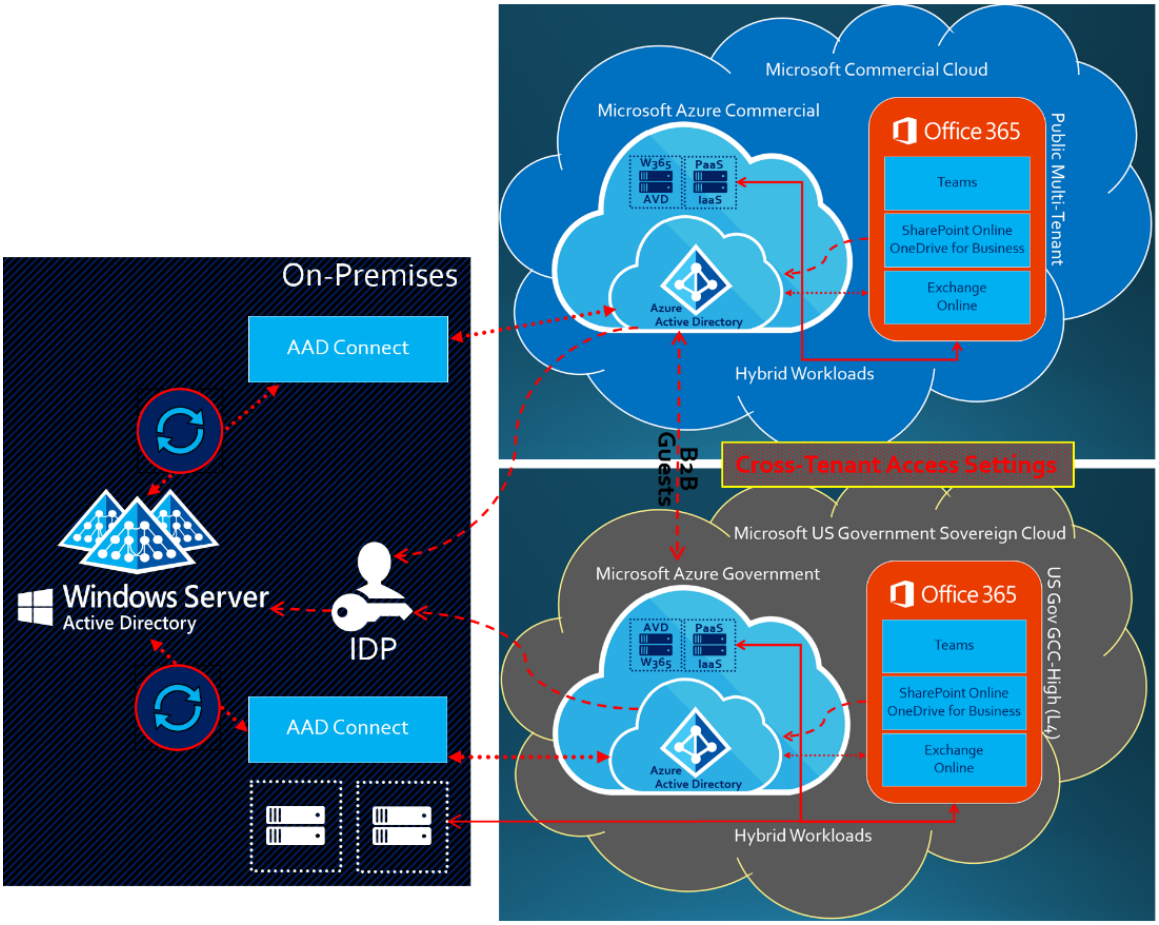


Illustration L: Split tenant with hybrid identity

For each tenant, there is a separate Entra Connect instance and configuration. The Entra Connect wired up to the commercial tenant is scoped to only synchronize internal Member user accounts that are homed and licensed in

commercial. Conversely, the Entra Connect paired with the government tenant is scoped to only synchronize internal Member user accounts that are homed and licensed in government. The user populations are fully bifurcated in such a manner that a single user in on-premises AD DS will only sync as an internal Member user to one and only one tenant.

As mentioned in the section Hybrid Identity with Multiple tenants, if an internal Member user (e.g. CommercialUser@ContosoAerospace.com) synchronizes to the commercial tenant only, it will not be visible in the GAL of the government tenant. The same applies in both directions. If an internal Member user (e.g. GCCHighUser@FabrikamDefense.us) synchronizes to the government tenant, that user will not be visible in the GAL of the commercial tenant. The result is each tenant will have a GAL consisting of only the users in scope for the tenant.

Now enter the solution for GALSync with B2B External User Accounts defined earlier in this white paper. It results in a mesh synchronization of all identities in all tenants that will fully populate the GAL in every tenant (*or as desired*). It has the added benefit of provisioning external Member users in resource tenants that allows Entra ID external identities across the tenants.

As described in the section Cross Tenant Access Settings, CTAS is currently a requirement for external identities to function in cross cloud scenarios. You may observe this in Illustration L with CTAS existing between the two tenants in a cross cloud configuration.

As described in the previous section, Illustration L depicts a "Hybrid Data Center" concept in the split tenant architecture, where hybrid workloads may be deployed both on-premises and in the cloud. An example of this may be:

- Azure Virtual Desktop (AVD) and Windows 365 in support of virtual desktop environments (VDI).
- AD DS domain controllers replicated to Virtual Machines (VMs) running in the cloud.
- Office 365 hybrid workloads with support for multiple deployments on-premises paired with multiple tenants in the cloud.
    - Exchange Online Hybrid Configuration Wizard supports multiple Exchange Server Organizations on-premises paired with multiple Exchange Online tenants in the cloud. It is an advanced implementation to support Exchange federation (e.g. Free/Busy Information Sharing) and mailbox migrations to multiple tenants and highly recommended to engage with a consulting services organization experienced with these types of migrations.
    - Hybrid OneDrive / SharePoint Online federated search segmented to the user populations homed in their respective tenants.
    - Skype for Business Hybrid to support federation with Teams in the cloud (e.g. presence and chat) in a full mesh.
- Product Lifecycle Management (PLM) solutions on IaaS, including CAD & CAM products for modeling and simulation.
- Enterprise Resource Planning (ERP) and Customer Relationship Management (CRM).
- Security solutions deployed within the compliance boundary.

Split tenant with on-premises hybrid

Another representation of the split tenant architecture is depicted in Illustration M below. This differentiates between various compliance regimes to include:

- **Commercial** cloud configured with Microsoft 365 Multi-Geo and multiple Azure Regions worldwide, including support for:
    - Data residency by Geo/Region (e.g. US, UK, FR, AU, etc.).
    - Regional regulations (e.g. EU Model Clauses, UK Official, etc.).

- Ubiquitous collaboration worldwide, such as In-Cloud external identities within commercial and across to government.
- Hybrid configurations to on-premises data centers.

- **Government** cloud including:
  - Data sovereignty in the US.
  - US regulations (e.g. CMMC, ITAR, EAR, etc.).
  - Restricted collaboration worldwide, such as In-Cloud external identities within government and across to commercial.
  - Hybrid configurations to on-premises data centers.
- **On-Premises Hybrid** including:
  - Data sovereignty in regions not supported in the cloud.
  - Regional regulations (e.g. export controls for CA Controlled Goods, UK Official Sensitive, etc.).
  - Collaboration based on legacy technologies that are not cloud-enabled.
  - Hybrid configurations to both commercial and government clouds.

The primary addition to this Illustration M includes the concept of the on-premises hybrid for data regulated by regional regulations that may not be suitable for the cloud. For example, export controls outside the US are likely forbidden from storage within a public cloud. In such cases, you may have no choice but to keep that data on-premises.

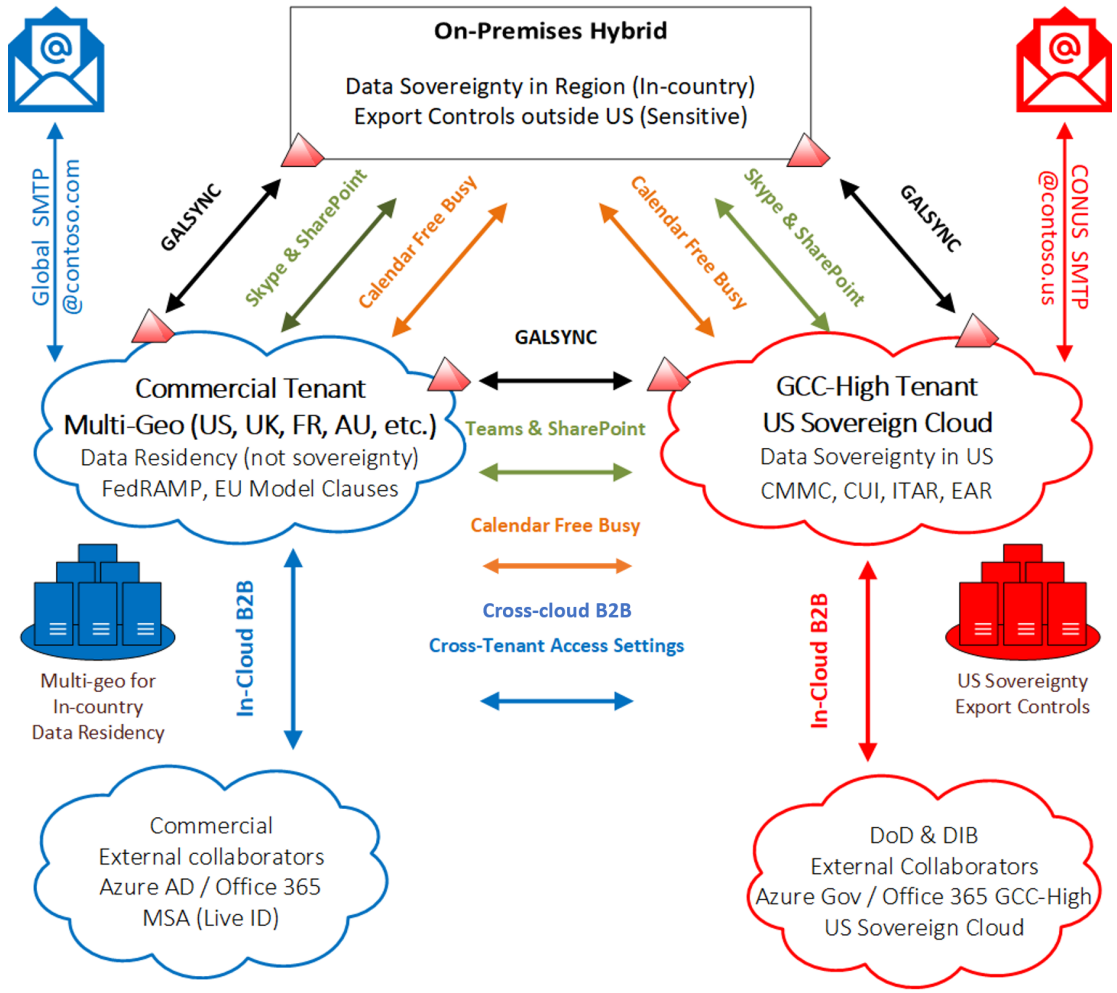


Illustration M: Split tenant with on-premises hybrid

This illustration also displays collaboration modalities, to include:

- GALSync for populating the address lists, where all identity is sourced from on-premises AD DS.
- Skype for Business and Teams federation (e.g. presence, chat, VOIP, etc.).
- SharePoint document sharing and federated search.
- Exchange federation (e.g. calendar free/busy).
- Entra ID external identities.
- Discrete Domains, such as for SMTP mail flow.

There are many permutations for this trifecta that are outside the scope of this white paper, such as options for non-US user populations. A discussion on how a US-based company approaches foreign subsidiaries and user populations deserves a white paper of its own.

Reference Architecture Considerations

Homed in commercial versus government

Finding the line of demarcation in your user populations is both an opportunity and challenge. Few organizations have the luxury of having a discrete line of demarcation determining what users are destined to be homed in commercial versus government.

There is not a hard rule that works for every organization. However, it's generally best to home your organization's enterprise services on either one side or the other. This will be the default home for all internal Member user accounts for the organization. Then you may have a decision matrix for exceptions that will either swivel seat the user (Data enclave approach) or re-home a user in the other cloud (Split Tenant approach).

Before we get into the exceptions, let's define what it means to have an "*enterprise*" home in a single tenant:

- Primary company branding (e.g. brand.com)
- Home for the C-Suite
- Enterprise-wide Information Systems
- Human Resources Department
- Legal Department
- Training
- Lunch room menu's… *etc*.

Ultimately, every individual in the organization will need to access the enterprise home tenant. This concept is often lost for many organizations that are first evaluating their options. It's also the reason why these reference architecture approaches are critical in deciding on data enclave versus split tenant versus "*Going All In*".

As an example, let's assume the enterprise home for the organization is commercial. Examples include:

- Predominately commercially-focused businesses (>50% of revenue)
- Organizations with headquarters outside the US aka FOCI (Foreign Ownership, Control, or Influence)
- Organizations with significant non-US user populations (>50% of employees)

Exceptions that may shift a user into the government cloud may include:

- Data handling for:

    - Controlled Unclassified Information (CUI)
    - Covered Defense Information (CDI)
    - Export-controlled information
    - Protected Critical Infrastructure Information (PCII)
    - Naval Nuclear Propulsion Information (NNPI)
    - Any data with US sovereignty requirements
- Subject to US regulations (e.g. DFARS 7012, CMMC, ITAR, EAR, etc.).
- Subject to competing jurisdictions. This is common for non-US organizations that are homed in commercial regions outside the US. These FOCI may need to re-home an entire US subsidiary in government to establish a cleaner line of demarcation for working within the US market.
- Employed by a US subsidiary, business unit or department where the above may be true.

A word of wisdom in regard to selecting commercial as the enterprise home. Make careful consideration with the decision based primarily on the cost of Microsoft commercial licensing compared to government. There is a hard reality and precedent set for organizations that figured out they were in the "*wrong*" cloud and faced with dual-licensing costs and very disruptive migrations shifting over to the government cloud. In some cases, that migration happened twice… from commercial to GCC and then to GCC High (government). At the end of the day, this is a risk decision for you to make.

Now let's flip the enterprise home over to government. Examples of organizations include:

- Predominately US government or defense-focused businesses (>50% of revenue).
- Manufacturing Companies with mixed-use products. Many manufacturing companies have an extremely difficult time defining the line of demarcation for users as they contribute to product development and operations subject to US regulations.
- Critical Infrastructure for the U.S.
- Desire to operate at the higher watermark for compliance. This measure of risk reduction ensures that if there is a spill into the enterprise environment, it will at least be contained in relation to US regulations.

Exceptions that may shift a user into the commercial cloud may include:

- Subject to competing jurisdictions. If a user has data residency requirements outside the US, it may be incompatible with the government cloud that is by definition sovereign to the US.
  Note: many non-US regulatory bodies are friendly to data storage in the US as compared to commercial cloud offerings that are global, even if it supports data residency in region. At the end of the day, commercial has global networks and follow-the-sun support personnel. In other words, many countries may be suitable for the government cloud.
- Subject to enterprise governance. Some organizations have a policy that commercial or non-US business is not conducted in the government tenant, even though the users will still need access for enterprise operations (e.g. HR, training, etc.).
- Network latency. While this concern has lessened as Microsoft has networks with global reach, it is still a concern in certain regions where connectivity back to the US is degraded.
- Employed by a subsidiary, business unit or department where the above may be true.

Although not as common, there are organizations that have clean lines of demarcation. This may include an organization with multiple autonomous business units or subsidiaries that do not overlap and have discrete enterprise services that neatly align with either commercial or government. The most common example of this is for holding companies. In this

case the "Organization" or "Enterprise" is at the subsidiary boundary. For each subsidiary in a holding company, the above considerations for defining the home will reside within the subsidiary.

For many organizations, the complexity of straddling multiple cloud environments is untenable. In this case, the default rule of Standard Organization Collaboration may be to simply "*go all in*" to a single tenant model within government.

Data enclave versus "Going All In"

Richard Wakeman from Microsoft has a blog article called The Microsoft 365 Government (GCC High) Conundrum - DIB Data Enclave vs Going All In. In this article, he describes a maturity evolution where organizations progress from the Data enclave approach (Swivel Seat) to the Split Tenant approach (Migrate) and finally to "*Going All In*" to the government cloud.

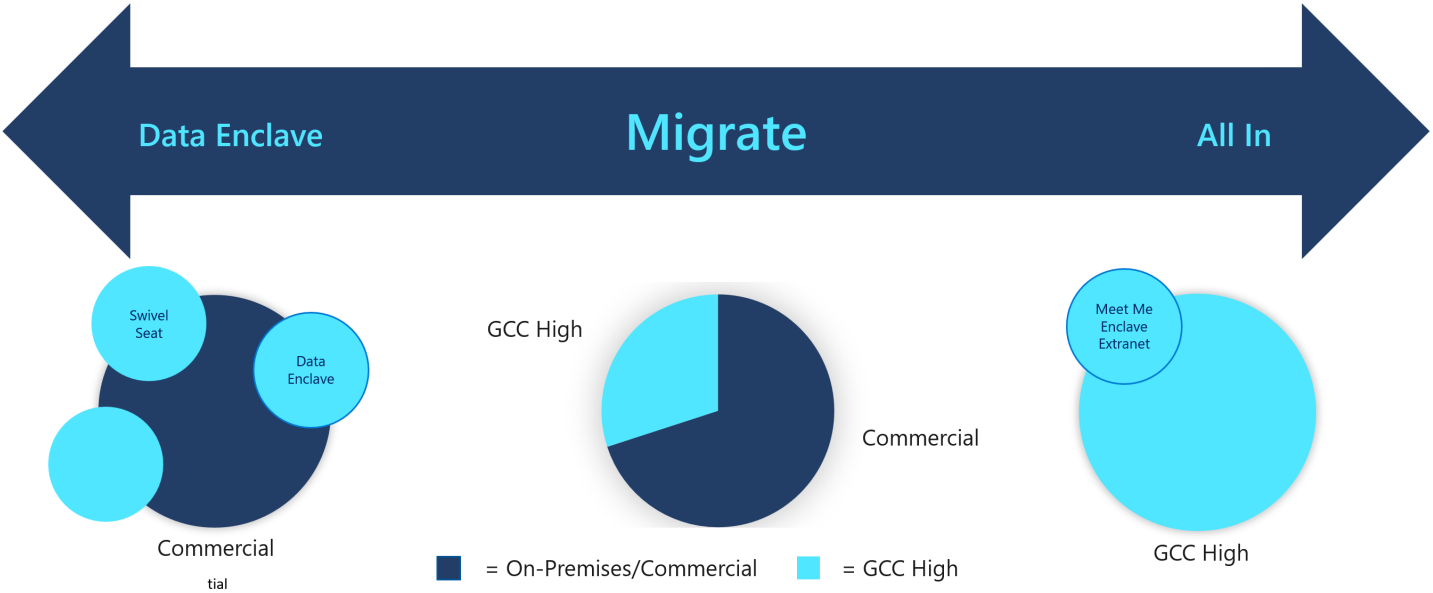


Illustration N: Data enclave versus "Going All In"

Most organizations begin by setting up a data enclave. Over time, the detractors of working with the data enclave force organizations to reconsider how they approach deployments in the government cloud. This may begin with end-users demanding they have an improved user experience, such as re-homing their endpoints (e.g. Laptop & mobile devices) within the government tenant, or to stop the swivel seat altogether. Then begins the re-homing and migration of the users into government with the Split Tenant approach. In Illustration N above, this is a shift from left to right with split tenant displayed in the middle. For those organizations that do not have a clean line of demarcation as described in the previous section, it subsequently results in more and more users having to either swivel seat into government, or force frequent user migrations from commercial to government. This may persist over a long duration to the point where the organization comes to the realization they will be better off "*Going All In*" to government with a single tenant.

This bodes the question if you may short-circuit the evolution and decide to go all in right out of the starting gate? This may be wise in the following circumstances:

- The organization is an SMB with <500 users. Even with the higher cost of the government cloud, the cost of dual-licensing and complexity having to straddle multiple tenants with a degraded user experience is sub-par.
- If there is no clean line of demarcation in the user population. Many organizations mistakenly believe they may save cost by homing in commercial. However, if they gradually need to give user accounts in government, it may actually cost more down the road when they are dual-licensing users that were intended to be in commercial (only).

- There are no competing jurisdictions that would force users into commercial.
- Desire to operate at the higher watermark for compliance. This measure of risk reduction ensures that if there is a spill into the enterprise environment, it will at least be contained in relation to US regulations.

A common misconception with the government cloud is that only US Persons are allowed into the government tenant, that would prohibit the organization from "*Going All In*" with a single tenant. Please see the section Is a US persons-only tenant required? for rationale.

Business-to-Business Collaboration

Entra ID external identities were originally established for business-to-business (B2B) collaboration scenarios. As B2B evolved and embraced additional capabilities of Azure and single organization scenarios as described in previous sections, Entra ID external identities took on a life of its own. The following section on external sharing is aligned with the original vision of B2B Collaboration.

B2B collaboration is a feature within Entra ID external identities empowering you to invite external Guest users to collaborate with your organization. With B2B collaboration, you can securely share your organization's applications and services with external partners, while maintaining control over your enterprise data.

For more information, see Entra ID B2B collaboration overview

External access directly within your tenant

The default architecture for B2B collaboration includes external access directly within a tenant.

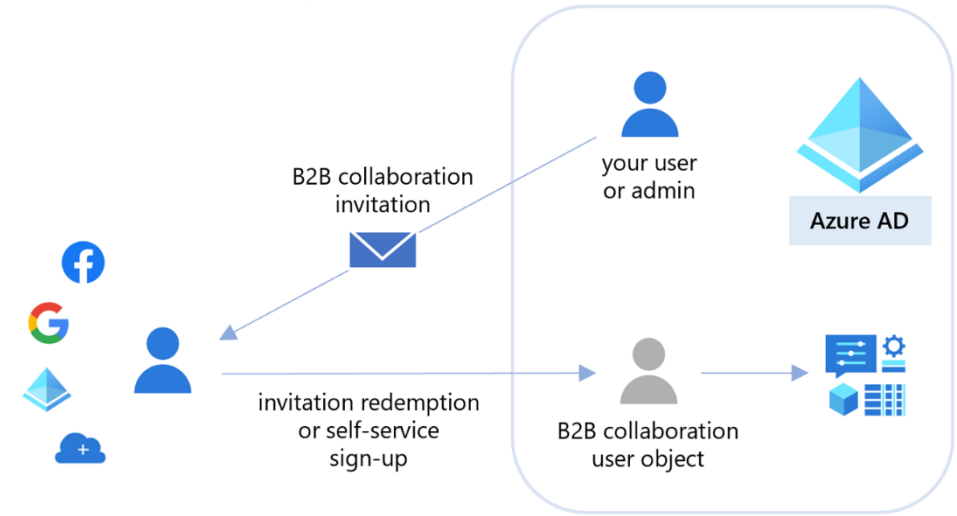


Illustration O: B2B Collaboration

An invitation and redemption process allows your partners to use their own credentials to access your organization's resources directly within the tenant. Once the external user redeems their invitation, they're represented in your Entra ID directory as an external Guest user account. The user type for these B2B collaboration users is typically set to "Guest" to indicate they are not employees of your organization.

Previous sections of this document focused exclusively on Entra ID external identities in support of internal Member user accounts that exist in some other Entra ID tenant outside your own. While that is valid for the Single organization in

multiple clouds architectures, it's not a hard requirement for B2B collaboration, as Entra ID supports multiple identity providers:

- One-time passcode (OTP) to support email-based authentication (on by default)
- Microsoft account (MSA) consumer identities
- Google account consumer identities
- Facebook consumer identities
- SAML/WS-Fed (Direct Federation) enterprise identities (e.g. with AD FS, OKTA, Ping Federate, etc.)

You should carefully review your options for what identity providers are permitted. Arguably, if you enforce Entra ID conditional access policies to protect your data (e.g. enforce MFA), it may be irrelevant how a user performs their first form of authentication. This may be especially helpful for partnering with the SMB while enforcing MFA from your tenant. Regardless, please consider the Guest User Screening and Creation section earlier in this white paper.

Identity-only Extranet

The concept of the "identity-only extranet" tenant originates before the ability to flip the user type on internal accounts from "Member" to "Guest". If an internal user has a type of "Member", it requires licensing and has all the default member permissions as described in Entra ID User Permissions. For those organizations managing user accounts and credentials in their enterprise directory for non-employee user populations (e.g. extranet users), this is undesirable. Now that you may leverage an internal Guest user account, the architecture has less utility in that respect. However, the identity-only extranet is in use and still relevant as it resembles an extranet directory. Extranet directory benefits include:

- Hosting an autonomous directory with "Sponsored IDs"
- Modelling a legacy DMZ approach to having a separate extranet directory
- Enables isolation of identity lifecycle management to a separate tenant
- May be leveraged in a long-term transition to true external identities

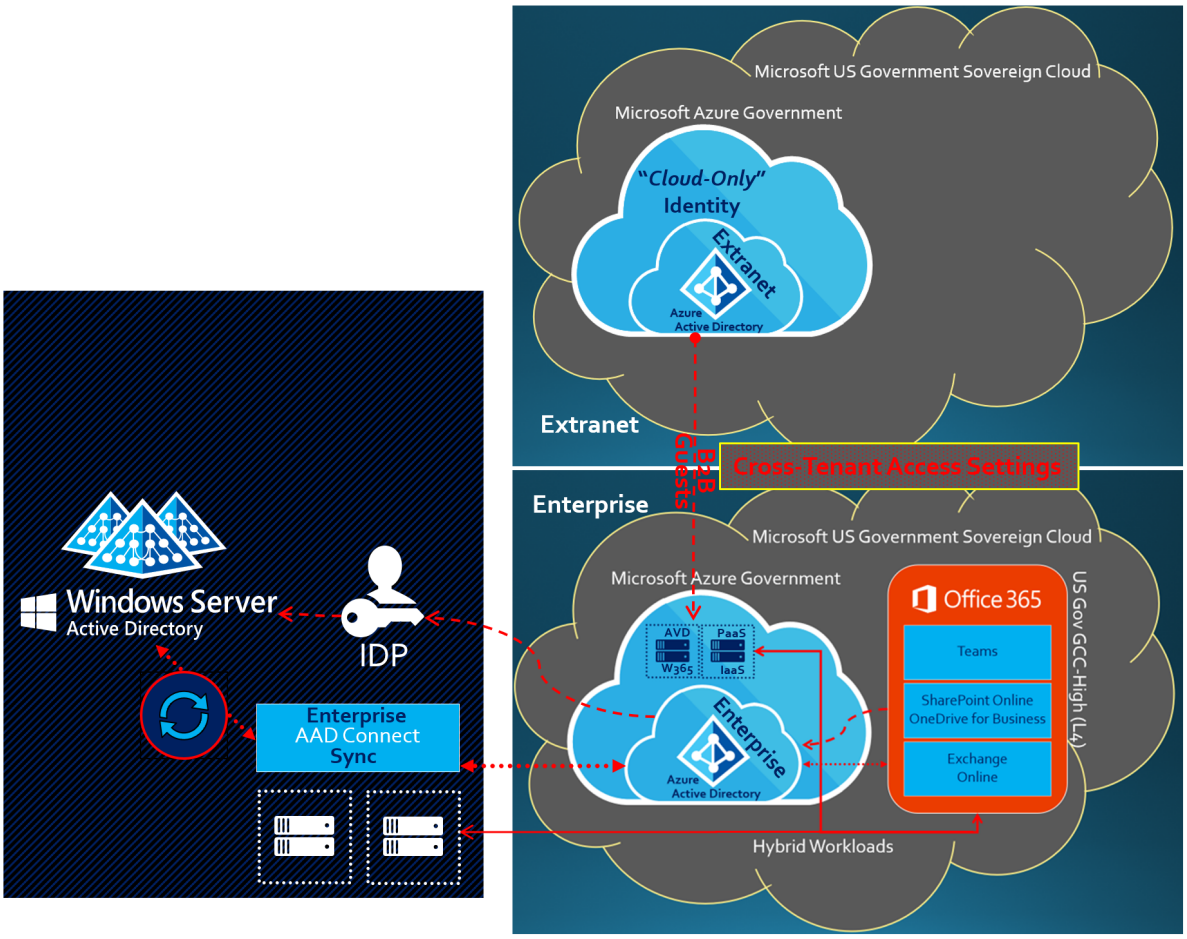


Illustration P: Identity-only extranet tenant

The primary use-case for the identity-only extranet tenant includes segmenting out a separate tenant directory that may be managed by another organization outside the enterprise IT department. An example may be a subcontractor directory managed by a supply-chain management department, or a former employee directory managed by HR. They may use the directory for many other purposes and utility outside the parameters of your enterprise tenant. In addition, the extranet tenant directory may contain many more identities as compared to those you invite in as external Guest users to your enterprise tenant.

Another reference architecture of the extranet tenant includes hybrid identity. This is extremely common for organizations that operate an extranet directory on-premises today.

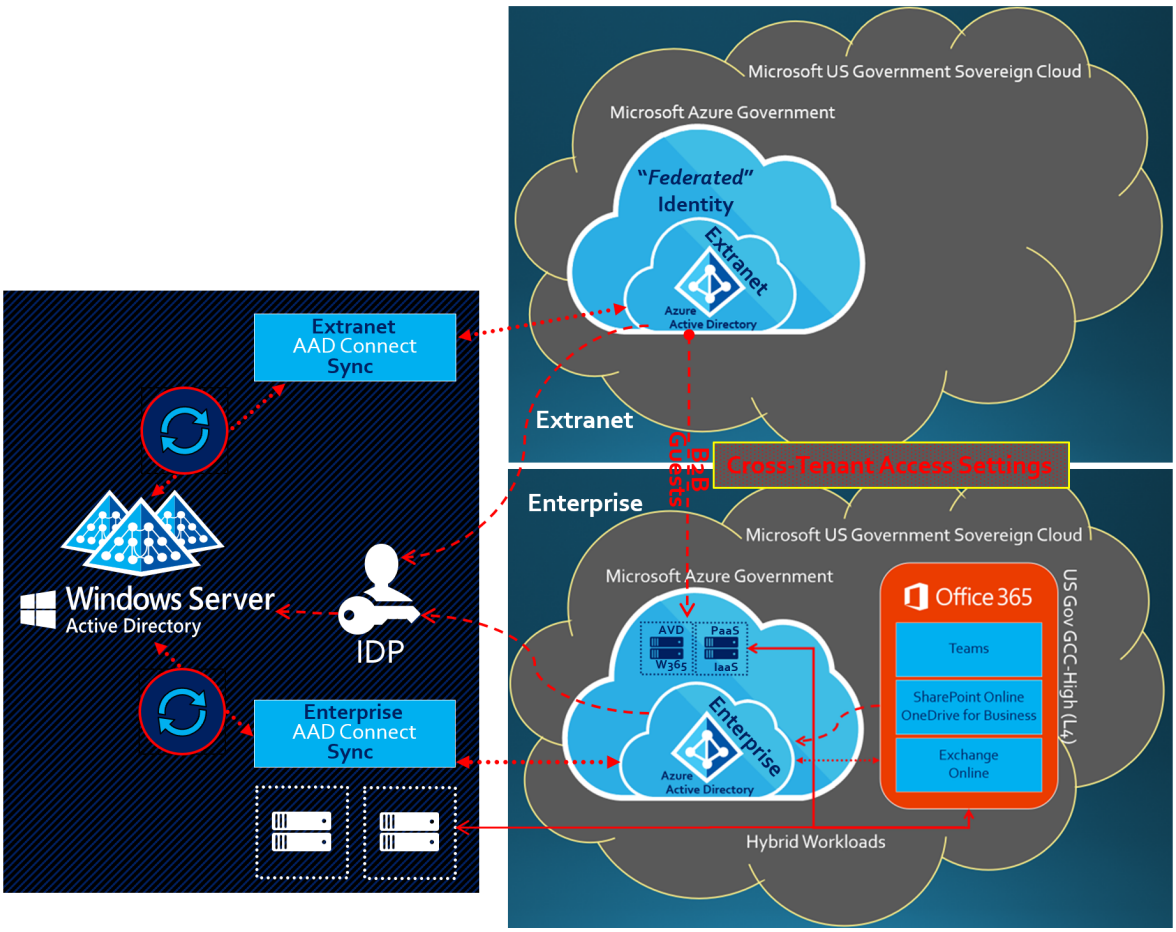


Illustration Q: Identity-only extranet tenant w/ hybrid identity

This very closely resembles the Split tenant with hybrid identity architecture. However, in this case, both the enterprise tenant and the extranet tenant are in the same cloud (e.g. government).

"Meet Me" Extranet Enclave

The "Meet Me" extranet enclave is essentially a dedicated resource tenant that does not host an enterprise user population. Most accounts in the "Meet Me" tenant are external Guest users invited into the resource tenant. Advantages of this architecture include:

- A highly scalable, low-cost solution for SMB to operate in a compliant enclave.
- Collaboration with partners, sub-contractors, suppliers & customers on a compliant, neutral ground.
- May be dedicated to a specific mission or program consisting of multiple parties aka "Mission Enclave".
- May be multi-instanced (e.g. missions, programs, development environments, proposal capture, etc.).
- May lift up the watermark for compliance where the home tenant is lesser (e.g. CMMC L2 -> L3).
- May drop down the compliance requirements where the home tenant is too restrictive (e.g. NOFORN -> FORN).
- May possibly by "type-accredited" with a known configuration demonstrating compliance (e.g. CMMC).
- May be owned by a Cloud Service Provider (*not Microsoft*) with FedRAMP + CMMC compliance.
- May be operated autonomously by a Managed Service Provider with CMMC compliance.

In addition, the extranet enclave enables:

- Logically isolated containers for protected data.
- Fully automated deployment with Infrastructure-as-Code (IaC).
- Known configuration to compare against supporting constant monitoring (CONMON) & accreditation (Continuous ATO).
- Conditional Access & Network isolation implementations.
- User authorization & caveat constraints (e.g. NOFORN).
- Policies preventing protected data from exfiltration, such as Protecting the compliance boundary.
- Mirroring an on-premises data enclave experience.
- Lift-and-sift strategy considered relatively inexpensive.

The "Meet Me" extranet enclave has all the advantages and detractors as the Considerations for the data enclave approach, with one notable exception. Unlike with the swivel seat, the extranet enclave does not support individual storage. The extranet enclave only supports shared data. This is a significant risk that must be governed against effectively. By having individual data outside of the extranet enclave, there is a high probability for data spillage of CUI into a non-compliant environment that hosts the individual data.

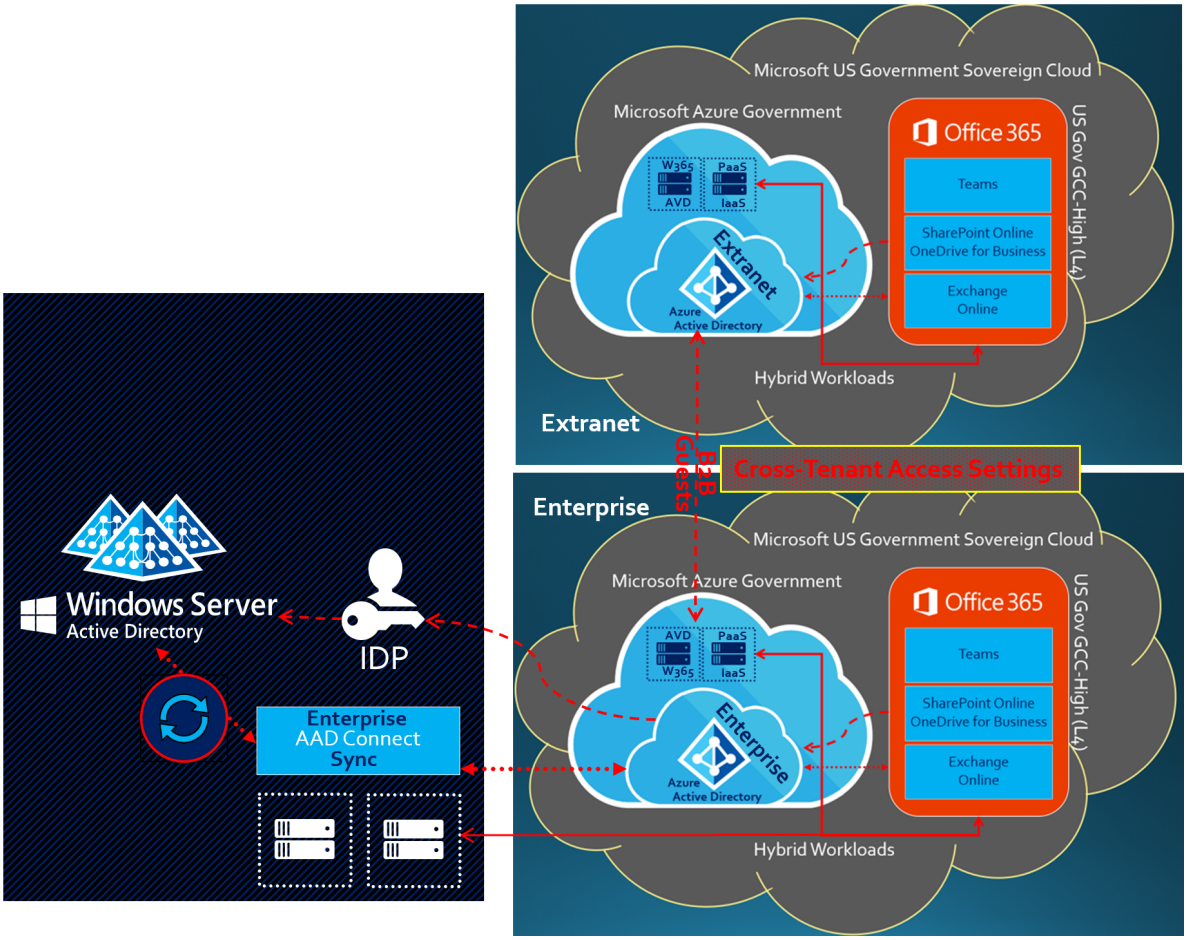


Illustration R: "Meet Me" extranet enclave

Illustration R illustrates a version of the "Meet Me" extranet enclave with cloud-only external identities. While the identity-only extranet did not host workloads, the "Meet Me" extranet enclave may host workloads spanning the productivity suite with Office 365, security solutions with Microsoft 365, Azure IaaS & PaaS, and beyond. Examples include:

- As of the time of this writing, neither Azure Virtual Desktop (AVD) or W365 support external identities, but is on the near-term roadmap for Microsoft.
- AD DS domain controllers replicated to Virtual Machines (VMs) running in the cloud.
- Product Lifecycle Management (PLM) solutions on IaaS, including CAD & CAM products for modeling and simulation.
- Enterprise Resource Planning (ERP) and Customer Relationship Management (CRM).

With the "Meet Me" extranet enclave, most external identities are of user type "Guest" that may access the tenant without an additional license. However, you should consider the section above on External User Licensing.

Note: Additional restrictions may impact extranet enclaves. For example, SharePoint Online storage limits allocated to the tenant scale up from the default 1 TB at 10 GB per license. If the extranet enclave does not have many licenses, the SharePoint Online storage may be limited and require purchasing additional storage.

Cloud-broker Managed Extranet Enclave

Entra ID external identities support third-party identity providers. This may include consumer identities (MSA, Google & Facebook) along with enterprise identities originating in Entra ID. Entra ID also supports SAML/WS-Fed identity providers for any external party that supports the SAML or WS-Fed protocols. This may include a partner's identity provider (e.g. AD FS, Ping Federate, F5, Entrust, SecureAuth, Shibboleth, etc.) supporting direct federation to them without having to proxy through a third party cloud broker (e.g. Entra ID, OKTA, Google, Exostar, etc.). However, there are distinct advantages to leveraging a cloud broker. This may include cloud brokers that issue credentials for external users with strong authentication (e.g., PIV/CAC smartcards, FIDO2 keys, OATH tokens, etc.) that your organization does not have to manage.

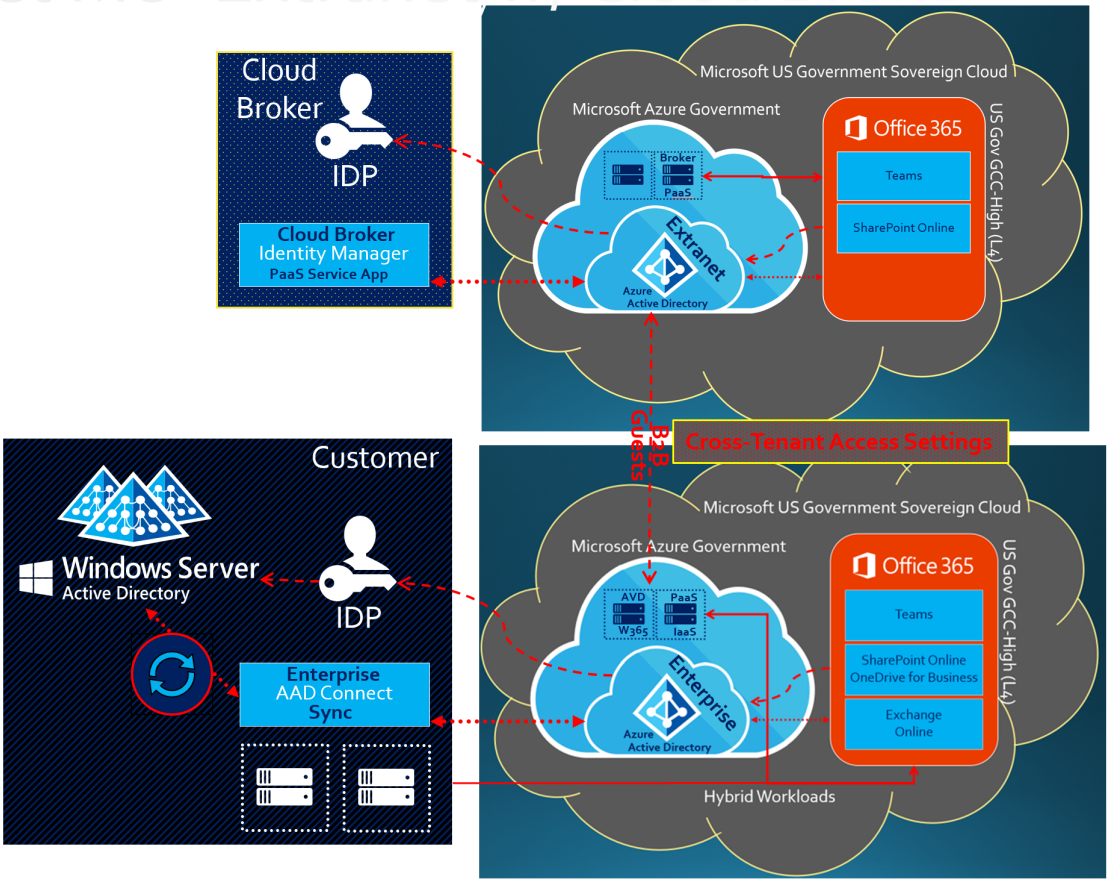


Illustration S: "Meet Me" extranet enclave with Cloud Broker

The cloud broker may be as simple as supporting consumer identities that your SMB supplier may prefer. Or enable you to implement a strong authentication strategy across your supply chain accessing the extranet tenant.

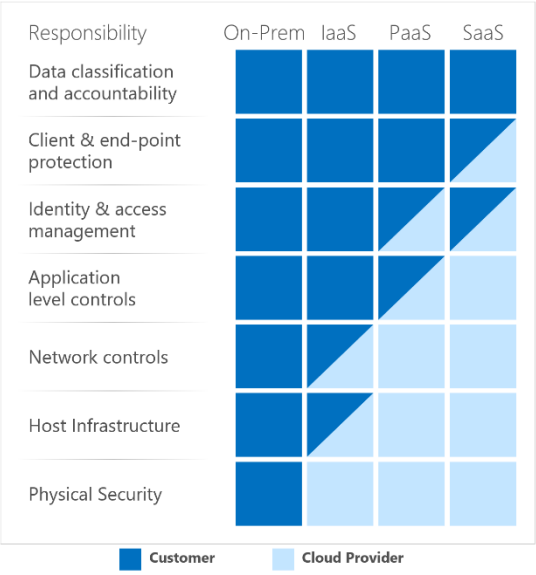
If you pair the "Meet Me" extranet enclave powered by a cloud broker together with an external service provider (e.g. CSP, MSP), it may offer an extremely low-cost, highly compliant solution (relatively speaking).

Reference Architecture Considerations

There are several considerations that apply to all identity reference architecture outlined in this white paper.

Shared Scope of Responsibility for Compliance

Organizations using Cloud Service Provider (CSP) offerings lessen their burden for compliance as the cloud represents a shared responsibility between the organization (Customer) and the CSP. For example, Microsoft as the CSP manages most controls for physical security and host infrastructure, thus organizations don't need to spend resources building and maintaining their own datacenters.



This graphic demonstrates the CSP responsibility in respective cloud models (On-Prem, IaaS, PaaS, SaaS) with light blue aligning with CSP and dark blue aligning with organizational responsibility.

For on-premises (On-Prem) environments, the organization owns 100% of the compliance. On the other end of the spectrum, for Software-as-a-Service (SaaS), the organization has the least burden for compliance, inheriting controls spanning the network and application level. However, as you introduce controls for Identity & access management and Client & end-point, the organization has less inheritance and more shared responsibility. Finally, data classification and accountability are always 100% the organization's responsibility.

As you can imagine, Azure Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS) fall in the middle of the shared scope of responsibility for compliance.

Considerations for US person-only Tenant for Government Clouds

This is an organizational decision, and not one that is required to achieve compliance.

There are no restrictions for US persons nor for citizenship checks imposed by Microsoft on tenant owners (organizations) giving access control to their tenants in US Government cloud service offerings. As with all Cloud Service Providers (CSP), it is a shared scope of responsibility for compliance. Microsoft commits to personnel that are US persons on the back end with the CSP specific scope of responsibility, but it is the organization's (customer's) responsibility to protect their content according to their own regulatory requirements.

There is a misconception that government tenants must enforce US persons access (NOFORN). This stems from several causes:

- Microsoft does not publicly document the requirements for the customer scope of responsibility to include (or not) a NOFORN requirement. Many people automatically assume it is a requirement after reading about

Microsoft's CSP specific scope of responsibility that does in fact require a citizenship check (*for the back end*). Ultimately, it may be derived from Microsoft's System Security Plan (SSP) documentation for government.

- There is a Microsoft Enterprise Agreement amendment that does have language calling for US persons in US locations. This is explicitly for eligibility and commerce for acquiring a government enrollment (tenant). The organization must have a US location to transact, and the organization's procurement official must be a US person. However, this in no way implies that the organization must restrict user populations to NOFORN. Again, this is a Shared scope of responsibility for compliance.
- Historically, organizations have enforced US persons at the boundary of an environment or enclave. While the perimeter boundary is still extremely important, new advances in data protection and zero-trust methodologies may blur the concept of the perimeter. This is especially true for collaboration. It is no longer sufficient to rely solely on the perimeter to protect data. It is wise to protect the data itself and assume the perimeter has been breached (aka zero-trust). In other words, you may decide to impose the restriction of NOFORN on the data (e.g. with Purview Information Protection) as opposed to at the tenant perimeter.
- Assessors that are not familiar with the new zero-trust frameworks of NIST and the DOD, may still be skeptical of organizations that allow for foreign-nationals into the same environment with CUI and other highly-regulated data. *Note: as the time of this writing, this is a non-productive argument as NIST SP 800-171 rev 2 does not accommodate zero-trust principles. However, this will inevitably change with rev 3 due out in 2023*.

Ultimately, it is nearly impossible to enforce a NOFORN policy with collaboration. The most common culprit is meetings. Users will initiate meetings and invite attendees where you have no idea of nationality. In addition, it's become more and more taboo to ask for an attendee's citizenship status for privacy reasons. If the meeting is hosted for non-regulated purposes from within a government tenant, the likelihood of foreign nationals being allowed in is nearly 100% (*penetrating the perimeter*). The same may apply for federated chat and external sharing of data that is not regulated.

Also for consideration, are organizations that are homed in government, especially for those that decide to "Go All In" to a single tenant in government. If the enterprise is homed in government, there will be a requirement to conduct business with employees and collaborators that are foreign nationals or for which you have no idea of the nationality. This is extremely common for the DIB primes and Tier 1 type personalities that are predominately homed in government.

Compliance Boundaries

What is in scope for your compliance boundary?

For those that have self-attested to DFARS 7012 compliance, and planning for a DIBCAC High or future CMMC Level 2/3 assessment, the compliance boundary is fundamental. A common theme is "*follow the CUI*" and/or regulated data. If regulated data may be stored, processed, or transmitted across a non-federal information system, it will likely be in scope for the compliance boundary. In fact, this is the first documentation an assessor asks for.

The compliance boundary has ultimately evolved over time. Historically, it may have been defined as an ITAR and/or Federal data enclave designated for shared storage in a location where the organization instructed users to place such data with tight perimeter controls in place. Other information systems were considered out-of-scope, such as endpoints, collaboration solutions, ERP systems, etc. This may have been enforced by end-user driven policies such as "*don't save CUI locally on your desktop*" and "*don't send CUI over email or in a meeting*".

The scope has broadened. Most notably, the endpoint (e.g. desktop or mobile device) accessing the regulated data comes into scope, regardless of whether the CUI is "*saved locally*". The endpoint will in fact "*process*" the CUI in plain text and is subject to compliance. In addition, the collaboration solutions end up falling into scope. The truth is people make mistakes while collaborating, or error for sake of convenience. But most notably, people outside your organization

may send you regulated data assuming you are compliant to handle it. For this reason, collaboration solutions become one of the highest exposures to data spillage, if not forced within the compliance boundary.

As organizations analyze how they "*follow the CUI*" both marked and mysteriously unmarked, additional information systems begin to fall into scope for the compliance boundary. This may be ERP systems, CRM, PLM, or even security products used at the enterprise level. If any of these IT information systems store, process, or transmit CUI, they will fall into scope. In such cases, you have two choices. You must either raise the watermark of compliance for that enterprise information system or create a new instance that resides cleanly within the compliance boundary. At the end of the day, the more enterprise systems that are in scope for the compliance boundary may lift your entire enterprise to the higher watermark of compliance. In other words, your enterprise home should be in government.

Protecting the Compliance Boundary

The perimeter is still relevant. Zero-trust principles assume breach, in which case you may assume the perimeter is no longer effective. However, the permitter is the first guard to protect your environment. It is also a clear boundary for compliance where you may implement data protection controls, such as Data Loss Prevention (DLP) to prevent data exfiltration and non-compliant endpoints that may breach your compliance boundary.

The following are not hard recommendations. There are alternative solutions, such as compliant endpoints, browser-based limited access solutions, DLP and CAS-B (cloud access security broker) solutions that may be effective (e.g. Microsoft Defender). However, the most common solution to protect the compliance boundary is with Virtual Desktop Infrastructure (VDI) such as Azure Virtual Desktop (AVD) and Windows 365 (W365).

Protecting the compliance boundary is a bi-directional concept. To protect against data exfiltration from the government tenant, you may decide to virtually segment the environments. This may include a requirement to "*browse down*" from government tenant to commercial with a virtual desktop. Policies applied to the virtual desktop many prohibit transmission of data from the government tenant to commercial. An example for an enterprise that is homed in commercial may include a government internal Member user accessing the commercial tenant for an HR resource. The Illustration below demonstrates how a government internal Member user may access a commercial tenant with an external Guest user account, proxied through a virtual desktop.

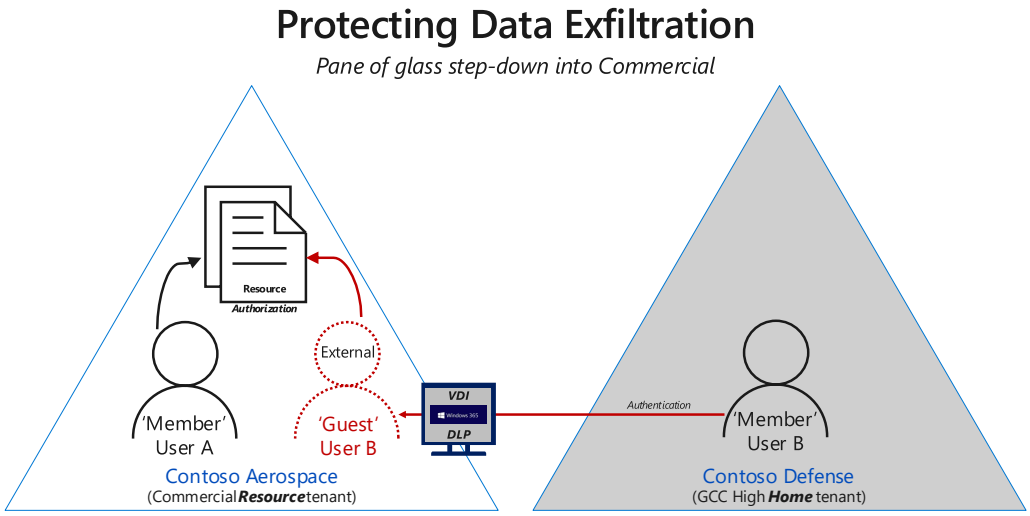


Illustration T: Protecting data exfiltration

For the reverse scenario, most government tenant deployements will not permit non-compliance endpoints from connecting. Compliant endpoints may include desktops and mobile devices that are joined to the government tenant. For end users homed in the government tenant, most likely their endpoints will be naturally joined to the government tenant as well. Assuming those endpoints are compliant, they may connect directly without having to proxy through a virtual desktop. However, if the endpoint is not trusted, or not compliant, the government tenant may reject the endpoint with Entra ID Conditional Access Policies. That leaves and enduser with no other choice but to connect in with a virtual desktop. This may be true for commercial user populations, or for partners that are in invited into the government tenant with Entra ID external identities. For those users connecting through a virtual desktop, it may be configured to prohibit exfiltrating information from the government tenant, such as preventing download, copy-and-paste, nor print functions.

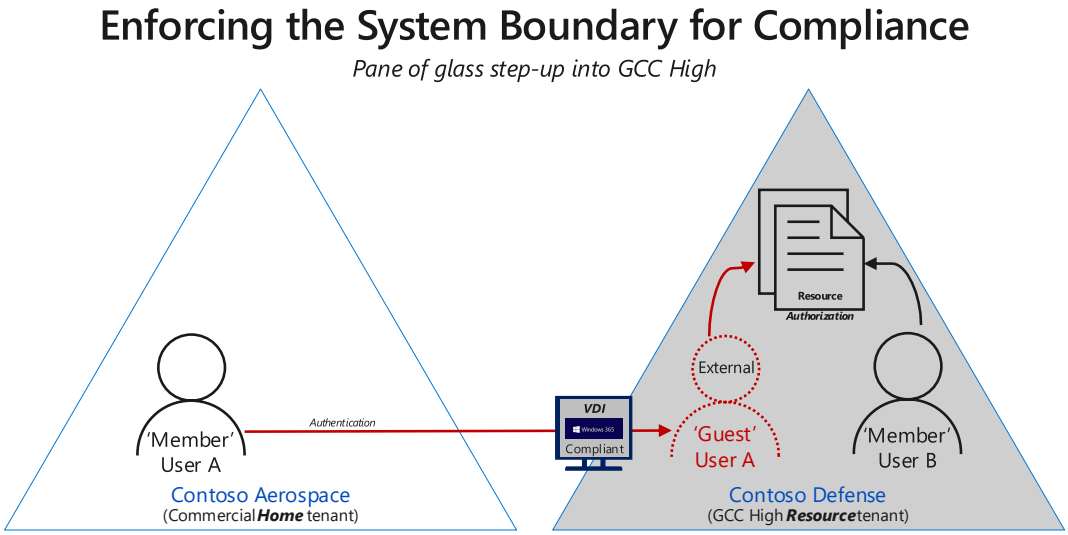


Illustration U: Enforcing the System Boundary for Compliance

Email One-time Passcode Authentication (OTP)

There are three different implementations of OTP across Microsoft 365 to be aware of.

The first implementation is aligned with external user accounts in Entra ID. One-time passcode authentication is a way to authenticate external users when they can't be authenticated through other means, such as Entra ID, Microsoft account (MSA), or social identity providers. When a B2B guest user tries to redeem an invitation or sign in to shared resources, they can request a temporary passcode, which is sent to their email address. Then they enter this passcode to continue signing in.

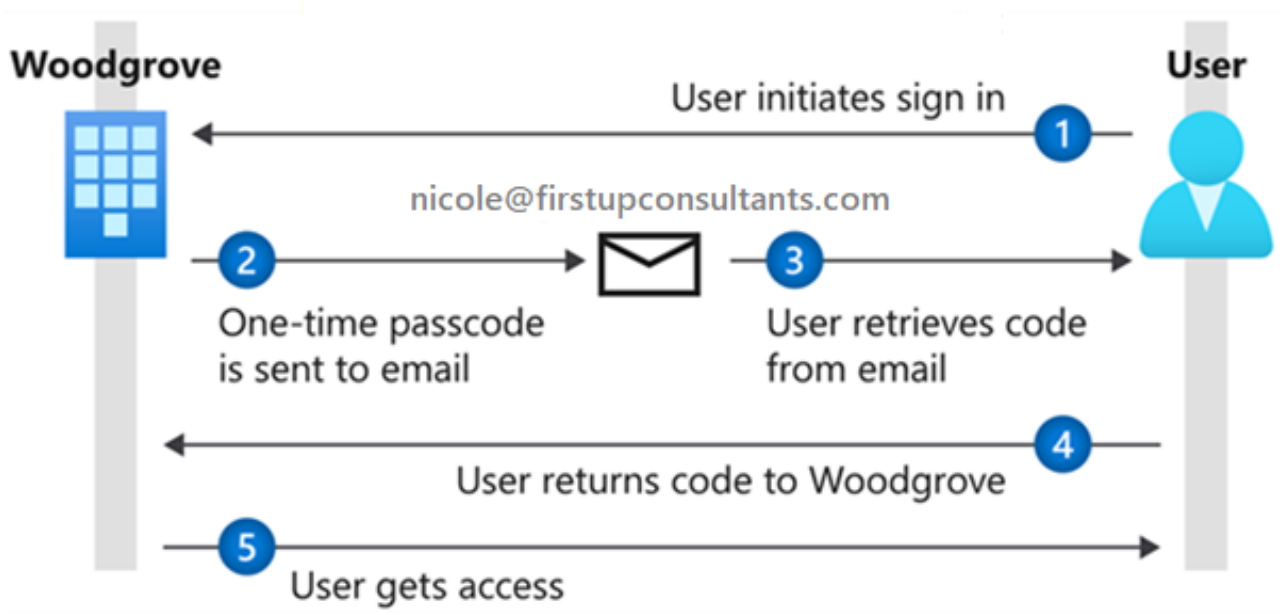


Illustration V: OTP Flow

Note: The email one-time passcode feature is now turned on by default for all new tenants and for any existing tenants where you haven't explicitly turned it off. This feature provides a seamless fallback authentication method for your guest users. If you don't want to use this feature, you can disable it, in which case users will be prompted to create a Microsoft account instead.

The second implementation of OTP is aligned with Office Message Encryption (OME). OME does not require external user accounts to be provisioned within Entra ID. Alternatively, OME has it's own ability to enable OTP. You can manage the behavior with OME PowerShell.

The third implementation of OTP is within legacy external sharing in SharePoint Online and OneDrive for Business. This feature pre-dates Entra ID external users and has been enabled within GCC High tenants since release. As described in 5: Ad-hoc Organic Collaboration, SharePoint Online may generate a sharing URL to a document, document library or site that may be shared with individual email addresses. When the recipient accepts the URL, SharePoint Online leverages OTP to provide temporary access to the resource. Ultimately, this legacy feature will transition over to Entra ID external identities and be phased out from GCC High. It's already been deprecated in Commercial tenants.

Configuring Multi-tenant User Management

The second half of this white paper is an article published by Microsoft and coauthored by Richard Wakeman. While the first half covered the concept, this will delve into the "How".

For the most recent update please see Configuring multi-tenant user management

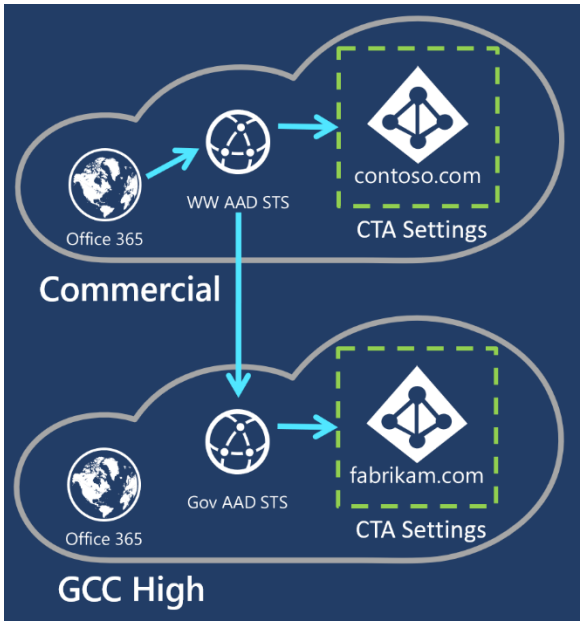
Appendix

Appendix A: Resources

- Blog Introduction: Build 2022: New frontier of collaboration with External Identities – Microsoft Tech Community
- Cross-Cloud Collaboration Overview: Cross-tenant access overview – Entra ID | Microsoft Docs
- How to configure: Configure B2B collaboration Microsoft cloud settings – Entra ID | Microsoft Docs
- Using the MS Graph API: Cross-tenant access settings API overview – Microsoft Graph beta | Microsoft Docs
- Set up governance for external users (including cross-cloud Entra ID orgs): Govern access for external users in Entra ID entitlement management | Microsoft Docs
- See how users are collaborating with other organizations: Cross-tenant access activity workbook in Entra ID | Microsoft Docs
- Configuring multi-tenant user management in Entra ID | Microsoft Docs
- John Savill's Technical Training: Entra ID Cross Cloud B2B – YouTube
- Tutorial for bulk inviting B2B collaboration users – Entra ID | Microsoft Docs
- Quickstart: Add a guest user with PowerShell – Entra ID | Microsoft Docs
- Common considerations for multi-tenant user management in Entra ID | Microsoft Learn
- Default user permissions – Entra ID | Microsoft Learn
- Properties of a B2B guest user – Entra ID | Microsoft Learn
- Add, invite guest external users to your organization – Azure DevOps Services | Microsoft Learn

Appendix B: Cross cloud external identities authentication flow

1. Resource access requests credentials for Commercial @contoso.com tenant at https://login.microsoftonline.com
2. User enters GCC High (Government) account name UserB@fabrikam.com
3. Worldwide (Commercial) Entra ID STS processes:
4. @fabrikam.com Cross Tenant Access Settings (inbound policy)
5. Validate external 'Guest' user exists for UserB@fabrikam.com in Commercial @contoso.com tenant
6. Cross cloud request to GCC High @fabrikam.com tenant
7. Government (GCC High) Entra ID STS processes:
8. @contoso.com Cross Tenant Access Settings (outbound policy)
9. User identified in GCC High @fabrikam.com tenant
10. Browser redirects to https://login.onmicrosoft.us
11. User is authenticated at login.onmicrosoft.us and token issued, redirected back to login.microsoftonline.com with OAUTH token
12. Token redemption and exchange occurs between WW STS and Gov STS for external 'Guest' user UserB@fabrikam.com
13. WW Entra ID STS token returned to Commercial @contoso.com tenant resource



Appendix C: Customer Responsibility Matrix

Microsoft has System Security Plan (SSP) documentation, authorization packages and assessor security audit reports available for government cloud customers. It is held under NDA within restricted portals. You may ask for access by sending an email to:

- For Microsoft 365 US Government (GCC High): O365FedRAMP@microsoft.com
- For Azure Government: AzFedDoc@microsoft.com

The SSP is written for FedRAMP High (NIST SP 800-53) and for the DOD Cloud Computing Security Requirements Guide (CC SRG), representing the high watermark of compliance in the government cloud achieving equivalency with CC SRG Impact Level 5 (IL5).

For more information, see Microsoft Richard Wakeman's blog article Understanding Compliance Between Microsoft 365 Commercial, Government and DoD Offerings.

Microsoft publishes a Customer Responsibility Matrix (CRM) for FedRAMP. It's documented in an Excel spreadsheet called the "Control Implementation Summary" or CIS.

Within the "CRM" tab of the CIS spreadsheet, you will see Control IDs that are met by the Cloud Service Provider (Microsoft). The control numbers shown correspond to NIST SP 800-53.

To map NIST SP 800-53 control numbers to NIST SP 800-171, you may reference the CMMC Technical Reference Guide from Microsoft. For example, for the NIST SP 800-171 control for 3.7.1 (CMMC Practice MA.L2-3.7.1), you can see the NIST SP 800-53 mappings.

Now looking at the CRM documentation, you may observe those controls are fully inherited from Microsoft. In other words, no additional share responsibility is required for the customer (*for cloud-only environments*).