## Identity and Access Management

A directory service is responsible for the storage of identity information. Directories expose the identity information using network protocols such as the Lightweight Directory Access Protocol (LDAP). To ensure a seamless user experience and minimize potential identity conflicts, each identity should have a single point of truth / source. Changes should be replicated to but not managed by other directories.

Identity and Access Management (IAM) is the framework upon which digital identities and access to resources are managed. Within a hybrid solution this framework needs to encompass both the on-premises and cloud components.

### Azure Active Directory

Azure Active Directory (Azure AD) is a cloud-based directory service which stores identity information and offers Information and Access Management (IAM) for Microsoft cloud products, custom developed applications, and third-party applications. The identities within this directory service can be either cloud based or synchronised from an on-premises AD domain via the Azure AD Connect client.

Azure AD allows users to sign in and access resources like Microsoft Office 365, the Azure management portal, and other SaaS applications. Azure AD also provides control over the following directory activities:

* Registration of applications – The registration of application controls whether users can grant permissions to applications and register them within Azure AD.
* Restriction of the Azure AD administrative portal – The restriction of the Azure AD portal controls who can viewing of the contents of the Azure AD. The contents include user identity data.
* LinkedIn account connection – LinkedIn account connection allows users to link their work account to LinkedIn.
* External user invitations – External user invitation controls who can be invited by users to collaborate within the tenant.
* Azure AD preview features – Azure AD preview features control how new self-service features are made available to users.

Azure IAM is configured using:

* Enterprise Applications - The registration of Microsoft and Third-party enterprise applications. The registration requires information regarding the name, publisher, permissions, authentication configuration and Redirect URIs (Uniform Resource Identifier) to be provided.
* App Registrations – The registration of custom-built enterprise applications. The registration requires information regarding the name, Application Identifier (APP ID), permissions, authentication configuration and Redirect URIs (Uniform Resource Identifier) to be provided.

Where an Agency has already determined that a HYBRID solution is required, [additional considerations](https://docs.microsoft.com/en-us/azure/active-directory/hybrid/plan-hybrid-identity-design-considerations-overview) will apply and these should also be reviewed.

Azure AD Design Decisions for all agencies and implementation types.

|  |  |  |
| --- | --- | --- |
| Decision Point | Design Decision | Justification |
| Cloud Based Service Accounts | Configured | Break glass accounts are required to be cloud based to ensure access to the tenant if there are issues with authentication. |
| Allow the registration of applications by users | Disabled | Only administrators can register applications. |
| Restrict access to the Azure AD administrative portal | Enabled | Only administrators have access to the portal. |
| Allow LinkedIn connections | Disabled | To meet the Agency’s requirements not to share information with third party Agencies without approval. |
| External Collaboration | Configured | As required by the Agency, provided the external Agencies are at the same classification. |
| Group Management | Configured | Naming policies and expiration as required by the Agency. |
| Azure Active Directory RBAC | Configured | For ease of administration, segregation and delegation of roles. Users and administrators will be assigned only the roles they need through PIM (Privileged Identity Management). |
| Enterprise Applications | Not Configured | No enterprise applications have been identified. |
| Device registration | Not Configured | Default settings. |
| Identity Governance | Not Configured | Default settings. |
| Application Proxy | Not Configured | No requirement has been identified. |
| Licences | Configured | Configured to assign Microsoft 365 licences to user groups. Ensures consistent configuration. |
| Custom Domain Names | Configured | {agency}.onmicrosoft.com{agency}.gov.au |
| Mobility (MDM and MAM) | Not Configured | Default settings. |
| Company Branding | Configured | Agency specific logos will be required. |

Additional Azure AD Design Decisions for cloud native implementations

|  |  |  |
| --- | --- | --- |
| Decision Point | Design Decision | Justification |
| Identity Source | Azure AD | As this is a cloud only implementation Azure AD will be the source of identity. |
| App registration | Not Configured | Default settings. |
| Password Reset | Configured | For self-service password reset, users will need to provide an alternate email address, mobile app and phone number during registration. To reset their password, they will need to provide two methods of verification. |
| Identity Format | Configured | Usernames will conform to firstname.lastname{sequence number}Note: The sequence number is only required if duplicate names would be created. |

Additional Azure AD Design Decisions for hybrid implementations

|  |  |  |
| --- | --- | --- |
| Decision Point | Design Decision | Justification |
| Identity Source | Active Directory | As this is a hybrid implementation Active Directory will be the source of identity. |
| Synchronize to Active Directory | Configured | Cloud identities or Synchronised or Federated in accordance with agency specific requirements. |
| App registration | Configured | Windows Defender ATP – SIEM integration is required. |
| Azure AD Connect | Configured | See Azure AD Connect section for details. |
| Identity Format | Not Configured | Usernames will be synchronised from the on-premises Active Directory and will inherit naming convention. |

### Emergency Access Admin Accounts

Emergency access or ‘break-glass’ accounts are accounts used to restore access to an environment or tenant. Break-glass accounts are an option of last resort and should only be used when normal administrative accounts cannot be used to restore access. Example of this is where conditional access has malfunctioned and both users and administrative staff are unable to authenticate into the environment, or all privileged administrator accounts are comprised in another capacity.

[Microsoft best practice](https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-emergency-access) recommends that two break-glass accounts are configured. These accounts should be stored according to the standard break-glass procedures. Best practice is for these accounts to meet the following minimum requirements:

* They are not to be associated with any individual user.
* They will use a different authorisation mechanism than standard administrative accounts.
* They are cloud only accounts that use the ’\*.onmicrosoft.com’ domain.
* The passwords to these accounts are set to never expire or be cleaned up or removed due to inactivity.
* The accounts are to be given the Global Administrator role assigned permanently.
* At least one of the accounts is to be excluded from Multi Factor Authentication (MFA).
* At least one of the accounts is to be completely excluded from all Conditional Access policies.
* The accounts are stored on paper, in two or three separate parts, in secure, fireproof safes that are in disparate locations.
* Use of these accounts is monitored and only used in genuine emergencies.

Emergency access account Design Decisions for all agencies and implementation types.

|  |  |  |
| --- | --- | --- |
| Decision Point | Design Decision | Justification |
| Emergency Access accounts | Configured | Two emergency access accounts will be configured in alignment to Microsoft and security best practice. |

Emergency access account configuration for all agencies and implementation types

|  |  |  |
| --- | --- | --- |
| Configuration | Value | Description |
| Username | Any value that is not associated to a specific user. | Accounts are not to be associated with any individual user. |
| Account type | Accounts are cloud only accounts that use the ’\*.onmicrosoft.com’ domain. | Only \*.onmicrosoft.com accounts should be used as per Microsoft best practice. |
| Password Expiry | Passwords are set to never expire. | Ensures the passwords for these accounts are valid in an emergency. |
| Roles | Emergency Access accounts will be assigned the Global Administrator role. | The accounts are to be given the Global Administrator role assigned permanently. |
| MFA | Both Emergency Access accounts will be excluded from MFA. | Multi Factor Authentication (MFA) device may not be available when the emergency access account is required. |
| Conditional Access | At least one of the accounts is to be completely excluded from all Conditional Access policies. | The emergency access account may need access to fix an issue and it would not be beneficial if a policy were to block access. |
| Physical access to account details | Account details will be stored on paper in an appropriate location. | It is strongly recommended that the accounts are stored on paper, in two or three separate parts, in secure, fireproof safes that are in disparate locations. |
| Monitoring of accounts | Account usage will be monitored via MCAS. | Use of these accounts is monitored and only used in genuine emergencies. |

### Azure Active Directory Identity Protection

Azure AD Identity Protection is the function of provisioning access rights to a resource. Azure AD Identity Protection can take the form of an access policy. An access policy defines the business rules on whether authenticated user is granted or denied access to a resource. Azure AD utilises Conditional Access to define the access policies for Office 365 data. Azure AD using Identity Protection utilises analytics further to minimise the risk that access is provisioned to a compromised authenticated user.

Azure AD Identity Protection enables configuration of automated responses to suspicious activities and actions related to user identities. With Azure AD Identity Protection, risk-based policies can be configured that automatically respond to detected issues when a specified risk level has been reached.

These policies, in addition to other conditional access controls provided by Azure AD, can either automatically block, Smart Lockout, or initiate adaptive remediation actions including password resets and MFA enforcement.

Azure AD Identity Protection uses the following mechanisms to detect anomalous activity within the environment:

* Vulnerabilities – Azure AD Identity Protection analyses identity configuration and detects vulnerabilities that can have an impact on user identities. Vulnerabilities can include items such as unmanaged cloud applications.
* Risk Events – Azure AD uses adaptive machine learning algorithms and heuristics to detect suspicious actions that are related to the user’s identities. The system creates a record for each detected suspicious action. These records are also known as risk events and include activities such as Sign-ins from anonymous IP addresses, sign-ins from IP addresses previously detected as exhibiting suspicious activity, or unfamiliar locations.

Azure AD Identity Protection provides mechanisms for logging and reporting functionality that simplify investigation activities.

Azure AD Identity Protection Design Decisions for all agencies and implementation types.

|  |  |  |
| --- | --- | --- |
| Decision Point | Design Decision | Justification |
| Azure AD Identity Protection | Enable the sign-in risk policy and user risk policy within the Azure AD tenant. | Provide reporting of detected suspicious sign-in activity based on defined MFA, sign-in risk and user risk policies for increased security. |
| User risk policy | Enabled | The user risk policy detects the probability that a user account has been compromised by detecting risk events that are a typical of a user’s behaviour, alerting when high risk behaviour is detected. |
| Sign-in risk policy | Enabled | Azure AD analyses each sign-in of a user. The objective of the analysis is to detect suspicious actions that come along with the sign-in. Automated actions will be configured to be taken when high risk behaviour is detected. |

### Azure AD Multifactor Authentication

Authentication is a primary security control to protect both information assets - ranging from logging into a Windows device, to sending an email or collaborating on a document. When deploying Microsoft 365, the identity for each individual staff member is either in the cloud or both in the cloud and on-premises. Employing multiple authentication factors present a significant challenge for attackers gaining access to a system. Traditional authentication methods rely purely on something the user knows, such as a password. Note, a username does not technically count as an authentication factor. A user enters a username to only claim an identity, then must provide an authentication factor to validate this claim (identification vs authentication). Multi-factor authentication (MFA) is recommended by the ACSC for all users to prove a user’s identity before being granted access.

Multi-factor authentication is any combination of two or more authentication sources from the following categories. Biometrics are yet to be accepted as part of the industry standard definition of an authentication factor.

* Something a user knows (such as a password or PIN).
* Something a user has (such as a specific hardened device).
* Something a user is (such as biometric trait, for example a fingerprint).

Azure Multifactor Authentication provides additional security by requiring a second form of authentication and delivers strong authentication via a range of easy to use authentication methods.

Azure MFA provides multiple verification methods, such as:

* Call to phone – Call to phone places an automated voice call to a phone number defined by the user.
* Verification code from mobile app – The Microsoft Authenticator app generates a new verification code every 30 seconds. The user enters the verification code into the sign-in interface.
* Notification through mobile app – Sends a push notification to a user’s phone or registered device using the Microsoft Authenticator app. The user views the notification and selects “Approve” to complete the verification process.
* Text message to phone – Sends a text message that contains a verification code that is used as the authentication token. The user is prompted to enter the verification code into the sign-in interface. This process is called one-way SMS.
* OAuth hardware token verification code – OATH is an open standard that specifies how one-time password (OTP) codes are generated. Various vendor tokens are supported.

Azure MFA integrates with Azure AD Conditional Access polices, or the Trusted IP ranges feature to determine under what circumstances and user’s physical location a challenge for additional authentication is required . Conditional Access polices are the recommended method to determine MFA conditions.

Azure AD Multifactor Authentication Design Decisions for all agencies and implementation types.

|  |  |  |
| --- | --- | --- |
| Decision Point | Design Decision | Justification |
| MFA | Configured – Mobile App – soft token code | Native Azure MFA will be configured to secure access to applications and desktops from outside of the environment, and any system administration functions. Use of a mobile app for verification instead of SMS message or phone call reduces any possibility of hack by cloning or swapping a sim card. The ACSC recommends implementing soft tokens without push notifications. |
| Hardware Token Support | Allowed (supported OATH tokens only) | The default method will be to use soft tokens which will meet maturity level 2 of the essential 8, although hardware tokens will be allowed. Hardware token support is required to support some use cases. Some working locations may not allow mobile phones, or users may have a specific physical token, biometrics or smartcard justification. Having hard tokens is a requirement to achieve Essential 8, level 3 maturity for multifactor authentication. |
| Trusted IP | Not configured | Conditional Access policies will be used in place of the legacy ‘Trusted IP’ feature. Trusted egress IP addresses will be defined by Conditional Access. |
| MFA for Administration | Configured | Administration through the Azure Portal and other Cloud Apps will require MFA. |
| MFA for User Apps | Configured | MFA is required. |

Note: OATH tokens are to be purchased separately if required.

### Conditional Access

Conditional Access provides access controls that can be applied to user login requests. These access controls provide an extra level of security to help protect corporate data and information.

When a user attempts to access an application or system from any device, one or more conditions must be met before authentication is successful. Conditional Access offers the following types of access controls:

* User and location based – User and location based Conditional Access limits or blocks user access based on their geo-location or IP address.
* Device based - Device based Conditional Access ensures only enrolled and approved devices can access corporate data.
* Application based - Application based Conditional Access policies provide the ability to allow or block an application based on policy configuration.
* Risk based - Risk based Conditional Access protects corporate data from malicious hackers based on a user’s Sign-In risk. The sign-in risk is an indicator for the likelihood (high, medium, or low) that a sign-in attempt was not performed by the legitimate owner of a user account. Azure AD calculates the sign-in risk level during the sign-in of a user.
* Session based – Session based Conditional Access policies enables the control of user sessions by redirecting the user through a reverse proxy instead of directly to the app. From then on, user requests and responses go through Cloud App Security rather than directly to the app.

Based on the above conditions, the user will either be allowed, prompted for multi-factor authentication, or blocked.

Conditional Access Design Decisions for all agencies and implementation types.

|  |  |  |
| --- | --- | --- |
| Decision Point | Design Decision | Justification |
| Conditional Access Enabled | Device Based | To meet security and business requirements. This allows only approved and agency issued devices access to the Agency’s resources. |

Additional Conditional Access Design Decisions for hybrid implementations

|  |  |  |
| --- | --- | --- |
| Configuration | Value | Description |
| Conditional Access Policies | BLOCK - Legacy Authentication | This global policy blocks all connections from insecure legacy protocols like ActiveSync, IMAP, POP3, etc. |
| ^^ | BLOCK - High-Risk Sign-Ins | This global policy blocks all high-risk authentications (requires Azure AD Premium P2). |
| ^^ | BLOCK - Countries not Allowed | This global policy blocks all connections from countries not in the Allowed countries whitelist. |
| ^^ | GRANT - Terms of Use | This global policy forces Terms of Use on all authentications. |
| ^^ | GRANT - Browser Access | General browser access policy that grants authentication from a browser on any device with MFA requirement. |
| ^^ | SESSION - Block Unmanaged Browser File Downloads | Browsers on unmanaged devices can never download files and attachments from SharePoint Online and Exchange Online. |
| ^^ | GRANT - Intune Enrolment | Devices can authenticate to Intune for enrolment. |
| ^^ | GRANT - Mobile Device Access | Grants access to managed mobile devices that are enrolled and compliant in Intune. An approved Microsoft app is required. |
| ^^ | GRANT - Windows Device Access | Grants access to managed Windows devices that are Hybrid Azure AD Joined (joined to on-prem AD and Azure AD). |
| ^^ | GRANT - Guest Access (B2B) | Approved apps that guest users can access (requires MFA). |
| ^^ | BLOCK - Guest Access (B2B) | Blocked apps that guest users can never access. |

### Active Directory

Active Directory is an on-premises directory service which stores identity information in a hierarchical structure. Identities within the service are composed of attributes which describe the object. These attributes include but are not limited to the following:

* First name
* Last name
* Password
* Email Address
* Proxy Address

Additional features and capabilities are available within Active Directory when the Forest and Domain Functional levels are raised. The Functional level of Active Directory is linked to several items including the operating system of the domain controllers. To access all features and capabilities the highest functional level is required. For hybrid identity a minimum Forest Functional level of 2003 is required. To use additional hybrid identity features such as password writeback a minimum Forest Functional level of 2008 R2 is required.

Active Directory Design Decisions for hybrid implementations

|  |  |  |
| --- | --- | --- |
| Decision Point | Design Decision | Justification |
| User Identity Source | On-premises Active Directory | The on-premises Active Directory will be used as the source for user identity, with identities being synchronised to Azure Active Directory. The directory functional level must meet the minimum requirements for Azure AD Connect synchronisation. |

### Domain

When a new Azure AD tenant is created it is assigned a default domain name. This domain is internet routable and aligns to “{tenant name}.onmicrosoft.com”. A second internet routable domain name is also provisioned if Exchange Online is activated within the tenant. The second internet routable domain aligns to “{tenant name}.mail.onmicrosoft.com”.

On-premises domains can also be registered to the tenant to be used by Azure and Exchange Online. These domains can then be used for receiving email and/or be utilised as the User Principal Name (UPN).

Domain Design Decisions for hybrid implementations

|  |  |  |
| --- | --- | --- |
| Decision Point | Design Decision | Justification |
| Registration of on-premises Domains | Configured | Required to utilise the on-premises identities. |
| Azure AD Primary domain | Configured - {agency}.gov.au | Required to ensure that Azure created resources contain the Agency’s Primary Domain. |

### Collaboration

Within Azure and Office 365 the ability to collaborate with other tenants exists through the External sharing, B2B (Business-to-Business) and B2C (Business-to-Customer) services. These are key features for any external or inter-Agency collaboration.

Utilising the Blueprints, an Agency can configure collaboration with other organisations where:

* A business requirement exists.
* Both organisations choose to collaborate.
* The organisations trust each other.
* Organisations staff possess the appropriate clearance levels.
* Risk assessments have been completed; and,
* Collaboration is based on the lowest classification level of any involved Organisation or Agency.

Collaboration between organisations assessed and operating at the same security level is relatively straightforward, while collaboration between organisations operating on networks that have been assessed at different security levels presents additional considerations and risk. The additional risks and considerations are similar to those that already exist for organisations today, with activities such as personnel clearances, physical security requirements and the secure creation, storage and destruction of physical artefacts. These considerations will need to be assessed on a case by case basis and risks accepted by the Chief Information Security Officers (CISO).

ACSC provides guidance on connecting networks with differing security classifications available at [Fundamentals of Cross Domain solutions](https://www.cyber.gov.au/publications/fundamentals-of-cross-domain-solutions). At the time of writing, there are no automated options for external collaboration from a PROTECTED environment and user validation for external collaboration remains a manual process. This is particularly the case should an Agency adopting this service seek to collaborate from a PROTECTED environment to an environment that is operating at a lower classification. The ISM stipulates that all users of a PROTECTED environment must have a valid security clearance. It is recommended that users of the higher classification Agency collaborate into the lower classification Agency, and that unified labelling be configured as per the Blueprints with PROTECTED content restricted to external sharing.

For Agencies operating at a PROTECTED level seeking to collaborate, B2C collaboration is not suitable as it allows authentication through publicly accessible domains such as Google and Facebook. Azure AD Business-to-Business (B2B) allows authentication between Azure tenants which provides a higher level of assurance.

B2B allows the most secure sharing of organisation applications, services, and data with external guest users from other organisations, while maintaining maximal control over corporate data. The collaboration options between two or more organisations can use the following platforms:

* Teams
* Planner
* SharePoint Online
* OneDrive for Business

Azure AD supports several B2B access scenarios to enable users within external organisations to collaborate with a host organisation. Users will be authenticated using an external identity source (e.g., Azure AD tenant credentials) which then generates a linked guest account within the host Azure AD tenant.

When an external user is invited to collaborate, the following items are checked:

* Is collaboration with the external domain allowed by B2B at the Azure AD level?
* Is guest access allowed by the application?
* Is external access with the external domain allowed by the application?

When the above are all true, the external user can be invited generating an invitation email. The user must accept the invitation by clicking on the link contained within the email causing a linked guest account to be created in the hosting Azure AD tenant. When the guest account has been created it is available for use by any of the applications that are configured to allow guest access.

B2B only requires a small amount of user information (name, and email), however it is recommended that CISOs consuming this document creates a process outside of technology that ensures Agency identity requirements are met. The identity requirements should include the properties listed in the table below and the external user’s nationality and clearances held.

The following table describes the identity properties that should be a minimum requirement before collaboration is enabled for all agencies and implementation types.

|  |  |  |
| --- | --- | --- |
| Field | Example | Justification |
| FirstName | John | Search and identify the user. |
| LastName | Smith | Search and identify the user. |
| UserName (UPN) = EmailAddress | john.smith3@{agency}.gov.au | Users agency and contract address. |
| UserName | john.smith3 | Identity in Microsoft. |
| EmailAddress | john.smith3@desktopa.gov.auUsers email contact. |  |
| OfficePhone | 61411 2999 | Users phone contact. |
| MobilePhone | 0411 123 456 | Users phone contact. |
| JobProfile | Finance | Users job description in identifying appropriate contact. |
| Agency | Digital Transformation Agency | Users agency. |
| Manager | Julie Citizen | Users manager for further consultation. |
| Photo | ID.JPEG | Viewing and identifying the user. |

In addition to the above, Conditional Access policies should be enforced requiring external individuals to use MFA, block legacy authentication, and block from disallowed locations.

The following table describes the minimal conditional access policies that should be applied by the partner agency for all agencies and implementation types.

|  |  |  |
| --- | --- | --- |
| Decision Point | Design Decision | Justification |
| Conditional Access Policies | **BLOCK - Legacy Authentication**:This global policy blocks all connections from unsecure legacy protocols like ActiveSync, IMAP, PO3, etc.**BLOCK - Countries not Allowed:**This global policy blocks all connections from countries not in the Allowed countries whitelist. | Minimises the risk of the user in the partner organisation using credentials that have been compromised. |

Azure AD design decisions in relation to inter-Agency collaboration for all agencies and implementation types

|  |  |  |
| --- | --- | --- |
| Decision Point | Design Decision | Justification |
| B2B Relationships | Not Configured | The Agency is pursuing a PROTECTED-level certification for the solution. To maintain a robust PROTECTED platform for the Agency, B2B collaboration will not be configured.In a future state, specified partner tenants can be listed assuming they are also rated at a PROTECTED level and approved by appropriate Agency personnel. Only users of these tenants would be allowed collaborative access. |
| B2C Relationships | Not Configured | Client collaboration other than partner organisations is not required. |
| External Sharing | Disabled | The Agency is pursuing a PROTECTED-level certification for the solution. To maintain a robust PROTECTED platform for the Agency, B2B collaboration will not be configured.In a future state, specified partner tenants can be listed assuming they are also rated at a PROTECTED level and approved by appropriate Agency personnel. Only users of these tenants would be allowed collaborative access. |

### Azure AD Connect

Azure Active Directory Connect (AAD Connect) is a product designed to synchronise directory objects and changes between Active Directory and Azure AD. AAD Connect enables the on-premises directory service to be the source of truth for identities within the environment and ensures that changes are replicated to Azure AD.

AAD Connect can be deployed in several patterns. These patterns follow the guiding principles of:

* Only one AAD Connect instance can be actively synchronising to an Azure AD tenant.
* On-premises AD can only be synchronised to one Azure tenant unless directory synchronisation and Microsoft Identity Manager (MIM) are leveraged.

As only one AAD Connect instance can be actively synchronising at a time high availability is not possible. A warm standby can be configured using a second AAD Connect server in Staging mode.

The following illustrates the user identity synchronisation between the Agency’s on-premises AD to Azure AD.

AD Connect Identity Synchronisation

AD Connect Identity Synchronisation

Within the AAD Connect client the synchronisation process can be customised in several ways including:

* Group Filtering – Group filtering limits the scope of the synchronisation to the members of a group within the on-premises directory.
* Organisational Unit (OU) Filtering – OU filtering limits the scope of the synchronisation to the objects in one or more OUs within the directory.
* Attribute Filtering – Attribute filtering controls which attributes from an object are synchronised to the cloud.
* Azure AD App Filtering – Azure AD app filtering assists in limiting the number of attributes synchronised to the cloud based on which Office 365 services are in use.

Each of the above customisations provide control over what directory information is synchronised to the cloud from the on-premises directory service. The AAD Connect client can also be leveraged to configure Single Sign-On (SSO) and Exchange Hybrid. AAD Connect must run on Windows Server 2012 or later and can synchronise many Active Directory objects to Azure AD and hence there is a range of hardware requirements to consider based on the number of objects in Active Directory that will be synchronised (refer to the [Azure AD Connect Prerequisites](https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-prerequisites)).

When AAD Connect is leveraged, a user would be created within the on-premises directory service (Active Directory) and then synchronised via the AAD Connect client into Azure AD (the cloud-based directory service).

The following illustrates a typical user account provisioning workflow for a hybrid configuration.

User Provisioning Workflow

User Provisioning Workflow

Firewall rules will be implemented for AAD Connect. Further details on firewall configuration can be found in the Network Configuration ABAC.

AAD Connect Design Decisions for hybrid implementations

|  |  |  |
| --- | --- | --- |
| Decision Point | Design Decision | Justification |
| AAD Connect | Configured | Identity synchronisation is a critical requirement and must be implemented based on ACSC guidance. The source of truth for account information will be on-premises Active Directory. |
| Attribute used for login | User ID | This attribute is commonly used for logins as it will ensure that the same credentials are maintained for on-premises and in-cloud authentication. |
| Organisational unit filtering | Configured | To target only the required identities for synchronisation. Whole directory synchronisations are not recommended. |
| Single Sign On | Configured | Single Sign-on. |
| Staging Server | Configured | Best practice dictates a secondary staging server be in place to be used in disaster recovery scenarios. |
| Password writeback | Not Configured | Password writeback is not recommended by the ACSC. |
| Self Service Password Reset | Not configured | The Self-Service Password Reset feature requires activation of password writeback in the AAD Connect configuration which is not recommended by the ACSC. Thus, this feature is not configured. |
| Azure AD App and attribute filtering | Configured | All Azure AD App and attribute filtering will be synchronised as recommended by Microsoft . |
| Exchange Hybrid | Configured | Exchange will be used in a hybrid configuration with Exchange Online, therefore this setting is required to be set as Configured. |
| Exchange Mail Public Folders | Not Configured | The Agency does not leverage Public folders currently, therefore this setting is not required. |
| Directory extension attribute synchronisation | Not Configured | Not required for this solution. |

AAD Connect configuration applicable to agencies leveraging a hybrid implementation.

|  |  |  |
| --- | --- | --- |
| Configuration | Value | Description |
| Installation Mode | Custom | The type of installation – Default or Custom. The Default install does not allow customisation of the filtering. |
| SQL Mode | Local DB | The location of the AAD Connect database. Local DB is the default configuration and the simplest to manage. |
| Directory to Connect to | {Agency}.gov.au | Azure AD Tenant of the Agency. |
| On-premises attribute to use for Azure AD (used for logging in to Azure AD) | User ID | This attribute is commonly used for logins as it will ensure that the same credentials are maintained for on-premises and in-cloud authentication. |
| Alternate ID | Not required | This is required in scenarios where primary ID may be duplicated between users in the organisation. |
| OU Filtering | Enabled {TBA by the Agency} | OU filtering will be used to ensure that specific OUs containing entities such as service accounts are not synchronised with Azure AD. OU filtering will be finalised during deployment and documented in As-Built-As-Configured documentation. |
| Uniquely Identifying Users | Users are represented only once across all directories.Let Azure manage the source anchor (ms-DS-ConsistencyGuid) | Default configuration. As users are not duplicated within the environment, this setting meets the solution requirements. The ms-DS-ConsistencyGuid is used when Azure manages the source anchor. |
| Azure AD Attributes | Default – All attributes | Default configuration. All attributes to be synchronised. |
| Synchronisation Interval | 30 minutes | Default synchronisation interval.Note: Password resets and new accounts are synchronised immediately. |

### Authentication Method

Authentication is the process of verifying one’s identity. Active Directory allows for the authentication of directory objects within the corporate network using a number of protocols such as LDAP and Kerberos.

In a hybrid scenario, authentication support is required outside the corporate network. In a hybrid scenario, credential authentication support is required outside the corporate network. This can be achieved using either:

* Cloud authentication – Cloud authentication utilises credentials stored within the cloud to authenticate users. The credentials can belong to cloud only accounts.
* Password hash synchronisation (PHS) – PHS synchronises a hash of the hash of a user’s on-premises password which has undergone a salting process before it is sent to Azure AD. If the user’s hashed password matches the stored password, the user is then authenticated. This means the authentication method will be handled in the cloud.
* Pass-through authentication (PTA) – This feature allows users to login to Azure services including Office 365 using their on-premises credentials. When authenticating, the user enters their credentials into an Azure authentication service. The service encrypts the credentials and place the request in a queue. The on-premises PTA agents read the queue and perform the decryption and validation against Active Directory. The outcome of the validation is sent via the PTA agent to the Azure authentication service to complete the user’s authentication request. Through the process no credentials are stored within Azure AD.
* Federation integration (AD FS) – Active Directory Federation Services (AD FS) allows users to login to Office 365 services using the organisations existing federation infrastructure. A federation trust is established between the corporate network and Azure AD with the authentication method being handled on-premises.

The following illustrates the pass-through authentication method and how it communicates across the network.

Authentication Architecture

Authentication Architecture

The following table describes the ports and protocols used in a hybrid configuration between on the PTA Agent and Azure AD. The hardware requirements for PTA agents are available in Appendix 1: AAD Connect and PTA agent hardware requirements.

|  |  |  |
| --- | --- | --- |
| Protocol | Port | Description |
| HTTP | 80 (TCP/UDP) | Enable outbound HTTP traffic for security validation such as SSL. Also needed for the connector auto-update capability to function properly. |

Authentication Method design considerations and decisions apply to the HYBRID solution.

|  |  |  |
| --- | --- | --- |
| Decision Point | Design Decision | Justification |
| Authentication method | PTA | To ensure passwords are controlled by on-premises Active Directory and are not synchronised and stored in the cloud. |
| Number of PTA agents | 3 | To ensure high availability 3 PTA agents will service authentication requests. The AAD Connect server and Staging server will form two of the agents. |
| HTTPS | 443 (TCP/UDP) | Enable outbound HTTPS traffic for operations such as enabling and disabling of the feature, registering connectors, downloading connector updates, and handling all user sign-in requests. |