Australian Government
Digital Transformation Agency

# Protected Utility Blueprint

## Platform Design

## March 2020

dta

# Contents

# Background

The DTA developed the Protected Utility Blueprint to enable Australian Government agencies to transition to a secure and collaborative Microsoft Office 365 platform. The solution is underpinned by proven technologies from the Microsoft Modern Workplace solution (Microsoft 365 including Office 365, Enterprise Mobility + Security, and Windows 10). The Blueprint design is delivered as three distinct documents:

- **Platform** – Provides technologies that underpin the delivery of the solution,
- **Workstation** – The client device, which is configured and managed by Microsoft Intune, and
- **Office 365** – Microsoft Office 365 productivity applications.

The Blueprints are accompanied by Configuration Guides and Security Documentation adhering to the Australian Cyber Security Centre (ACSC) PROTECTED requirements for Information and Communication Technology (ICT) systems handling and managing Government information. These artefacts provide a standard and proven Microsoft 365 solution aimed to fast track the adoption of the Microsoft Modern Workplace experience.

The following Blueprint documentation contains considerations for best practice deployment advice from the Australian Government Information Security Manual (ISM), relevant Microsoft hardening advice, the ACSC Essential Eight and the ACSC hardening guidelines for Microsoft Windows 10.

# Overview

## Purpose

This document provides the design of the platform technology components that will be implemented to support the solution. For technologies and services not covered, refer to the respective design document.

## Scope

*Table 1* describes the components that are in scope for the design.

Table 1 In Scope Components

| Component | Inclusions |
|---|---|
| Azure Active Directory | Domains<br>User Accounts<br>Agency Collaboration |
| Azure Active Directory Connect | Azure Active Directory Connect Client |
| Security | Microsoft Cloud App Security<br>Microsoft Defender Advanced Threat Protection<br>Security Information and Event Management<br>Monitoring |
| Client Configuration | Microsoft Intune<br>Printing |
| Backup | Office 365 Backup |
| System Administration | Windows Deployment<br>Role based Access Control |

## Beyond the Blueprint

The Blueprint is designed to provide a baseline cloud only offering for all government agencies. Even if a product is licenced for use under Microsoft, it may not be included in this Blueprint if it is not required for all agencies. An organisation may have additional requirements that will need to be considered outside of this Blueprint

# Documentation

## Associated Documentation

*Table 2* identifies the Associated Documents that were referenced during the creation of this design.

Table 2 Associated Documentation

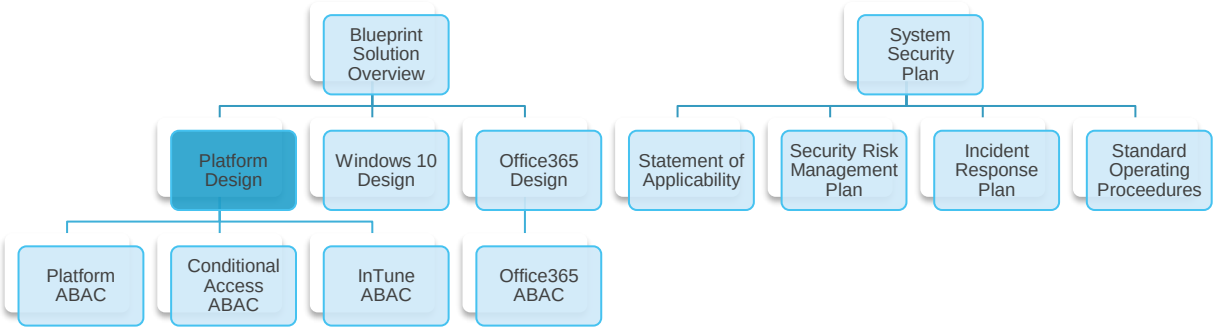
| Name | Version | Date |
|---|---|---|
| ACSC - Hardening Microsoft Office 365 ProPlus, Office 2019 and Office 2016[1] | N/A | 01/2020 |
| ACSC - Hardening Microsoft Windows 10, version 1709, Workstations[2] | N/A | 01/2020 |
| Azure - ACSC Consumer Guide - Protected - 2018 | N/A | 08/2018 |
| Australian Government Information Security Manual (June 2019) | N/A | 10/2019 |
| DTA – Blueprint Solution Overview | March | 03/2020 |
| DTA – Workstation Design | March | 03/2020 |
| DTA – Office 365 Design | March | 03/2020 |
| DTA – Office 365 – ABAC | March | 03/2020 |
| DTA – Platform – ABAC | March | 03/2020 |
| DTA – Intune Security Baselines – ABAC | March | 03/2020 |
| DTA – Software Updates – ABAC | March | 03/2020 |
| DTA – Intune Applications – ABAC | March | 03/2020 |
| DTA – Intune Enrolment – ABAC | March | 03/2020 |
| DTA – Conditional Access Policies – ABAC | March | 03/2020 |
| DTA – Intune Compliance – ABAC | March | 03/2020 |
| DTA – Intune Configuration – ABAC | March | 03/2020 |
| Protective Security Policy Framework – Sensitive and classified information[3] | 2018.2 | 02/2018 |

[1] https://www.cyber.gov.au/publications/hardening-microsoft-office-2016
[2] https://www.cyber.gov.au/publications/hardening-microsoft-windows-10-build-1709
[3] https://www.protectivesecurity.gov.au/sites/default/files/pspf-infosec-08-sensitive-classified-information.pdf

## Document Structure

This document is part of the blueprint set of documents as shown in Figure 1 and assumes the audience is familiar with Azure AD and Office 365  installation and configuration.

Figure 1 - Blueprint Documentation Set




This document covers the information as described in *Table 3*

Table 3 Document Structure

| Section | Description |
|---|---|
| Design Considerations | This section details items that should be taken into consideration during and after the deployment of this solution. |
| Licencing | This section describes the VSA licence and recommendations. |
| Identity and Access Management | This section details the authentication and authorisation methods used within the blueprint. |
| Collaboration | This section details the applications used for collaboration and recommendations guiding when and how to decide who to collaborate with. |
| Security | This section details the cloud-based security components available within the Microsoft 365 suite. |
| Client Configuration | This section details the Intune management methods and design decisions for the client configuration. |
| Backup and Operational Management | This section details the backup design decisions |

| | |
|---|---|
| System Administration | This section details how the solution will be managed, the administrative consoles that will be used to administrator the various components, and how Role Based Access Control (RBAC) is implemented to control access. |

# Design Considerations

This section details items that should be taken into consideration during and after the deployment of this solution. These items do not affect this design but may impact the success of the solution once deployment has commenced or completed.

## Hardware MFA Token Support

Azure Multifactor Authentication (MFA) natively supports the OATH (Open Authentication) standard for selected hardware tokens. To use Azure MFA with OATH support, hard tokens would need to be purchased and deployed to users. Hard tokens are required to achieve an Essential 8 Maturity level of 3.

## Security Information and Event Management

Microsoft Office 365 and Microsoft Azure solutions hold audit data for a period of time based on the service and the license level of the organisation. The time period for most services is under 2 years. For organisations with a requirement to hold audit data past this period, Security Information and Event Management (SIEM) integration should be considered.

Service audit data within the Microsoft Office 365 and Azure clouds is often housed in discrete systems and the opportunities to bring the data under a single pane is limited. Azure Monitor or Azure Sentinel are two Microsoft offerings which could be leveraged for this purpose however a holistic solution should be considered to ensure any legislative requirements are met.

## Internet Access

The solution has been designed to allow government organisation end user devices internet access from anywhere (head office, regional office or home) direct connected and via proxy servers, VPN servers or Security Internet Gateways (SIGs).

Where connected through a proxy server, rules will be configured to allow direct connection for some Office 365 services.

Mobile users will access Microsoft 365 services directly, not via the SIG. These users will be subject to Conditional Access policies to reduce unauthorised access risk.

# Licencing

While agencies could meet their obligations under the ISM, PSPF, and ACSC cloud guidance under alternate licensing models, agencies will achieve a more cost-effective approach through a single subscription of Microsoft 365 E5. Agencies will also have access to additional components that may assist in future enhancements to their environment.

The recommended licensing model to deploy the Blueprint is a single subscription of Microsoft 365 E5, with one licence required for each user as described in Table 4.

For agencies looking to alternate licensing arrangements, at a minimum, Microsoft recommends the following licensing in addition to the VSA 4 Common Cloud Commitment:

- Microsoft 365 E5 Security
- Microsoft 365 E5 Compliance

The VSA 4 Common Cloud Commitment[4] consists of:

- Windows 10 E3
- Office 365 E3
- Enterprise Mobility and Security E3
- Productivity server licences (Exchange Server, SharePoint Server, Lync/Skype Server)
- Office Device licences

These recommendations require a minimum subscription requirement of Microsoft 365 E3, Enterprise Mobility and Security E5 and Microsoft 365 E5 Compliance with one licence required for each user.

This alternate configuration will not provide access to Azure Active Directory Premium P2 licencing meaning that the following components would need to be removed from this design:

- Azure Active Directory Identity Protection
- Azure Active Directory Privileged Identity Management (PIM)

While this meets the Microsoft minimum guidance and will comply with the requirements of the ISM, the exclusion of these two features reduces the effectiveness of the security controls. Specifically, the Just-In-Time administrative access provided by PIM and the automated responses to detected suspicious activities will not be available.

[4] July 2019 – July 2022

Table 4 describes the Licence design decisions.

Table 4 Licence Design Decisions

| Decision Point | Design Decision | Justification |
|---|---|---|
| Subscription Count | One | Only one subscription is required for the deployment. Within this subscription one licence will be required for each user. |

*Table 5* describes the Subscription configuration.

Table 5 Subscription Configuration

| Configuration | Value | Description |
|---|---|---|
| Subscription Name | Agency Name | As per Agency naming standards. |
| Subscription Purpose | Production workload | Subscription required to support the desktop solution. |
| Subscription ID | Generated after the subscription has been activated | Provided by Microsoft. |
| Subscription type | Enterprise Agreement | Provided by the Agency. |
| Subscription offer | Pay-As-You-Go | Agencies will only pay for what they use. |

# 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

### Description

Azure Active Directory (Azure AD) is a cloud-based directory service which stores identity information and offers 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.

### Design Considerations

Azure Active Directory (AAD) is Microsoft's cloud-based identity and access management service, which allows users to sign in and access to 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 feature**s – Azure AD preview features control how new self-service features are made available to users.
- **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.

## Design Decisions

*Table 6* describes the Azure AD design decisions.

Table 6 Azure AD Design Decisions

| Decision Point | Design Decision | Justification |
|---|---|---|
| Identity Source | Azure AD | As this is a cloud only solution Azure AD will be the source of identity. |
| Restrict access to the Azure AD administrative portal | Enabled | To meet the Department's security requirements. |
| Allow LinkedIn connections | Disabled | To meet the Department's requirements not to share information with third party organisations without approval. |
| Restrict access to the Azure AD administrative portal | Enabled | To meet the Department's security requirements. |
| Synchronise to Active Directory | Not Configured | Not required as on-premises Active Directory will not be deployed. |
| Azure Self Service 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. |
| Role Based Access | Configured | Role Based Access Control (RBAC) will be used for assigning access to resources through PIM (Privileged Identity Management). |

| | | |
|---|---|---|
| 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. |
| Identity Format | Configured | Usernames will conform to firstname.lastname<sequence number><br>Note: The sequence number is only required if duplicate names would be created. |
| Enterprise Applications | Not Configured. | No enterprise applications have been identified |

# Emergency Access Admin Accounts

## Description

Emergency access or 'break glass' accounts are required in case all accounts are locked out.

## Design Considerations

To avoid accidental lockout scenarios that can occur if, for example Conditional Access is misconfigured, or all privileged administrator accounts are compromised in another capacity, mitigation must be implemented in the way of 'emergency access administrative accounts.

Microsoft best practice[5], two emergency access accounts (otherwise known as Break Glass accounts) are to be generated and stored safely.

## Design Decisions

*Table 7* describes the Emergency Access Account design decisions.

Table 7 Emergency Access Account Design Decisions

| Decision Point | Design Decision | Justification |
|---|---|---|
| Emergency Access accounts required | Create 2 break glass accounts | Microsoft and security best practice |

[5] https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-emergency-access

*Table 8* describes the Emergency Access Account configuration.

Table 8 Emergency Access Account Configuration

| 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 |
| Password Expiry | Passwords are set to never expire | The passwords to these accounts are set to never expire or be cleaned up or removed due to inactivity |
| 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 |
| 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

## Description

Azure AD Identity Protection enables configuration of automated responses to suspicious activities and actions related to user identities.

## Design Considerations

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 (TOR), 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.

## Design Decisions

*Table 9* describes the Azure AD Identity Protection design decisions.

Table 9 Azure Active Directory Identity Protection Design Decisions

| Decision Point | Design Decision | Justification |
|---|---|---|
| Azure AD Identity Protection | Enable the sign-in risk policy and user risk policy within the Azure AD tenants. | Provide reporting of detected suspicious sign-in activity based on defined MFA, sign-in risk and user risk policies. |
| 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. |

| | | |
|---|---|---|
| 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. |

# Azure AD Multifactor Authentication

## Description

Employing multiple authentication factors present a significant challenge for attackers gaining access to a system. Even if an attacker manages to learn the user's password, it is useless without also having possession of the additional authentication method. It works by requiring two or more of the following authentication methods:

- Something you know (a password)
- Something physically, you have (a hardware token or software token on a phone)
- Something you are (biometrics)

## Design Considerations

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[6]. Conditional Access polices are the recommended method to determine MFA conditions.

## Design Decisions

*Table 10* describes the Azure AD Multifactor Authentication design decisions.

Table 10 Azure AD Multifactor Authentication Design Decisions

| Decision Point | Design Decision | Justification |
|---|---|---|
| MFA | Configured – Mobile App | 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. |
| MFA for Administration | Enforced | Administration though the Azure Portal and other Cloud Apps will require MFA. |
| MFA for User Apps | Enforced | MFA is required. |
| Hardware Token Support | Allowed (supported OATH tokens only)[7] | The default method will be to use soft tokens 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 justification. Having hard tokens will ensure you reach Essential 8, level 3 maturity for multifactor authentication. |
| Trusted IPs | Not configured | Conditional Access policies will be used in place of the legacy 'Trusted IP' feature. |

[6] For more information about Trusted IPs see https://docs.microsoft.com/en-au/azure/active-directory/authentication/howto-mfa-mfasettings#trusted-ips.

[7] **Note**: OATH tokens are to be purchased separately if required.

| | | |
|---|---|---|
| Azure AD MFA Configuration | Enforced | Native Azure MFA will be configured to secure access to applications and desktops from outside of the Blueprint environment, and administration functions. Refer to DTA-Platform-ABAC document for detailed settings. |

# Conditional Access

## Description

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.

## Design Considerations

Conditional Access provides 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.

## Design Decisions

*Table 11* describes the Conditional Access design decisions.

Table 11 Conditional Access Design Decisions

| 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. |

Table 12 describes the Conditional Access configuration.

Table 12 Conditional Access Configuration

| Configuration | Value | Description |
|---|---|---|
| Conditional Access Policies | BLOCK - Legacy Authentication | This global policy blocks all connections from unsecure legacy protocols like ActiveSync, IMAP, PO3, 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. |

# Collaboration

## Description

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

## Design Considerations

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
- The partner organisation has been assessed at the same security level

Collaboration between organisations assessed at the same security level is relatively straight forward while collaboration between organisations with 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 things like printing or faxing of documents, taking a photo of a computer screen, etc. 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[8]. 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.

In the context of this solution, Azure AD Business-to-Business has been identified as the optimal collaboration option. 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

[8] https://www.cyber.gov.au/publications/fundamentals-of-cross-domain-solutions

- SharePoint Online

Azure AD supports a number of B2B access scenarios to enable users within external organisations to collaborate with a host organisation. The method to be implemented based on this design is to grant a user authentication 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 the external users that are being invited have the appropriate nationality and clearances held.

Commonality across a base set of identity factors will assist in guiding decision making on external collaboration. Agencies adopting this solution should follow the below standards as a minimum, to achieve a level of consistency and assurance to other organisations seeking to collaborate using this platform.

CISOs will need to assess and accept any risks associated with collaboration with outside organisations.

## Design Decisions

*Table 13* describes the identity properties that should be considered to be a minimum requirement before collaboration is enabled.

Table 13 Identity properties

| Field | Example | Justification |
|---|---|---|
| FirstName | John | |
| LastName | Smith | |

| | | |
|---|---|---|
| UserName (UPN) = EmailAddress | john.smith3@desktop.onmicrosoft.gov.au or john.smith3@desktop.gov.au | Be able to validate outside of the technology that the user being invited to the collaborative workspace is who they say they are. |
| UserName | John.smith3 | |
| EmailAddress | John.smith3@desktopa.gov.au | |
| OfficePhone | 61411 2999 | |
| MobilePhone | 0411 123 456 | |
| Photo | ID.JPEG | |
| JobProfile | Finance | Users job description in identifying appropriate contact. |
| Department | Digital Transformation Agency | Manager of the guest user for further verification if required. |
| Manager | Julie Citizen | |

In addition to the identity properties listed above, multi-factor authentication and conditional access policies should also be enabled in the partner organisation.

*Table 14* describes the minimal conditional access policies that should be applied by the partner organisation.

Table 14 Conditional Access Policies

| Decision Point | Design Decision | Justification |
|---|---|---|
| Conditional Access Policies | **BLOCK - Legacy Authentication:**<br>This global policy blocks all connections from unsecure legacy protocols like ActiveSync, IMAP, PO3, etc.<br>**BLOCK - Countries not Allowed:**<br>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 |

# Security

## Microsoft Cloud App Security

### Description

Microsoft Cloud App Security provides administrators visibility into cloud application activities. It contains several tools to help uncover shadow IT, assess risk, enforce policies, investigate activities, and stop threats.

### Design Considerations

To complete these tasks, Cloud App Security:

- Maps and identifies the cloud apps being leveraged within the environment using Cloud Discovery
- Sanctions and un-sanction apps within the environment
- Integrates with apps using app connectors
- Integrates with conditional access to provide real time visibility and control over access and activities within your cloud apps
- Allows the setting and fine tuning of policies
- Integrates with Microsoft Flow to perform automated actions based on policy alerts

### Design Decisions

*Table 15* describes the Cloud App Security design decisions.

Table 15 Cloud App Security Design Decisions

| Decision Point | Design Decision | Justification |
|---|---|---|
| Cloud App Security | Configured | Cloud App Security will be deployed with default settings to increase the security of the solution and report on shadow IT activities.<br>Policies will be tuned over the life of the system as required. |

# Cloud Discovery

## Description

The Cloud Discovery component of Cloud App Security utilises traffic logs to discover and analyse the cloud apps being used. These traffic logs can be manually uploaded from proxies and firewalls or automatically through the use of Cloud App Security Log collectors.

## Design Considerations

Once uploaded, the logs are compared against Microsoft's Cloud App Catalogue of over 16,000 cloud apps. The results are then ranked and scored based on 70+ risk factors. These risk factors provide visibility into cloud use and shadow IT risks.

Cloud Discovery is useful in scenarios where Office 365 and cloud identities have been used for a period of time with little oversight.

## Design Decisions

*Table 16* describes the Cloud App Security Cloud Discovery design decisions.

*Table 16 Cloud App Security Cloud Discovery Design Decisions*

| Decision Point | Design Decision | Justification |
|---|---|---|
| Cloud Discovery | Not Configured | Cloud applications to be deployed by this solution are first-party Microsoft applications in a new Office 365 tenant. As adding of new applications is blocked by policy, this feature is not required for this solution |

# App Connectors

## Description

App Connectors represent API integration between cloud apps and Cloud App Security. The use of app connectors enhances the visibility administrators have into the cloud apps being utilised within the environment. At the time of writing there are 11 available App Connectors. These are:

- Microsoft Azure

- Microsoft Office 365
- Amazon Web Services
- Box
- Cisco Webex
- Workday
- Dropbox
- G Suite
- Okta
- Salesforce
- ServiceNow

## Design Considerations

Depending on the connector, this visibility can include:

- **Account information -** Visibility into users, accounts, profile information, status (suspended, active, disabled), groups, and privileges
- **Audit trail -** Visibility into user activities, admin activities and sign in activity
- **Data scan -** Scanning of unstructured data using two processes -periodically (every 12 hours) and in real-time scan (triggered each time a change is detected)
- **App permissions -** Visibility into issued tokens and their permissions
- **Account governance -** Ability to suspend users, revoke passwords
- **Data Governance -** Ability to quarantine files, including files in trash, and overwritten files
- App permission governance - Ability to remove tokens

## Design Decisions

Table 17 describes the App Connectors design decisions.

*Table 17 App Connectors Design Decisions*

| Decision Point | Design Decision | Justification |
|---|---|---|
| App Connectors | Configured | To provide insights into Office 365 and Azure components building the overall security picture. |

| | | |
|---|---|---|
| Applications Connected | Office 365 | Microsoft Office 365 will be connected as it is the main business application for agencies. |

Table 18 describes the App Connectors configuration.

*Table 18 App Connector Configuration*

| Configuration | Value | Description |
|---|---|---|
| Configured Connectors | Microsoft Azure<br>Microsoft Office 365 | Applications which have API integration with Cloud App Security. |
| Microsoft Azure Connector Configuration | N/A | The Microsoft Azure Connector does not have any configuration settings |
| Microsoft Office 365 Connector Configuration | Selected Components:<br>Azure AD Users and Groups<br>Azure AD Management events<br>Azure AD Sign-in events<br>Azure AD Apps<br>Office 365 activities<br>Office 365 files | All components of Office 365 on which Cloud App Security can obtain information |

# Conditional Access App Control protection

## Description

Cloud App Security integrates with Conditional Access policies within Azure AD to provide additional functionality in the form of App Control Protection. App Control Protection reverse proxies' access to applications as opposed to granting direct access.

## Design Considerations

This reverse proxy architecture allows:

- **Block on download -** Block the download of sensitive information
- **Protect on download -** Require documents to be encrypted on download
- **Monitor low-trust user sessions -** Risky users actions are logged for analysis
- **Block access -** Block access to specific applications if the user is coming from unmanaged devices or non-corporate networks

- **Create read-only mode -** Monitoring and blocking custom in-app activities
- **Restrict user sessions from non-corporate networks -** Restricted application access when a user is coming from a non-corporate network

## Design Decisions

*Table 19* describes the Conditional Access App Control Protection design decisions.

*Table 19 Conditional Access App Control Protection Design Decisions*

| Decision Point | Design Decision | Justification |
|---|---|---|
| Conditional Access App Control Protection | Not Configured | Conditional Access App Control Protection will not be configured as Conditional Access policies will prevent untrusted devices and users from accessing to information. |

# Policies

## Description

A Policy within Cloud App Security is a selection of activities which are monitored. When the activity occurs, alerts are triggered. Policies are designed to detect when risky behaviour, violations, or suspicious data points and activities are detected within the environment.

## Design Considerations

Cloud App Security has a number of templates that can be used to configure policies. These templates are categized into the following categories:

- **Access Policy** – Real time monitoring and control over user logins to cloud apps
- **Activity Policy** – Enforcement of automated processes using the app API
- **Anomaly Detection Policy** – Monitoring for unusual activities within the cloud
- **App Discovery Policy** – Monitoring for new applications within the organisation
- **Cloud Discovery Anomaly Detection Policy** – Monitoring for unusual occurrences within the cloud app discovery logs
- **File Policy** – Scanning cloud applications for specified files, file types, or data types and enforcing governance actions

- **Malware Detection Policy** – Scanning cloud applications for files containing malware
- **OAUTH App Policy** – Monitoring of cloud application registrations and the permissions requested
- **Session Policy** – Real time monitoring and control over user activities in cloud apps

## Design Decisions

*Table 20* describes the Cloud App Security Policies design decisions.

Table 20 Cloud App Security Policies Design Decisions

| Decision Point | Design Decision | Justification |
|---|---|---|
| Cloud App Security Policies | Default Configuration | The default policies provide visibility into the activities conducted within the environment. Policies can be created, reviewed, and tuned by agency administrators at a later stage. This includes detection of risk behaviour, violations etc. |

# Microsoft Defender Advanced Threat Protection

## Description

Microsoft Defender Advanced Threat Protection (ATP) extends the standard Microsoft Defender capabilities to provide additional reporting, pre-breach protection, post-breach detection, automation and response. Microsoft Defender ATP does not require an agent on the endpoint or any on-premises infrastructure, instead it leverages Microsoft's cloud platform. A single dashboard allows administrators to monitor the compliance and security of all ATP-enabled devices, as well as providing ISO27001 certified Endpoint Detection and Response (EDR) functionality.

## Design Considerations

Microsoft Defender Advanced Threat Protection can be configured with the following options:

- **Data Retention Period** - Data Retention Period defines how long gathered telemetry data is stored and available for use in online reporting
- **Alert Notifications** - Alert Notifications are configurable rulesets that allow a person or group of people to receive a notification on the occurrence of a pre-set event

- **Secure Score Baseline** - Secure Score Baseline configures the product baselines for calculating the score of Microsoft Defender security controls on the secure score dashboard. If third-party solutions are in use the corresponding controls should be excluded from the calculations
- **Administration Roles and Machine Groups** - Administration roles provide the ability to configure role-based access and granular options for regulating permissions to portal features and data. Machine groups enabled machines to be organised into groups and apply configured automated remediation levels and assigned administrators

## Design Decisions

*Table 21* describes the Microsoft Defender Advanced Threat Protection design decisions.

Table 21 Microsoft Defender Advanced Threat Protection Design Decisions

| Decision Point | Design Decision | Justification |
|---|---|---|
| Microsoft Defender ATP | Configured | To provide increased security and meet the requirements of this document. |
| Sample Collection | Enabled | Required configuration to enable Windows ATP. |
| Data storage location | US | As of June 2019, the available Azure data centres to host Windows Defender ATP are located in the US, UK and Europe. All data used by Windows Defender ATP is protected at minimum by Advanced Encryption Standard (AES) 256-bit encryption, both at rest and inflight[9] |
| Data Retention Period | 180 Days | Default configuration and suitable for the organisation's requirements. |
| Alert Notifications | Send Information, Low, Medium, High to Security team. | Alerts will be sent to organisation Cyber Intelligence team for action. |

[9] For more information, please refer to https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/data-storage-privacy-windows-defender-advanced-threat-protection

| | | |
|---|---|---|
| Secure Score Baseline | Windows Defender Antivirus<br>Windows Defender Application Control<br>Windows Defender Exploit Guard<br>Windows Defender Application Guard<br>Windows Defender SmartScreen<br>Windows Defender Firewall<br>Windows Defender Credential Guard<br>Windows Defender Attack Surface Reduction | Meets the requirements of this design |
| Administration Roles | Configured. Refer to DTA – Intune Configuration - ABAC document. | Administrative roles will be segregated as per the ACSC Restricting Administrative Privileges (April 2019) guide. |
| Machine Groups | All Clients | Machines will be segregated into groups with automated remediation levels assigned the administrators that monitor these groups. Groups will be developed with the Department and documented in the As-Built-As-Configured documentation. |

# Log Analytics

## Description

Log data collected is stored in a Log Analytics workspace.

## Design Considerations

Log data stored in Log Analytics data can be consumed in various ways:

- **Azure Portal** - Azure Portal allows you to create Log queries and analyse the results.
- **Azure Monitor Alert rules** - An alert rule is a search that is automatically run at regular intervals. The results are inspected to determine if an alert in Azure Monitor should be generated.
- **Azure Dashboards** - Dashboards can be used per Azure user to visualise data gathered from Log Analytics, these dashboards can be shared amongst Azure administrators.
- **Export** - Data from Azure Monitor can be imported into Excel or Power BI for further visualisation.

- **PowerShell** – PowerShell from a command line or using Azure Automation, can programmatically retrieve data for various use-cases.
- **Azure Monitor Logs API** - The native API, uses REST to retrieve log data from the workspace.

Log Analytics is billed per gigabyte (GB) of data ingested and retained into the service. When ingesting into a SIEM, data retention periods can be shortened.

Log Analytics is available is certain regions only. At the time of writing, these regions are Australia Southeast (Melbourne) and AU Central (Canberra CDC Fyshwick).

## Design Decisions

*Table 22* describes the Log Analytics design decisions.

Table 22 Log Analytics Design Decisions

| Decision Point | Design Decision | Justification |
|---|---|---|
| Log Analytics Workspace | Deployed | The Log Analytics workspace will primarily be used to store log data for Intune managed workloads. |
| Pricing mode | Per GB | Log Analytics pricing is based on data consumed. |
| Incurs Subscription Cost? | Yes | Log Analytics pricing is based on data consumed. Data Volume could be reduced to 90 days if the agency has an existing SIEM for further custom log analysis. |

*Table 23* describes the Log Analytics Configuration.

Table 23 Log Analytics Workspace Configuration

| Configuration | Value | Description |
|---|---|---|
| Workspace Name | agency-log-workspace | Organisation log workspace name to be confirmed by the Department |
| Azure Subscription | Agency subscription | Configured by Office 365 |
| Region | Australia Central | Closest location of Log Analytics to the Department |
| Log retention | Retention Period: 1 year<br>Data Volume Cap: Off | One year aligns with other data retention periods in this solution and meets the system requirements |
| Log Analytics Contributor Group | rol-agency-log-admin | Organisation log workspace name to be confirmed by the Department |

# Client Configuration

This section details the methods of client configuration.

## Group Policies

This blueprint does not make use of group policies.

## System Center Configuration Manager

This blueprint does not make use of System Center Configuration Manager.

## Co-Management

This blueprint does not make use of Co-Management.

## Intune

### Description

Microsoft Intune is an Azure service that provides Mobile Device Management (MDM) and Mobile Application Management (MAM) capabilities for Apple iOS, Google Android and Microsoft Windows devices to enhance security and protection.

### Design Considerations

Intune manages which devices can access corporate data, protects company information by controlling the way data is shared, and enforces device configuration to ensure security requirements are met. It does this via:

- **Device Enrolment Profiles** – Prior to managing devices in Intune they must be enrolled as either Personal or Corporate devices. These can either be self-enrolled or automatically enrolled.
- **Device Compliance Policies** – Device Compliance Policies are rules, such as device PIN length or encryption requirements, that can be applied to devices. These rules must be met before a device is considered compliant. Device Compliance can then be used by services such as Conditional Access.

- **Device Configuration Profiles** - Device Configuration Profiles provide the ability to control settings and features on supported endpoints. These include, device and user settings, browser settings and hardware settings. Device Configuration Profiles can be deployed to specific users or devices in Azure AD groups
- **Device Security Baselines** – Security baselines are pre-configured groups of Windows settings that are recommended by Microsoft security teams. The security baselines are templates and are used to create a profile that is specific to the environment for deployment.
- **Client Applications** – Client applications can be delivered to devices registered in Intune based on device type and group membership. Application types that can be distributed include store apps, MS Office suite, MS Edge browser, web links, line of business and Win32 applications. Monitoring of application distribution is provided.
- **Software Updates** – Software update policies store the configuration of updates without the updates themselves. This prevents the need to approve individual updates allowing for a faster turnaround time. Individual policies can be created and targeted to different groups of devices.

When devices are enrolled into Intune, authorised administrators are able to view hardware details, how the device is used, and what compliance levels currently are for the device's software, hardware, and operating system.

Additionally, Intune can present a customised Company Portal to end users which can be used to install and launch applications or websites via single sign-on (SSO) authentication.

Intune is a component of EMS and integrates with other EMS components such as Azure AD and Azure Information Protection (AIP) natively. This allows for total granular visibility of all endpoints within the Enterprise Mobility Management sphere and simplifies the approach for management.

To compliment this visibility, an Intune Data Warehouse can be deployed to capture and create custom reports from Intune data using a reporting service. This can assist in gaining insight into which users are using Intune, what licences are being used, operating system and device breakdowns, and compliance trends. The Data Warehouse also has the capability to export directly to Power BI and create interactive & dynamic reports.

Intune can also configure Windows Information Protection (WIP) polices. WIP can be deployed to:

- **Protect against potential data leakage** – WIP protects against potential data leakage without any impact to user functionality
- **Protect enterprise applications and data** - WIP protects against accidental data leakage on enterprise-owned and personal devices. This can occur without changes to the corporate environment or applications

Within WIP, Network boundaries are created as a network perimeter that controls what applications can be accessed on the network.

## Design Decisions

*Table 24* describes the individual Intune design decisions.

Table 24 Intune Features Design Decisions

| Decision Point | Design Decision | Justification |
|---|---|---|
| Co-management | Disabled | Co-Management is disabled as this is not a function that is used in a cloud only solution. |
| Enrolled Device Types | Windows 10: 10.0.17134 (minimum)<br>iOS | The use of Windows 10 on designated hardware is mandatory.<br>The following platforms will be disabled:<br>macOS<br>Android |
| Device Compliance | Enabled | Device Compliance will be enabled. All devices will be Intune enrolled and have a custom set of compliance policies applied. |
| Device Enrolment | Enabled | All users must be enrolled to ensure device compliance. |
| Company Portal | Enabled | The Company Portal will be enabled for application deployment. Applications to be deployed will be set by requirements. |
| Conditional Access | Enabled | Conditional Access is enabled. It will leverage device & user compliance to allow or disallow access to the corporate environment. |
| Mobile Device Management (MDM) | Enabled | MDM will be used to control what a user can and cannot do on their mobile device defined by policies set by administrators. |
| Mobile Application Management (MAM) | Enabled | MAM will be used to ensure that users have access to the apps they need to do their work. |
| Windows Information Protection mode | Configured | Default settings prevent copying and pasting of data between ‘work’ locations and other ‘personal’ locations. |

| | | |
|---|---|---|
| Network Boundaries | Cloud resources | Network boundaries create a list of resources that are considered to be on the enterprise network. These boundaries are used to apply policies that reside in these locations. |
| Cloud Resources Protected via Network Boundaries | SharePoint<br>Office 365 | Different policies will be created depending on the network location of the client. |
| Intune Data Warehouse | Not enabled | While this feature is available, it will not be deployed for the solution. |
| *Self Service Group Management* | | |
| Owners can manage group membership requests in the Access Panel | No | Group creation and modification is to be locked down and controlled by authorised personnel, such as service desk staff, or Administrators. |
| Restrict access to Groups in the Access Panel | No | Accessing groups is an Administrative function and has been locked down to Administrators. |
| *Security Groups* | | |
| Users can create security groups in Azure portals | No | Group creation and modification is to be locked down and controlled by authorised personnel, such as service desk staff, or Administrators. |
| *Office 365 Groups* | | |
| Users can create Office 365 groups in the Azure portals | No | Group creation and modification is to be locked down and controlled by authorised personnel, such as service desk staff, or Administrators. |
| *Directory-wide Groups* | | |
| Enable an "All Users" group in the directory | No | This group is not required. All users to be a member of a controlled group. |

# Mobile Application Management

## Description

MAM allows the management and protection of an organization's data within an application.

## Design Considerations

Using MAM without enrolment (MAM-WE), a work-related app that contains sensitive data can be managed on almost any device. Many productivity apps, such as the Microsoft Office apps, can be managed by Intune MAM.

## Design Decisions

*Table 25* describes the Mobile application management design decisions.

Table 25 Mobile application management design decisions

| Decision Point | Design Decision | Justification |
|---|---|---|
| Mobile Application Management Method | Intune | Mobile applications will be deployed via Intune as this is a cloud only solution. |
| Applications Managed | Microsoft Suite- Outlook, Word, Excel, SharePoint and Teams | These core Microsoft business applications will be managed via Intune as all users will require them to conduct their day to day business. |

# Enrolment

## Description

Prior to managing devices in Intune, devices must be enrolled as either Personal or Corporate devices. These can either be self-enrolled or automatically enrolled.

## Design Considerations

After devices are enrolled, they become managed. Agencies can assign policies and apps to the device through a mobile device management (MDM) provider, such as Intune.

## Design Decisions

Table 26 describes the Enrolment design decisions.

Table 26 Enrolment Design Decisions

| Decision Point | Design Decision | Justification |
|---|---|---|
| Windows Enrolment | Configured | Windows 10 devices must be enrolled in Intune prior to management of the device. |

# Windows AutoPilot

## Description

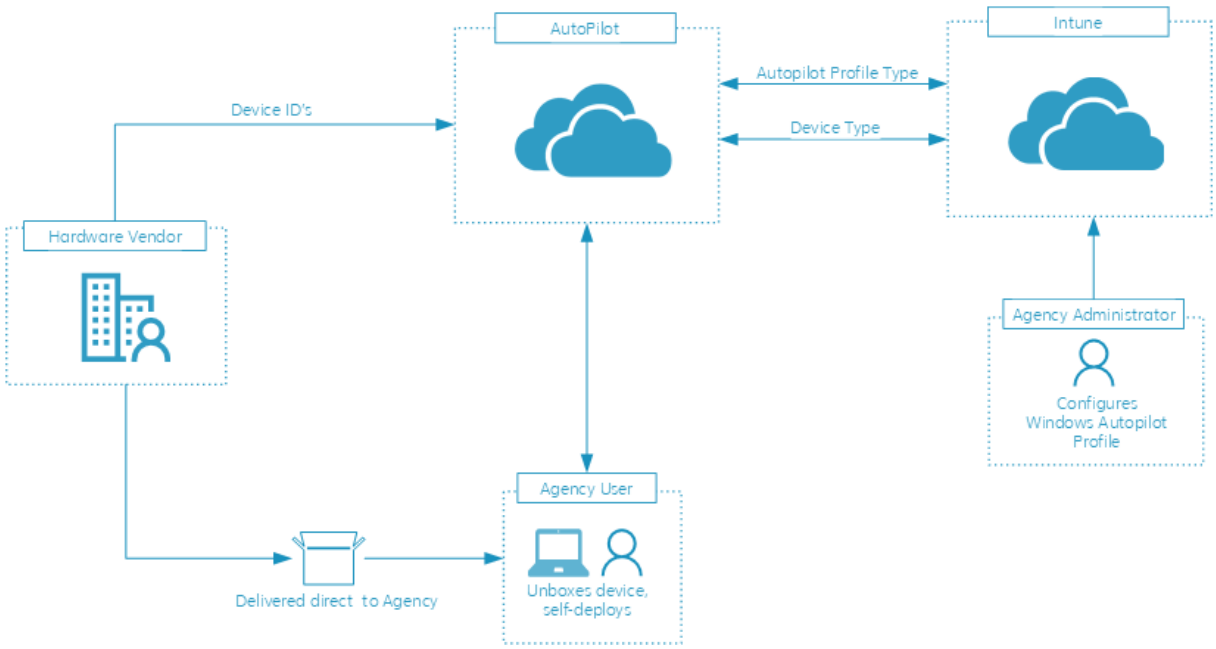
Windows Autopilot provides the ability to set up and pre-configure new devices without the need for on premises infrastructure. It is also possible to use Windows Autopilot to reset, repurpose and recover devices.

## Design Considerations

Windows Autopilot provides the ability to:

- **Automatically join devices** – Azure Active Directory (Azure AD)
- **Auto-enrol devices** – Auto-enrol MDM services, such as Microsoft Intune
- **Restrict the Administrator** – Restrict administrator account creation
- **Create and auto-assign devices** – Auto assign to configuration groups based on a device's profile

Figure 2 – Autopilot Deployment




## Design Decisions

*Table 27* describes the Autopilot Design Decisions design decisions.

Table 27 Autopilot Design Decisions

| Decision Point | Design Decision | Justification |
|---|---|---|
| Automatically Join Devices | Azure Active Directory (Azure AD) | Devices will automatically joint the Azure Active Directory |
| Auto-enrol devices | Configured | Enrolled automatically into Intune MDM |
| Restrict the Local Administrator Account | Configured | Aligns with the ACSC Hardening Microsoft Windows 10 1709 Workstations |
| Create and auto-assign devices | Configured | For ease of management and enrolment for devices within organisations |
| Deployment profile | Refer to DTA – Intune Enrolment - ABAC document | Deployment profile will ensure that all workstations are configured in accordance with the agency standards with no user intervention. |

# Compliance Assessment

## Description

Compliance policies define the rules and settings that users and devices must meet to be compliant.

## Design Considerations

Multiple compliance policies increase the complexity of evaluating the compliance.

Where multiple compliance policies are used it is recommended that there are no overlapping settings.

## Design Decisions

*Table 28* describes the Compliance Assessment design decisions.

Table 28 Compliance Assessment Design Decisions

| Decision Point | Design Decision | Justification |
|---|---|---|
| Compliance Assessment | Configured | Since mobile devices routinely leave the office environment, and the protection it affords, it is important that organisations develop a mobile device usage policy governing their use. |

# Device Configuration

## Description

Device configuration profiles are created and assigned to groups of users or devices enabling the automatic configuration of devices in much the same way as group policies.

## Design Considerations

Device configuration profiles can be created for the following platforms:

- Android
- iOS/iPadOS

- macOS
- Windows Phone 8.1
- Windows 8.1 and later
- Windows 10 and later

Within each platform there are number of profile types allowing many settings to be configured. The profile types and settings that are configurable vary depending on the platform.

In general terms, configuration profiles either configure the device for use by the user or secure the device.

Custom profiles can be created for a platforms although this should be considered a last resort if the settings are not available in any other way.

## Design Decisions

*Table 29* describes the Device Configuration design decisions.

Table 29 Device Configuration Design Decisions

| Decision Point | Design Decision | Justification |
|---|---|---|
| iOS policies | Configured | Intune policies are applied easing management |
| Windows 10 and later polices | Configured | Intune policies are applied easing management |
| Device security policies | Configured by exception | Security baselines as discussed below provide a better option when the settings are available. |

# Security Baselines

## Description

Security baselines are pre-configured groups of Windows settings. The pre-configured settings include the recommended settings by each relevant Microsoft product group.

## Design Considerations

When using a security baseline in Intune, a profile is created using a template that consists of multiple device configuration profiles.

A security baseline profile is created using an instance of the template which is then modified as required using the Microsoft best practice as the starting point.

Over time it is expected that Microsoft will update the baseline templates.

The following security baselines templates are currently available:

- Windows 10 Security Baselines
- Microsoft Defender ATP Baselines
- Microsoft Edge Baseline

## Design Decisions

Table 30 describes the Security Baseline design decisions.

*Table 30 Security Baseline Design Decisions*

| Decision Point | Design Decision | Justification |
|---|---|---|
| Windows 10 Security Baseline | Configured | Microsoft best practice is applied with modifications to align with ACSC guidance |
| Microsoft Defender ATP Baseline | Configured | Microsoft best practice is applied with modifications to align with ACSC guidance |
| Microsoft Edge Baseline | Configured | Microsoft best practice is applied with modifications to align with ACSC guidance |

# Applications

## Description

The lifecycle of applications can be managed using Intune. Applications can be deployed, configured, protected and removed.

## Design Considerations

Managed applications can be provisioned to the following platforms:

- Android
- iOS
- Windows Phone
- Windows 8.1
- Windows 10 and later

Applications types that can be managed include:

- Store Apps (Android, iOS, Windows Phone, Microsoft Store and Google Play)
- The Microsoft Office suite
- Microsoft Edge
- Microsoft Defender ATP
- Web links
- Built-In applications
- Line of Business applications
- Win32 applications
- Android Enterprise system applications

## Design Decisions

*Table 31* describes the Security Baseline design decisions.

*Table 31 Applications Design Decisions*

| Decision Point | Design Decision | Justification |
|---|---|---|
| Application Deployment | Configured | Deployment and monitoring of the deployment can be assigned to users or devices. |
| Application Configuration | Configured | Store applications are easily updated while Win32 applications will need some packaging. |

| | | |
|---|---|---|
| Application Protection | Configured | In combination with conditional access and network boundaries, applications are limited with respect to the copy, paste, forwarding, printing capabilities. |
| Application Removal | Configured | When applications (or versions of applications) are no longer required they are removed via Intune. |

# Information Protection

## Description

Application protection policies are rules that ensure an organization's data remains safe or contained in a managed application.

## Design Considerations

An application protection policy can be a rule that is enforced when the user attempts to access or move "corporate" data, or a set of actions that are prohibited or monitored when the user is inside the app.

## Design Decisions

*Table 32* describes the Application Protection policy design decisions.

Table 32 Application Protection Policy Design Decisions

| Decision Point | Design Decision | Justification |
|---|---|---|
| MAM or MDM policies | MDM will be used to apply application protection policies | MAM based policy is not able to manage non-enlightened line of business applications. (Non-Microsoft Office apps). |
| Desktop Protected Apps | All Microsoft Office desktop applications will be protected. Detailed settings are in the DTA – Platform – ABAC document | No additional desktop applications have been identified. |
| Mobile Apps | Default set will be protected on mobile devices. Detailed settings are in the DTA – Platform – ABAC document | Default set of mobile apps covers all of the apps in this design. |

| | | |
|---|---|---|
| Network Boundary – Cloud Resources | Default SharePoint URLs will be protected. Detailed settings are in the DTA – Platform – ABAC document | If additional URLs are identified these can also be added to the Cloud Resources scope. |
| Network Boundary – Network Domain | Production domain will be protected. Detailed settings are in the DTA – Platform – ABAC document | If additional network subnets are identified these can also be added to the Network Domain scope. |

# Software Updates

## Description

Windows Update for Business uses Intune to manage the installation of updates and features from Microsoft Windows Update servers. There is no requirement for on-premises servers or storage of update files.

## Design Considerations

Intune stores the update policy assignments not the updates themselves. No requirement for on-premises infrastructure.

There is no requirement or ability to selectively enable or disable a particular update.

Fast and slow update rings can be configured and assigned to different groups or users or devices allow early adopters to provide a level of validation before all users are provided with updates.

## Design Decisions

*Table 33* describes the Software Update design decisions.

*Table 33 Software Update Design Decisions*

| Decision Point | Design Decision | Justification |
|---|---|---|
| Servicing Channel | Semi-Annual Channel | Aligns with ACSC guidance for Operating System updates. |
| Microsoft Product updates | Allow | Aligns with ACSC guidance for product updates. |
| Windows Drivers | Allow | Aligns with ACSC guidance for driver updates. |

| | | |
|---|---|---|
| Quality Deferral period | 0 days | Aligns with general ACSC guidance for updates. |
| Feature Deferral | 0 days | Aligns with general ACSC guidance for updates. |
| Feature Update uninstall period | 10 days | Allows reversal for a short period of time in the event of breaking change updates. |

# iOS

## Description

iOS devices will be enrolled with the Intune Agency Portal to gain secure access to agency data.

## Design Considerations

After devices are enrolled, they become managed. Agencies can assign policies and apps to the device through a mobile device management (MDM) provider, such as Intune.

## Design Decisions

*Table 34* describes the iOS design decisions.

Table 34 iOS Design Decisions

| Decision Point | Design Decision | Justification |
|---|---|---|
| iOS Enrolment | Configured | iOS is the standard government issue device so there is a requirement to have this provisioned. |
| iOS Configuration | Implement as much of the ACSC hardening guide for iOS devices as possible using Intune. Refer to DTA – Intune Configuration - ABAC document | Aligns with the ACSC Hardening guide for iOS devices. |

# Printing

## Description

Printing is a legitimate method of data transfer out of an environment. Printing allows users to physically export data from a network and hence also it can be leveraged by malicious actors for data exfiltration. To minimize the risks associated with printing, the location where printing is allowed should be controlled.

## Design Considerations

For a user to leverage an available printer, connectivity and a device driver is often required. The drivers can be delivered and updated using Intune and Windows Update. Connectivity depends on the connected network(s) of the client. The options include:

- **Workplace printing** – In the workplace, the agency's existing printer fleet should be made available for printing through out of the box Windows 10 drivers. If necessary, specialty or specific printer drivers can be packaged and delivered by Intune.
- **Unsecure location printing** – Users should not be able to print outside of their normal place of work due to the risk of data loss.

The agency needs to provide printer details from which a print connection script can be generated. This would allow all workplace printers to be connected. Intune policy can prevent users from being able to add printers themselves. Users will be able to print direct to the printer without needing a print server.

Microsoft Universal Printing[10] is a print solution from Microsoft that is currently in private preview (March 2020). This solution runs entirely in Microsoft Azure needing no on-premises infrastructure. This solution is being reviewed by DTA for possible inclusion in the next iteration of the blueprint.

## Design Decisions

*Table 35* describes the Printing design decisions.

Table 35 Printing Design Decisions

[10] https://docs.microsoft.com/en-au/universal-print/

| Decision Point | Design Decision | Justification |
| --- | --- | --- |
| Workplace Printing | Configured | Configured using scripts deployed via Intune. Printers will need to be supported out of the box in Window 10. |
| Unsecure location Printing | Configured | Out of office printing will be restricted as adequate controls cannot be implemented to prevent the creation of classified content on untrusted print device. |

# Backup and Operational Management

## Description

As with an on-premises environment, backups play an important part of an overall cloud solution capability. It is important that critical information is backed up to enable recovery for scenarios such as accidental deletion or corruption.

## Design Considerations

To ensure a successful backup, configuration of the following items should be taken into consideration:

- **What to backup** - understanding what configuration, files and mailboxes that need to be backed up is important. If only a partial configuration is backed up, successful restoration may not be possible
- **Recovery Point Objective (RPO)** - RPO defines an acceptable loss of data (in time) for a data type in a data-loss event. RPOs are expressed in hours / days and directly influence the backup approach used, and how backups are performed with sufficient frequency to meet the defined RPO. For example, if an RPO of 12 hours was defined for a given data type, backups of this data type could not be scheduled further than 12 hours apart
- **Recovery Time Objective (RTO)** - RTO is used to define the acceptable level of service interruption (in time) between a data loss event and the recovery of the data to a point at which normal service is resumed. When determining RTOs for a given data type, consideration must also be given to any additional recovery process that are undertaken after the restoration of data. The RTO directly influences the type of backups performed and may dictate additional protection mechanisms outside of the backup platform for data types where a very short RTO is defined.
- **Legislative Requirements** – The essential 8 details that backups of important information, software and configuration settings are performed. More detail on these controls are listed in the *Protective Security Policy Framework* [11][12]

It is important that prior to defining the backup and restore policies, RTO and RPO objectives for each data type hosted the environment are defined in line with business requirements and Service Level Agreements (SLA).

All Office 365 data is replicated by Microsoft to at least two geographically dispersed data centres.

[11] Refer to Protective Security Policy Framework link https://www.protectivesecurity.gov.au/sites/default/files/2019-11/pspf-infosec-10-safeguarding-information-cyber-threats.pdf

[12] Refer to Essential Eight Maturity Model link https://www.cyber.gov.au/publications/essential-eight-maturity-model

There are several enterprise Backup software solutions which can backup data on-premises or in the cloud such as:

- Commvault Simpana
- Veeam Availability Suite
- Azure Backup

Depending on the requirements, a backup solution can cover the following scenarios:

- Backup local data directly to on-premises infrastructure from on-premise
- Backup local data to on-premises infrastructure and to the Azure storage blob from on-premise
- Backup cloud data directly from the cloud

Using the native Office 365 tools only, in combination with recycle bins the following data recovery options are available:

- Documents, Desktops and Pictures for each user is redirected from the Windows client device to OneDrive using Windows Known Folders providing a backup of data to the cloud.
- OneDrive includes recycle bins allowing recovery of data for up to 93 days.
- SharePoint data includes recycle bins allowing recovery of data for up to 93 days.

Exchange Online has a recover deleted items from server option.

Retention policies are created that ensure that data is retained forever for:

- Exchange
- SharePoint
- OneDrive
- Office 365 Groups
- Skype for Business
- Exchange Public Folders
- Teams channel messages
- Teams chats

Workstation configuration is stored in Intune. (AutoPilot rebuild).

## Design Decisions

*Table 36* describes the individual Backup design decisions.

Table 36 Backup Design Decisions

| Decision Point | Design Decision | Justification |
|---|---|---|
| Restoration tools | Microsoft back up and restoration tools. | The Agency will leverage Microsoft Office 365 native tools in the first instance to recover user data. |
| Items to Backup | Exchange Online<br>SharePoint Online<br>Microsoft Teams<br>OneDrive for Business<br>Office 365 Groups | Backups will need to cover the Microsoft suite of tools at a minimum. |

# System Administration

This section details how the solution will be managed, the administrative consoles that will be used to administrator the various components, and how Role Based Access Control (RBAC) is implemented to control access.

## Administrative Consoles

### Description

To manage and configure the solution, administrators will user various administrative consoles. These consoles are a mixture of server based and web-based consoles that exist internally or in the cloud.

### Design Considerations

Web based administrative consoles are provided by Microsoft however the urls for these consoles are constantly changing. The consoles listed below are correct at the time of writing.

### Design Decisions

*Table 37* describes the Administrative Consoles design decisions.

Table 37 Administration Consoles Design Decisions

| Decision Point | Design Decision | Justification |
|---|---|---|
| Azure Portal | Available from web console | The console is available from a standard Web browser with internet access. The FQDN used for access will be https://portal.azure.com.<br>Standard users do not have access to the portal. |
| Office 365 Admin Center | Available from web console | The console is available from a standard Web browser with internet access. The FQDN used for access will be https://portal.office.com/adminportal/home. |
| Microsoft Defender ATP Portal | Available from web console | The console is available from a standard Web browser with internet access. The FQDN used for access will be https://securitycenter.microsoft.com/ |

| | | |
|---|---|---|
| MCAS Portal | Available from web console | The console is available from a standard Web browser with internet access. The FQDN used for access will be https://portal.cloudappsecurity.com/ |
| Security and Compliance | Available from web console | The console is available from a standard Web browser with internet access. The FQDN used for access will be https://protection.office.com/homepage |

# Role Based Access Control

## Description

Role Based Access Control (RBAC) defines what an end user or administrator can do. In relation to system administration, RBAC provides various roles each of which can only perform certain tasks. For example, help desk staff may be able to only view certain resources, whereas system administrators could view, create, and delete certain resources.

## Design Considerations

Azure Active Directory has 51 built-in RBAC roles to ensure least privilege access is implemented.

Privileged Identity Management (PIM) can be leveraged to enhance the RBAC model for Azure Active Directory role-based management access, and parts of other Microsoft services like Office 365 and Intune. With PIM, requests are made through the Azure portal for elevated access only when they are required and access is expired after a specified period.

PIM is initially configured by a Global Administrator, after initial consent is given to use PIM, roles can be discovered and configured for use with PIM.

Each PIM managed role can be configured with an approver, if an approver is not configured, the 'Privileged Role Administrators' role is delegated the responsibility to approve PIM role activation requests.

Each PIM role assignment can have the following attributes:

- **Activation Duration** - The Activation Duration attribute specifies the duration to allow the access request, the maximum is 72 hours
- **Notification –** The Notification attribute specifies that an email to the approver to notify the approver that there is a request pending is sent

- **Incident Request Ticket –** The Incident Request Ticket attribute specifies that the approver add an incident ticket number to the approval request
- **Multi-factor Authentication –** The Multi-factor Authentication attribute specifies whether MFA is required for activation

The following Office 365 roles can be assigned via PIM:

- Exchange Administrator
- SharePoint Administrator
- Teams Administrator

A brief description of the relevant Azure AD roles is:

- **Global Administrators** - Users with this role have access to all administrative features in Azure Active Directory, as well as services that federate to Azure Active Directory like Exchange Online, SharePoint Online, and Skype for Business Online.
- **Global Readers** - Users with this role can read everything that a Global Administrator can, but not update anything.
- **Exchange Service Administrators** - Users with this role have global permissions within Microsoft Exchange Online, when the service is present.
- **SharePoint Service Administrators** - Users with this role have global permissions within Microsoft SharePoint Online, when the service is present, as well as the ability to manage support tickets and monitor service health.
- **Teams Service Administrators** - Users in this role can manage all aspects of the Microsoft Teams workload via the Microsoft Teams & Skype for Business admin center and the respective PowerShell modules
- **User Administrators** - Users with this role can create and manage all aspects of users and groups.
- **Intune Service Administrators** - Users with this role have global permissions within Microsoft Intune Online, when the service is present. Additionally, this role contains the ability to manage users and devices in order to associate policy, as well as create and manage groups.

## Design Decisions

*Table 38* describes the Azure Active Directory RBAC design decisions.

Table 38 Azure AD RBAC Design Decisions

| Decision Point | Design Decision | Justification |
| --- | --- | --- |
| Azure AD Role Based Management | PIM will be utilised to provide Just-in-Time Role based management to ensure elevated access is only provided when required. | Only the Azure AD roles will be used to provide administrative access as this allows the time limited use and logging. Other roles must be permanently assigned. |
| Azure AD Roles | Only the Azure AD Global Administrator and Global Reader roles will be used. | The Azure AD Global Reader and Global Administrator will be assigned with PIM |
| Office 365 Roles | The Azure AD Exchange Administrator, Teams Administrator and SharePoint Administrator roles will be inherited | Only the Exchange Administrator, Teams Administrator and SharePoint Administrator roles can be assigned with PIM. |
| Intune Roles | The Azure AD Intune Service Administrator role will be inherited | Intune roles cannot be assigned with PIM and would therefore be permanently assigned to user. Only the Azure AD Intune Service Administrators role will be used. |
| PIM approval | Privileged Role Administrators role | Initially, the Privileged Role Administrators role will be leveraged to approve requests for elevation. Further approval delegation can be made as roles and responsibilities are determined for management of the solution. |

# Abbreviations and Acronyms

*Table 39* details the abbreviations and acronyms used throughout this document.

Table 39 Abbreviations and Acronyms

| Acronym | Meaning |
|---|---|
| AAD | Azure Active Directory |
| ABAC | As-built as-configured |
| ACSC | Australian Cyber Security Centre |
| AD | Active Directory |
| AD DS | Active Directory Domain Services |
| AES | |
| AIP | Azure Information Protection |
| API | Application Programming Interface |
| ASD | Australian Signals Directorate |
| ATP | Advanced Threat Protection |
| ConfigMgr | System Center Configuration Manager |
| EDR | Endpoint Detection and Response |
| IaaS | Infrastructure as a Service |
| IP | Internet Protocol |
| ISM | Information Security Manual |
| MFA | Multi-Factor Authentication |
| OATH | Open Authentication |
| PIN | Personal Identification Number |
| PIM | Privileged Identity Management |
| PSPF | Protective Security Policy Framework |
| RBAC | Role Based Access Control |
| RPO | Recovery Point Objective |
| SaaS | Software as a Service |
| SSO | Single Sign On |