Australian Government

Digital Transformation Agency

Platform – As-built as-configured

March 2020

dta

Contents

Overview

Purpose

The purpose of this as-built as-configured (ABAC) document is to detail the settings and configuration of the modules that form the Platform. These settings, policies, and configurations align to the design decisions captured within the associated blueprint documentation. All settings captured within this ABAC were captured as of the time of writing.

Associated Documentation

The following table lists the documents that were referenced during the creation of this ABAC.

Table 1 Associated Documentation

Name	Version	Date
DTA – Blueprint Solution Overview	March	03/2020
DTA – Platform Design	March	03/2020
DTA – Workstation Design	March	03/2020
DTA – Office 365 Design	March	03/2020
DTA – Office 365 – 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

Enterprise Mobility and Security

Identity and Access Management

Azure Active Directory

Table 2 Azure Active Directory Settings

Item	Configuration
Directory Properties Name	Digital Transformation Agency
Directory ID	4da78362-d2a4-4007-8e6c-97a224d2ca1f
Technical Contact	brendan.reilly@dta.gov.au
Initial Domain Name	dtadesktop.onmicrosoft.com
Country or Region	Australia
User Settings | *Enterprise Applications – User settings*	
Users can consent to apps accessing information on their behalf.	No
Users can add gallery apps to their access panel	No
Users can only see Office 365 Apps in the Office 365 Portal	No
User Settings | *App Registration*	
Users can register applications	No
User Settings | *Administration Portal*	
Restrict non-administrator access to Azure AD Administration Portal	Yes
User Settings | *LinkedIn Account Connections*	
Allow users to connect work or school account with LinkedIn	No
User Settings | *External Collaboration Settings*	
Guest user permissions are limited	Yes
Admins and users in the guest inviter role can invite	Yes
Members can invite	No
Guests can invite	No

Enable Email On-time passcode for guests	No
User Settings | *External Collaboration Settings – Collaboration restrictions*	
Allow invitations only to the specified domains (most restrictive)	Selected
Target domains	dta.gov.au
Groups – General | *Self Service Group Management*	
Owners can manage membership requests in the access panel	No
Restrict access to Groups in the Access Panel	Yes
Groups - General | *Security Groups*	
Users can create security groups in the Azure portals	No
Owners who can assign members as group owners in Azure Portals	All
Groups - General | *Office 365 Groups*	
Users can create Office 365 groups in Azure portals	No
Owners who can assign members as group owners in Azure portals	All
Groups - General | *Directory-wide Groups*	
Enable an “All Users” group in the directory	No
Groups – Expiration	
Group lifetime (in days)	365
Email contact for groups with no owners	itsa@desktop.gov.au
Enable expiration for these Office 365 groups	None
Groups – Naming policy	
Blocked words	N/A
Group naming policy	Prefix = String = DGA
Custom Domain Names	
Custom Domains	desktop.gov.au (Primary) dtadesktop.onmicrosoft.com

Company Branding	
Sign-in Page background	Generic Government Background <1920x1080px>
Banner Logo	<280x60px>
Username hint	user@agency.gov.au
Sign-in page Text	Not Configured. *Note*: User terms will be configured using Conditional Access Policies.
Background Colour	<TBD>
Allow Option to remain signed in (Keep Me Signed In)	Disabled
Devices – Device Settings | *Devices – Device settings*	
Users may join devices to Azure AD	Selected
Display Name	grp-agency-IntuneEnrolment
Additional local administrators on Azure AD joined devices	None
Require Multi-Factor Auth to join devices	Yes
Devices – Device settings | *Enterprise State Roaming*	
Users may sync settings and app data across devices	All
Password reset – Properties	
Self-service password reset enabled	All
Password reset – Authentication methods	
Number of methods required to reset	2
Methods available to users	Mobile app notification Email Mobile phone
Password reset – Registration	
Require users to register when signing in?	Yes
Number of days before users are asked to re-confirm their authentication information	180
Password reset – Notifications	
Notify users on password resets?	Yes

Notify all admins when other admins reset their password?	Yes

Azure Active Directory Identity Protection

The following policies are required to be configured to enable Azure AD Identity Protection.

- Azure AD MFA policy – Refer to the Azure Multi-Factor Authentication section for configuration settings of this policy.
- Sign-in risk policy – Settings to calculate the sign-in risk level.
- User risk policy – Settings to determine the user risk level.

Table 3 Azure AD Identity Protection Design Decisions

Decision Point	Design Decision	Rationale / Justification
Sign-in Risk Policy		
Include users	All users	All Azure AD accounts will be included within the sign-in risk policy to provide suspicious log monitoring.
Exclude users	Break glass account	The listed Azure AD accounts should be excluded from this policy.
Sign-in risk settings	Medium and above	Microsoft recommended setting the sign-in risk threshold.
Access	Allow access	Sign-in policy configured to allow access when the risk level is met. MFA is selected as required to use MFA on sign-in.
Enforce policy	On	Apply sign-in risk policy to all Azure AD accounts.
User Risk Policy		
Include users	All users	All Azure AD accounts will be included within the user risk policy to provide suspicious log monitoring.
Exclude users	None	Listed Azure AD accounts should be excluded from this policy.
User risk setting	Medium and above	Microsoft recommended setting the user risk threshold.
Access	Allow access (with require password change selected)	User policy configured to allow access when risk level is met. Password change is mandatory until this feature is further tested.
Enforce policy	On	Apply user risk policy to all Azure AD accounts.

Azure AD Multifactor Authentication

Table 4 Azure AD Multi-Factor Authentication Configuration

Item	Configuration
Allow Users to Submit Fraud Alerts	On
Automatically Block Users Who Report Fraud	On

Table 5 Azure MFA Logging and Monitoring Design Decisions

Report	Location	Description
Blocked User History	Azure AD | Security | MFA Server | Block/unblock users	Shows the history of requests to block or unblock users.
Usage and fraud alerts	Azure AD | Sign-ins	Provides information on overall usage, user summary, and user details; as well as a history of fraud alerts submitted during the date range specified.
Usage and On-Premises components	Azure AD | Security | MFA Server | Activity Report	Provides information on overall usage for MFA through the NPS extension, and AD FS.
Bypassed User History	Azure AD | Security | MFA Server | One-time bypass	Provides a history of requests to bypass MFA for a user.

Table 6 Azure MFA Design Decisions

Item	Configuration	Rationale / Justification
App Passwords	Do not allow users to create app passwords to sign-in to non-browser apps	MFA will be configured for all authentication to Azure as a security mechanism to protect users and resources. App passwords will not be allowed as they would provide a mechanism to bypass MFA. App passwords are only required for legacy applications and are not supported when Conditional Access policies are used.
Trusted IPs	Disabled	Conditional Access policies will be used and named locations associated with policy.
Disabled Verification options	• Call to phone • Text message to phone	These options have been disabled in accordance with guidance from the Australian Cyber Security Centre (ACSC) as published in the ‘Essential Eight Maturity Model’.

Privileged Identity Management

Table 7 Privileged Identity Management Role Configuration

Role	Notification Emails	Incident Request Ticket	MFA	Require Approval	Approver
Global Reader	Enable	Disable	Disable	Disable	N/A
Global Administrator	Enable	Disable	Enable	Enable	itsa@agency.gov.au

Information Protection

Windows Information Protection

Application protection policies are rules that ensure an organization's data remains safe or contained in a managed app. A 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. A managed app is an application that has app protection policies applied to it.

Application Protection Policies

Table 8 describes how Information Protection policies were created to allow labels to apply to compliant devices for the pilot.

Table 8 Application Protection Configuration

Information Protection Policy	
Home | Microsoft Intune | Client apps – App Protection policies	
General	
Name	Windows Information Protection
Description	Application Protection policies
Enrollment state	With enrollment
Targeted apps	
Protected apps	23 selected
Exempt apps	0 selected
Required settings	
Windows Information Protection mode	Block
Corporate identity	desktop.gov.au
Advanced settings	

Network perimeter

Network boundary	1 Configured
Boundary type	Cloud resources
Boundary name	Office365
Boundary value	dtadesktop.sharepoint.com|dtadesktop-my.sharepoint.com|dtadesktop-files.sharepoint.com|tasks.office.com|protection.office.com|meet.lync.com|teams.microsoft.com|www.yammer.com|yammer.com|persona.yammer.com|outlook.office.com|outlook.office365.com|attachments.office.net|dtadesktop.crm.dynamics.com|dtadesktop.visualstudio.com|dtadesktop.powerbi.com
Enterprise Proxy Servers list is authoritative (do not auto-detect)	Off
Enterprise IP Ranges list is authoritative (do not auto-detect)	Off

Data protection

Upload a Data Recovery Agent (DRA) certificate to allow recovery of encrypted data	Not configured
Prevent corporate data from being accessed by apps when the device is locked. Applies only to Windows 10 Mobile	Off
Revoke encryption keys on unenroll	On
Show the enterprise data protection icon	On
Use Azure RMS for WIP	Off
Specify the template ID to use for Azure RMS	--
Allow Windows Search Indexer to search encrypted items	On
Encrypted file extensions	0 configured

Assignments

Included groups	rol-Agency-Administrators rol-Agency-Users
Excluded groups	--

Scope tags

Default

Windows Autopilot

Table 9 describes the Windows Autopilot design decisions, and the justification taken by the business and technical teams for the decisions.

Table 9 Windows Autopilot Design Decisions

Decision Point	Design Decision	Rationale / Justification
Deployment Style	Autopilot	Autopilot will be utilised to deploy enrol a workstation. This will ensure an agency wide standard of endpoint look and feel.
Import Method	.CSV	This is the most efficient and effective way to import large amounts of devices for administrators.
Autopilot device group name	grp-Security-Baselines	To make ease of administration and identification of groups easier.
Autopilot deployment profile name	IntuneEnrollerDevices	To make ease of administration and identification of profiles easier for administrators.
oobe Deployment mode	User Driven	This will reduce the burden on administrators enrolling large numbers of devices in bigger agencies.
Join Azure AD as	Azure AD joined	Azure AD is the main source of identity for a cloud only deployment.
End-user license agreement (EULA)	Hide	Faster deployment and less user interaction.
Privacy settings:	Hide	Standard settings for all users, if set to show users can change privacy settings.
Hide change account options	Hide	This enables users to change accounts if hot desking.
User account type	Standard	To meet security requirements users will only be allowed access to a standard user account.
Allow White Glove OOBE	No	Faster deployment for end users.
Apply device name template	DGA-%SERIAL%	Makes asset identification and management easier.
Language (Region)	English (Australia)	Default language used in every department.
Automatically configure keyboard	Yes	Default language used in every department.
Included Groups - Assigned to	grp-Security-Baselines	This is the group for the agencies production users that the profile will be assigned to.

Threat Protection

Microsoft Defender Advanced Threat Protection

Table 10 describes the Microsoft Defender Advanced Threat Protection settings that are configured within Intune.

Table 10 Microsoft Defender Advanced Threat Protection

Item	Configuration
General	
Data Storage	US
Data Retention	180 Days
Alert Notifications	High Severity – Any machine in my organization – itsa@desktop.gov.au
	Medium Severity – Any machine in my organization – itsa@desktop.gov.au
	Low Severity – Any machine in my organization – itsa@desktop.gov.au
Power BI reports	Not Configured
Advanced features	Automated Investigation: ON
	Live Response: OFF
	Live Response unsigned script execution: OFF
	Automatically Resolve Alerts: ON
	Allow or Block File: ON
	Custom network indicators: OFF
	Show user details: ON
	Skype for Business integration: ON
	Azure ATP integration: OFF
	Office 365 Threat Intelligence connection: ON
	Microsoft Cloud App Security: ON
	Azure Information Protection: OFF
	Web content filtering: ON
	Microsoft Intune connection: ON
	Preview Features: ON

Roles	
Name	Microsoft Defender ATP administrator (default)
Assigned Group	rol-agency-security-defenderatp-admins
Description	Default role with full permissions to the service. It cannot be modified or deleted.
Permission	Administrator
Name	Microsoft Defender ATP Viewer
Assigned Group	rol-agency-security-defenderatp-viewer
Description	Viewer privileges
Permission	• Security operations – view data, • Threat and vulnerability management
Name	Microsoft Defender ATP Remediation
Assigned Group	Investigate and remediate alerts
Description	Active remediation actions, Security operations, threat and vulnerability management, remediation handling, exception handling.
Permission	Windows 10
Machine Groups	Ungrouped machines (default)
APIs	
SIEM	Not enabled
Rules	
Custom Detections	None configured
Alert Suppression	None configured
Indicators	None Configured
Automation allowed/blocked lists	Default - 20 certificates from Apple and Microsoft
Web content filtering	
Name	Adult Sites
Blocked Categories	Cults, Gambling, Nudity, Pornography/Sexually explicit, Sex education, Tasteless, Violence
Scope	All machines
Name	High Traffic Sites
Blocked Categories	Download sites, Image sharing, Peer-to-peer, Streaming media & downloads

Scope	All machines
Automation uploads	Content Analysis: ON File extension names: vb,'',tcl,inf,ps1,scr,rgs,py,elf,dll,msi,reg,pl,rb,gadget,js,sys,job,ws,ko.gz,bat,exe,cpl,vbe,wsf,url,cmd,ko,air,vbs,sh,com Memory Content Analysis: ON
Automation folder exclusions	None configured
Machine management	
Onboarding – Operating System	Windows 10
Onboarding – Deployment Method	Local Script (for up to 10 machines)
Offboarding – Operating System	Windows 10
Offboarding – Deployment Method	Local Script (for up to 10 machines)

Intune Policy

Table 11 identifies the Intune Policy configuration that relates to Microsoft Defender ATP.

Table 11 Intune Policy Configuration

Item	Configuration
Devices – Configuration Profiles	
Policy Name	Agency-MSDefenderATP
Sample sharing for all files	Enabled
Expedite telemetry reporting frequency	Enabled
Assignment	grp-Windows-10-Devices

Microsoft Intune Configuration

All Windows 10 client configuration is accomplished via Microsoft Intune policies. These Intune configuration policies are detailed in separate documents that are explained in *Table 12* below. The table follows the structure of the Intune configuration console as shown in *Figure 1*.

Figure 1 | Intune Configuration Console

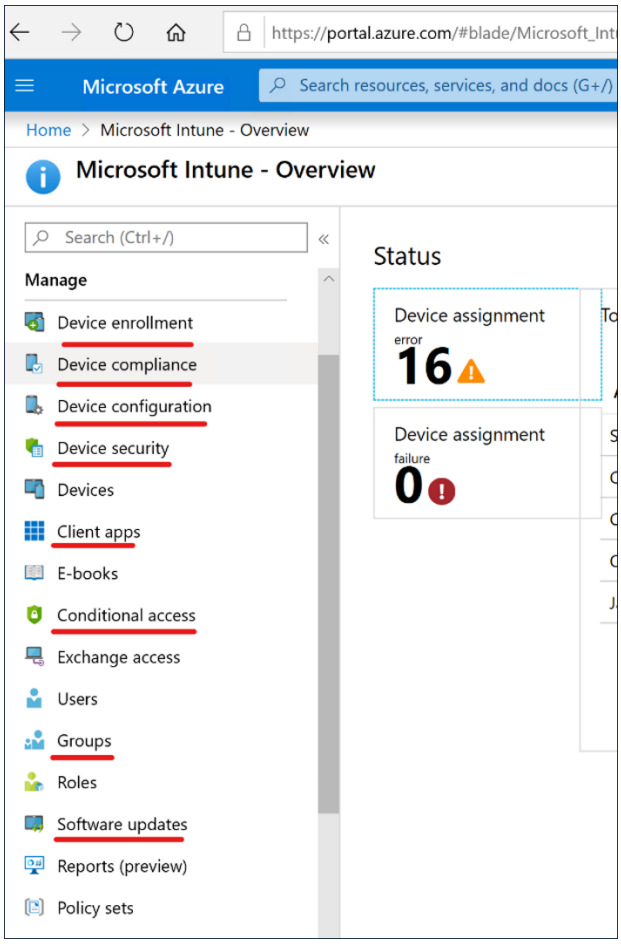

Table 12 Additional Intune Configuration Documents

Section	Description	Document Name
Device enrollment	Automatic Enrolment, Enrolment Status page, Deployment Profiles	DTA – Intune Enrollment - ABAC
Device compliance	Device compliance policies	DTA – Intune Compliance - ABAC
Device configuration	Configuration Profiles, PowerShell scripts	DTA – Intune Configuration – ABAC
Device security	Windows 10 Security Baselines, Microsoft Defender ATP Baselines, Microsoft Edge Baseline	DTA – Intune Security Baselines - ABAC
Client apps	Win32 Apps, Web links, Windows MSI Line of Business apps, Office 365 installation, Windows Information Protection	DTA – Intune Applications - ABAC
Conditional Access	Conditional Access policies	DTA – Conditional Access Policies - ABC
Software Updates	Windows 10 update rings	DTA – Software Updates – ABAC

Autopilot Deployment profile

Table 13 describes the Autopilot Profile design decisions, and the justification taken by the business and technical teams for the decisions.

Table 13 Autopilot Profile Design Decisions

Item	Configuration
Name	IntuneEnrollerDevices
Description	Devices enrolled in Intune via autopilot
Convert all targeted devices to Autopilot	No
Out-of-box experience (OOBE)	
Automatically configure keyboard	No
Deployment mode	User-Driven
Join to Azure AD as	Azure AD Joined
Language (Region)	English (Australia)
Automatically configure keyboard	Yes
Microsoft Software License Terms	Hide
Privacy settings	Hide
Hide change account options	Hide
User account type	Standard
Allow White Glove OOBE	No
Apply device name template	Yes
Enter a name	<Agency>-%SERIAL%
Out-of-box experience (OOBE)	
Included groups	grp-Security-Baselines grp-SecBaselines
Excluded groups	

Delivery Optimisation

Table 14 describes the Delivery Optimisation design decisions, and the justification taken by the business and technical teams for the decisions.

Table 14 Delivery Optimisation Design Decisions

Item	Configuration
Download mode	HTTP blended with peering behind same NAT
Bandwidth	
Bandwidth optimization type	Percentage
Maximum foreground download bandwidth (in %)	70
Maximum background download bandwidth (in %)	25
Delay background HTTP download (in seconds)	60
Delay foreground HTTP download (in seconds)	60
Caching	
Minimum RAM required for peer caching (in GB)	4
Minimum disk size required for peer caching (in GB)	32
Minimum content file size for peer caching (in MB)	5
Minimum battery level required to upload (in %)	40
Modify cache drive	%SystemDrive%
Maximum cache age (in days)	7
Maximum cache size type	20

Software Updates

Table 15 describes the Software Update ring for Production design decisions, and the justification taken by the business and technical teams for the decisions.

Table 15 Software Update Production Design Decisions

Item	Configuration
Update Settings	
Servicing Channel	Semi-Annual Channel
Microsoft Product Updates	Allow

Windows Drivers	Allow
Quality Update deferral period (days)	0
Feature update deferral period (days)	0
Set feature update uninstall period (2 - 60 days)	10
User Experience Settings	
Automatic update behaviour	Auto install at maintenance time
Active hours start	8 AM
Active hours end	5 PM
Restart checks	Allow
Option to pause Windows updates	Disable
Option to check for Windows updates	Enable
Require user's approval to restart outside of work hours	Not configured
Remind user prior to required auto-restart with dismissible reminder (hours)	--
Remind user prior to required auto-restart with permanent reminder (minutes)	--
Change notification update level	Use the default Windows Update notifications
Use deadline settings	Not configured
Assignment – Included groups	rol-Agency-Administrators rol-Agency-Users