Australian Government

Digital Transformation Agency

Conditional Access Policies – As-built as-configured

March 2020

dta

Contents

Overview

Purpose

The purpose of this as-built as-configured (ABAC) document is to detail the Conditional Access policies deployed within the solution. These policies align to the design decisions captured within the associated blueprint document.

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 – 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 – Intune Compliance – ABAC	March	03/2020
DTA – Intune Configuration – ABAC	March	03/2020

Conditional Access Policies

Each conditional access policy is described in the tables below.

Legacy Authentication

Table 2 BLOCK - Legacy Authentication

Configuration Item	Setting
Home > Conditional Access - Policies	
Name	BLOCK – Legacy Authentication
Description	This global policy blocks all connections from unsecure legacy protocols like ActiveSync, IMAP, PO3, etc.
Targeted Groups - Include	All Users
Targeted Groups - Exclude	Excluded from CA
Targeted Apps - Include	All Cloud Apps
Targeted Apps - Exclude	None
Conditions	
Sign-In Risk	N/A
Device Platforms – Include	N/A
Device Platforms – Exclude	N/A
Locations - Include	N/A
Location – Exclude	N/A
Client Apps	Exchange Active Sync clients Other clients
Device State – Exclude	N/A
Access Controls	
Block Access	Yes
Grant Access	No
Require Multifactor Authentication	N/A
Require Device to be marked as compliant	N/A
Require Hybrid Azure AD Joined device	N/A
Require approved client app (iOS only)	N/A
Terms of Use	N/A

Require ALL of the selected controls	N/A
Require ONE of the selected controls	N/A
Use App enforced restrictions	N/A
Enabling limited access with SharePoint Online	N/A
Enabling limited access with Exchange Online	N/A
Persistent Browser session	N/A
Policy Enabled	Yes

High Risk Sign-Ins

Table 3 BLOCK – High Risk Sign-Ins

Configuration Item	Setting
Home > Conditional Access - Policies	
Name	BLOCK – High Risk Sign-Ins
Description	This global policy blocks all high-risk authentications (requires Azure AD Premium P2).
Targeted Groups - Include	All Users
Targeted Groups - Exclude	Excluded from CA
Targeted Apps - Include	All Cloud Apps
Targeted Apps - Exclude	None
Conditions	
Sign-In Risk	High - Yes
Device Platforms – Include	N/A
Device Platforms – Exclude	N/A
Locations - Include	N/A
Location – Exclude	N/A
Client Apps	N/A
Device State – Exclude	N/A
Access Controls	
Block Access	Yes
Grant Access	No

Require Multifactor Authentication	N/A
Require Device to be marked as compliant	N/A
Require Hybrid Azure AD Joined device	N/A
Require approved client app (iOS only)	N/A
Terms of Use	N/A
Require ALL of the selected controls	N/A
Require ONE of the selected controls	N/A
Use App enforced restrictions	N/A
Enabling limited access with SharePoint Online	N/A
Enabling limited access with Exchange Online	N/A
Persistent Browser session	N/A
Policy Enabled	Yes

Allowed Countries

Table 4 BLOCK – Countries Not Allowed

Configuration Item	Setting
Home > Conditional Access - Policies	
Name	BLOCK – Countries Not Allowed
Description	This global policy blocks all connections from countries not in the Allowed countries whitelist.
Targeted Groups - Include	All Users
Targeted Groups - Exclude	Excluded from CA
Targeted Apps - Include	All Cloud Apps
Targeted Apps - Exclude	None
Conditions	
Sign-In Risk	N/A
Device Platforms – Include	N/A
Device Platforms – Exclude	N/A
Locations - Include	Any (all) location
Location – Exclude	Allowed Countries
Client Apps	N/A
Device State – Exclude	N/A
Access Controls	
Block Access	Yes
Grant Access	No
Require Multifactor Authentication	N/A
Require Device to be marked as compliant	N/A
Require Hybrid Azure AD Joined device	N/A
Require approved client app (iOS only)	N/A
Terms of Use	N/A
Require ALL of the selected controls	N/A
Require ONE of the selected controls	N/A
Use App enforced restrictions	N/A

Enabling limited access with SharePoint Online	N/A
Enabling limited access with Exchange Online	N/A
Persistent Browser session	N/A
Policy Enabled	Yes

Terms of Use

Table 5 GRANT - Terms of Use

Configuration Item	Setting
Home > Conditional Access - Policies	
Name	GRANT - Terms of Use
Description	This global policy forces Terms of Use on all authentications
Targeted Groups - Include	All Users
Targeted Groups - Exclude	Excluded from CA
Targeted Apps - Include	All Cloud Apps
Targeted Apps - Exclude	None
Conditions	
Sign-In Risk	N/A
Device Platforms – Include	N/A
Device Platforms – Exclude	N/A
Locations - Include	N/A
Location – Exclude	N/A
Client Apps	N/A
Device State – Exclude	N/A
Access Controls	
Block Access	No
Grant Access	Yes
Require Multifactor Authentication	N/A
Require Device to be marked as compliant	N/A
Require Hybrid Azure AD Joined device	N/A
Require approved client app (iOS only)	Yes

Terms of Use	Yes
Require ALL of the selected controls	N/A
Require ONE of the selected controls	Yes
Use App enforced restrictions	N/A
Enabling limited access with SharePoint Online	N/A
Enabling limited access with Exchange Online	N/A
Persistent Browser session	N/A
Policy Enabled	Yes

Browser Access

Table 6 GRANT - Browser Access

Configuration Item	Setting
Home > Conditional Access - Policies	
Name	GRANT - Browser Access
Description	General browser access policy that grants authentication from a browser on any device with MFA requirement.
Targeted Groups - Include	All Users
Targeted Groups - Exclude	Excluded from CA
Targeted Apps - Include	All Cloud Apps
Targeted Apps - Exclude	None
Conditions	
Sign-In Risk	N/A
Device Platforms – Include	N/A
Device Platforms – Exclude	N/A
Locations - Include	N/A
Location – Exclude	N/A
Client Apps	Browser
Device State – Exclude	N/A
Access Controls	
Block Access	No
Grant Access	Yes
Require Multifactor Authentication	Yes
Require Device to be marked as compliant	N/A
Require Hybrid Azure AD Joined device	N/A
Require approved client app (iOS only)	N/A
Terms of Use	N/A
Require ALL of the selected controls	N/A
Require ONE of the selected controls	Yes
Use App enforced restrictions	N/A

Enabling limited access with SharePoint Online	N/A
Enabling limited access with Exchange Online	N/A
Persistent Browser session	N/A
Policy Enabled	Yes

Block Unmanaged Browser File Downloads

Table 7 SESSION - Block Unmanaged Browser File Downloads

Configuration Item	Setting
Home > Conditional Access – Policies	
Name	SESSION - Block Unmanaged Browser File Downloads
Description	Browsers on unmanaged devices can never download files and attachments from SharePoint Online and Exchange Online.
Targeted Groups - Include	All Users
Targeted Groups - Exclude	Excluded from CA
Targeted Apps - Include	Exchange Online SharePoint Online
Targeted Apps - Exclude	None
Conditions	
Sign-In Risk	N/A
Device Platforms – Include	N/A
Device Platforms – Exclude	N/A
Locations - Include	N/A
Location – Exclude	N/A
Client Apps	Browser
Device State – Exclude	Exclude Devices marked as compliant
Access Controls	
Block Access	N/A
Grant Access	N/A
Require Multifactor Authentication	N/A
Require Device to be marked as compliant	N/A

Require Hybrid Azure AD Joined device	N/A
Require approved client app (iOS only)	N/A
Terms of Use	N/A
Require ALL of the selected controls	N/A
Require ONE of the selected controls	N/A
Use App enforced restrictions	N/A
Enabling limited access with SharePoint Online	Yes
Enabling limited access with Exchange Online	Yes
Persistent Browser session	N/A
Policy Enabled	Yes

Intune Enrolment

Table 8 GRANT - Intune Enrolment

Configuration Item	Setting
Home > Conditional Access - Policies	
Name	GRANT - Intune Enrolment
Description	Devices are allowed to authenticate to Intune for enrolment.
Targeted Groups - Include	All Users
Targeted Groups - Exclude	Excluded from CA
Targeted Apps - Include	Intune Intune Enrolment
Targeted Apps - Exclude	None
Conditions	
Sign-In Risk	N/A
Device Platforms – Include	iOS Windows
Device Platforms – Exclude	N/A
Locations - Include	N/A
Location – Exclude	N/A

Client Apps	Modern Authentication Exchange Active Sync clients
Device State – Exclude	N/A
Access Controls	
Block Access	No
Grant Access	Yes
Require Multifactor Authentication	Yes
Require Device to be marked as compliant	N/A
Require Hybrid Azure AD Joined device	N/A
Require approved client app (iOS only)	N/A
Terms of Use	N/A
Require ALL of the selected controls	N/A
Require ONE of the selected controls	Yes
Use App enforced restrictions	N/A
Enabling limited access with SharePoint Online	N/A
Enabling limited access with Exchange Online	N/A
Persistent Browser session	N/A
Policy Enabled	Yes

Mobile Device Access

Table 9 GRANT - Mobile Device Access

Configuration Item	Setting
Home > Conditional Access - Policies	
Name	GRANT - Mobile Device Access
Description	Grants access to managed mobile devices that are enrolled and compliant in Intune. An approved Microsoft app is required
Targeted Groups - Include	All Users
Targeted Groups - Exclude	Excluded from CA
Targeted Apps - Include	All Cloud Apps
Targeted Apps - Exclude	Intune Intune Enrolment

Conditions	
Sign-In Risk	N/A
Device Platforms – Include	iOS
Device Platforms – Exclude	N/A
Locations - Include	N/A
Location – Exclude	N/A
Client Apps	Modern Authentication Exchange Active Sync clients
Device State – Exclude	N/A
Access Controls	
Block Access	No
Grant Access	Yes
Require Multifactor Authentication	Yes
Require Device to be marked as compliant	Yes
Require Hybrid Azure AD Joined device	N/A
Require approved client app (iOS only)	Yes
Terms of Use	N/A
Require ALL of the selected controls	Yes
Require ONE of the selected controls	N/A
Use App enforced restrictions	N/A
Enabling limited access with SharePoint Online	N/A
Enabling limited access with Exchange Online	N/A
Persistent Browser session	N/A
Policy Enabled	Yes

Windows Device Access

Table 10 GRANT - Windows Device Access

Configuration Item	Setting
Home > Conditional Access - Policies	
Name	GRANT - Windows Device Access

Description	Grants access to managed Windows devices that are Azure AD Joined.
Targeted Groups - Include	All Users
Targeted Groups - Exclude	Excluded from CA
Targeted Apps - Include	All Cloud Apps
Targeted Apps - Exclude	Intune Intune Enrolment
Conditions	
Sign-In Risk	N/A
Device Platforms – Include	Windows
Device Platforms – Exclude	N/A
Locations - Include	N/A
Location – Exclude	N/A
Client Apps	Modern Authentication Exchange Active Sync clients
Device State – Exclude	N/A
Access Controls	
Block Access	No
Grant Access	Yes
Require Multifactor Authentication	Yes
Require Device to be marked as compliant	Yes
Require Hybrid Azure AD Joined device	N/A
Require approved client app (iOS only)	N/A
Terms of Use	N/A
Require ALL of the selected controls	Yes
Require ONE of the selected controls	N/A
Use App enforced restrictions	N/A
Enabling limited access with SharePoint Online	N/A
Enabling limited access with Exchange Online	N/A
Persistent Browser session	N/A
Policy Enabled	Yes

GRANT - Guest Access (B2B)

Table 11 GRANT - Guest Access (B2B)

Configuration Item	Setting
Home > Conditional Access - Policies	
Name	GRANT - Guest Access (B2B)
Description	Approved apps that guest users can access (requires MFA).
Targeted Groups - Include	All Users
Targeted Groups - Exclude	Excluded from CA
Targeted Apps - Include	Teams SharePoint Online Planner
Targeted Apps - Exclude	None
Conditions	
Sign-In Risk	N/A
Device Platforms – Include	N/A
Device Platforms – Exclude	N/A
Locations - Include	N/A
Location – Exclude	N/A
Client Apps	N/A
Device State – Exclude	N/A
Access Controls	
Block Access	No
Grant Access	Yes
Require Multifactor Authentication	Yes
Require Device to be marked as compliant	N/A
Require Hybrid Azure AD Joined device	N/A
Require approved client app (iOS only)	N/A
Terms of Use	N/A
Require ALL of the selected controls	Yes
Require ONE of the selected controls	N/A

Use App enforced restrictions	N/A
Enabling limited access with SharePoint Online	N/A
Enabling limited access with Exchange Online	N/A
Persistent Browser session	N/A
Policy Enabled	Yes

BLOCK - Guest Access

Table 12 BLOCK - Guest Access (B2B)

Configuration Item	Setting
Home > Conditional Access - Policies	
Name	BLOCK - Guest Access (B2B)
Description	Blocked apps that guest users can never access
Targeted Groups - Include	All Users
Targeted Groups - Exclude	Excluded from CA
Targeted Apps - Include	All Cloud Apps
Targeted Apps - Exclude	Teams SharePoint Online Planner
Conditions	
Sign-In Risk	N/A
Device Platforms – Include	N/A
Device Platforms – Exclude	N/A
Locations - Include	N/A
Location – Exclude	N/A
Client Apps	N/A
Device State – Exclude	N/A
Access Controls	
Block Access	Yes
Grant Access	No

Require Multifactor Authentication	N/A
Require Device to be marked as compliant	N/A
Require Hybrid Azure AD Joined device	N/A
Require approved client app (iOS only)	N/A
Terms of Use	N/A
Require ALL of the selected controls	N/A
Require ONE of the selected controls	N/A
Use App enforced restrictions	N/A
Enabling limited access with SharePoint Online	N/A
Enabling limited access with Exchange Online	N/A
Persistent Browser session	N/A
Policy Enabled	Yes