Australian Government
Digital Transformation Agency

Intune Applications – As-built as-configured

March 2020

dta

Contents

Overview

Purpose

The purpose of this as-built as-configured (ABAC) document is to detail each Intune application deployed within the solution. These applications 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 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

Intune Applications

The following tables list all deployed Intune applications within the tenant.

CMTrace Install

Table 2 CMTrace Install settings

Name	Value
Type	Windows app (Win32)
Name	CMTrace Install
Description	Install CMTrace.exe and create shortcut on desktop to Intune log location to monitor.
Publisher	Microsoft
Category	
Show this as a featured app in the Company Portal	Yes
Information URL	
Privacy URL	
Developer	
Owner	
Notes	
Logo	
Install command	powershell.exe -executionpolicy bypass -file CMtraceInstall.ps1
Uninstall command	
Install behaviour	powershell.exe -executionpolicy bypass -file CmtraceRemove.ps1
Device restart behaviour	System
Return codes	0 Success 1707 Success 3010 Soft reboot 1641 Hard reboot 1618 Retry
Operating system architecture	X64
Minimum operating system	Windows 10 1903
Disk space required (MB)	

Physical memory required (MB)	
Minimum number of logical processors required	
Minimum CPU speed required (MHz)	
Additional requirement rules	
Rules format	Manually configure detection rules
Detection rules	File %windir%
Dependencies	
Assignments - Required	rol-Agency-Administrators; rol-Agency-Users
Available for enrolled devices	
Uninstall	

Janusseal for Outlook

Table 3 Janusseal for Outlook settings

Name	Value
Type	Windows MSI line-of-business app
Name	Janusseal for Outlook
Description	Janusseal for Outlook
Publisher	Janusseal
App install context	Device
Ignore app version	Yes
Command-line arguments	
Category	
Show this as a featured app in the Company Portal	No
Information URL	
Privacy URL	
Developer	
Owner	
Notes	
Logo	
Assignments - Required	grp-app-Janusseal

Uninstall	

Office 365 Monthly Targeted

Table 4 Office 365 Monthly Targeted settings

Name	Value
Type	Office 365 ProPlus Suite (Windows 10)
Name	Office 365 Monthly Targeted
Description	Office 365 Monthly Targeted
Publisher	Microsoft
Category	Productivity
Show this as a featured app in the Company Portal	Yes
Information URL	
Privacy URL	
Developer	Microsoft
Owner	Microsoft
Notes	
Logo	Microsoft Office logo
Apps to be installed as part of the suite	Excel, OneDrive Desktop, Outlook, PowerPoint, Publisher, Skype for Business, Teams, Word
Architecture	64-bit
Update channel	Monthly (Targeted)
Remove other versions	Yes
Version to install	Latest
Use shared computer activation	Yes
Accept the Microsoft Software License Terms on behalf of users	Yes
Apps to be installed as part of the suite	1 language(s) selected
Assignments - Required	grp-SecBaselines
Uninstall	

App protection policies

The following tables list the Intune App protection policies deployed within the tenant.

iOS App Protection Policy

Table 5 iOS App Protection Policy settings

Setting	Value
Policy	iOS App Protection Policy
Deployed	Yes
Platform	iOS/iPadOS
Management Type	All app types
Apps	15

Table 6 iOS App Protection Policy configuration

Setting	Value
Basics	
Name	iOS App Protection Policy
Description	--
Platform	iOS/iPadOS
Apps	
Target to apps on all device types	Yes
Device types	--

Public apps	Managed Browser Skype for Business Excel Outlook PowerPoint Word OneNote Microsoft Planner Azure Information Protection Microsoft SharePoint OneDrive Microsoft Teams Microsoft Stream Microsoft To-Do Microsoft Visio Viewer
Custom apps	--
Data protection	
Prevent backups	Block
Send org data to other apps	Policy managed apps
Select apps to exempt	Default: tel;telprompt;skype;app-settings;calshow;itms;itmss;itms-apps;itms-appss;itms-services;
Save copies of org data	Block
Allow user to save copies to selected services	OneDrive for Business SharePoint
Receive data from other apps	Policy managed apps
Restrict cut, copy, and paste between other apps	Policy managed apps
Cut and copy character limit for any app	0
Third party keyboards	Block
Encrypt org data	Require
Sync app with native contacts app	Block
Printing org data	Block
Restrict web contact transfer with other apps	Intune Managed Browser
Unmanaged browser protocol	--
Org data notifications	Allow

Access requirements

PIN for access	Not required
PIN type	Numeric
Simple PIN	Block
Select minimum PIN length	4
Touch ID instead of PIN for access (iOS 8+/iPadOS)	Block
Override Touch ID with PIN after timeout	Require
Timeout (minutes of inactivity)	30
Face ID instead of PIN for access (iOS 11+/iPadOS)	Block
PIN reset after number of days	Yes
Number of days	365
App PIN when device PIN is set	Require
Work or school account credentials for access	Require
Recheck the access requirements after (minutes of inactivity)	30

Conditional launch

Setting	*Value*	*Action*
Offline grace period	720	Block access (minutes)
Offline grace period	90	Wipe data (days)
Jailbroken/rooted devices		Block access
Min OS version	12.0	Block access

Scope tags

Default

Assignments

Included groups	grp-iOS-Devices
Excluded groups	--

Windows Information Protection

Table 7 Windows Information Protection settings

Setting	Value
Policy	Windows Information Protection
Deployed	Yes
Platform	Windows 10
Management Type	With enrollment
Apps	--

Table 8 iOS App Protection Policy configuration

Setting	Value
Basics	
Name	Windows Information Protection
Description	Application Protection policies
Platform	With enrollment
Targeted Apps	
Protected apps	23 selected
Exempt apps	0 selected
Required settings	
Network perimeter	
Network boundary	1 Configured
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	