Australian Government
Digital Transformation Agency

Protected Utility Blueprint

Workstation 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 technology components that will be implemented to support the Windows 10 Standard Operating Environment (SOE).

Scope

Table 1 describes the components that are in scope for the Windows 10 design.

Table 1 In Scope Components

Component	Inclusions
Windows 10 Enterprise	• Windows 10 Enterprise SOE • Windows Analytics • Windows Defender Application Control • Windows BitLocker • Microsoft Defender Advanced Threat Protection (ATP)
Security Compliance	• Essential Eight • Australian Cyber Security Centre (ACSC) Hardening

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 still may not be included in this Blueprint if it is not required for all agencies. An Agency may have additional requirements that will need to be considered outside of this Blueprint including the following:

- Application Packaging. Organisations will have specific requirements with regard to packaging of applications and this is therefore not included in this Blueprint

Documentation

Associated Documentation

Table 2 identifies the documents that were referenced during the creation of this design.

Table 2 Associated Documentation

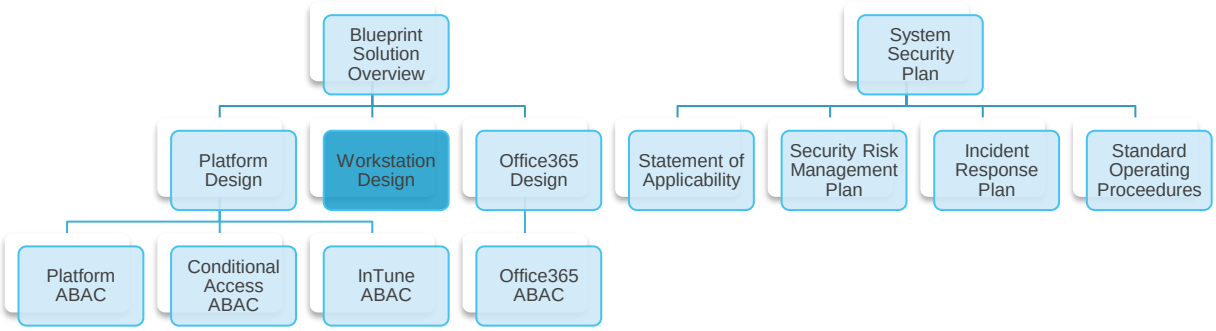
Name	Version	Date
ACSC - Hardening Microsoft Office 365 ProPlus, Office 2019 and Office 2016[1]	N/A	01/2020
ACSC - Hardening Microsoft Windows 10, version 1709, Workstations[2]	N/A	01/2020
Azure - ACSC Consumer Guide - Protected - 2018	N/A	08/2018
Australian Government Information Security Manual (June 2019)	N/A	10/2019
DTA – Blueprint Solution Overview	March	03/2020
DTA – Platform 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 is technical in nature with the audience expected to be familiar with Windows 10 installation and configuration.

Figure 1 - Blueprint Documentation Set



This document covers the information as described in Table 3.

Table 3 Document Structure

Section	Description
Hardware Platform	The Hardware Platform section includes the physical hardware, firmware drivers, and peripherals.
Standard Operating Environment	The SOE section defines all the operating system components that are installed on the physical hardware. It includes the operating system and core services.
Microsoft Office	The Microsoft Office section includes the edition, architecture, features language pack and OneDrive for Business client configuration.
Windows Security	The Windows Security section describes the configuration and methods of locking down the configuration in order to align with Microsoft security best practices and ACSC guidance for Windows 10 clients.

For each component within the document there is a brief description of the contents of the section, a commentary on the things that have been considered in determining the decisions and the design decisions themselves.

Hardware Platform

Hardware Requirements

Description

The hardware platform chosen to support the SOE is key to its stability and provides the components that can be configured by the operating system and applications.

Design Considerations

The selected processor architecture and associated firmware capability directly influence the supportability of applications and security features of an operating system. The minimum hardware listed below will ensure that the system runs reliably.

Design Decisions

Table 4 describes the Hardware Requirements design decisions, and the justification taken by the business and technical teams.

Table 4 Hardware Platform Design Decisions

Decision Point	Design Decision	Justification
Hardware requirements	As listed below in *Table 4*.	To ensure all Blueprint capabilities are supported

Table 5 Windows 10 SOE Hardware requirements

Component	Requirement
Architecture	X64
Processor	At least 4 logical processors, VT-x (Intel) or AMD-V CPU extensions, 2 GHz or higher with Second Level Address Translation (SLAT) support.
RAM	8 Gigabyte (GB)
Input Device(s)	Keyboard Mouse
Min HDD Space	64 GB
BIOS	Minimum (Unified Extensible Firmware Interface) UEFI 2.3.1

TPM	Minimum version 2.0

Device Hardware

Description

The device hardware encompasses all physical components that the user will touch excluding peripherals.

Design Considerations

Providing the hardware selected meets or exceeds the minimum specifications listed above the overriding requirement is that the selected models meet organisational procurement and support requirements.

Design Decisions

Table 6 describes the Device Hardware design decisions, and the justification taken by the business and technical teams.

Table 6 Device Hardware Design Decisions

Decision Point	Design Decision	Justification
Laptop Model	Any device that meets the above requirements and is available through the Whole of Government ICT Hardware Panel	To ensure all Blueprint capabilities are supported
Desktop Model	Any device that meets the above requirements and is available through the Whole of Government ICT Hardware Panel	To ensure all Blueprint capabilities are supported

Drivers and Peripherals

Description

End user peripherals may require drivers to provide functionality. It is critical these drivers are supported on the Operating System version and deployed at the right time.

Design Considerations

Drivers can be deployed in the base reference image, during device deployment task sequence or later by Microsoft Windows Update. Drivers such as network drivers are critical during the deployment phase, whereas a printer driver is not. The more generic a reference image, the lower the deployment and maintenance costs.

Design Decisions

Table 7 describes the Drivers and Peripherals design decisions, and the justification taken by the business and technical teams.

Table 7 Drivers and Peripherals Design Decisions

Decision Point	Design Decision	Justification
Driver Integration	Configured	Deployed via Microsoft Windows Update which aligns with the ACSC guidance.
Approved Peripheral Devices	Configured	Deployed via Microsoft Windows Update which aligns with the ACSC guidance.
Unapproved Peripheral Devices	Blocked	The SOE will block the installation of unapproved peripheral devices.
Signed Device Driver Store	Configured	Deployed via Microsoft Windows Update which aligns with the ACSC guidance.
Peripheral Drivers	Configured	Deployed via Microsoft Windows Update which aligns with the ACSC guidance.
Workstation Device Drivers	Configured	Deployed via Microsoft Windows Update which aligns with the ACSC guidance.
Printer Drivers	Configured	Deployed via Microsoft Windows Update which aligns with the ACSC guidance.

Firmware Configuration

Description

The firmware is the software that provides the interface between the hardware and the operating system. Firmware configuration and capabilities can directly influence the supportability of applications and security features of an operating system.

Design Considerations

Two important Firmware capabilities are detailed below:

- **UEFI** - UEFI is a replacement for the older Basic Input / Output System (BIOS) firmware interface and the Extensible Firmware Interface (EFI) 1.10 specifications
- **Secure Boot** - Secure Boot is a security standard developed by members of the PC industry to help make sure that the device boots using only software that is trusted by the PC manufacturer. When the PC starts, the firmware checks the signature of each piece of boot software, including firmware drivers (Option ROMs) and the operating system. If the signatures are valid, the PC boots, and the firmware gives control to the operating system

Firmware that meets the UEFI 2.3.1 or newer specifications provides the following benefits:

- Faster boot and resume times
- Ability to use security features such as Secure Boot and factory encrypted drives that help prevent untrusted code from running before the operating system is loaded
- Ability to more easily support large hard drives (more than 2 terabytes) and drives with more than four partitions
- Compatibility with legacy BIOS. Some UEFI-based PCs contain a Compatibility Support Module (CSM) that emulates earlier BIOS, providing more flexibility and compatibility for end users. To use the CSM, Secure Boot must be disabled
- Support for multicast deployment, which allows PC manufacturers to broadcast a PC image that can be received by multiple PCs without overwhelming the network or image server
- Support for UEFI firmware drivers, applications, and Option ROMs
- UEFI 2.3.1 is a requirement for the use of Device Guard

Design Decisions

Table 8 describes the Firmware Configuration design decisions, and the justification taken by the business and technical teams.

Table 8 Firmware Configuration Design Decisions

Decision Point	Design Decision	Justification
UEFI version	At least 2.3.1	This is minimum UEFI version required for Device Guard
Secure Boot	Enabled	Secure Boot is a requirement for the use of Windows Defender Credential Guard and provides greater security protection
Secure Boot Configuration Method	Configured via Intune	To align with the ACSC Windows 10 hardening guide

Trusted Platform Module

Description

A Trusted Platform Module (TPM) is a microchip designed to provide basic security-related functions, primarily involving encryption keys. The TPM is usually installed on the motherboard of a computer or laptop and communicates with the rest of the system using a hardware bus.

Design Considerations

With a TPM, private portions of key pairs are kept separated from the memory controlled by the Operating System. Keys can be sealed to the TPM, and certain assurances about the state of a system—that define its "trustworthiness"—can be made before the keys are unsealed and released for use. The TPM uses its own internal firmware and logic circuits for processing instructions, it does not rely upon the Operating System and is not exposed to external software vulnerabilities.

Design Decisions

Table 9 describes the TPM design decisions, and the justification taken by the business and technical teams.

Table 9 Trusted Platform Module Design Decisions

Decision Point	Design Decision	Justification
TPM	Enabled in BIOS from hardware vendor or manually configured.	Required for BitLocker
TPM Version	2.0	To align with the ACSC Windows 10 hardening guide

TPM Configuration Method	Configured via Intune	To align with the ACSC Windows 10 hardening guide

Standard Operating Environment

A SOE is a specific solution built in accordance with the Australian Cyber Security Centre hardening principles and deployed to meet specific business requirements. It is comprised of an operating system, core services, a standard application set, a defined security configuration and a defined user configuration.

Operating System

Description

The operating system allows software application to interface with the hardware. The operating system manages input and output device components like the mouse, keyboard, network and storage.

Design Considerations

Windows 10 is available in several editions for businesses. These editions include:

- **Windows 10 Pro for Workstations** – is designed for people with advanced data needs such as data scientists, CAD professionals, researchers, media production teams, graphic designers, and animators.
- **Windows 10 Pro** –includes management and deployment features and can be joined to both an on-premises and Azure AD domain
- **Windows 10 Enterprise** –has additional enterprise security features including WDAC, Microsoft Defender ATP as well as the UE-V and App-V clients built in. This edition is only distributable through Microsoft's Volume Licensing Program

Microsoft has aligned servicing models for Windows 10 and Office 365 with twice per year feature update releases. Releases are currently targeting March and September with each September release of the Enterprise edition offering a 30-month servicing timeline allowing organisations to skip a release or optionally delay a release and still be fully supported.

Common terminology has also been updated to simplify the servicing process. Servicing now falls into three distinct channels:

- **Windows Insider Program** – Windows Insider Program receive features updates immediately allowing piloting machines to evaluate early builds prior to the arrival to the semi-annual channel. A business must opt-in for this service and install a specific Microsoft provide Windows Insider Program for Business Preview build

- **Semi-Annual Channel** – Semi-Annual Channel receives feature update releases twice per year and is designed for the broad population of general-purpose devices within an organisation
- **Long-Term Servicing Channel** – Long-Term Servicing Channel receives releases much more gradually (expected every 2 - 3 years) and is designed for special purpose devices such as those used in Point of Sale (POS) systems or controlling factory or medical equipment, and those machines without Microsoft Office. Additionally, the following applications are not supported on LTSC Windows devices
  - Microsoft Edge
  - Microsoft Store
  - Cortana (though limited search capabilities remain available)
  - Microsoft Mail
  - Calendar
  - OneNote
  - Weather
  - News
  - Sports
  - Money
  - Photos
  - Camera
  - Music
  - Clock

Design Decisions

Table 10 describes the Operating System design decisions, and the justification taken by the business and technical teams.

Table 10 Operating System Design Decisions

Decision Point	Design Decision	Justification
Windows 10 Edition	Enterprise	The Enterprise edition of Windows is required to support security features such as BitLocker and Windows Defender Application Control (WDAC).

Windows 10 Servicing Channels	Semi-Annual Channel	Semi-Annual Channel is the recommended ring to deploy to most enterprise clients. This will be the default servicing channel for the Agency's Windows 10 devices.
Windows 10 Build	1909	At the time of writing build 1909 is the latest Semi-annual Channel release and recommended by Microsoft.[4] This September release will also provide 30 months of support.

Architecture

Description

The architecture of the operating system within the context of the SOE refers to the width of the data bus. Microsoft and Linux 64-bit operating systems have been available since 2002.

Design Considerations

Windows 10 is available in two processor architectures.

- **32-bit Architecture** - 32-bit Windows is not capable of executing 64-bit applications, although it is capable of being installed on 64-bit capable hardware. 32-bit Windows can run 16-bit software using a 16-bit subsystem. The 32-bit architecture imposes limits of the amount of memory that applications and Windows can address. 32-bit Windows cannot utilise more than 4GB of memory
- **64-bit architecture** - The 64-bit Windows architecture can only be installed on computers with a 64-bit capable processor. When running 64-bit Windows, all device drivers must be 64-bit. 64-bit Windows can run 32-bit software using a 32-bit subsystem, although some 32-bit applications are not compatible with 64-bit Windows. 64-bit Windows does not have a 16-bit subsystem and does not support 16-bit applications.

[4] For more information on each servicing channel refer to https://technet.microsoft.com/en-us/windows/release-info.aspx

Design Decisions

Table 11 describes the Windows 10 Architecture design decisions, and the justification taken by the business and technical teams.

Table 11 Windows 10 Architecture Design Decision

Decision Point	Design Decision	Justification
Windows Architecture	64-bit	To align with the ACSC Windows 10 hardening guide. Provides maximum flexibility for application support.

Activation and Licencing

Description

When a licence key has been assigned to a Windows device Microsoft needs to be notified that the licence key is in use. This notification to Microsoft is the activation process.

Design Considerations

Windows 10 licencing has evolved significantly since the initial release. In addition to the traditional activation methods for on premises networks (KMS, MAK and AD Based Activation) it is also possible to use Windows 10 Subscription Activation. The evolution of Windows 10 activation is described below:

- Windows 10, version 1909 updates Windows 10 Subscription Activation to enable step up from Windows 10 Pro Education to Windows 10 Education for those with a qualifying Windows 10 or Microsoft 365 subscription
- Azure Active Directory (Azure AD) available for identity management

Office 365 products require licensing to enable full functionality and support. The available activation methods are:

- **Office 365 based activation** - Office 365 is Microsoft's productivity solution in the cloud. Office 365 has two sets of suites: one for the small and medium business segment and one for the enterprise segment. These suites are sold across different channels and programs designed to meet each segment's needs. Products are assigned to users and then activated through the online Microsoft Office 365 licensing service

Design Decisions

Table 12 describes the Activation and Licensing design decisions, and the justification taken by the business and technical teams.

Table 12 Activation and Licensing design decisions

Product	Quantity	Justification
Microsoft Windows 10 Enterprise 1909 Microsoft Office 365 E5	One Microsoft 365 E5 licence per user to allow the use of a Windows 10 enterprise device.	For agencies to meet their obligations under the ISM, PSPF, and ACSC cloud guidance as they relate to PROTECTED security classification. it is recommended in this design that agencies purchase a Microsoft 365 E5 licence for each user.

Windows Activation Method	Windows 10 Subscription	All devices will meet the requirements for Subscription Activation, and this is the easiest solution to implement.
Office Activation Method	Office 365	Office 365 activation will be used for Office products such as Office 365 ProPlus.

Windows Features

Description

Windows 10 incorporates optional features that can be enabled to offer additional functionality.

Design Considerations

All unnecessary features are removed from the image.

Design Decisions

Table 13 lists which optional Windows Features will be included in the SOE and the justification taken by the business and technical teams.

Table 13 Windows Features

Feature	Description	Justification
Windows Media Features	Controls and displays media content.	Supports media content functionality.
Windows 10 Ink	Allows users to enter text into applications with a pen or stylus.	Required to support full functionality of devices to be deployed, including Handwriting support.
Print and Document Services - Windows Fax and Scan	Enable fax and scan support for the device.	Supports scanning functionality.
Printing	Enabled	Printing enabled for office use only. Printer drivers must be supported by Windows 10.
Microsoft Print to PDF	Provides built in Print to PDF functionality.	Enables user support for Print to PDF.

Microsoft XPS Doc Writer	Enables creation of XML Paper Specification (XPS) files.	Enables user support for Microsoft XPS Doc Writer functionality.
Remote Differential Compression Application Programming Interface (API) Support	Support for Remote Differential Compression applications.	Required for application compatibility.
Windows PowerShell	Windows PowerShell engine.	Support administration scripting activities.

Universal Windows Platform Applications

Description

Universal Windows Platform (UWP) applications are a new type of application that run on Windows 10 and newer devices. Developers can build line of business Windows Store apps using standard programming languages. The new Windows Runtime (WinRT) supports C#, C++, JavaScript and Visual Basic.

Design Considerations

UWP applications cannot access user resources unless the application specifically declares a need to use those resources. This ensures a clear connection between apps and the types of resources the app has access to.

Design Decisions

Table 14 lists the UWP applications design decisions, and the justification taken by the business and technical teams.

Table 14 Universal Windows Platform Applications design decisions

Application Name	Description	Provisioning State
Alarms and Clock	A versatile combination of alarm clock app, world clock, timer, and stopwatch.	Removed
Bing	Weather and News	Removed
Calculator	A simple yet powerful calculator that includes standard, scientific, and programmer modes, as well as a unit converter.	Provisioned

Camera	The redesigned Camera is faster and simpler than ever before.	Removed
Mail and Calendar	The Mail and Calendar apps provides access to a user's email, schedule, and contacts.	Removed
Maps	Provides search functionality for places to get directions, contact numbers, business info, and reviews.	Removed
Microsoft OneDrive	OneDrive is a cloud storage, file hosting service that allows a user to sync files and later access them from a web browser or mobile device.	OneDrive personal removed. OneDrive for Business will be used.
Microsoft Solitaire Collection	Microsoft Solitaire Collection on Windows 10.	Removed
Microsoft Video	The Movies & TV app brings a user the latest entertainment in one simple, fast, and elegant app on Windows.	Removed
Mixed Reality	3D Viewer, Print 3D, Mixed Reality Portal	Removed
Mobile	YourPhone, Mobile Plans, Connect App	Removed
OfficeHub	MyOffice	Removed
OneNote	Microsoft OneNote Application	Provisioned
Paint3D	Microsoft Paint3d Application	Provisioned
People	The People app in Windows is a modern take on the flat contact lists of the past. It is built for the way people communicate today and is connected to cloud services.	Removed
Photos	The best place to enjoy, organise, edit, and share digital memories.	Removed
Snip and Sketch	Capture a specific area of the screen.	Provisioned
MS Paint	Creative paint and drawing tool.	Provisioned
Sticky Notes	Sticky Notes	Provisioned

Store	Shopfront for purchasing and downloading applications.	Microsoft Store for Business will be used.
Microsoft Xbox	The Xbox experience on Windows 10. The Xbox app brings together friends, games, and accomplishments across Xbox One and Windows 10 devices.	Removed
Zune	Groove Music and Movies	Removed

Microsoft Store

Description

The Microsoft Store is an online store for applications available for Windows 8 and newer operating systems. The Microsoft Store has been designed to be used in both public and enterprise scenarios depending on whether the Microsoft Public Store or Microsoft Store for Business is configured.

Design Considerations

The Microsoft Public Store is the central location for browsing the library of available Windows UWP Applications that can be installed on Windows 10. The Microsoft Public Store includes both free and paid applications. Applications published by Microsoft and other developers are available.

The Microsoft Store for Business allows organisations to purchase applications in larger volumes and customise which applications are available to users. Applications which are made available can either be distributed directly from the store or through a managed distribution approach. Applications which have been developed within the organisation can also be added and distributed as required.

Licensing can also be managed through the Microsoft Store for Business and administrators can reclaim and reuse application licenses.

Design Decisions

Table 15 describes the Microsoft Store design decisions, and the justification taken by the business and technical teams.

Table 15 Windows Store Design Decisions

Decision Point	Design Decision	Justification
Windows Public Store	Disabled via Intune	To align with the ACSC Windows 10 hardening guide.
Microsoft Store for Business	Enabled	Apps will be delivered by Microsoft Store for Business.

Enterprise Applications

Description

Enterprise applications provide organisations and end users the functionality they require to perform day to day activities.

Design Considerations

Applications can be delivered to the user's desktop by one of the following methods:

- **Installed** – The application is part of the desktop deployment. Every user receiving the image also receives the application. Typically, common applications are installed into the reference image. Applications targeted to a small set of users can be installed post deployment or delivered via a streamed application
- **Stream/App-V** – The application is delivered, via the network, to the desktop and cached. The application is not technically installed, instead it executes within a temporary runtime environment
- **Hosted** – The application is hosted on an application server or VDI, such as Citrix XenApp/XenDesktop. To the end user the application looks as if it's been started from the local machine
- **Self Service** – Applications can be delivered via the new Software Center which is installed as part of the ConfigMgr client. As of ConfigMgr version 1802 "user-available" apps now appear in Software Centre under the applications tab where they were previously available in the Application Catalogue
- **Intune** – Applications can be delivered via Intune. In addition to installation of Office 365 and Microsoft Edge, application can be installed as web links, line of business applications or Win32 applications.

Applications that can be installed are broken down into two categories:

- **Available** – These applications will be made available for installation via Software Centre under the applications tab

- **Restricted** – Applications that are restricted by licensing, security or operational limitations and cannot be made available to all staff. The existing approval processes for delivery of these applications will be used. Once approved restricted applications will then be made available for staff via group membership. Users can then install the requested application from the software catalogue

Design Decisions

Table 16 describes the Enterprise Applications design decisions, and the justification taken by the business and technical teams.

Table 16 Enterprise Applications Design Decisions

Decision Point	Design Decision	Justification
Application Delivery Technologies	Deployed via Intune	Applications deployed via Intune and will be installed during the build deployment.
Installed Application Delivery Method(s)	Deployed via Intune	Intune policies provide a consistent configuration and reporting method for the Blueprint
Self Service	Self Service Microsoft Store for Business	Allow users to install the apps needed while ensuring the SOE remains as light weight as possible.

Power Management

Description

The power settings in Windows 10 can be fully managed by Intune. Individual settings can be enforced or set as defaults that can then be changed by the user as desired.

Design Considerations

Users can adjust power and performance options via the system tray power slider icon to either:

- **Better Battery / Recommended** - Better Battery / Recommended provides extended battery life than the default settings on previous versions of Windows
- **Better Performance** - Better Performance is the default slider mode that slightly favours performance over battery life and is appropriate for users who want to trade-off power for better performance of applications
- **Best Performance** - Best Performance prioritizes performance over battery life

Design Decisions

Table 17 describes the Power Management design decisions, and the justification taken by the business and technical teams.

Table 17 Power Management Design Decisions

Decision Point	Design Decision	Justification
Management method	Configured via Intune	Intune policies provides a consistent configuration and reporting method for the Blueprint
Default Power Option Battery	Balanced	Default setting, no requirement to change has been identified
Default Power Option Powered	Better Performance	Default setting, no requirement to change has been identified
Power Management Configuration	Refer to DTA - Intune Security Baselines - ABAC for power management configurations details	To align with the ACSC Windows 10 hardening guide

Windows Search and Cortana

Description

The Windows Search feature of Windows 10 provides indexing capability of the operating and file system allowing rapid searching for content stored on an attached hard disk. Once indexed a file can be searched using either the file name or the content contained within the file.

Design Considerations

Cortana's features include being able to set reminders, recognise natural voice without the user having to input a predefined series of commands, and answer questions using information from Bing (like current weather and traffic conditions, sports scores, and biographies).

Cortana can be used to perform tasks like setting a reminder, asking a question, or launching the app.

Configuration of Cortana features can be managed by group policy or modern management (such as Microsoft Intune).

Design Decisions

Table 18 describes the Windows Search and Cortana design decisions, and the justification taken by the business and technical teams.

Table 18 Windows Search and Cortana Design Decisions

Decision Point	Design Decision	Justification
Cortana	Disabled	As per the ACSC hardening guidelines the Cortana feature will be disabled to align with security requirements.
Windows Search	Enabled (limited to local items only)	Windows Search will be limited to local items only to prevent data leakage
Management method	Configured via Intune	Intune policies provide a consistent configuration and reporting method for the Blueprint

Internet Browser

Description

The internet browser is a software application used for access web pages. This may be built into the operating system or an application installed later.

Design Considerations

Microsoft Edge Chromium version is the default web browser for Windows 10 which has been developed to modern standards and provides greater performance, security and reliability. Microsoft Edge also provides additional features such as Web Note, Reading View and Cortana integration.

Alternate browsers may also be deployed to support specific business needs or requirements.

Design Decisions

Table 19 describes the Windows 10 Internet Browser configuration design decisions, and the justification taken by the business and technical teams.

Table 19 Internet Browser Design Decisions

Decision Point	Design Decision	Justification
Default Browser	Microsoft Edge Chromium – Stable edition	Maximum life of configured applications
Configuration	Configured via Intune	Intune policies provide a consistent configuration and reporting method for the Blueprint
Alternate Browsers	Internet Explorer 11	Maximum compatibility

Tablet Mode

Description

Tablet Mode is a new, adaptive user experience offered in Windows 10 that optimises the look and behaviour of applications and the Windows shell for the physical form factor and end-user's usage preferences.

Design Considerations

Tablet Mode is a feature that switches a device experience from tablet mode to desktop mode and back. The primary way for an end-user to enter and exit "tablet mode" is manually through the Action Centre. In addition, Original Equipment Manufacturers (OEMs) can report hardware transitions (for example, transformation of 2-in-1 device from clamshell to tablet and vice versa), enabling automatic switching between the two modes.

Design Decisions

Table 20 describes the Tablet Mode design decisions, and the justification taken by the business and technical teams.

Table 20 Tablet Mode Design Decisions

Decision Point	Design Decision	Justification
Tablet Mode	Enabled by default on devices that support it	To provide the option to manipulate Tablet Mode behaviour through the Action Centre

Fast User Switching

Description

Fast User Switching allows more than one concurrent connection to a Windows 10 device, however only one session can be active at a time.

Design Considerations

The drawback to Fast User Switching is, if one user reboots or shuts down the computer while another user is logged on, the other user may lose work as applications may not automatically save documents.

Design Decisions

Table 21 describes the Fast User Switching design decisions, and the justification taken by the business and technical teams.

Table 21 Fast User Switching Design Decisions

Decision Point	Design Decision	Justification
Fast User Switching	Enabled	The Fast User Switching feature in Microsoft Windows 10 allows users to login to a PC while keeping other users logged in and their applications running. It is expected that this will only be used by support staff when fault finding.
Management Method	Intune	Intune policies provide a consistent configuration and reporting method for the Blueprint

Corporate Branding

Description

Organisational branding enables a consistent corporate user experience.

Design Considerations

Windows 10 permits the image displayed at the lock screen, logon screen and desktop wallpaper to be customised and support various resolution backgrounds. The appropriate resolution is selected based on an image file name. Windows will automatically select the appropriate image based on the current screen resolution. If a file matching the screen resolution cannot be found, a default image file is used, and the picture stretched to fit the screen.

Custom themes can be deployed to workstations either enforcing the theme or allowing a user to customise it after the initial SOE deployment. Each client Agency would be required to provide information necessary to customise the branding.

Although the system will capable of being assessed as Protected, we should not set banners to PROTECTED in the SOE or Desktop background.

Design Decisions

Table 22 describes the Corporate Branding design decisions, and the justification taken by the business and technical teams.

Table 22 Corporate Branding Design Decisions

Decision Point	Design Decision	Justification
Lock Screen	Custom Agency logo	To enable the Blueprint to be personalised in line with Agency requirements
Logon Screen	Custom Agency logo	To enable the Blueprint to be personalised in line with Agency requirements
Wallpaper	Custom Agency image	To enable the Blueprint to be personalised in line with Agency requirements
Account Picture	User account picture must correspond to the user security pass	To enable the Blueprint to be personalised in line with Agency requirements

Theme	Default	No requirement for a custom theme has been identified
Theme Colour	Default	No requirement for a custom theme has been identified
Windows Colour	Default	No requirement for a custom theme has been identified
Corporate Account Picture	Default	No requirement for corporate account pictures has been identified
User Ability to Change Account Picture	Disabled	Intune policies provide a consistent configuration and reporting method for the Blueprint

System Properties

Description

The System Properties window can be customised in several ways. Within the System Properties window, the Manufacturer and Model values can be displayed.

Design Considerations

Support information can also be populated which includes a:

- Support phone number
- Support hours
- Support website

A custom OEM logo can also be displayed below the Windows logo.

The system Computer Description can also be used to display the build date, time and SOE version.

The Manufacturer value is used in the title string displayed in the support section, being “<Manufacturer> support”. If the actual computer manufacturer were to be populated, then the support section heading would be “Lenovo support”, for example, which would be misleading for users. Therefore, setting the Manufacturer value to “Digital Transformation Agency” would set the support section heading to “Digital Transformation Agency support”.

Design Decisions

Table 23 describes the System Properties design decisions, and the justification taken by the business and technical teams .

Table 23 System Properties Design Decisions

Decision Point	Design Decision	Justification
Company Name	Not Configured	Not required to support solution.
OEM Logo	Not Configured	Not required to support solution.
Manufacturer Value	Configured – Agency Name	To identify the Agency as the device owner
Model Value	Configured – Asset Number	To identify the device via asset label
Support Hours Value	Configured - Support hours of internal ICT support	To simplify Blueprint desktop support
Support Phone Value	Configured	To simplify Blueprint desktop support
Support URL Value	Configured	To simplify Blueprint desktop support
Computer Description	Configured - Asset type and model	To simplify Blueprint desktop support

Start Menu

Description

The Windows 10 Start Menu contains tiles that represent different programs that a user can launch by clicking on the tile.

Design Considerations

One of the features of this new interface is that the tiles themselves can display real-time information directly on the Start menu. The default Start Menu layout can be configured for all users that will use the device. This layout can be enforced, if required, so end users cannot change what applications are available on the Start Menu.

Design Decisions

Table 24 describes the Start Menu design decisions, and the justification taken by the business and technical teams .

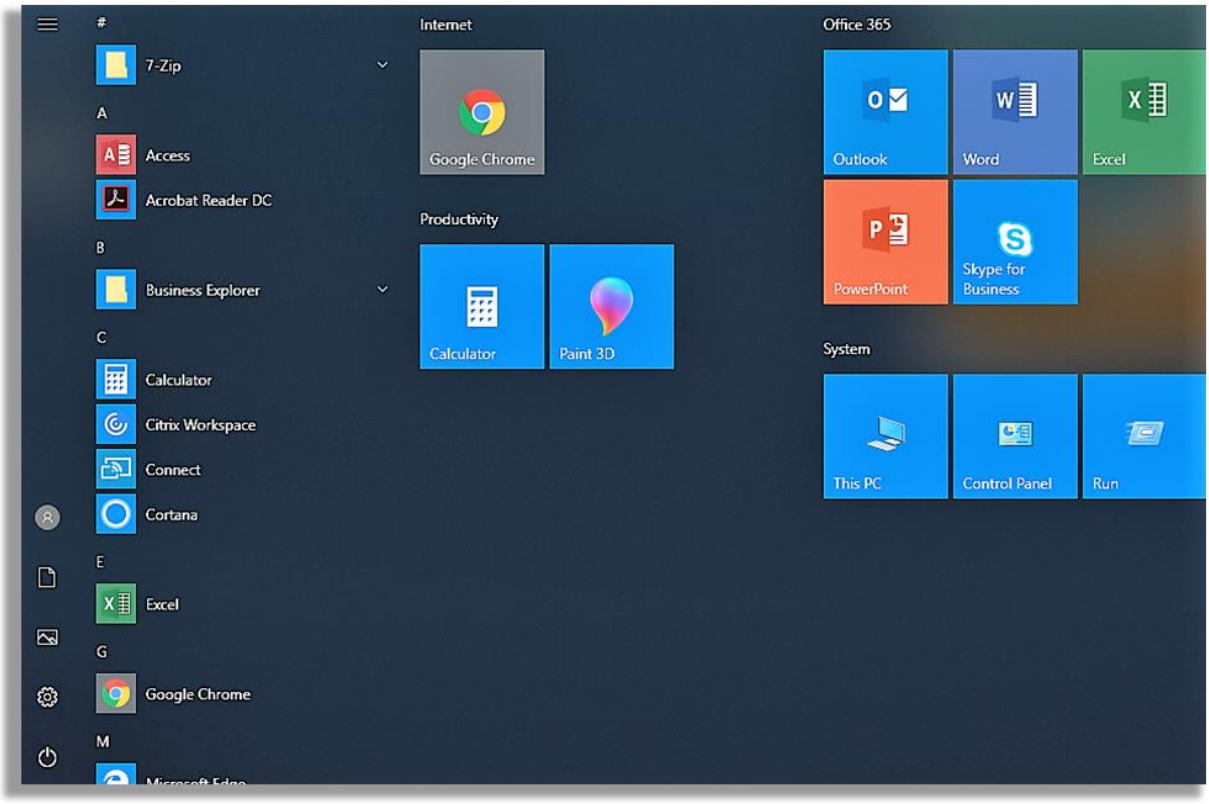
Table 24 Start Menu Design Decisions

Decision Point	Design Decision	Justification
Start Menu Layout	Custom – as illustrated below in *Figure 2*	To display commonly used corporate applications
Start Menu Custom Layout Deployment	Deployed via Intune	Intune policies provide a consistent configuration and reporting method for the Blueprint
Start Menu Layout Enforced	No	To enable end-users can customise the Start Menu to suit specific needs, including the ability to resize, reorganise and choose whether to list most recent shortcuts.

Figure 2 provides an example of the Windows 10 user start menu.[5]

[5] Image is taken from an example Windows 10 SOE. This image is likely to change and as such may not be the most up to date reflection.

Figure 2 - Windows 10 User Start Menu



Screen Saver

Description

The screen saver was originally designed prevent burn-in on Cathode Ray Tube (CRT) and plasma screens. Modern usage of the screen saver allows the operating system to detect a period of inactivity and lock or blank the screen reducing power usage.

Design Considerations

Microsoft does not recommend enabling a screen saver on devices. Instead, Microsoft recommends using automatic power plans to dim or turn off the screen as this can help reduce system power consumption.

Configuration can be applied to restrict the end-user ability to configure or change the screen saver settings.

Design Decisions

Table 25 describes the Screen Saver design decisions, and the justification taken by the business and technical teams.

Table 25 Screen Saver Design Decisions

Decision Point	Design Decision	Justification
Screen Saver	Disabled	Not required, the device will be configured to sleep after 15 minutes.
Users Can Configure the Screen Saver	No	To disable the ability for users to configure the screen saver for all Windows 10 SOE devices.
Require Password on Wake	Configured	To require users to enter their password on machine wake in accordance with security requirements

Profiles, Personalization and Folder Redirection

Description

Profiles are a collection of data and settings for each user of a Windows computer. Examples of data captured as part of a user's profile are documents, pictures, videos, and music.

Design Considerations

While the parameters pertain to all users, the configuration values are specific to a single user and are stored in a single folder known as the 'User Profile'. These configuration parameters (themes, window colour, wallpapers, and application settings) determine the look and feel of the operating environment for a specific user.

Microsoft includes several standard options for user profiles, or personalisation. Alternatively, technologies such as Microsoft UE-V, can be used to address user profile and personalisation requirements. If no user profile is configured, a desktop local profile is used, which without some form of personalisation service, is seldom optimal.

Microsoft provide the following profile management solutions:

- **Local Profiles** – Local user profiles are stored on the workstation. When the user logs on for the first time, a local user profile is created for the user and stored by default in

"C:\Users\%USERNAME%". Whenever a user logs on to the workstation, the user's local user profile is loaded. When the user logs off the workstation, any configuration changes made to the user's profile are saved in the user's profile

- **Mandatory Profiles** – Mandatory profiles are a profile that does not save profile changes and are enforced at each logon
- **Roaming Profiles** – Roaming user profiles are stored in a central location on the network, which is generally a shared folder on a server. When the user logs on to a workstation, the roaming user profile is downloaded from the network location and loaded onto the workstation. When the user logs off the workstation, any profile changes are saved to the network share. In addition to maintaining a copy of the roaming profile on the network share, Windows also keeps a locally cached copy of the roaming profile on each workstation that the user logs on. FSLogix, while being the preferred Roaming Profile option as it is able to provide a cloud-based roaming profile, adds technical complexity as the cloud storage location would need to also be rated at PROTECTED. This additional cloud infrastructure includes Azure framework components such as Firewalls, VNETs, and a PROTECTED level RBAC model. Due to this reliance on infrastructure, FSLogix is not included in the design as end users are expected to have their own endpoints

Design Decisions

Table 26 describes the Profiles, Personalisation, and Folder Redirection design decisions, and the justification taken by the business and technical teams.

Table 26 Profiles, Personalisation and Folder Redirection Design Decisions

Decision Point	Design Decision	Justification
Profile Type	Local Profiles	Local Profiles will be configured to support end-user assigned laptops. This configuration assumes that users will not share devices.
Folder Redirection	Redirect Windows Known Folders	Users can continue using the folders they're familiar with. Files are automatically backed up to the users OneDrive folder in the cloud.
Known Folder Redirection Configuration	Configured as listed below in *Table 27*	To enable user personalisation

Table 27 Known Folder Redirection Configuration

Folder	Path
AppData	Not Configured
Contacts	Not Configured

Desktop	C:\Users\%username%\OneDrive\Desktop
Documents	C:\Users\%username%\OneDrive\Documents
Downloads	Not Configured
Favourites	Not Configured
Links	Not Configured
Searches	Not Configured
Music	Not Configured
Pictures	C:\Users\%username%\OneDrive\Pictures
Videos	Not Configured

Operational Support

Description

Windows 10 and supporting management tools offer various SOE support features to allow support personnel to access a machine remotely or provide users with the option to perform automated repairs.

Design Considerations

The following support components are available in Windows 10:

- **Windows Remote Management (WinRM)** – WinRM is the Microsoft implementation of the WS-Management Protocol, a standard Simple Object Access Protocol (SOAP)-based, firewall-friendly protocol that allows hardware and Operating Systems from different vendors to interoperate
- **WS-Management protocol** - The WS-Management protocol specification provides a common way for systems to access and exchange management information across an IT infrastructure. WinRM and Intelligent Platform Management Interface (IPMI), along with the Event Collector are components of the Windows Hardware Management features
- **Windows Remote Assistance** – Windows Remote Assistance in Windows 10 uses the Remote Desktop Protocol (RDP) protocol to provide a remote desktop connection that is interactive between the locally logged on user and a remote user
- **Remote Desktop** – Remote Desktop enables a user to remotely logon interactively to a workstation from another computer with a supported Remote Desktop client

Design Decisions

Table 28 describes the Operational Support design decisions, and the justification taken by the business and technical teams.

Table 28 Operational Support Design Decisions

Decision Point	Design Decision	Justification
WinRM	Enabled	To meet operating support requirements for the Blueprint
WS Management Protocol	Enabled	To meet operating support requirements for the Blueprint
Windows Remote Assistance	Enabled	To meet operating support requirements for the Blueprint
Remote Desktop	Enabled	To meet operating support requirements for the Blueprint

Windows Update and Patching

Description

Many updates released for operating systems and application contain bug fixes but more importantly they contain security updates. Vulnerabilities can be exploited by malicious code or hackers and need to be patched as soon as possible.

Design Considerations

A risk assessment of a vulnerability is essential in determining the timeframe for applying patches. There are many different sources and indicators that will help with this assessment, for example if the vendor releases a patch outside of their normal patching cycle and its marked as a critical update then it's worth immediate investigation to see how it could affect an organisation.

It is vital to have a robust and reliable patch management solution based on industry best practices.

For Microsoft Windows environments the primary patching technologies are:

- **Windows Server Update Service** – WSUS enables administrators to deploy the most recent Microsoft updates. A WSUS server connects directly to Microsoft Update or an "upstream" WSUS server. This allows administrators to control what updates are applied and when, rather than having every computer on the network going to the Internet and installing every available update immediately

- **Microsoft System Centre Configuration Manager** –ConfigMgr still requires a WSUS server, however the two are integrated. WSUS obtains updates from the internet and ConfigMgr is used to deploy the updates. Using ConfigMgr to deploy software updates allows for more control over many aspects of the process such as targeting, maintenance windows, scheduling and reporting
- **Microsoft Intune** – Windows Update for Business provides management policies for several types of updates to Windows 10 devices
  - **Feature updates**: previously referred to as upgrades, feature updates contain not only security and quality revisions, but also significant feature additions and changes; they are released semi-annually in the fall and in the spring
  - **Quality updates**: these are traditional operating system updates, typically released the second Tuesday of each month (though they can be released at any time). These include security, critical, and driver updates. Windows Update for Business also treats non-Windows updates (such as those for Microsoft Office or Visual Studio) as quality updates. These non-Windows Updates are known as "Microsoft updates" and can configure devices to receive or not receive such updates along with their Windows updates
  - **Driver updates**: these are non-Microsoft drivers that are applicable to the devices. Driver updates can be turned off by using Windows Update for Business policies
  - **Microsoft product updates**: these are updates for other Microsoft products, such as Office. These updates can be enabled or disabled by using Windows Update for Business policy
  - Use Intune to define update rings that specify how and when Windows as a Service updates Windows 10 devices. Update rings are policies that are assigned to groups of devices. By using update rings, it is possible to create an update strategy that mirrors business needs

In order to deploy patches to endpoints as quickly as possible the client-side settings should not restrict or delay the installation of patches where it does not interfere with critical operation or cause loss of data due to unexpected reboots.

Design Decisions

Table 29 describes the Windows Update and Patching design decisions, and the justification taken by the business and technical teams.

Table 29 Windows Update and Patching Design Decisions

Decision Point	Design Decision	Justification
Patching Method	Intune - Windows Update Rings	Intune policies provide a consistent configuration and reporting method for the Blueprint

Decision Point	Design Decision	Justification
Software update rings	Production and Pilot	Allows early issue of Windows Insider updates to selected users prior to the full release of Semi-Annual Channel (Targeted) updates to the remaining users. See DTA – Software Updates - ABAC for more detailed information.
Feature Updates	Enabled	To align with the ACSC Windows 10 hardening guide
Quality Updates	Enabled	To align with the ACSC Windows 10 hardening guide
Driver Updates	Enabled	To align with the ACSC Windows 10 hardening guide
Microsoft Product Updates	Enabled	To align with the ACSC Windows 10 hardening guide

Networking

Description

Windows 10 contains many networking technologies that can provide benefits to end users. Some of these are visible and some, such as IPv6, operate in the background.

Design Considerations

Windows 10 provides support for several wireless networking technologies that allow devices to connect to a wireless network. The two most popular technologies supported in Windows currently are Wi-Fi and Mobile Broadband networking.

The deployment of wireless networks has promoted the use of Layer 2 network authentication, such as 802.1x, to ensure that only appropriate users or devices can connect to a protected network and that data is secure at the radio transmission level. The Single Sign-On (SSO) feature executes Layer 2 network authentication at the appropriate time, given the network security configuration, while at the same time integrating with the user's Windows logon experience.

Design Decisions

Table 30 describes the Networking design decisions, and the justification taken by the business and technical teams.

Table 30 Networking Design Decisions

Decision Point	Design Decision	Justification
IPv6	Disabled	As per ISM guidance IPv6 will be disabled unless a specific use is identified.
Wireless	Enabled	Where applicable, wireless capable devices will have WIFI enabled to allow use case of mobile working.
Wireless Configuration	Refer to Table 31 for wireless configuration recommendations.	To align with the ACSC Windows 10 hardening guide Note, these settings will be configured via Intune if the Agency requires.
Broadband	Not Configuredef	Requires Subscriber Identity Module (SIM) capability which is not required for Blueprint devices Note, if Agency devices have SIM capability this can be enabled

Table 31 Wireless Configuration

Decision Point	Design Decision	Justification
Connect to Wireless Hotspots	Enabled	Allows users to connect to wireless hotspots when working remotely.
Automatically Connect to Suggested Open Hotspots	Disabled	To align with the ACSC Windows 10 hardening guide
Prohibit installation and configuration of Network Bridge	Enabled	To align with the ACSC Windows 10 hardening guide
Single Sign On 802.1x	Enabled	To align with the ACSC Windows 10 hardening guide
Wireless Profile Configuration	Configured	Will be configured depending on Agency requirements.

Microsoft Office

Microsoft Office Edition

Description

Microsoft Office is available in two release cycles and within those release cycles there are multiple editions.

Design Considerations

Office 365 – Office 365 combines the Microsoft Office desktop suite with cloud-based versions of Microsoft's communications and collaboration services—including Microsoft Exchange Online, Microsoft SharePoint Online, Office Online, and Microsoft Teams. Office 365 is upgraded with new features on a regular basis; and

Traditional Office – Traditional Office is sold as a one-time purchase and provides Office applications for a single computer. There are no upgrade options which means to upgrade to the next major release, another copy of Office will have to be procured. Traditional Office is not upgraded with new features for the life of the release.

Microsoft Office is further divided into distinct editions. For enterprise environments, Office 365 is offered in the following versions:

- **Office 365 ProPlus** – Office applications plus cloud file-storage and sharing. Business email is not included
- **Office 365 Enterprise E1** – Business services—email, file storage and sharing, Office Online, meetings and IM, and more. Office applications are not included
- **Office 365 Enterprise E3** – All the features of Office 365 ProPlus and Office 365 Enterprise E1 plus security and compliance tools, such as legal hold and data loss prevention
- **Office 365 Enterprise E5** – All the features of Office 365 Enterprise E3 plus advanced security, analytics, and voice capabilities

For Traditional Office, two traditional enterprise edition offerings are available, each comprises different products and features:

- **Standard** – This edition includes the core office applications, as well as Outlook and Publisher; and
- **Professional Plus** – This suite includes the core applications, as well as Outlook, Publisher, Access and Teams.

Design Decisions

Table 32 describes the Microsoft Office Edition design decisions, and the justification taken by the business and technical teams.

Table 32 Microsoft Office Edition Design Decisions

Decision Point	Design Decision	Justification
Microsoft Office Version	Office 365 Pro Plus	Includes the locally installed applications and provides access to the latest and most updated features.
Microsoft Office Edition	Office 365 Enterprise E5	Meets functionality requirements and advanced security guidance.
Deployment Method	Intune	Simplest deployment with all features available.

Microsoft Office Architecture

Description

Microsoft Office is available in both 32-bit and 64-bit editions. It is critical to understand the advantages and disadvantages in full before selecting a specific architecture.

Design Considerations

Microsoft recommends that the 32-bit version of Office is installed on both 32-bit and 64-bit operating systems if users depend on existing extensions to Office including:

- ActiveX controls
- Third party add-ins and / or in-house solutions or
- Any 32-bit application that interfaces directly with Microsoft Office

An application cannot have both a 32-bit and 64-bit application architecture and 64-bit Office product cannot load 32-bit components / add-ins.

Design Decisions

Table 33 describes the Microsoft Office Architecture design decisions, and the justification taken by the business and technical teams.

Table 33 *Microsoft Office Architecture Design Decisions*

Decision Point	Design Decision	Justification
Microsoft Office Architecture	64-bit version of Office will be installed by default	Where the organization requires that Hardware Data Execution Prevention (DEP) be enforced for Office applications. For 64-bit installations DEP will always be enforced, while on 32-bit installations DEP needs to be configured through settings.

Office Features

Description

The Office 365 features include the application set that will be provided to the users.

Design Considerations

The Microsoft Office feature section includes the details of the following components:

- Microsoft Access
- Microsoft Excel
- Microsoft Teams
- Microsoft Office OneNote
- Microsoft Outlook
- Microsoft Publisher
- Microsoft PowerPoint
- Microsoft Word

Design Decisions

Table *34* describes the Microsoft Office Feature design decisions, and the justification taken by the business and technical teams.

Table 34 *Microsoft Office Features Design Decisions*

Decision Point	Design Decision	Justification
Installed components	All except Microsoft Access	To provide required user productivity capabilities. No requirement for Microsoft Access identified

Language Pack

Description

Language packs add additional display, help, and proofing tools to Microsoft Office. Multiple language packs can be installed to support specific user requirements.

Design Considerations

If additional language packs are installed it is also likely that keyboards other than US will be required.

Design Decisions

Table 35 describes the Language Pack design decisions, and the justification taken by the business and technical teams.

Table 35 *Microsoft Office Language Pack Design Decisions*

Decision Point	Design Decision	Justification
Default Language	English (UK) – AU Default	Required to support the Microsoft Office deployment and allow user productivity Note, English (US) language pack is removed from the SOE as part of the English (UK) install. English (UK) contains the AU region language pack which is then set as default.
Additional Language	Not Configured	No requirement for additional language has been identified

OneDrive for Business

Description

OneDrive for Business provides a robust cloud storage platform for government agencies.

This OneDrive for Business section considers the client component only. The configuration of the server component of OneDrive for Business is contained in the Office 365 Design document.

Design Considerations

OneDrive enables the secure sharing of files and:

- **Access files from all devices** – OneDrive allows access to files and those files others share on all permitted devices, including mobile, Mac, PC and web browser
- **Internal and external sharing** - Securely share files with staff inside or external of an organisation
- **Collaboration with Microsoft Office integration** – Document co-authoring is available via Office web apps, Office mobile apps, and Office desktop apps, helping staff maintain a single working version of any file
- **Enterprise-grade security** – OneDrive for Business has many security and compliance features, enabling organisations to meet compliance requirements

The OneDrive for Business client has access to two distinct primary rings and an additional preview ring:

- **Production Ring** – The Production ring provides new features and improvements as soon as released by Microsoft
- **Enterprise Ring** – The enterprise ring rolls out changes after validated in the Production ring, reducing the risk of issues. This ring enables administrators to deploy updates from an internal network location and control the timing of the deployment (within a 60-day window). This is the recommended update ring for most large scale or high-risk organisations
- **Insiders Ring** – Insider ring users will receive builds that let them preview new features coming to OneDrive

The Windows Known Folder feature of OneDrive for Business enables administrators to easily move files in a users' Desktop, Documents, and Pictures folders to OneDrive.

OneDrive Files On-Demand enables users to view, search for, and interact with files stored in OneDrive from within File Explorer without downloading them all to the local device. The feature

delivers a unified look and feel for both OneDrive and local files whilst saving on space normally taken up on the local hard drive.

Design Decisions

Table 36 describes the OneDrive For Business design decisions, and the justification taken by the business and technical teams.

Table 36 OneDrive for Business Design Decisions

Decision Point	Design Decision	Justification
OneDrive for Business	Enabled and silently configured	OneDrive is used in place of folder redirection. Will be configured to sign in without user intervention.
Sync Client Update Ring	Enterprise	As per Microsoft recommendations for large environments
OneDrive Personal Account	Disabled	Aligns with ACSC Windows 10 guidance.
Default Location	%userprofile%	Default OneDrive folder location is suitable for the Windows 10 SOE.
Allow Changing Default Location	Disabled	As per Microsoft recommendation for shared devices users will be prevented from changing the default OneDrive folder location.
Files On-Demand	Enabled	Files On-Demand will be configured to save storage space on users' computers and minimize the network impact of sync.
Backup - Sync Windows Known Folders	Enabled	Syncing Windows known folders to OneDrive for Business will be configured for the Windows 10 SOE. This will enable the users Documents, Pictures and Desktop folders to be saved in OneDrive automatically.
Network settings – Upload	Don't limit	Allow dynamic network configuration to provide best performance
Network settings – Download	Don't limit	Allow dynamic network configuration to provide best performance

File Collaboration Policy	Disabled	File collaboration within OneDrive is not required as it is achieved via Microsoft Teams and SharePoint.
Sync Conflict Policy	Let me choose to merge changes or keep copies	The OneDrive sync conflict policy will be configured to allow the user to choose in order to prevent loss of data.

Windows Security

Security configuration affects the end user experience, and more importantly, could affect the organisation through data leakage or infiltration.

Security Baselines

Description

Microsoft security engineers have developed best practice guidance and within Intune have released Security Baselines for:

- Windows 10 MDM management[6]
- Microsoft Defender Advanced Threat Protection[7]
- Microsoft Edge[8]

The Security Baselines are pre-configured groups of settings and default values recommended by the relevant Microsoft security teams. The Security Baselines as published by Microsoft are templates and from these a profile is created. The profile is then assigned to a group of devices.

The ACSC recommended settings that would normally be applied by group policy are applied in the Blueprint using Intune with most of the settings applied using the Security Baselines.

Design Considerations

While Microsoft do not provide a Security Baseline template that is equivalent to ACSC guidance (or indeed any single security Agency) the same team of engineers that provides guidance to security agencies manage the Security Baselines resulting in a great deal of commonality[9].

The Security Baseline template can be equated to a single ADMX file that has been merged from all of the available best practice security ADMX files and the profile could then be equated to the group policy file that is created from that ADMX file.

[6] https://docs.microsoft.com/en-us/intune/protect/security-baseline-settings-mdm
[7] https://docs.microsoft.com/en-us/intune/protect/security-baseline-settings-defender-atp
[8] https://docs.microsoft.com/en-us/intune/protect/security-baseline-settings-edge
[9] https://docs.microsoft.com/en-us/intune/protect/security-baselines

Many of the components that would normally be configured via group policies in an on-premise network are able to be configured with the Security Baselines.

Design Decisions

The approach taken within the Blueprint to secure the workstation is to use Intune to lock down the workstation by:

1. Using a Microsoft Security Baseline template.
2. Creating a profile from the baseline template and adjusting the default settings where appropriate to align with ACSC guidance.
3. Where required, create additional Intune security policies.
4. Where any additional security recommendations are identified that are not able to be addressed within the Security Baseline template a PowerShell script will be generated and delivered via Intune. The settings that require a script will be fed back to Microsoft for incorporation into the next version of the Security Baseline template.

Table 37 describes Security Baseline design decisions, and the justification taken by the business and technical teams.

Table 37 Security Baseline Design Decisions

Decision Point	Design Decision	Justification
Windows 10 MDM management	Configured via Intune	The majority of Microsoft default settings applied via the Security Baselines are in line with the ACSC requirements.
Microsoft Defender Advanced Threat Protection	Configured via Intune	The majority of Microsoft default settings applied via the Security Baselines are in line with the ACSC requirements.
Microsoft Edge	Configured via Intune	The majority of Microsoft default settings applied via the Security Baselines are in line with the ACSC requirements.
Additional settings required	PowerShell script will be created to set registry entries as required	Where Microsoft Defender ATP identifies new security recommendations these will be addressed via a PowerShell script delivered via Intune

Windows 10 MDM management Security Baseline

Description

The MDM security baseline settings support Windows 10 version 1809 and later.

Design Considerations

The security baseline has pre-configured groups of Windows settings and the default settings as advised by the relevant Microsoft security teams.

Design Decisions

Table 38 describes the Windows 10 MDM management Security Baseline design decisions, and the justification taken by the business and technical teams.

Table 38 Windows 10 MDM management Security Baseline Design Decisions

Decision Point	Design Decision	Justification
Above Lock	Configured	Default configuration, no requirement to change it has been identified.
App Runtime	Configured	Default configuration, no requirement to change it has been identified.
Application Management	Configured	Default configuration, no requirement to change it has been identified.
Auto Play	Configured	Default configuration, no requirement to change it has been identified.
BitLocker	Configured	Default configuration, no requirement to change it has been identified.
Browser	Configured	Default configuration, no requirement to change it has been identified.
Connectivity	Configured	Default configuration, no requirement to change it has been identified.

Decision Point	Design Decision	Justification
Credentials Delegation	Configured	Default configuration, no requirement to change it has been identified.
Credentials UI	Configured	Default configuration, no requirement to change it has been identified.
Data Protection	Configured	Default configuration, no requirement to change it has been identified.
Device Guard	Configured	Default configuration, no requirement to change it has been identified.
Device Installation	Configured	Default configuration, no requirement to change it has been identified.
Device Lock	Configured	Prevent use of camera, require password, Disable the lock screen slide show settings, Set password minimum age in days
DMA Guard	Configured	Default configuration, no requirement to change it has been identified.
Event Log Service	Configured	Event log sizes modified to align with ACSC guidance.
Experience	Configured	Default configuration, no requirement to change it has been identified.
Exploit Guard	Configured	Default configuration, no requirement to change it has been identified.
File Explorer	Configured	Default configuration, no requirement to change it has been identified.
Firewall	Configured	Default configuration, no requirement to change it has been identified.
Internet Explorer	Configured	Default configuration, no requirement to change it has been identified.
Local Policies Security Options	Configured	UAC settings have been modified to align with ACSC guidance

Decision Point	Design Decision	Justification
Microsoft Defender	Configured	Scheduled scan has been disabled in this baseline. This is set in Defender ATP baseline to avoid conflicts.
MS Security Guide	Configured	Default configuration, no requirement to change it has been identified.
MSS Legacy	Configured	Default configuration, no requirement to change it has been identified.
Power	Configured	Default configuration, no requirement to change it has been identified.
Remote Assistance	Configured	Default configuration, no requirement to change it has been identified.
Remote Desktop Services	Configured	Default configuration, no requirement to change it has been identified.
Remote Management	Configured	Default configuration, no requirement to change it has been identified.
Remote Procedure Call	Configured	Default configuration, no requirement to change it has been identified.
Search	Configured	Default configuration, no requirement to change it has been identified.
Smart Screen	Configured	Default configuration, no requirement to change it has been identified.
System	Configured	System boot start driver initialization modified to align with ACSC guidance.
Wi-Fi	Configured	Default configuration, no requirement to change it has been identified.
Windows Connection Manager	Configured	Default configuration, no requirement to change it has been identified.

Decision Point	Design Decision	Justification
Windows Hello for Business	Configured	Default configuration, no requirement to change it has been identified.
Windows Ink Workspace	Configured	Default configuration, no requirement to change it has been identified.
Windows PowerShell	Configured	Default configuration, no requirement to change it has been identified.

Microsoft Defender ATP Security Baseline

Description

The Microsoft Defender ATP security baseline settings support Windows 10 version 1809 and later.

Design Considerations

The security baseline has pre-configured groups of Windows settings and the default settings as advised by the relevant Microsoft security teams.

Design Decisions

Table 39 describes the Microsoft Defender ATP Security Baseline design decisions, and the justification taken by the business and technical teams.

Table 39 Microsoft Defender ATP Security Baseline Design Decisions

Decision Point	Design Decision	Justification
Application Guard	Not Configured	Testing of Application Guard produced unreliable results. Not configured at this time.
Application Reputation	Configured	Default configuration, no requirement to change it has been identified.
Attack Surface Reduction Rules	Configured	Default configuration, no requirement to change it has been identified.

Decision Point	Design Decision	Justification
BitLocker	Configured	Device encryption changed to AES 256-bit XTS to align with ACSC guidance
Device Control	Configured	Default configuration, no requirement to change it has been identified.
Endpoint Detection and Response	Configured	Default configuration, no requirement to change it has been identified.
Exploit Protection	Configured	Default configuration, no requirement to change it has been identified.
Firewall	Configured	Default configuration, no requirement to change it has been identified.
Microsoft Defender Antivirus	Configured	Default configuration, no requirement to change it has been identified.
Web & Network Protection	Configured	Network protection changed to Enable to align with ACSC guidance.
Windows Hello for Business	Configured	Default configuration, no requirement to change it has been identified.

Microsoft Edge Security Baseline

Description

The Preview Microsoft Edge security baseline settings support Edge version 77 and later.

Design Considerations

The security baseline has pre-configured groups of Windows settings and the default settings as advised by the relevant Microsoft security teams. This security baseline is in preview and it is expected that the available settings will increase over time.

Design Decisions

Table 40 describes the Microsoft Edge Security Baseline design decisions, and the justification taken by the business and technical teams.

Table 40 Microsoft Edge Security Baseline Design Decisions

Decision Point	Design Decision	Justification
Microsoft Edge Settings	Configured	Default configuration, no requirement to change it has been identified.

Windows Defender Application Control

Description

Application control is a crucial line of defence for protecting enterprises given today's threat landscape, and it has an inherent advantage over traditional antivirus solutions. Specifically, application control moves away from the traditional application trust model where all applications are assumed trustworthy by default to one where applications must earn trust in order to run. Many organisations, like the Australian Signals Directorate, understand this and frequently cite application control as one of the most effective means for addressing the threat of executable file-based malware (.exe, .dll, etc.).

Design Considerations

Windows Defender Application Control (WDAC) can help mitigate these types of security threats by restricting the applications that users can run and the code that runs in the System Core (kernel). WDAC policies also block unsigned scripts and MSIs, and Windows PowerShell runs in Constrained Language Mode.

Design Decisions

Table 41 describes the Application Whitelisting design decisions, and the justification taken by the business and technical teams.

Table 41 Application Whitelisting Design Decisions

Decision Point	Design Decision	Justification
Application Whitelisting Product	WDAC	Microsoft recommended product for application whitelisting[10]
Whitelisted method	A combination of publisher certificate and path rules and will be used.	Controlled via Intune to align with the ACSC Windows 10 1709 hardening guidance. WDAC policies are natively supported in Intune
Microsoft Block Rules	Configured	To align with the ACSC Windows 10 1709 hardening guidance.
Intelligent Security Graph connection	Configured	In accordance with Microsoft best practice.

Windows Defender

Description

Microsoft delivers several threat protection and mitigation capabilities in Windows 10 Enterprise devices delivered through Windows Defender.

These capabilities do not require additional agents and are manageable via Intune Endpoint Protection Profiles.

Design Considerations

The following details the Windows Defender capabilities:

- **Microsoft Defender Antivirus** – Provides anti-malware and spyware protection including always-on scanning, dedicated protection updates and cloud-delivered protection. Integration with Internet Explorer and Microsoft Edge browsers enable real time scanning of files as they are downloaded to detect malicious software
- **Microsoft Defender Exploit Guard** – Provides Host-based Intrusion Protection System (HIPS) capabilities and replaces the Microsoft Enhanced Mitigation Experience Toolkit (EMET)

[10] https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/windows-defender-application-control#choose-when-to-use-wdac-or-applocker

- **Microsoft Defender Application Guard** – Provides hardware isolation of Microsoft Edge to protect against malicious websites. Protection is provided through the use of Hyper-V enabled containers isolated from the host operating system for opening untrusted websites
- **Microsoft Defender Credential Guard** – Provides virtualisation-based security to isolate credentials to protect against identity theft attacks. Much like Device Guard, Credential Guard uses Virtual Secure Mode (VSM) to isolate processes, in this case the Local Security Authority (LSA). The LSA performs various security operations, including the storage and management of user and system credentials. Unauthorised access to the LSA can lead to credential theft attacks, such as Pass-the-Hash or Pass-The-Ticket
- **Microsoft Defender Firewall** – Provides stateful packet inspection and blocking of network traffic. Windows Defender Firewall blocks unauthorized network traffic flowing into and out of the client endpoint reducing the attack surface of the device
- **Microsoft Defender SmartScreen** – Provides malware and phishing website protection including downloaded files. SmartScreen protects users by performing the following

Analysing webpages for signs of distrustful behaviour and shows a warning page if it identifies suspicious activity.

- Validates sites against a dynamic list of known phishing and malicious software sites and shows a warning page if it identifies page
- Validates downloaded files against a list of known software sites and programs and shows a warning page if it identifies the site or program may be malicious
- Validates downloaded files against a list of files that are known and used by a large number of windows users. If not found on the list SmartScreen shows a warning

Microsoft Defender Exploit guard comprises of the below features:

- **Exploit protection** – Exploit protection applies exploit mitigation mechanisms to applications. Works with third-party antivirus solutions and Windows Defender Antivirus
- **Attack surface reduction** – Attack Surface Reduction (ASR) rules reduce the attack surface of applications with rules that stop the vectors used by Office, script and mail-based malware
- **Network protection** – Network protection extends the malware and social engineering protection offered by Windows Defender SmartScreen in Microsoft Edge to cover network traffic and connectivity on Agency devices
- **Controlled Folder Access** – Controlled folder access protects files in key system folders from changes made by malicious and suspicious apps

Design Decisions

Table 42 describes the Windows Defender design decisions, and the justification taken by the business and technical teams.

Table 42 Windows Defender Design Decisions

Decision Point	Design Decision	Justification
Microsoft Defender	Enabled	Microsoft Defender will be enabled to align with ACSC guidance.
Microsoft Defender Capabilities Enabled in the SOE	Components: Microsoft Defender Antivirus Microsoft Defender Exploit Guard Microsoft Defender Application Control Microsoft Defender SmartScreen Microsoft Defender Application Guard Microsoft Defender Credential Guard Microsoft Defender Firewall	Provides required security controls for the SOE.
Microsoft Defender Configuration	Intune	Meets Agency platform requirements.
Microsoft Defender Antivirus Exclusions	Enabled and configured as per ACSC Windows 10 1709 hardening guidelines. Refer to DTA - Intune Security Baselines - ABAC document for configuration information.	Required for user experience and acceptable system usability.
Microsoft Defender Exploit Guard Configuration	Enabled and configured as per ACSC Windows 10 1709 hardening guidelines. Refer to DTA - Intune Security Baselines - ABAC document for configuration information.	Aligns with ACSC Windows 10 hardening guide and aligns with security and compliance requirements.
Microsoft Defender Application Control Configuration	Enabled and configured as per ACSC Windows 10 1709 hardening guidelines. Refer to DTA - Intune Security Baselines - ABAC document for configuration information.	To align with the ACSC Windows 10 hardening guide and aligns with security and compliance requirements.

Decision Point	Design Decision	Justification
Microsoft Defender Smart Screen Configuration	Enabled and configured as per ACSC Windows 10 1709 hardening guidelines. Refer to DTA - Intune Security Baselines - ABAC document for configuration information.	To align with the ACSC Windows 10 hardening guide and aligns with security and compliance requirements.
Microsoft Defender Credential Guard Configuration	Enabled and configured as per ACSC Windows 10 1709 hardening guidelines. Refer to DTA - Intune Security Baselines - ABAC document for configuration information.	Aligns with security and compliance requirements. Enabled without lock allows Microsoft Defender Credential Guard to be managed remotely.
Microsoft Defender Firewall Configuration	Enabled and configured as per ACSC Windows 10 1709 hardening guidelines. Refer to DTA - Intune Security Baselines - ABAC document for configuration information.	To align with the ACSC Windows 10 hardening guide and aligns with security and compliance requirements.

Identity Providers

Description

The identity providers section considers the different methods of logging on to the Windows 10 device. The local administrator account is addressed in a separate section.

Design Considerations

Windows 10 provides various user account types or identity providers. This section outlines the identity providers that can be implemented for a Windows 10 device.

- **Local Accounts** - A local account is an account on a single Windows system. Local accounts are not replicated and do not grant access to corporate resources and may be implemented for controlled access to local storage only. It may be desirable to disable, rename and scramble the passwords for the in-built local accounts
- **Active Directory Domain** - Domain identities are used to grant access to corporate resources and are implemented using Active Directory Domain Services. Administrators manage domain identities and ensure that users have access to the appropriate resources when group policies or any other User State Virtualisation (USV) solution is applied to the account. Domain identities are recommended if personalisation data will be stored in a corporate datacentre and will be synchronised to multiple corporate devices

- **Azure Active Directory (Azure AD)** - Azure AD is Microsoft's multi-tenant cloud-based directory and identity management service. Azure AD includes a full suite of identity management capabilities including multi-factor authentication, device registration, self-service password management, self-service group management, privileged account management, role-based access control, application usage monitoring, rich auditing and security monitoring and alerting. These capabilities can help secure cloud-based applications, streamline IT processes, cut costs and help assure corporate compliance goals are met. Azure AD is a prerequisite for Microsoft Intune mobile device management
- **Microsoft Account** - A Microsoft Account is an email address issued by or linked to a Microsoft authentication service. A Microsoft Account can be connected to a domain account (called a Connected Account). With a Connected Account, users that logon with a domain account will receive a consistent and personal experience (settings) and will also have access to the Windows Store and purchased applications. It is important to understand the implications for disabling access to the Microsoft Account service

The following features will be unavailable if access to the service is disabled:

- Windows Store applications delivered by the Windows store will be inaccessible
- The Windows Store Mail and Calendar applications require that the first account linked to it must be a Microsoft Account. User personal settings will not be synced online between Windows 10 devices

Windows Hello for Business provides an enterprise grade MFA capability for Windows 10 by leveraging specific hardware devices to enable 'something you have' and either 'something you know' (compulsory) or 'something you are' (optional) authentication factors.

Windows Hello for Business can be configured by application of policies by Intune or via Group Policy. Both methods have the capability of enforcing the same requirements such as using a TPM, setting PIN length and complexity, and whether to use biometric authentication.

Design Decisions

Table 43 describes the Identity Provider design decisions, and the justification taken by the business and technical teams.

Table 43 Identity Provider Design Decisions

Component	Decision	Justification
Guest Account	Disabled	The local guest account will be disabled during the image deployment. In line with the ACSC Windows 10 1709 hardening guidelines
Guest Account Name	Renamed	The local guest account will be renamed during the image deployment. In line with the ACSC Windows 10 1709 hardening guidelines.
Azure Active Directory Accounts	Enabled	Machines will be Azure AD Joined.
Domain Accounts	Disabled	Machines will be Azure AD Joined.
Microsoft Accounts	Disabled	The use of Microsoft Accounts for the Windows 10 SOE will be disabled to meet security and compliance requirements.
Windows Hello for Business	Disabled	Windows Hello for Business does not meet the organisational password complexity requirements.
Windows Hello for Business Configuration Method	Intune	Windows Hello for Business will be configured via Security Policies in Intune.

Telemetry Collection

Description

Windows 10 and Windows Server include the Connected User Experiences and Telemetry component, which uses Event Tracing for Windows (ETW) trace logging technology that gathers and stores diagnostic data events and data.

Design Considerations

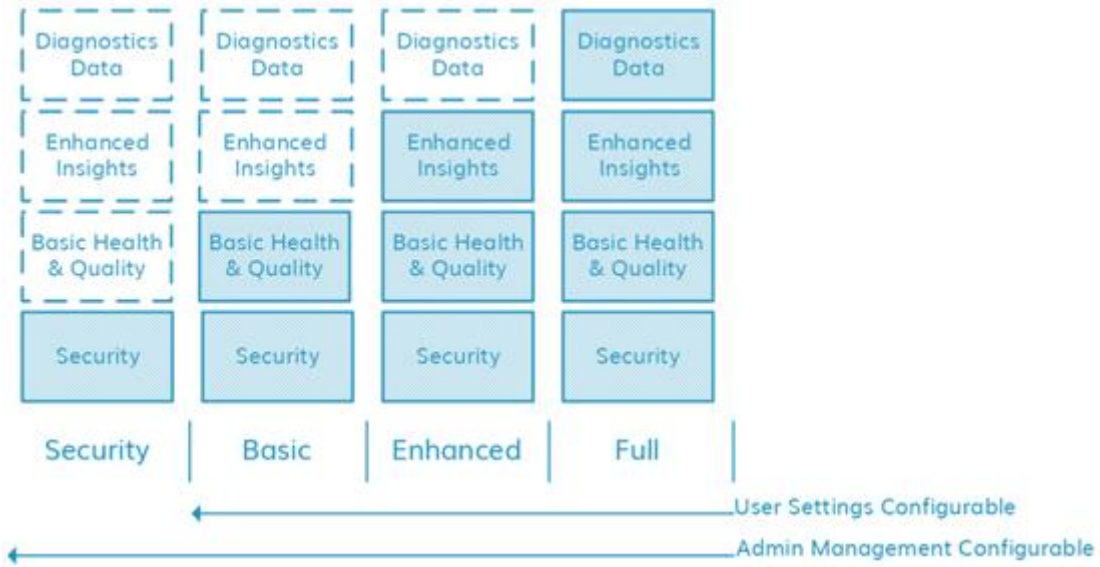
The operating system and some Microsoft management solutions, such as ConfigMgr use the same logging technology.

Windows uses telemetry information to analyse and fix software problems. It also helps Microsoft improve its software and provide updates that enhance the security and reliability of devices within organisations.

Telemetry level options are:

- **Off** – Disable telemetry data collection
- **Security** – Information that's required to help keep Windows secure, including info about telemetry client settings, the Malicious Software Removal Tool, and Windows Defender. This level is available only on Windows 10 Enterprise and Windows 10 Education, and Windows 10 IoT Core
- **Basic** – Basic device info, including quality-related info, application compatibility, and info from the Security level
- **Enhanced** – Additional insights, including how Windows and Windows apps are used, how they perform, advanced reliability info, and info from both the Basic and the Security levels
- **Full** – All info necessary to identify and help to fix problems, plus info from the Security, Basic, and Enhanced levels
- *Figure 3* shows the information in each of the different Telemetry Collection levels.

Figure 3 - Telemetry Options



Design Decisions

Table 44 describes the Telemetry Collection design decisions, and the justification taken by the business and technical teams.

Table 44 Telemetry Collection Design Decisions

Decision Point	Design Decision	Justification
Allow Telemetry	Enabled	In line with the ACSC hardening guideline policy recommendations and meets requirements for future Windows Analytics use.
Telemetry Level	0 – Security	In line with the ACSC hardening guideline policy recommendations.
Configuration Method	Intune	Telemetry will be configured via Intune.

Office Macro Hardening

Description

Microsoft Office files can include Visual Basic for Applications (VBA) programming code (macro) embedded into the document.

A macro can comprise of a number of repeatable actions that can be coded or recorded and rerun later to automate repetitive tasks. Macros are powerful tools that can be easily created by novice users to greatly improve their productivity.

However, an adversary can also create macros to perform a variety of malicious activities, such as assisting in the compromise of workstations in order to exfiltrate or deny access to sensitive information.

Design Considerations

The ACSC provides guidelines in securing systems against malicious macros and recommend they be implemented in all Windows environments in one of the following approaches:

- All macros are disabled
- Only macros from trusted locations are enabled
- Only digitally signed macros are enabled (hardened implementation)
- Only digitally signed macros are enabled (standard implementation)

Design Decisions

Table 45 describes the Office Macro Hardening design decisions, and the justification taken by the business and technical teams.

Table 45 Office Macro Hardening Design Decisions

Decision Point	Design Decision	Justification
Implementation approach	Only digitally signed macros are enabled	In line with the ACSC Microsoft Office Macro security policy recommendation.
Email and Web Content Filtering	Enabled	In line with the ACSC Microsoft Office Macro security policy recommendation.
Configuration Method	Intune	Macro hardening will be configured via Intune and Attack Surface Reduction in Windows Defender Exploit Guard.

Local Administrator

Description

The default local Administrator account is a highly privileged user account found on every Windows operating system. The Administrator account is the first account that is created during the installation for all Windows client operating systems.

Design Considerations

The Administrator account can be used to create local users and assign user rights and access control permissions. It can also be used take control of local resources at any time simply by changing the user rights and permissions.

The default Administrator account cannot be deleted or locked out, but it can be renamed and / or disabled. It is Microsoft best practice and an ACSC hardening guideline recommendation to leave the Administrator account disabled and renamed.

If there is a requirement to utilise the local Administrator account in an environment, Microsoft provides Local Administrator Password Solution (LAPS), an Active Directory integrated Access Control List (ACL) protected password management tool.

LAPS allows system administrators the ability to set a different, random password for the common local administrator account on each computer in the domain and store the password for the computer's local administrator account in Active Directory, secured in a confidential attribute in the computer's corresponding Active Directory object.

Design Decisions

Table 46 describes the Local Administrator design decisions, and the justification taken by the business and technical teams.

Table 46 *Local Administrator Design Decisions*

Decision Point	Design Decision	Justification
Local Administrator Account	Disabled	The local administrator account will be disabled in line with the ACSC Windows 10 1709 hardening guideline policy recommendations.
Local Administrator Account Name	Renamed	The local administrator account will be renamed during the image deployment. In line with the ACSC Windows 10 1709 hardening guideline policy recommendations.
Local Administrator Account Password	Randomised	The local administrator account password will be randomised during the image deployment. In line with the ACSC Windows 10 1709 hardening guideline policy recommendations.
Local Administrator Configuration Method	Intune	In line with the ACSC Windows 10 1709 hardening guideline policy recommendations.
Additional Local Administrator Accounts	Not Configured	Additional administrator accounts will not be created during the image deployment.
LAPS	Not Configured	Not required as the local Administrator account will be disabled and renamed.

Abbreviations and Acronyms

Table 47 details the abbreviations and acronyms used throughout this document.

Table 47 Abbreviations and Acronyms

Acronym	Meaning
ABAC	As-built as-configured
ACL	Access Control List
ACSC	Australian Cyber Security Centre
AD	Active Directory
ADMX	Administrative Template Xml-Based (Microsoft)
AES	Advanced Encryption Standard
API	Application Programming Interface
ASR	Attack Surface Reduction
ATP	Advanced Threat Protection
AU	Australia
BIOS	Basic input/output System
CPU	Central Processing Unit
CRT	Cathode Ray Tube
CSM	Compatibility Support Module
DTA	Digital Transformation Agency
DVR	Digital Video Recorder
EFI	Extensible Firmware Interface
EMET	Enhanced Mitigation Experience Toolkit
ETW	Event Tracing for Windows
HDD	Hard Disk Drive
HIPS	Host-based Intrusion Protection System
HTTP	HyperText Transfer Protocol
ICMP	Internet Control Message Protocol
ICT	Information and Communications Technology
IM	Instant Messenger

IP	Internet Protocol
IPMI	Intelligent Platform Management Interface
ISM	Information Security Manual
IT	Information Technology
KB	Kilobyte(s)
KMS	Key Management Service
LAN	Local Area Network
LAPS	Local Administrator Password Solution
LSA	Local Security Authority
LTSC	Long-Term Servicing Channel
MAK	Multiple Activation Key
MDM	Mobile Device Management
MFA	Multi-factor Authentication
MS	Microsoft
NTLM	NT LAN Manager
OEM	Original Equipment Manufacturer
OSPF	Open Shortest Path First
PC	Personal Computer
PDF	Portable Document Format
PIN	Personal Identification Number
POS	Point of Sale
PSPF	Protective Security Policy Framework
RAM	Random-access Memory
RBAC	Role-based Access Control
RDP	Remote Desktop Protocol
RPC	Remote Procedure Call
SAM	Security Account Manager
SIM	Subscriber Identity Module
SLAT	Second Level Address Translation
SMB	Server Message Block

SOAP	Simple Object Access Protocol
SOE	Standard Operating Environment
SSO	Single Sign-On
SSP	Shared Service Provider
TPM	Trusted Platform Module
TV	Television
UAC	User Account Control
UEFI	Unified Extensible Firmware Interface
UI	User Interface
UK	United Kingdom
UNC	Universal Naming Convention
URL	Uniform Resource Locator
US	United States
USV	User State Virtualisation
UWP	Universal Windows Platform
VBA	Visual Basic for Applications
VDI	Virtual Desktop Infrastructure
VSM	Virtual Secure Mode
WDAC	Windows Defender Application Control
WDAC	Windows Defender Application Control
WDDM	Windows Display Driver Model
Wi-Fi	Wireless Fidelity
WINS	Windows Internet Name Service
WS	Web Services (Management)
WSUS	Windows Server Update Service
XML	Extensible Markup Language
XPS	XML Paper Specification
XTS	XEX-based tweaked-codebook mode with ciphertext stealing