Device Management Technical Guide



Configuration Manager 1610

Prepared for

[Type Customer Name Here]

9/22/2017

Version Draft

Prepared by

**[Type Author Here]**

Contributors

**[Type Contributors Here]**

Revision and Signoff Sheet

Change Record

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Author | Version | Change Reference |
|  |  | 1 | Initial draft for review/discussion |
|  |  |  |  |
|  |  |  |  |

Reviewers

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Version Approved | Position | Date |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[1 Overview 8](#_Toc474850044)

[2 Technical Design 9](#_Toc474850045)

[2.1 Company Resource Access 9](#_Toc474850046)

[2.1.1 Email Profiles 11](#_Toc474850047)

[2.1.2 Windows Hello for Business 12](#_Toc474850048)

[2.1.3 Delegation of Administration 14](#_Toc474850049)

[2.2 Compliance Settings 15](#_Toc474850050)

[2.2.1 Windows Configuration Items 16](#_Toc474850051)

[2.2.2 User Data and Profiles Configuration Items 17](#_Toc474850052)

[2.2.3 Configuration Baselines 18](#_Toc474850053)

[2.2.4 Delegation of Administration 19](#_Toc474850054)

[2.2.5 Edition Upgrade 20](#_Toc474850055)

[2.2.6 Policy sync for Intune enrolled devices 21](#_Toc474850056)

[2.2.7 Windows Information Protection 21](#_Toc474850057)

[2.3 Endpoint Protection 22](#_Toc474850058)

[2.3.1 Core Infrastructure Pre-Requisites 23](#_Toc474850059)

[2.3.2 Configuration Manager Pre-Requisites 23](#_Toc474850060)

[2.3.3 Protection Alerts 24](#_Toc474850061)

[2.3.4 Anti-Malware Policy 26](#_Toc474850062)

[2.3.5 Client Settings 27](#_Toc474850063)

[2.3.6 Windows Firewall Policy 27](#_Toc474850064)

[2.3.7 Delegation of Administration 29](#_Toc474850065)

[2.3.8 Windows Defender Advanced Threat Protection 30](#_Toc474850066)

[2.3.9 Health Attestation Service 30](#_Toc474850067)

[2.3.10 Lookout Integration 31](#_Toc474850068)

[2.4 Power Management 32](#_Toc474850069)

[2.4.1 Core Infrastructure Pre-Requisites 32](#_Toc474850070)

[2.4.2 Configuration Manager Pre-Requisites 32](#_Toc474850071)

[2.4.3 Client Settings 33](#_Toc474850072)

[2.4.4 Collection Targeting 33](#_Toc474850073)

[2.5 Device Enrollment 33](#_Toc474850074)

[2.5.1 Microsoft Intune Subscription 35](#_Toc474850075)

[2.5.2 Exchange Server Connector 38](#_Toc474850076)

[2.5.3 Device Category 41](#_Toc474850077)

[2.5.4 Predeclare Devices 41](#_Toc474850078)

[3 Technical Implementation 43](#_Toc474850079)

[3.1 Device Enrollment 43](#_Toc474850080)

[3.1.1 Microsoft Intune 43](#_Toc474850081)

[3.1.2 Exchange Server Connector 44](#_Toc474850082)

[3.1.3 Device category 44](#_Toc474850083)

[3.1.4 Predeclare devices 44](#_Toc474850084)

[3.2 Compliance Settings 45](#_Toc474850085)

[3.2.1 Configure Compliance Settings for Windows 45](#_Toc474850086)

[3.2.2 New Configuration Item for Systems with the Configuration Manager Client 45](#_Toc474850087)

[3.2.3 New Configuration Item for Systems without the Configuration Manager Client 47](#_Toc474850088)

[3.2.4 User Data and Profiles 48](#_Toc474850089)

[3.2.5 Compliance Policy 49](#_Toc474850090)

[3.2.6 Edition Upgrade 50](#_Toc474850091)

[3.2.7 Policy sync 50](#_Toc474850092)

[3.2.8 Windows Information Protection 50](#_Toc474850093)

[3.3 Company Resource Access 51](#_Toc474850094)

[3.3.1 Email Profiles 52](#_Toc474850095)

[3.4 Power Management 53](#_Toc474850096)

[3.5 Endpoint Protection 54](#_Toc474850097)

[3.6 Windows Defender Advanced Threat Protection 55](#_Toc474850098)

[3.7 Health Attestation Service 55](#_Toc474850099)

[3.8 Lookout Integration 56](#_Toc474850100)

[3.9 Windows Hello for Business 57](#_Toc474850101)

[4 Test Plan 58](#_Toc474850102)

[4.1 Device Enrollment 58](#_Toc474850103)

[4.2 Company Resource Access 58](#_Toc474850104)

[4.2.1 Profile Deployment 58](#_Toc474850105)

[4.3 Compliance 58](#_Toc474850106)

[4.4 Endpoint Protection 59](#_Toc474850107)

[4.5 Power Management 59](#_Toc474850108)

[4.6 Windows Hello for Business 59](#_Toc474850109)

[4.7 Windows Defender Advanced Threat Protection 60](#_Toc474850110)

[4.8 Health Attestation Service 60](#_Toc474850111)

[4.9 Lookout Integration 60](#_Toc474850112)

We are very interested in your input!  If you have comments or would like to request an update to this document, please provide your feedback to the [SDM Suggestions alias](mailto:msdmods@microsoft.com).   Attach the document and clearly describe the changes you would like and explain why the changes are needed.

**Spell/grammar check is turned ON within all SDM Word templates -** Remember to turn off spell/grammar check before sending out the document if you want to avoid showing spelling and grammar red mark-ups. To turn this feature off, do the following:

1. Click on File
2. Click on the Options on the left
3. Click on Proofing
4. Scroll to bottom and check the two boxes shown below:



**To remove all the Visible Guidance (Hot Pink text with Grey Background) all at once:**

1. Click Ctrl H to open the Find and Replace box
2. Make sure your cursor is in the ‘Find what’ box.
3. Click on the More button at the bottom left
4. Click on the Format Button at the bottom left and select Style
5. Scroll down, locate select the “Visible Guidance”
6. Make sure the ‘Replace with’ box is empty:
7. Click ‘Replace All”
8. If not empty - click on the format button in the lower left hand corner. Scroll down and chose ‘(no style)’then replace all.

**IMPORTANT – Finalize This Document**

**REMOVE** all pink text, guidance, comments, changes, and hidden text in this document before submitting it to the customer. You can do this in two ways:

* **Save as PDF** and send the PDF version to the customer.   
  ~ OR ~

**Inspect document and remove comments, revisions, any document properties you do not want included, personal information, and hidden text.** For guidance on how to do this, see [Remove hidden data and personal information from Office documents](http://office.microsoft.com/client/helppreview.aspx?AssetID=HA100375931033&QueryID=ALdFua2no0&respos=6&rt=2&ns=WINWORD&lcid=1033&pid=CH100487501033#3)

1. Overview

The purpose of this document is to detail all aspects of the Device Management Service design and implementation as it relates to the <PROJECTNAME> project. This document is for use by the project manager and technical implementation specialists.

This document should also be made available for review to any program team members, affected business unit(s), IS/IT infrastructure owners/managers, IS Security and any device build team that are identified.

Readers should have a good level of understanding in the following technical areas:

* System Center Configuration Manager Infrastructure
* Application Management design and implementation
* Microsoft Active Directory design and implementation
* Networking and communication implementations
* Knowledge on various types of devices including Laptops, Tablets, Phablets, Smartphones
* Cloud based device management approach
* Device Enrollment through Cloud or Microsoft System Center Configuration Manager
* Policy Settings Management
* Application Management through Cloud
* Microsoft Intune and Extensions for Microsoft System Center Configuration Manager
* Understanding of certificates (CA, PKI, NDES, SCEP)

System Center Configuration Manager collects usage data about your sites and infrastructure. This information is compiled and submitted to the Microsoft cloud service by the service connection point (a new site system role) and is required to enable Configuration Manager to download updates for your deployment that apply to the version of Configuration Manager you use. When you configure the service connection point you can configure both the level of data that is collected, and whether this is submitted automatically (online mode) or manually (offline mode).

1. Technical Design

This section details the implementation of the Device Management features for the production environment and the steps to install, configure, and operate the required components.

The following high-level activities are included in the design:

| Section | Activity |
| --- | --- |
| 2.1 Company Resource Access | Design the features that will enable users to access company resources |
| 2.2 Compliance Settings | Design the configuration items and baselines for compliance to protect company resources |
| 2.3 Endpoint Protection | Design the Endpoint Protection antimalware solution |
| 2.5 Device Enrollment | Design how devices will be added to the device management solution |

Table 1: Design activities for device management.

For detailed documentation of settings, refer to the **TechnicalDesign\_Planning** Excel workbook.

Consultant: Delete the following content if no Company Resource Access features will be implemented.

* 1. Company Resource Access

This section details the technical design of features that may be used to configure and manage company resource access for devices.

Figure 1, below, illustrates the design process from the bottom up for all components of Company Resource Access features. This design approach assumes that all Core Infrastructure and a Core Configuration Manager Infrastructure are deployed and functional. The design will extend the Configuration Manager core infrastructure with the requirements for enabling company resource access.

The document will only include the design of elements required to enable the specific company resource access features.

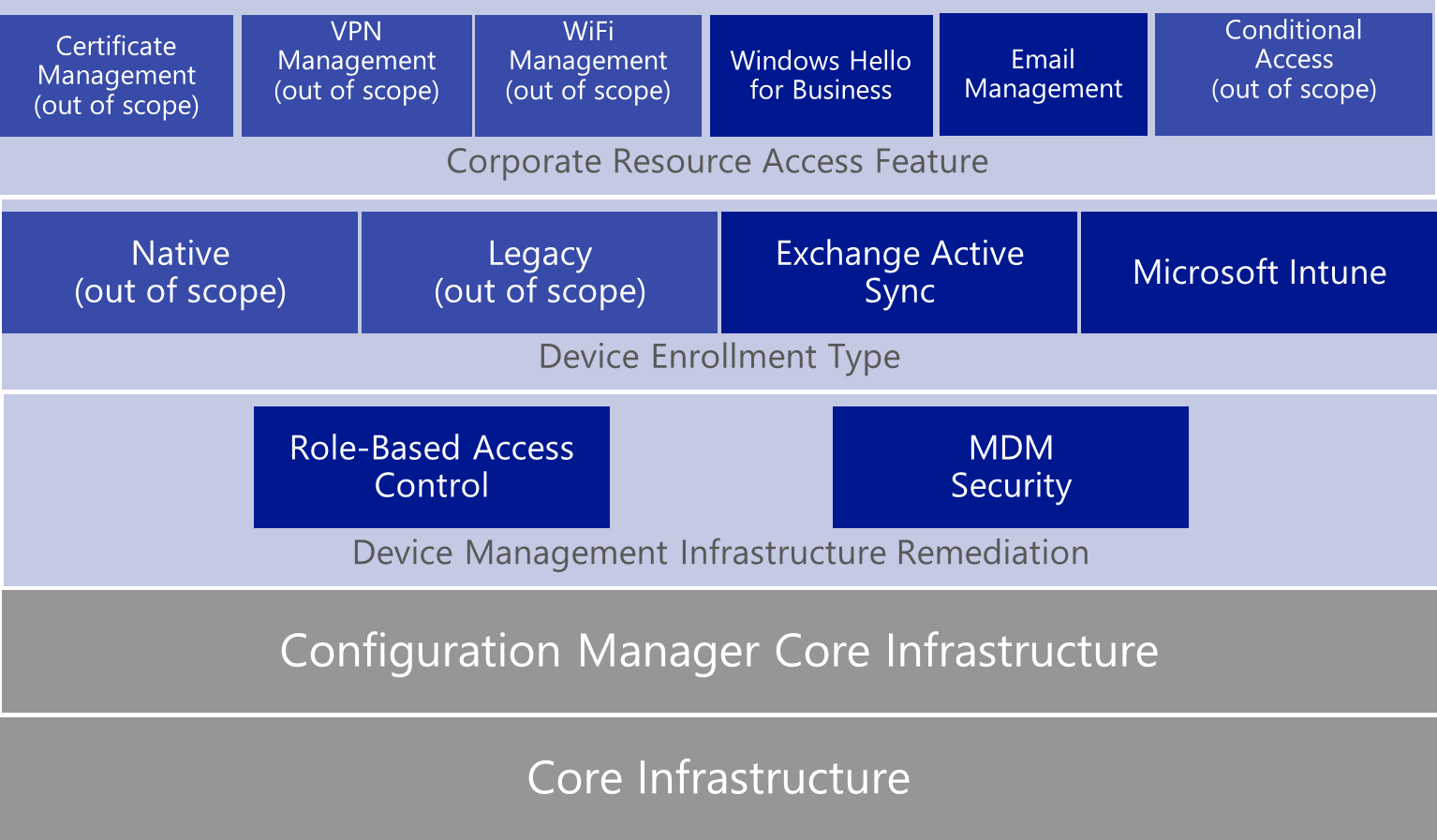


Figure 1. Design approach for corporate resource access.

| Design Decision | Design Options | Decision | Justification |
| --- | --- | --- | --- |
| Email Profile Management | * **Yes** * No | **Yes** | Microsoft Intune is required for Email profile management to:   * Configure an email account on the device, * Configure synchronization settings for contacts, calendars, and tasks.   Configure security settings, including certificates for identity, encryption and signing that have been provisioned by using Configuration Manager certificate profiles. |
| Windows Hello for Business Management | * **Yes** * No | **Yes** | Microsoft Intune is required to deploy Windows Hello for Business profiles that allow users to sign in into Windows 10 devices without passwords. |

Table 2. Features required for Company Resource Access design.

The remainder of this section will detail the design of each of the selected features in Table 2. Items not selected are considered out of scope for the design.

Consultant: Remove any of the subsequent sub-sections that will not be part of the design.

* + 1. Email Profiles

This is an optional extension for Microsoft Intune that allows the provisioning of devices with email profiles and restrictions by using Exchange ActiveSync. Users can access corporate email on their devices with minimal setup.

* + - 1. Core Infrastructure Pre-Requisites

The following core infrastructure services must be configured prior to using email profiles

| Component | Pre-Requisite Met | Additional Information |
| --- | --- | --- |
| Microsoft Intune subscription | <YES | NO> | To deploy profiles to iOS, Android, Windows Phone, and enrolled Windows 8.1 devices, these devices must be enrolled into Microsoft Intune |
| Supported Devices | <YES | NO> | * Windows 8.1 or later * Windows Phone 8.1 or later * iOS 5 or later * Android 4 or later |
| Mail attribute in active directory | <YES | NO> | To generate the users email address in an email profile by using the user’s primary SMTP address, this address must exist in the **mail** attribute in Active Directory |

Table 3. Core infrastructure requirements for email profiles.

* + - 1. Configuration Manager Pre-Requisites

The following core infrastructure and cloud services must be configured prior to implementing

| Component | Pre-Requisite Met | Additional Information |
| --- | --- | --- |
| Email Profiles Extension | <YES | NO> | This extension must be installed and enabled. |
| Company Resource Access Manager permissions | <YES | NO> | The role includes all rights required to manage certificate profiles. |

Table 4. Core infrastructure requirements for email profiles.

* + - 1. Collection Targeting

Email profiles will be deployed to the collections listed below.

| Email Profile Name | Applied To | Justification |
| --- | --- | --- |
| MailProf#1 | Finance mobile users |  |
| MailProf#2 | HR mobile users |  |

Table 5. Target collections for email profiles.

The detailed configuration of each email profile may be found in the **DM-EmailProfile** worksheet of the **Technical Design Planning** workbook.

* + 1. Windows Hello for Business

Microsoft Windows Hello for Business enables the use of gestures to log in to a Windows 10 or Windows 10 Mobile system instead of using passwords. The user gesture may include a PIN, biometric credentials such as Windows Hello or a fingerprint.

Configuration Manager may be used to control Windows Hello for Business as follows:

* Allowed/disallowed gestures
* Store certificates for authentication within the Windows Hello for Business key storage provider (KSP).

This functionality is available using Microsoft Intune in a hybrid configuration. Windows Hello for Business may also be configured using Group Policy for systems that are domain joined or have the Configuration Manager client installed. The design and deployment of Group Policy is out of scope for this design and implementation.

* + - 1. Core Infrastructure Pre-Requisites

This section identifies services required for the capability to operate. This section assumes that all infrastructure components for implementing or using Windows Hello for Business have been met, only Windows 10 and Windows 10 Mobile devices are in-scope and supported, and that only manageability aspects of Windows Hello for Business will be included in this engagement.

* + - 1. Configuration Manager Pre-Requisites

The Configuration Manager design must meet the following pre-requisites.

| Component | Pre-Requisite Met | Description |
| --- | --- | --- |
| System Center Configuration Manager 1602 or later | <YES | NO> | Configuration Manager 1602 or later is required to manage Windows Hello for Business. |
| Microsoft Intune | <YES | NO> | Windows Hello for Business is configurable on in a hybrid architecture with Microsoft Intune. |
| Certificate Profile | <YES | NO> | The device must obtain a certificate to use Windows Hello for Business certificate-based logon. |

Table 6: Configuration Manager dependencies for implementing Windows Hello for Business

* + - 1. Windows Hello for Business Configuration

The following table lists the configurable parameters for Windows Hello for Business as required by the organization.

| Design Consideration | Design |
| --- | --- |
| Windows Hello for Business will be used on all Windows 10 and Windows 10 Mobile devices | <YES | NO> |
| Require Trusted Platform Module (TPM) | <REQUIRED | PREFERRED> |
| Require minimum PIN length | <4 | DEFAULT = 6> |
| Require Maximum PIN length | <0 - 127> |
| Require lowercase letters in PIN | <ALLOWED | REQUIRED | DEFAULT = NOT ALLOWED> |
| Require uppercase letters in PIN | <ALLOWED | REQUIRED | DEFAULT = NOT ALLOWED> |
| Require special characters | <ALLOWED | REQUIRED | DEFAULT = NOT ALLOWED>  ! " # $ % & ' ( ) \* + , - . / : ; < = > ? @ [ \ ] ^ \_ ` { | } ~. |
| Require PIN expiration (days) | <DEFAULT = 41> |
| Prevent reuse of previous PINS | <DEFAULT = LAST 5> |
| Enable biometric gestures | <ENABLED | DISABLED> |
| Use enhanced anti-spoofing, when available | <ENABLED | DISABLED> |
| Use Remote Passport | <ENABLED | DISABLED> |

Table 7. Windows Hello for Business configuration

Windows Hello for Business target devices:

| Design Consideration | Design |
| --- | --- |
| Azure AD Domain Joined Client | <YES | NO> |
| Domain Joined Clients | <YES | NO> |

Table 54. Deployment of Windows Hello for Business Policy

* + 1. Delegation of Administration

Role-based administration combines security roles, security scopes, and assigned collections, to define the administrative scope for each administrative user. An administrative scope includes the objects a user can view in the Configuration Manager console, and the tasks related to those objects that the user has permission to perform. Role-based administration configurations are applied at each site in a hierarchy. System Center Configuration Manager provides several built-in security roles. Custom security roles can be created or a copy of an existing security role can be made, and modified.

The Company Resource Access Manager role is granted the following permissions:

* To view and manage alerts and reports for VPN profiles: **Create**, **Delete**, **Modify**, **Modify Report**, **Read**, and **Run Report** permissions for the **Alerts** object.
* To create and manage certificate profiles: **Author Policy**, **Modify Report**, **Read** and **Run Report** permissions for the **Certificate Profile** object.
* To manage Wi-Fi, certificate, and VPN profile deployments: **Deploy Configuration Policies**, **Modify Client Status Alert**, **Read**, and **Read Resource** permissions for the **Collection** object.
* To manage all configuration policies: **Create**, **Delete**, **Modify**, **Read** and **Set Security Scope** permissions for the **Configuration Policy** object.
* To run queries that are related to VPN profiles: **Read** permission for the **Query** object.
* To view VPN profiles information in the Configuration Manager console: **Read** permission for the **Site** object.
* To view status messages for VPN profiles: **Read** permission for the **Status Messages** object.
* To create and modify the Trusted CA certificate profile: **Author Policy**, **Modify Report**, **Read** and **Run Report** permissions for the **Trusted CA Certificate Profile** object.
* To create and manage VPN profiles: **Author Policy**, **Modify Report**, **Read**, and **Run Report** permissions for the **VPN Profile** object.
* To create and manage Wi-Fi profiles: **Author Policy**, **Modify Report**, **Read**, and **Run Report** permissions for the **Wi-Fi Profile** object.

| Configuration Manager Role | Active Directory Group Member |
| --- | --- |
| Company Resource Access Manager | <AD Group #1>  <AD Group #2>  <AD Group #3> |

Table 8. Security roles and scopes for company resource access.

* 1. Compliance Settings

Compliance settings in Configuration Manager provides the ability to centrally manage the configuration and compliance of devices. The toolset includes the ability to assess compliance of users and client devices. Compliance is evaluated by defining a configuration baseline that comprises specific configuration items and the desired level of compliance.

Microsoft recommends that the following be considered when developing compliance settings

* Do not monitor sensitive data.
* Do not configure compliance rules that use data that can be modified by end users.
* Only import configuration packs and other configuration data from external sources if they have a valid digital signature.
* Implement access control to protect reference computers.
* Secure the communication channel when browsing to a reference computer.
* Restrict and monitor administrative users that are assigned the Compliance Settings Manager role.

Compliance settings must be enabled for devices in the hierarchy. This procedure configures the default client settings for compliance settings.

| Client Setting | Design Options | Decision | Justification |
| --- | --- | --- | --- |
| Enable compliance evaluation on client | * **True** * False | **True** | Client devices must be evaluated for compliance with mandated configuration baselines. |
| Schedule compliance evaluation | * **Default Schedule** * Custom Schedule | **Default schedule** | Client devices must be periodically evaluated for compliance. |
| Enable User Data and Profile | * Enabled * **Disabled** | **Disabled** | There is no requirement to configure and deploy user data or profile configuration items. |

Table 9. Client configuration for Compliance settings.

* + 1. Windows Configuration Items

There are three types of Windows configuration items that can be applied to endpoints:

* **Application configuration item** - used to determine compliance for an application. This can include whether the application is installed and details about its configuration.
* **Operating system configuration item** - used to determine compliance for settings that relate to the operating system and its configuration.
* **Software updates configuration item** - this is automatically created when software updates are downloaded with System Center Configuration Manager.
* **General configuration items -** used to determine compliance for mobile devices.

The configuration item can be set to **Remediate non-compliant settings** which will enforce the configuration settings defined in the configurations items.

Child configuration items in System Center Configuration Manager are copies of configuration items that retain a relationship to the original configuration item; therefore, they inherit the original configuration from the parent configuration item.

Configuration items may be created using any of the following four methods:

* **New configuration items**

The Create Configuration Item Wizard is used to create a configuration item when all properties will be configured, or there is no existing configuration item from which a duplicate or a child configuration item can be created.

* **Child configuration items**

A configuration item is created such that it continues to inherit the properties of an existing configuration item, but refines them with more detailed configuration. Child configuration items cannot be created for mobile devices.

* **Duplicate existing configuration items**

Configuration item are created such that they are an exact copy of an existing configuration item that is used as a starting point. The new configuration item may then be modified it to create an independent configuration item from the original.

* **Import existing configuration items**

Configuration items are defined and validated outside the Configuration Manager hierarchy, such as in a test environment and will be used in the production system, or best practices can be imported from a Configuration Pack that vendors provided.

| Design Decision | Design Options | Decision | Justification |
| --- | --- | --- | --- |
| Configuration item creation method | * New * Duplicate * Child * **Import** | **Import** | Configuration items are defined and validated outside the production Configuration Manager hierarchy, in a test environment and will be imported into the production system. Best practices may be imported from a Configuration Pack that vendors provided. |

Table 10. Methods to create configuration items.

* + 1. User Data and Profiles Configuration Items

User data and profile configuration items may be used to manage folder redirection, offline files, and roaming profiles.

Note

User data and profiles configuration items can only be applied to user collections.

| Design Decision | Design Options | Decision | Justification |
| --- | --- | --- | --- |
| Folder redirection | * Yes * **No** | **No** | Folder redirection is not implemented in the environment |
| Offline Files | * Yes * **No** | **No** | Offline files are not implemented in the environment |
| Selective Synchronization | * Yes * **No** | **No** | Roaming profiles is not implemented in the environment |

Table 11. User data and profile configuration items.

Recommendation

Microsoft does not recommend the implementation of a new roaming user profile system. Instead, consider the use of User Experience Virtualization which is part of the Microsoft Desktop Optimization Pack.

| Configuration Item | Applies To | Justification |
| --- | --- | --- |
| Folder redirection | Finance |  |
| Offline Files | HR |  |
| Selective Synchronization | Finance |  |

Table 12. Target collections for user data and profiles configuration items.

* + 1. Configuration Baselines

Configuration baselines in System Center Configuration Manager contain predefined configuration items and optionally, other configuration baselines. Configuration baselines can contain specific revisions of configuration items or can be configured to always use the latest version of a configuration item.

Configuration baselines in System Center Configuration Manager must be deployed to one or more collections of end-users or devices before devices in those collections can assess their compliance with the configuration baseline.

| Baseline | Configuration Items | Applied To |
| --- | --- | --- |
| BL#1 | * CI #1 * CI #2 | Finance mobile users |

Table 13. Configuration items included in baselines and deployment targets.

Deployment of configuration baseline can be configured to remediate non-compliant rules when supported enforcing settings, defined in the configuration items included in the configuration baseline, on devices that are members of the collection. Each baseline in Table 13 will be deployed using the settings defined in Table 14.

| Baseline | Remediate | Remediate in Maintenance Window | Alert | Eval Schedule |
| --- | --- | --- | --- | --- |
| <Name> | <Yes | No> | <Yes | No> | <Yes | No> |  |

Table 14. Configuration baselines deployment settings.

* + 1. Delegation of Administration

Role-based administration combines security roles, security scopes, and assigned collections, to define the administrative scope for each administrative user. An administrative scope includes the objects a user can view in the Configuration Manager console, and the tasks related to those objects that the user has permission to perform. Role-based administration configurations are applied at each site in a hierarchy. System Center Configuration Manager provides several built-in security roles. Custom security roles can be created or a copy of an existing security role can be made, and modified.

The Compliance Settings Manager role is granted the following permissions:

* To view and manage alerts and reports for compliance settings: **Create**, **Delete**, **Modify**, **Modify Report**, **Read**, and **Run Report** for the **Alerts** object.
* To manage configuration baseline deployments: **Deploy Configuration Items**, **Modify Client Status Alert**, **Modify**, **Read**, and **Read Resource** for the **Collection** object.
* To create and manage configuration baselines and configuration items: **Create**, **Delete**, **Modify**, **Modify Folder**, **Modify Report**, **Move Object**, **Read**, **Run Report**, and **Set Security Scope** permission for the **Configuration Item** object.
* To run queries related to compliance settings: **Read** permission for the **Query** object.
* To view compliance settings information in the Configuration Manager console: **Read** permission for the **Site** object.
* To select software updates to be used in configuration baselines: **Read** permission for the **Software Updates** object.
* To view status messages for compliance settings: **Read** permission for the **Status Messages** object.
* For System Center 2012 Configuration Manager SP1 and later, to manage user data and profiles configuration items: **Author Policy**, **Modify Report**, **Read** and **Run Report** for the **Settings for user data and profile management** object.

| Configuration Manager Role | Active Directory Group Member |
| --- | --- |
| Compliance Settings Manager | <AD Group #1>  <AD Group #2>  <AD Group #3> |

Table 15. Security roles and scopes for compliance settings.

* + 1. Edition Upgrade

The System Center Configuration Manager Edition Upgrade Policy lets you automatically upgrade devices that run one of the following Windows 10 versions to a newer edition:

* Windows 10 Desktop
* Windows 10 Mobile
* Windows 10 Holographic

The following upgrade paths are supported:

* From Windows 10 Pro to Windows 10 Enterprise
* From Windows 10 Home to Windows 10 Education
* From Windows 10 Mobile to Windows 10 Mobile Enterprise
* From Windows 10 Holographic Pro to Windows 10 Holographic Enterprise

The devices must be enrolled in Microsoft Intune or run the Configuration Manager client software. This policy is currently not compatible with PCs that are managed by on-premises MDM.

| Design consideration | Decision |
| --- | --- |
| Product key which is valid to install the new version of Windows | <Product Key available / not available> |
| A license file from Microsoft which contains the licensing information | <License file available / not available> |
| Creator of Edition Upgrade Policy must be a full admin | <Associate function with Full Administrator Role / AD Group> |

Table 16. Edition Upgrade.

* + 1. Policy sync for Intune enrolled devices

You can now request a policy sync for an Intune-enrolled device from the Configuration Manager console instead of needing to request a sync from the Company Portal app on the device itself. Sync request state information is available as a new column in device views, called Remote Sync State, as well as in the discovery data section of the Properties dialog for each device.

| Design consideration | Decision |
| --- | --- |
| Enable RBAC for **Send Sync Request** in the **Remote Device Actions** menu for helpdesk. | <RBAC Value enabled for Helpdesk Role/Group> |

Table 17. Security roles and scopes for compliance settings.

* + 1. Windows Information Protection

After you’ve installed and set up System Center Configuration Manager for your organization, you must create a configuration item for WIP, which in turn becomes your WIP policy.

| Design consideration | Decision |
| --- | --- |
| Policy Name | <Value> |
| Setting for devices managed by MDM or native SCCM | <Both, Intune, SCCM> |
| App Rules | <Value> |
| WIP-protection level for your enterprise data | <Value> |
| Define your enterprise-managed identity domains | <Value> |
| Enterprise Cloud Resources | <Value> |
| Enterprise Network Domain Names | <Value> |
| Enterprise Proxy Servers | <Value> |
| Enterprise Internal Proxy Servers | <Value> |
| Enterprise IPv4 Range | <Value> |
| Enterprise IPv6 Range | <Value> |
| Neutral Resources | <Value> |
| Enterprise Proxy Servers list is authoritative (do not auto-detect) | <Value> |
| Enterprise IP Ranges list is authoritative (do not auto-detect) | <Value> |
| Show the Windows Information Protection icon overlay on your allowed apps that are WIP-unaware on corporate files in the File Explorer | <Value> |
| Create Data Recovery and Encryption File | <YES/NO> |
| **Show the Personal option in the File ownership menus of File Explorer and the Save As dialog box** | <Value> |
| **Prevent corporate data from being accessed by apps when the device is locked. Applies only to Windows 10 Mobile** | <Value> |
| **Allow Windows Search to search encrypted corporate data and Store apps** | <Value> |
| **Revoke local encryption keys during the unenrollment process** | <Value> |

Table 18. Windows Information Protection settings.

* 1. Endpoint Protection

Endpoint Protection provides an antimalware and security solution for the Microsoft platform. Together with Configuration Manager, Endpoint Protection enables the following:

* Centrally deploy and configure the Endpoint Protection client.
* Configure default and custom antimalware policies that apply to groups of computers.
* Create and deploy Windows Firewall settings to groups of computers.
* Use Configuration Manager software updates to automatically download the latest antimalware definition files to keep client computers up-to-date.
* Control who manages the antimalware policies and Windows Firewall settings by using the Endpoint Protection Manager security role.
* Use email notifications to alert you when computers report that malware is installed.
* View summary and detailed information from the Configuration Manager console and reports.
  + 1. Core Infrastructure Pre-Requisites

This section identifies services required for the capability to operate. This includes the following services:

| Component | Pre-Requisite Met | Description |
| --- | --- | --- |
| WSUS | <YES | NO> | Windows Server Update Services must be configured to enable the functionality provided by the Configuration Manager Software Update Point for security and definition updates. |
| Microsoft Update | <YES | NO> | Microsoft Update must be accessible if clients are configured to:   * Update from Microsoft Update * Update from Microsoft Malware Protection Center. |
| SMTP service | <YES | NO> | Mail service for sending email alerts from Configuration Manager. |

Table 19: Infrastructure dependencies

* + 1. Configuration Manager Pre-Requisites

Endpoint Protection requires specific configuration of a Configuration Manager hierarchy. The configuration changes to enable Endpoint Protection include the following:

| Component | Pre-Requisite Met | Description |
| --- | --- | --- |
| Endpoint Protection point | <YES | NO>  <server name that hosts the role> | The site system role must be installed on one site system server only, and it must be installed at the top of the hierarchy on a central administration site or a stand-alone primary site. |
| Software update point | <YES | NO> | This site system role is used to deliver definition and engine updates |
| Client settings | <YES | NO> | Enable the installation and configuration of Endpoint Protection. |
| Reporting services point | <YES | NO> | This site system role is used to run Endpoint Protection reports. |
| Security permissions | <YES | NO> | Ensures that only authorized personnel can manage the system. |

Table 20: Configuration Manager dependencies for implementing Endpoint Protection

* + 1. Protection Alerts

Endpoint Protection alerts in Configuration Manager are used to inform service administrators when specific events have occurred. Alerts are displayed in the Alerts node of the Monitoring workspace, or optionally can be emailed to specified users. Alerts will be configured as documented in Table 21.

| Design Decision | Design Options | Decision | Justification |
| --- | --- | --- | --- |
| Email notification | * **Enable** * **Disable** | **Enable** | Administrative users of the capability will be notified when selected events occur. |
| SMTP Server | * **None** | **<IP/FQDN>** | All outbound email alerts will use the corporate notification SMTP server. |
| SMTP Port | * **25** | **25** | The port on the corporate notification SMTP server will be used. |
| SMTP Connection Account | * None * Computer account * **Specify Account** | **<Account>** | All outbound notifications will use a specific service account. |
| Sender Address | * None | **<Email Address>** | All outbound notifications will use a specific service account. |
| Alert Recipient | * **Endpoint Administrators** | **<Email Addresses>** | The alerts must be sent to, at least, all Endpoint administrators. |
| Malware detection alert | * **Enable** * Disable | **Enable** | This alert is generated if malware is detected on any computer in a monitored collection |
| * **High** * Medium * Low | **High** | * High – All detections - The alert is generated when there are one or more computers in the specified collection on which any malware is detected, regardless of the action taken by the Endpoint Protection client. * Medium – Detected, pending action - The alert is generated when malware is detected on one or more computers in the specified collection and requires manual removal. * Low – Detected, still active - The alert is generated when there are one or more computers in the specified collection on which malware is detected and is still active. |
| * **All Workstations** | **All Workstations** | Alerts must be generated for all workstations. The All Workstations collection will be defined as part of the Core Architecture. |
| Malware Outbreak | * **Enable** * Disable | **Enable** | This alert is generated if specified malware is detected on a specified percentage of computers in the monitored collection. |
| * 1 – 99 % | **75** | The alert is generated when the percentage of computers with malware detected in the collection exceeds the percentage you specify. |
| * **All Workstations** | **All Workstations** | Outbreak alerts must be generated for all workstations. The All Workstations collection will be defined as part of the Core Architecture. |
| Repeated malware detection | * **Enable** * Disable | **Enable** | This alert is generated if specific malware is detected more than a specified number of times over a specified number of hours on computers in the monitored collection. |
| * 2 - 32 incidents | **4** | The alert is generated when the same malware is detected on computers in the collection more than the specified number of times. |
|  | * 1 – 168 hours | **24** | Specify the detection interval (in hours) in which the number of malware detections must occur. Specify a number from 1 through 168. |
| * **All Workstations** | **All Workstations** | Repeated detection alerts must be generated for all workstations. The All Workstations collection will be defined as part of the Core Architecture. |
| Multiple Malware Detection | * Enable * **Disable** | **Disable** | This alert is generated if more than a specified number of malware types are detected over a specified number of hours on computers in the monitored collection. |
| * 2 - 32 incidents | **4** | The alert is generated when the specified number of different malware types are detected on computers in the collection. |
| * 1 – 168 hours | **24** | Specify the detection interval, in hours, in which the number of malware detections must occur |
| * **All Workstations** | **All Workstations** | Repeated detection alerts must be generated for all workstations. The All Workstations collection will be defined as part of the Core Architecture. |

Table 21. Endpoint Protection alert configuration.

* + 1. Anti-Malware Policy

Antimalware policies are configured and deployed to collections of computers. The policies specify how Endpoint Protection protects the system from malware and other threats. The policies include configuration information about the follow:

* Scan schedule
* Types of files and folders to scan
* Actions that are taken when malware is detected
* File, folder, process, or file-type exclusions
* User interface.

Once installed, a default policy template is applied unless a custom policy is detected and applied. The custom policy applied to the devices in the specific collection is detailed configuration parameters of antimalware policies may be found in the **DM-AMPolicy** worksheet of the **Technical Design Planning** workbook.

| Design Decision | Design Options | Decision | Justification |
| --- | --- | --- | --- |
| Protect Workstations | * **Yes** * No | **Yes** | All supported client device must include antimalware protection. |
| Protect Servers | * **Yes** * No | **Yes** | The preferred server antimalware solution will protect all servers. Implementation is out of scope for this engagement. |

Table 22. Devices protected by Endpoint Protection antimalware.

* + 1. Client Settings

The Configuration Manager client requires configuration to enable the functionality of Endpoint Protection. The default client settings in Configuration Manager applies to all computers registered in the hierarchy.

Implementing collection-specific settings will allow the following:

* Customize antimalware and security settings for different parts of the organization.
* Plan, test and refine settings on small, targeted groups of systems.
* Phase deployment over a specific duration or business scope.

| Design Decision | Design Options | Decision | Justification |
| --- | --- | --- | --- |
| Default client settings will be used | * Yes * **No** | **No** | Settings will be configured based on risks associated with the user/system profile. |

Table 23. Client settings design decision.

* + 1. Windows Firewall Policy

Endpoint Protection Windows Firewall Policies offer basic Windows Firewall configuration. These policies do not have the same capabilities of controlling Windows Firewall rules and exceptions as offered by Active Directory Group Policy. In order to implement Endpoint Protection Windows Firewall Policies, the Endpoint Protection client must be installed on the managed device. This in turn may require Windows Firewall exception configured to allow the client push.

Endpoint Protection Windows Firewall policies can be used to perform the following tasks:

* Control whether Windows Firewall is turned on or off.
* Control whether incoming connections can client computers.
* Control whether users are notified when Windows Firewall blocks a new program.

| Design Decision | Design Options | Decision | Justification |
| --- | --- | --- | --- |
| Domain Profile | * **Yes** * No * Not Configured | **Yes** | The Windows firewall must protect the system when connected to the internal domain network. |
| Private Profile | * **Yes** * No * Not Configured | **Yes** | The Windows Firewall must protect the system when connected to private networks. |
| Public Profile | * **Yes** * No * Not Configured | **Yes** | The Windows Firewall must protect the system when connected to public networks. |

Table 24. Windows Firewall profile use.

| Design Decision | Design Options | Decision | Justification |
| --- | --- | --- | --- |
| Block all incoming connections, including those in the list of allowed programs | * Domain Profile * Private Profile * Public profile |  | The Windows Firewall must block inbound network connections, including the list of allowed programs when the configured firewall profile is active. |
| Block all outbound connections, including those in the list of allowed programs | * Domain Profile * Private Profile * Public profile |  | The Windows Firewall must block outbound network connections, including the list of allowed programs when the device is on untrusted networks when the configured firewall profile is active. |
| Notify the user when Windows Firewall blocks a new program | * Domain Profile * Private Profile * Public profile |  | The Windows Firewall must notify the user when a program is blocked for a specific active profile. |

Table 25. Windows Firewall profile configuration.

* + 1. Delegation of Administration

Role-based administration combines security roles, security scopes, and assigned collections, to define the administrative scope for each administrative user. An administrative scope includes the objects a user can view in the Configuration Manager console, and the tasks related to those objects that the user has permission to perform. Role-based administration configurations are applied at each site in a hierarchy. System Center Configuration Manager provides several built-in security roles. Custom security roles can be created or a copy of an existing security role can be made, and modified.

The Endpoint Protection Manager role is granted the following permissions:

* To create and manage subscriptions to Endpoint Protection alerts: **Create**, **Delete**, **Modify**, **Read**, **Set Security Scope** for the **Alert Subscription** object.
* To create and modify alerts for Endpoint Protection: **Create**, **Delete**, **Modify**, **Modify Report**, **Read**, **Run Report** for the **Alerts** object.
* To create and modify antimalware policies: **Create**, **Delete**, **Modify**, **Modify Default**, **Modify Report**, **Read**, **Read Default**, **Run Report** for the **Antimalware Policy** object.
* To deploy antimalware and Windows Firewall policies to computers: **Audit Security**, **Delete**, **Deploy Antimalware Policies**, **Deploy Firewall Policies**, **Enforce Security**, **Read**, **Read Resource** for the **Collection** object.
* To view and manage Endpoint Protection in the Configuration Manager console: **Read** permissions for the **Site** object.
* To create and modify Windows Firewall policies: **Create Policy**, **Delete Policy**, **Modify Policy**, **Read Policy**, **Read Settings** for the **Windows Firewall Policy** object.

| Configuration Manager Role | Active Directory Group Member |
| --- | --- |
| Endpoint Protection Manager | <AD Group #1>  <AD Group #2>  <AD Group #3> |

Table 26. Security roles and scopes for Endpoint Protection.

* + 1. Windows Defender Advanced Threat Protection

Windows Defender ATP is a service in the [Windows Security Center](https://securitycenter.windows.com/). By adding and deploying a client onboarding configuration file, Configuration Manager can monitor deployment status and Windows Defender ATP agent health. Windows Defender ATP is only supported on PCs running the Configuration Manager client. On-premises mobile device management and Intune hybrid MDM-managed computers are not supported.

| Design consideration | Decision |
| --- | --- |
| Configuration Manager 1606 (min) | <YES/NO> |
| Subscription to the Windows Defender Advanced Threat Protection online service | <YES/NO> |
| Clients running Windows 10, version 1607 and later | <YES/NO> |

Table 27. Windows Defender Advanced Threat Protection.

* + 1. Health Attestation Service

Beginning with System Center Configuration Manager current branch version 1602, administrators can view the status of [Windows 10 Device Health Attestation](https://technet.microsoft.com/library/mt592023.aspx) in the Configuration Manager console. This functionality is available for PCs and on-premises resources managed by Configuration Manager and mobile devices managed with Microsoft Intune. Administrators can specify whether reporting is done via the cloud or on-premises infrastructure. This enables client PCs without internet access to enable and monitor devices using health attestation. Device health attestation lets the administrator ensure that client computers have the following trustworthy BIOS, TPM, and boot software configurations enabled:

* Early-launch antimalware - Early launch anti-malware (ELAM) protects your computer when it starts up and before third-party drivers initialize.
* BitLocker - Windows BitLocker Drive Encryption is software that lets you encrypt all data stored on the Windows operating system volume. [How to turn on Bitlocker](https://gallery.technet.microsoft.com/How-to-turn-on-BitLocker-34294d3d)
* Secure Boot - Secure Boot is a security standard developed by members of the PC industry to help make sure that your PC boots using only software that is trusted by the PC manufacturer.
* Code Integrity - Code Integrity is a feature that improves the security of the operating system by validating the integrity of a driver or system file each time it is loaded into memory. [Learn about Code Integrity](https://technet.microsoft.com/library/dd348642.aspx)

| Design consideration | Decision |
| --- | --- |
| Client devices running Windows 10 | <YES/NO> |
| Windows Server 2016 with [Device Health Attestation enabled](https://technet.microsoft.com/windows-server-docs/security/device-health-attestation) | <YES/NO> |
| TPM 2 enabled | <YES/NO> |
| Unblock communication between Configuration Manager client agent and has.spserv.microsoft.com (port 443) Health Attestation service | <YES/NO> |

Table 28. Health Attestation Service.

* + 1. Lookout Integration

You can control access from mobile devices to company resources, based on risk assessment conducted by Lookout, a device threat protection solution that is integrated with Microsoft Intune. The risk is based on telemetry that the Lookout service collects from devices for operating system (OS) vulnerabilities, installed malicious apps, and malicious network profiles.

Based on Lookout's reported risk assessment enabled through System center configuration manager (SCCM) compliance policies, you can configure conditional access policies and allow or block devices that have been determined to be noncompliant due to threats detected on those devices.

| Design consideration | Decision |
| --- | --- |
| Intune Subscription (Hybrid MDM in Configuration Manager) | <YES/NO> |
| Enterprise subscription of Lookout Mobile EndPoint Security | <YES/NO> |
| Supported platform: Android 4.1 and later & iOS8 and alter | <YES/NO> |

Table 29. Lookout integration

* 1. Power Management

Configuration Manager provides a set of tools that allows the management and monitoring of power consumption of client computers in the hierarchy.

* + 1. Core Infrastructure Pre-Requisites

This section identifies services required for the capability to operate. This includes the following services:

| Component | Pre-Requisite Met | Description |
| --- | --- | --- |
| Client computers support the required power states | <YES | NO> | Client computers must be able to support the sleep, hibernate, wake from sleep, and wake from hibernate actions |

Table 30: Infrastructure dependencies

* + 1. Configuration Manager Pre-Requisites

The Configuration Manager design must meet the following pre-requisites.

| Component | Pre-Requisite Met | Description |
| --- | --- | --- |
| Power management is enabled | <YES | NO> | Configures the default client settings for power management and will apply to all the computers in the hierarchy. |
| Reporting services point | <YES | NO> | Required for viewing power management reports. |

Table 31: Configuration Manager dependencies for implementing Power Management

* + 1. Client Settings

The Configuration Manager client must be configured to enable the power management function.

| Design Decision | Design Options | Decision | Justification |
| --- | --- | --- | --- |
| Allow users to exclude their device from power management | * **Yes** * No | **Yes** | User can exclude their computer from any configured power management settings |
| Enable wake-up proxy | * Yes * **No** | **No** | IT admins must be able to wake devices to perform required system maintenance tasks. |
| Wake-up proxy port number (UDP) | * **Default** * Custom | **Default** |  |
| Wake on LAN port number (UDP) | * **Default (9)** * Custom | **Default** |  |

Table 32: Client settings for power management.

* + 1. Collection Targeting

Power management policies will NOT be deployed to the collections listed below.

| Policy Name | Applied To | Justification |
| --- | --- | --- |
| PMP#1 | Finance mobile users |  |

Table 33. Target collections for power management policies.

* 1. Device Enrollment

Devices must be enrolled into the management system before any of the configuration capabilities are effective. Enrollment will register the device in the management system with a unique identity, using the reference as a target for configuration. Enrollment may be performed through several methods, however, only one method should be used per device i.e. a device must be de-registered before enrolling using a different method. However, the method of enrollment is determined by the manageability required. Hence, while all enrollment methods are discussed below, only those supporting the required manageability are implemented.

* **Microsoft Intune Subscription**

The Service Connection Point configured with a Microsoft Intune subscription creates a hybrid device management infrastructure by enabling management, configuration, and reporting tasks from Configuration Manager to be executed by the configured Microsoft Intune service. Devices enroll through the Intune services.

* **Native Enrollment**

The System Center Configuration Manager mobile device client is installed on the endpoint to provide management capabilities. Domain-joined Windows clients and servers are also managed in this manner. Devices are enrolled directly into the Configuration manager system. *Native enrollment is not included in this design, except for domain-joined Windows systems.*

* **Exchange Connector**

The Exchange Server Connector enables Configuration Manager to connect to multiple Exchange servers, centralizing management of devices that can connect to the Exchange ActiveSync (EAS). Devices enroll into EAS and are configured by Configuration Manager.

* **Legacy Client**

The mobile device legacy client provides software deployment, software inventory and monitoring for Windows CE and Windows Mobile 6.0 devices. *Legacy clients are beyond the scope of this design.*

Detailed information related to specific devices used within the organization and enrollment information can be found in the **DM-Enrollment Worksheet** of the **Technical Design Planning Workbook**. Based on the device management features selected as part of the design workshop, the following enrollment configurations are required:

| Design Decision | Design Options | Decision | Justification |
| --- | --- | --- | --- |
| Exchange Active Sync | * **Yes** * No | **Yes** | Add justification from Workshop |
| Microsoft Intune | * **Yes** * No | **Yes** | Add justification from Workshop |

Table 34. Mobile device enrollment method.

* + 1. Microsoft Intune Subscription

The Service Connection Point is used to register a Microsoft Intune subscription to send settings and software deployment information to mobile devices and to retrieve status and inventory information from mobile devices via Microsoft Intune. Configuration Manager will be integrated with the Microsoft Intune subscription. This solution will provide the flexibility to manage all devices from a single administrative environment and improve the scalability.

The Service Connection Point role is used to establish the link between a specific part of the Configuration Manager hierarchy and a Microsoft Intune subscription.

* + - 1. Core Infrastructure Pre-Requisites

The following core infrastructure and cloud services must be configured prior to implementing

| Component | Pre-Requisite Met | Additional Information |
| --- | --- | --- |
| Microsoft Intune subscription | <YES | NO>  <Tenant Name> | Initial setup of the Intune tenant is completed. |
| Management Authority is **NOT** configured | <YES | NO> | The Hybrid design requires Configuration Manager to be the mobile device management authority. If Intune is configured, please have an Intune Global Administrator contact Microsoft Support using the information at <https://technet.microsoft.com/en-US/jj839713.aspx>. |
| Healthy Directory Synchronization with Azure Active Directory or Intune tenant is implemented | <YES | NO> | Users from the on-premises Active Directory have been synchronized with the Intune tenant or associated Azure AD tenant. |
| Publicly registered domain name | <YES | NO> | All user accounts must have a publicly registered UPN that can be verified by Intune. |
| Users have a public domain user principal name | <YES | NO> | Before synchronizing the Active Directory user account, verify that user accounts have a public domain UPN.  To verify that the UPN of the users who are discovered is consistent with the Intune Account Portal, create a Configuration Manager custom report by using the following SQL query:  SELECT UserPrincipalName,  COUNT(\*) AS NumOfOccurances FROM (SELECT RIGHT(User\_Principal\_Name0,  LEN(User\_Principal\_Name0)-PATINDEX('%@%',  User\_Principal\_Name0)) AS UserPrincipalName FROM CM\_EC1.dbo.v\_R\_User)  AS sub GROUP BY UserPrincipalName |
| Deploy and configure Active Directory Federation Services [OPTIONAL, but strongly recommended] | <YES | NO> | Required when all authentication must occur on premises. |
| DNS alias created for manage.microsoft.com | <YES | NO> | The device uses the domain of the user UPN to locate the enrollment service located at EnterpriseEnrollment.<registered domain name>. |

Table 35. Core infrastructure requirements for Microsoft Intune connector.

* + - 1. Configuration Manager Pre-Requisites

Configuration of the Service Connection Point requires the following pre-requisites from the Configuration Manager implementation:

| Component | Pre-Requisite Met | Additional Information |
| --- | --- | --- |
| Available Central Administration Site or Stand-Alone Primary Site | <YES | NO> | The Service Connection Point site system role may only be installed on these elements of the hierarchy. |
| Internet Connectivity | <YES | NO> | The Service Connection Point site system role must have an initial and persistent connection to the Microsoft Intune cloud service. |

Table 36. Configuration Manager requirements for using the Microsoft Intune connector.

* + - 1. Service Connection Point Configuration

The Service Connection Point site system role is supported for installation on either a Central Administration server or a standalone primary site server. The site system role may be moved from one supported server to another in the hierarchy.

Note

The Service Connection Point may only be configured on a single server at any point. The secondary server is used if the primary server hosting the role is offline.

| Location | Server Name | Intune Subscription Name |
| --- | --- | --- |
| <primary server location> | <primary server name> | <Subscription #1> |
| <secondary server location> | <secondary server name> | <Subscription #1> |

Table 37. Service Connection Point role placement.

* + - 1. Device Enrollment Manager

Configuration Manager and Microsoft Intune can be used to manage large numbers of devices with a single user account. Microsoft Intune provides a special type of user account that can enroll more than 5 devices – the Device Enrollment Manager. This account type enables the following capabilities on each device enrolled with these credentials:

* Enrolls device for management
* Install company apps from the Company Portal
* Install and uninstall software
* Configure access to company resources.

The following table lists the accounts that will be configured as Device Enrollment Manager.

| Username | Rationale |
| --- | --- |
| <primary server location> | <primary server name> |
| <secondary server location> | <secondary server name> |

Table 38. Device enrollment manager accounts.

* + 1. Exchange Server Connector

The Exchange Server connector is used when mobile devices need to be managed via a connection to an Exchange Server infrastructure using the Exchange ActiveSync (EAS) protocol, and where they cannot be enrolled by using native System Center Configuration Manager enrollment. Managing mobile devices by using the Exchange Server connector, does not install the System Center Configuration Manager client on the mobile devices, which means that some management functions are limited.

* + - 1. Core Infrastructure Pre-Requisites

This section identifies services required for the Exchange Server connector. This includes the following services:

| Component | Pre-Requisite Met | Description |
| --- | --- | --- |
| Supported Exchange infrastructure | <YES | NO> | Ensure that the implemented version of Configuration Manager supports the version of Exchange. The latest support information can be found at <https://technet.microsoft.com/en-US/library/mt589738.aspx#bkmk_ExSrvConOS> |

Table 39: Infrastructure dependencies

* + - 1. Configuration Manager Pre-Requisites

Endpoint Protection requires specific configuration of a Configuration Manager hierarchy. The configuration changes to enable Endpoint Protection include the following:

| Component | Pre-Requisite Met | Description |
| --- | --- | --- |
| Full Administrator rights | <YES | NO> | The role includes all rights required to configure the Exchange Server connector. |
| Operations Administrator rights | <YES | NO> | The role includes all rights required to manage mobile devices using the connector. |

Table 40: Configuration Manager dependencies for implementing the Exchange Server Connector

* + - 1. Connector Configuration

A System Center Configuration Manager site can have one or more Exchange Server connectors to connect to multiple Exchange environments. The Exchange Server connector can connect to an on-premise Exchange Server or a Hosted Exchange environment such as Office 365. When multiple Exchange CAS servers are available in the same site the Exchange Server connector can be configured to connect to specific Exchange CAS servers.

The discovery information for ActiveSync connected mobile devices will also be requested by the Exchange Server Connector to the Exchange CAS server.

Consultant: For a Configuration Manager design that has multiple Exchange Server connectors please use the DM-EAS Worksheet in the Technical Design Planning workbook. **Do not paste multiple tables into this document**, instead, reference the worksheet in the workbook and update the next line accordingly and remove the referenced Appendix.

The design will use the Exchange Server Connector to connect to the Exchange environments listed in Table 41. Detailed configuration of each connector may be found in the **DM-EAS-Connectors** worksheet of the **Technical Design Planning** workbook.

| Exchange Environment | Server Address |
| --- | --- |
| <Exchange 1> | <https://url.to.environment> |
| <Exchange 1> | <https://url.to.environment> |

Table 41. Exchange environments connected to Configuration Manager.

Each Exchange connector that is used may be configured with specific settings. The settings are grouped into the following categories:

* General

Configures the general behavior of devices enrolled with the connector.

* Password

Enables the configuration of device protectors such as enforcing a password, failed logons, and simple passwords.

* Email Management

Allows the configuration of mail synchronization parameters such as attachments, Direct Push when roaming and more.

* Security

Enables the allow or block of device hardware items such as camera, Wi-Fi, or Bluetooth.

* Applications

Provides the ability to allow/deny the use or installation of applications.

* External Mobile Management

Allows the Exchange Server to continue to manage the device after enrollment into Configuration Manager.

If at least one of the settings in a group is configured, Configuration Manager will manage all settings in the group. If no settings in a group are configured, the Exchange server will continue to manage all settings for the group. Exchange Active Sync and mailbox policies will continue to be applied.

The detailed configuration for the connector for each Exchange environment is found on the **DM-EAS-Settings** worksheet in the **Technical Designing Planning** workbook.

* + - 1. Connector Access Rules

Each Exchange connector may be used to control access to the Exchange server. Devices may be actively allowed, blocked or quarantined. Table 42 indicates which exchange connectors will have access rules enabled.

The detailed configuration for the Access Rules is found on the **DM-EAS-Settings** worksheet in the **Technical Designing Planning** workbook.

| Exchange Connector | Access Rules Enabled |
| --- | --- |
| <Exchange Connector #1> | <YES | NO> |
| <Exchange Connector #2> | <YES | NO> |

Table 42. Access rule usage for Exchange connectors.

* + - 1. Remote Wipe

Remote Wipe is an action that can be remotely performed on a specific mobile device, deleting all user data. The device will be restored to a factory state, either based on the manufacturer’s or the cellular carrier’s specification. If required, Exchange and Configuration Manager can be configured to wipe all device data, including attached storage cards. The remote wipe capability may be provided as a self-service action to users through the Application Catalog.

| Design Consideration | Design |
| --- | --- |
| Remote wipe will be configured | <YES | NO> |
| Users can initiate a remote wipe | <YES | NO> |

Table 43. Remote wipe configuration

* + 1. Device Category

You can create device categories, which can be used to automatically place devices in device collections when you are using Configuration Manager with Microsoft Intune. Users then must choose a device category when they enroll a device in Intune. You can change a device category from the Configuration Manager console.

| Design Consideration | Design |
| --- | --- |
| Create device category | <Category> |
| Choose Collection for device category | <Collection> |

Table 442. Device Category

* + 1. Predeclare Devices

You can identify corporate-owned devices by importing their international station mobile equipment identity (IMEI) numbers or iOS serial numbers. You can upload a comma-separated values (.csv) file containing device IMEI numbers or you can manually enter device information. Imported information will set **Ownership** of the devices that enroll as **Corporate** in lists of devices. An Intune license is still required for each user that accesses the service.

| Design Consideration | Design |
| --- | --- |
| Check CYOD vs. BYOD scenario at customer | <CYOD available / CYOD not available> |
| List of all Corporate Owned Devices from CUSTOMER asset management database | <Assets available / Assets not available> |

Table 453. Predeclare Devices

1. Technical Implementation

This section outlines the activities, tasks and steps required for implementing each aspect of the design.

* 1. Device Enrollment

This section includes resources to assist in configuring either the Microsoft Intune subscription or the Exchange Server connector for device management.

* + 1. Microsoft Intune

Complete all tasks outlined at <https://technet.microsoft.com/en-us/library/mt627883.aspx> or each of the platforms that the system will support.

| Task | Rationale | Implementation Guidance |
| --- | --- | --- |
| Configure Microsoft Intune Subscription | The Intune subscription enables the specification of configuration settings for the Intune service | * Complete **Configuring the Microsoft Intune subscription** at <https://technet.microsoft.com/en-us/library/mt627883.aspx> |
| Service Connection Point | The SCP establishes the connection to Microsoft Intune. | * Complete **The Service Connection Point Site System Role** at <https://technet.microsoft.com/en-us/library/mt627883.aspx> |
| Enable Mobile Device Enrollment | Establish a trust relationship between the managed mobile device and the management solution | * Complete **Enable Mobile Device Enrollment** at <https://technet.microsoft.com/en-us/library/mt627883.aspx> |
| Device Enrollment Manager [OPTIONAL] | Required to bulk enroll and manage large number of devices with a single user account. | * Complete **Enroll Corporate-Owned Devices with the Device Enrollment Manager** at <https://technet.microsoft.com/en-us/library/mt627883.aspx> |

* + 1. Exchange Server Connector

Complete all tasks outlined at <https://technet.microsoft.com/en-us/library/mt627895.aspx>.

* + 1. Device category

This section outlines how to create and associate a device category.

|  |  |  |
| --- | --- | --- |
| Task | Rationale | Implementation Guidance |
| Create and configure device category | Define device category | <https://docs.microsoft.com/en-us/sccm/core/clients/manage/collections/automatically-categorize-devices-into-collections#create-device-categories> |
| Associate device category | When you associate a collection with a device category, all devices in that category will be added to the collection. | <https://docs.microsoft.com/en-us/sccm/core/clients/manage/collections/automatically-categorize-devices-into-collections#associate-a-collection-with-a-device-category> |

* + 1. Predeclare devices

This section outlines how to import predeclared devices.

|  |  |  |
| --- | --- | --- |
| Task | Rationale | Implementation Guidance |
| Predeclare corporate owned devices | Imported information will set **Ownership** of the devices that enroll as **Corporate** in lists of devices | <https://docs.microsoft.com/en-us/sccm/mdm/deploy-use/predeclare-devices-with-hardware-id#how-to-predeclare-corporate-owned-devices> |
| Check format for uploading \*.csv file | Each row must contain either an IMEI number or iOS serial number. | <https://docs.microsoft.com/en-us/sccm/mdm/deploy-use/predeclare-devices-with-hardware-id#format-for-uploading-csv-files> |

* 1. Compliance Settings

This section outlines the specific steps to implement:

* Configuration Items
* User Data and Profiles
* Compliance Policies
  + 1. Configure Compliance Settings for Windows

This section outlines the steps to set the default client configuration for compliance settings for Windows computers.

| Task | Rationale | Implementation Guidance |
| --- | --- | --- |
| Enable and configure compliance settings | Default client settings must be configured for all systems in the hierarchy. | * Complete **Configure Compliance Settings for Windows computer** at <https://technet.microsoft.com/en-us/library/mt595720.aspx#BKMK_Configure> |

* + 1. New Configuration Item for Systems with the Configuration Manager Client

This section pertains to systems that have the Configuration Manager client installed. Configuration items may be created based upon the target platform. Depending on the platforms that will be managed, use the appropriate tasks below to create the configuration items.

* + - 1. Windows 10

This section outlines the steps to create configuration items for compliance settings applicable to Windows 10 devices with the Configuration Manager client installed.

| Task | Rationale | Implementation Guidance |
| --- | --- | --- |
| Complete the wizard | Configuration items will be created for Windows 10 systems managed with the Configuration Manager client installed | * Complete the steps at <https://technet.microsoft.com/en-us/library/mt629315.aspx> |

* + - 1. Windows Desktop and Server

This section outlines the steps to create configuration items for Windows desktop and server devices with the Configuration Manager client installed.

| Task | Rationale | Implementation Guidance |
| --- | --- | --- |
| Create a Configuration Item | Configuration items will be created for supported Windows desktop and server systems managed with the Configuration Manager client installed | * Complete the steps at <https://technet.microsoft.com/en-us/library/mt629322.aspx> |

* + - 1. Mac OS X

This section outlines the steps to create configuration items for OS X devices with the Configuration Manager client installed.

| Task | Rationale | Implementation Guidance |
| --- | --- | --- |
| Create a Configuration Item | Configuration items will be created for supported OS X systems managed with the Configuration Manager client installed | * Complete the steps at <https://technet.microsoft.com/en-us/library/mt629308.aspx> |

* + 1. New Configuration Item for Systems without the Configuration Manager Client

This section pertains to systems that do not have the Configuration Manager client installed. Configuration items may be created based upon the target platform. Depending on the platforms that will be managed, use the appropriate tasks below to create the configuration items.

* + - 1. Windows 8.1 and 10

This section outlines the steps to create configuration items for compliance settings applicable to Windows 8.1 and 10 devices.

|  |  |  |
| --- | --- | --- |
| Task | Rationale | Implementation Guidance |
| Complete the wizard | Configuration items will be created for Windows 8.1 and 10 devices managed without the Configuration Manager client installed | * Complete the steps at <https://technet.microsoft.com/en-us/library/mt629341.aspx> |

* + - 1. Windows Phone

This section outlines the steps to create configuration items for Windows Phone devices.

|  |  |  |
| --- | --- | --- |
| Task | Rationale | Implementation Guidance |
| Create a Configuration Item | Configuration items will be created for supported Windows Phone devices managed without the Configuration Manager client installed | * Complete the steps at <https://technet.microsoft.com/en-us/library/mt629325.aspx> |

* + - 1. OS X and iOS

This section outlines the steps to create configuration items for OS X and iOS devices.

|  |  |  |
| --- | --- | --- |
| Task | Rationale | Implementation Guidance |
| Create a Configuration Item | Configuration items will be created for supported OS X and iOS devices managed without the Configuration Manager client installed | * Complete the steps at <https://technet.microsoft.com/en-us/library/mt629339.aspx> |

* + - 1. Android and Samsung KNOX

This section outlines the steps to create configuration items for Android and Samsung KNOW devices.

|  |  |  |
| --- | --- | --- |
| Task | Rationale | Implementation Guidance |
| Create a Configuration Item | Configuration items will be created for supported Android and Samsung KNOX devices managed without the Configuration Manager client installed | * Complete the steps at <https://technet.microsoft.com/en-us/library/mt629346.aspx> |

* + 1. User Data and Profiles

This section outlines the steps to enable, create and deploy user data and profiles configuration items.

|  |  |  |
| --- | --- | --- |
| Task | Rationale | Implementation Guidance |
| Enable user data and profiles | Configure the default client setting for user data and profiles compliance settings which will apply to all computers in your hierarchy | * Complete the Enable User Data and Profiles for Compliance Settings at https://technet.microsoft.com/en-us/library/mt595719.aspx |
| Create user data and profiles configuration item | Create the user data and profiles configuration item | * Complete the How to Create a User Data and Profiles Configuration Item at <https://technet.microsoft.com/en-us/library/mt629329.aspx> * Repeat the step for each configuration item documented in **Table 12 in Section 2.2.2**. |
| Deploy user data and profiles configuration items | Unlike other configuration items, user data and profiles configuration items are deployed directly. | * Complete the How to Deploy a User Data and Profiles Configuration Item at <https://technet.microsoft.com/en-us/library/mt629329.aspx> * Repeat the step for each configuration item documented in **Table 12 in Section 2.2.2**. |

* + 1. Compliance Policy

This section outlines how to create, deploy, and monitor a compliance policy that will be used with a conditional policy.

|  |  |  |
| --- | --- | --- |
| Task | Rationale | Implementation Guidance |
| Create a compliance policy | Define the rules and settings that a device must comply with to be considered compliant. | * Complete step 1 at <https://technet.microsoft.com/en-us/library/mt131417.aspx> * Configuration parameters may be found in the **DM-CondAccess** worksheet of the **TechnicalDesign\_Planning** Excel workbook. * Repeat the steps for each compliance policy documented in **Section 2.1.2**. |
| Deploy a compliance policy | Deploy the compliance policy to target users or devices | * Complete step 2 at <https://technet.microsoft.com/en-us/library/mt131417.aspx> * Repeat the steps for each compliance policy documented in **Section 2.1.2**. |
| Monitor a compliance policy | View the compliance results. | * Complete step 3 at <https://technet.microsoft.com/en-us/library/mt131417.aspx> * Repeat the steps for each compliance policy documented in **Section 2.1.2**. |

* + 1. Edition Upgrade

This section outlines how to create, deploy, and monitor an Edition Upgrade policy.

|  |  |  |
| --- | --- | --- |
| Task | Rationale | Implementation Guidance |
| Create and configure Edition Upgrade policy | Define the settings for Windows 10 edition | <https://docs.microsoft.com/en-us/sccm/compliance/deploy-use/upgrade-windows-version#configure-the-edition-upgrade-policy> |
| Deploy Edition Upgrade policy | Target policy to device collection or user collection | <https://docs.microsoft.com/en-us/sccm/compliance/deploy-use/upgrade-windows-version#deploy-the-edition-upgrade-policy> |

* + 1. Policy sync

Check Role Based Access Control for Helpdesk Role.

Additional documentation: <https://docs.microsoft.com/en-us/sccm/mdm/deploy-use/sync-intune-device>

* + 1. Windows Information Protection

This section outlines how to create, deploy, and monitor a Windows Information Protection policy.

|  |  |  |
| --- | --- | --- |
| Task | Rationale | Implementation Guidance |
| Add app rules to your policy |  | <https://technet.microsoft.com/en-us/itpro/windows/keep-secure/create-wip-policy-using-sccm#add-app-rules-to-your-policy> |
| Manage the WIP-protection level for your enterprise data |  | <https://technet.microsoft.com/en-us/itpro/windows/keep-secure/create-wip-policy-using-sccm#manage-the-wip-protection-level-for-your-enterprise-data> |
| Define your enterprise-managed identity domains |  | <https://technet.microsoft.com/en-us/itpro/windows/keep-secure/create-wip-policy-using-sccm#define-your-enterprise-managed-identity-domains> |
| Choose where apps can access enterprise data |  | <https://technet.microsoft.com/en-us/itpro/windows/keep-secure/create-wip-policy-using-sccm#choose-where-apps-can-access-enterprise-data> |
| Choose your optional WIP-related settings |  | <https://technet.microsoft.com/en-us/itpro/windows/keep-secure/create-wip-policy-using-sccm#choose-your-optional-wip-related-settings> |
| Review your configuration choices in the Summary screen |  | <https://technet.microsoft.com/en-us/itpro/windows/keep-secure/create-wip-policy-using-sccm#review-your-configuration-choices-in-the-summary-screen> |

* 1. Company Resource Access

This section outlines the implementation steps for each of the features that provide access to company resources as shown in Table 46.

|  |  |
| --- | --- |
| Section | Activity |
| 3.3.1 | Configure email profiles |

Table 46: List of tasks to implement access to company resources.

* + 1. Email Profiles

This section details how email profiles are created, deployed, and monitored.

|  |  |  |
| --- | --- | --- |
| Task | Rationale | Implementation Guidance |
| Create an email Profile | An email profile must be created with all the correct settings to enable corporate email. | * Complete steps 1-6 at <https://technet.microsoft.com/en-us/library/mt629448.aspx> * Configuration parameters may be found in the **DM-EmailProfile** worksheet of the **TechnicalDesign\_Planning** Excel workbook. * Repeat the step for each email profile documented in **Table 5 Section 2.1.1**. |
| Deploy email profiles to user or device collections | Deployment of an email profile will distribute and install the configuration to the targeted users or devices. | * Complete the instructions at <https://technet.microsoft.com/en-us/library/mt629449.aspx> * Repeat the step for each email profile documented in **Table 5 Section 2.1.1**. |
| Monitor deployed email profiles | Report on the compliance of deployed email profiles | * Complete the instructions at <https://technet.microsoft.com/en-us/library/mt629447.aspx> * Repeat the step for each email profile documented in **Table 5 Section 2.1.1**. |

* 1. Power Management

This section outlines the steps for configuring power management.

|  |  |  |
| --- | --- | --- |
| Task | Rationale | Implementation Guidance |
| Enable and configure client settings for power management | Configure the default client settings for power management and will apply to all the computers in the hierarchy. | * Complete the steps at <https://technet.microsoft.com/en-US/library/mt629384.aspx#BKMK_PowMgmtDeviceSettings> using the documented settings in **Table 32 in Section 2.4.3**. |
| Exclude computers from power management | Prevent collections of computers from receiving power management settings. | * Complete the *To exclude a collection of computers from power management* at <https://technet.microsoft.com/en-us/library/mt629343.aspx> configuring the collections documented in **Table 33 in Section 2.4.4**. |
| Report | Run reports that provide data on power consumption. | * Use the administrative console to run the report required. |

Custom power plans may be created and deployed by following the guidance at <https://technet.microsoft.com/en-us/library/mt629352.aspx>.

* 1. Endpoint Protection

This section outlines the steps for configuring the Endpoint Protection client.

|  |  |  |
| --- | --- | --- |
| Steps | Rationale | Implementation Guidance |
| Create an Endpoint Protection point site system role | The Endpoint Protection point site system role must be installed before you can use Endpoint Protection. | * Complete Step 1 at <https://technet.microsoft.com/en-us/library/mt613207.aspx#BKMK_Step1> on the server specified in Table 20 in Section 2.3.2. |
| Configure alerts for Endpoint Protection | Alerts inform the administrator when specific events have occurred, such as a malware infection. | * Complete Step 2 at <https://technet.microsoft.com/en-us/library/mt613207.aspx#BKMK_EPalerts> * Configure the alerts as documented in **Table 21 in Section 2.3.3**. |
| Configure definition update sources for Endpoint Protection clients | Endpoint Protection can be configured to use various sources to download definition updates. | * Complete all steps at <https://technet.microsoft.com/en-us/library/mt613207.aspx#BKMK_EPdefs> * Configure the appropriate update source as defined in the **DM-AMPolicy** worksheet in the **TechnicalDesign\_Planning** Excel workbook. |
| Configure the default antimalware policy and create any custom antimalware policies | The default antimalware policy is applied when the Endpoint Protection client is installed. | * Complete all steps at <https://technet.microsoft.com/en-us/library/mt613199.aspx> * Configure the parameters as defined in the **DM-AMPolicy** worksheet in the **TechnicalDesign\_Planning** Excel workbook and in **Table 22 in Section 2.3.4**. |
| Configure custom client settings for Endpoint Protection | Use custom client settings to configure Endpoint Protection settings for collections of computers in the hierarchy. | * Complete step 5 at <https://technet.microsoft.com/en-us/library/hh508770.aspx> |

* 1. Windows Defender Advanced Threat Protection

This section outlines how to configure Windows Defender Advanced Threat Protection.

|  |  |  |
| --- | --- | --- |
| Task | Rationale | Implementation Guidance |
| How to create an onboarding configuration file | Configuration File is needed | <https://docs.microsoft.com/en-us/sccm/protect/deploy-use/windows-defender-advanced-threat-protection#how-to-create-an-onboarding-configuration-file> |
| Onboard devices for Windows Defender ATP | Devices must be onboarded | <https://docs.microsoft.com/en-us/sccm/protect/deploy-use/windows-defender-advanced-threat-protection#onboard-devices-for-windows-defender-atp> |
| Monitor Windows Defender ATP | Monitor | <https://docs.microsoft.com/en-us/sccm/protect/deploy-use/windows-defender-advanced-threat-protection#monitor-windows-defender-atp> |
| How to create and deploy an offboarding configuration file | Create and deploy ATP Configuration File | <https://docs.microsoft.com/en-us/sccm/protect/deploy-use/windows-defender-advanced-threat-protection#how-to-create-and-deploy-an-offboarding-configuration-file> |

* 1. Health Attestation Service

This section outlines how to configure Health Attestation Service.

|  |  |  |
| --- | --- | --- |
| Task | Rationale | Implementation Guidance |
| Enable Configuration Manager Clients | How to enable Health Attestation service communication on Configuration Manager client computers | <https://docs.microsoft.com/en-us/sccm/core/servers/manage/health-attestation#device-health-attestation> |
| View Health Attestation | How to view Health Attestation | <https://docs.microsoft.com/en-us/sccm/core/servers/manage/health-attestation#how-to-view-health-attestation> |

* 1. Lookout Integration

This section outlines how to integrate Lookout into Configuration Manager / Intune.

|  |  |  |
| --- | --- | --- |
| Task | Rationale | Implementation Guidance |
| Set up your subscription with Lookout mobile threat protection | To get your subscription ready for the Lookout device threat protection service | <https://docs.microsoft.com/en-us/sccm/protect/deploy-use/set-up-your-subscription-with-lookout> |
| Enable Lookout MTP connection in Intune | This topic shows you how to enable the Lookout MTP connection in Intune | <https://docs.microsoft.com/en-us/sccm/protect/deploy-use/enable-lookout-connection-in-intune> |
| Configure and deploy Lookout for work application | This article explains how to configure and deploy the Lookout for Work app for Android and iOS devices | <https://docs.microsoft.com/en-us/sccm/protect/deploy-use/configure-and-deploy-lookout-for-work-apps> |
| Configure compliance policy | You can create a compliance policy rule in Configuration Manager to include the risk assessment to determine if the device is compliant | <https://docs.microsoft.com/en-us/sccm/protect/deploy-use/enable-device-threat-protection-rule-compliance-policy> |
| Troubleshoot Lookout integration | Troubleshoot Lookout Integration with Intune | <https://docs.microsoft.com/en-us/sccm/protect/deploy-use/troubleshoot-lookout-integration> |

* 1. Windows Hello for Business

This section outlines the steps for configuring Windows Hello for Business with Configuration Manager. These options assume that Group Policy is not available for technical or business reasons.

|  |  |  |
| --- | --- | --- |
| Steps | Rationale | Implementation Guidance |
| Configure Microsoft Windows Hello for Business | Configure the settings for Windows Hello for Business | * Complete to Configure Windows Hello for Business settings at <https://technet.microsoft.com/en-us/library/mt488797.aspx> |
| Deploy a PowerShell Script | Windows Hello for Business must be enabled. | * Complete Step 1 Option 2 at <https://technet.microsoft.com/en-us/library/mt488797.aspx> |
| [OPTIONAL]  Configure Certificate Profile enrollment | Required when using Windows Hello for Business certificate-based logon. | * Complete Step 1 Option 2 at <https://technet.microsoft.com/en-us/library/mt488797.aspx> |

1. Test Plan

This section details the test plan for device management. The following sections define the description of how testing should start, pause, and stop for each test criteria. These are key quality metrics to be used in ensuring the items under test are ready to progress to the next stage in the testing process.

* 1. Device Enrollment

List of tasks to perform to verify device enrollment.

|  |  |  |
| --- | --- | --- |
| Task ID | Description | Pass / Fail |
| 1 | Enrolled devices are visible in the administrative console | Choose an item. |

Table 47: Device enrollment tests.

* 1. Company Resource Access
     1. Profile Deployment

List of tasks to perform to test company resource access.

|  |  |  |
| --- | --- | --- |
| Task ID | Description | Pass / Fail |
| 1 | Device can receive an email profile and sync email | Choose an item. |

Table 48: Company resource access tests.

* 1. Compliance

List of tasks to perform to verify compliance settings.

|  |  |  |
| --- | --- | --- |
| Task ID | Description | Pass / Fail |
| 1 | Configuration items are enforced on devices | Choose an item. |
| 2 | Configuration items are remediated where configured | Choose an item. |
| 3 | Configuration item for Windows Information Protection is remediated | Choose an item. |

Table 49: Compliance settings tests.

* 1. Endpoint Protection

List of tasks to perform to verify Endpoint protection functionality. Note that this test is not designed to verify malware detection rate.

|  |  |  |
| --- | --- | --- |
| Task ID | Description | Pass / Fail |
| 1 | Client is configured per the policy definition | Choose an item. |
| 2 | Alerts are detected as configured | Choose an item. |

Table 50: Endpoint Protection tests.

* 1. Power Management

List of tasks to perform to verify power management functionality.

|  |  |  |
| --- | --- | --- |
| Task ID | Description | Pass / Fail |
| 1 | Devices explicitly excluded do not receive the power management policy | Choose an item. |
| 2 | Users can turn off power management using the software center | Choose an item. |

Table 51: Power management tests.

* 1. Windows Hello for Business

List of tasks to perform to verify Windows Hello for Business functionality.

|  |  |  |
| --- | --- | --- |
| Task ID | Description | Pass / Fail |
| 1 | Windows Hello for Business sign in with PIN or biometrics | Choose an item. |

Table 52: Windows Hello for Business tests.

* 1. Windows Defender Advanced Threat Protection

List of tasks to perform to verify Windows Defender Advanced Threat Protection functionality.

|  |  |  |
| --- | --- | --- |
| Task ID | Description | Pass / Fail |
| 1 | Windows Defender Advanced Threat Protection configured devices are reporting to WDATP | Choose an item. |

Table 53: Windows Defender Advanced Threat Protection tests.

* 1. Health Attestation Service

List of tasks to perform to verify Health Attestation Service functionality.

|  |  |  |
| --- | --- | --- |
| Task ID | Description | Pass / Fail |
| 1 | Health Attestation Service is functional as configured | Choose an item. |

Table 54: Health Attestation Service tests.

* 1. Lookout Integration

List of tasks to perform to verify Lookout integration functionality.

|  |  |  |
| --- | --- | --- |
| Task ID | Description | Pass / Fail |
| 1 | Lookout integration is functional as configured | Choose an item. |

Table 55: Lookout integration tests.