|  |
| --- |
|  |
|  |
| **D** |
|  |
|  |
|  |
|  |
| |  |  |  |  |  | | --- | --- | --- | --- | --- | |  |  |  |  |  | |  | **Detailed design Windows 10** |  |  |  | |  | Smart Workspace |  |  |  | |  |  |  |  | |  |  |  |  |  | |
|  |
|  |
|  |
|  |
|  |

Version information

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Comments | Author |
|  |  |  |  |

Distribution

|  |  |
| --- | --- |
| Title |  |
|  |  |

Table of content

[1 Purpose of this document 1](#_Toc34069972)

[1.1 Scope 1](#_Toc34069973)

[2 Requirements and solution direction 2](#_Toc34069974)

[2.1 Requirements and use case 2](#_Toc34069975)

[2.2 Solution 2](#_Toc34069976)

[3 Design 4](#_Toc34069977)

[3.1 Client Hardware Requirements 4](#_Toc34069978)

[3.1.1 Windows 10 4](#_Toc34069979)

[3.1.2 PXE, TPM, firmware and other requirements 5](#_Toc34069980)

[3.1.3 Disk Partitioning 5](#_Toc34069981)

[3.2 Client Software Requirements 5](#_Toc34069982)

[3.2.1 Operating System 6](#_Toc34069983)

[3.2.2 Core Applications 6](#_Toc34069984)

[3.2.3 Language Support 7](#_Toc34069985)

[3.3 Deployment and management platform 8](#_Toc34069986)

[3.3.1 Scenarios for deployment 8](#_Toc34069987)

[3.3.2 Deployment and Management infrastructure 9](#_Toc34069988)

[3.3.3 Management scenarios 13](#_Toc34069989)

[3.3.4 The best scenario for Smart Workspace 14](#_Toc34069990)

[3.4 Upgrades and Updates 18](#_Toc34069991)

[3.4.1 Feature Updates (Upgrades) 18](#_Toc34069992)

[3.4.2 Deployment 19](#_Toc34069993)

[3.5 Licensing Services 20](#_Toc34069994)

[3.6 Computer Naming 20](#_Toc34069995)

[3.7 Driver Management 21](#_Toc34069996)

[3.8 Windows 10 Security 21](#_Toc34069997)

[3.8.1 User Account Control 22](#_Toc34069998)

[3.8.2 Windows Firewall 23](#_Toc34069999)

[3.8.3 BitLocker Drive Encryption 24](#_Toc34070000)

[3.8.4 BitLocker To Go 25](#_Toc34070001)

[3.8.5 Anti-virus and Anti-Malware (Endpoint Protection) 25](#_Toc34070002)

[3.8.6 Windows Hello for Business 26](#_Toc34070003)

[3.8.7 Device Guard 26](#_Toc34070004)

[3.8.8 Credential Guard 26](#_Toc34070005)

[3.9 Privacy 27](#_Toc34070006)

[3.10 Windows Features 28](#_Toc34070007)

[3.11 Proxy configuration 31](#_Toc34070008)

[4 Additional Configuration 32](#_Toc34070009)

[4.1 Local administration 32](#_Toc34070010)

[4.2 Folder Redirection 32](#_Toc34070011)

[4.3 Branding 32](#_Toc34070012)

[4.4 Browser configuration 33](#_Toc34070013)

[4.5 Cortana 33](#_Toc34070014)

[4.6 Microsoft Store 34](#_Toc34070015)

# Purpose of this document

Welcome to the detailed technical design document for the Windows 10 workspace. This document describes the technical design for the Windows 10 workspaces (desktops and laptops) that will be used in the workspace environment for Smart Workspace, Sogeti Smart Workspace (SSW).

## Scope

This document is limited to devices with the Windows 10 operating system. These Windows 10 clients will be used for:

* Providing users with a device that can be used in both online and offline scenarios, at Smart Workspace locations or on other locations without connection to the Smart Workspace network;
* Providing users with a device that can be used for secure access to the Smart Workspace Office 365 tenant and to Smart Workspace LOB applications;

This design covers the installation and configuration for the Windows 10 operating system. The following items are partly covered in this design only. Because these items are important for the configuration, use and experience of Windows 10, they will be mentioned in this design:

* OS deployment is managed by Microsoft Deployment Toolkit (MDT);
* Devices will be joined to Azure Active Directory;
* Device management is covered by Microsoft Intune (auto-enrollment during Azure AD join);
* Application packaging and deployment is covered in the Intake and packaging Standards and Guidelines.

# Requirements and solution direction

## Requirements and use case

In the SSW, Smart Workspace will be using Windows 10 on laptop and desktop computers for where these concern company owned devices. As the SSW is cloud based, these devices will be Azure Active Directory (AAD) domain joined and managed with Microsoft Intune. The device is enrolled in Microsoft Intune during the AAD domain join automatically.

The devices will be provided with a base set of local applications only. Line of Business Applications (LOB) will be offered through SaaS, Web or applications in the central (remote) workspace service.

Existing devices will be semi-automatically deployed, using MDT with little user actions (Light Touch Installation; LTO). A new task sequence is created for Windows 10 computers which installs a current version of Windows 10.

## Solution

With the release of Windows® 10, Smart Workspace will move to a platform based on Windows 10 and Microsoft ® Office 365. The combination of these two products offers significant functionality, productivity and security improvements over previous versions.

Planning for a new client operating system is a balance between client architecture and supporting infrastructure architecture. To leverage all the Windows 10 features, new functionality must be implemented, or modifications must be made to the supporting infrastructure.

The design takes a layered approach to the core client design, which provides an opportunity for the core operating system and application layers to be properly independent of each other. This in turn allows incremental revisions to either the application components or the underlying operating system without having to re-qualify both.



In addition to providing required changes in manageability and a reduction to support costs, Smart Workspace will also realize a significant improvement in user productivity and functional gains for users. Another key aim is to optimize the balance between essential security protection and the impact it has on user functionality.

The client core image will consist of the following elements, as configured by the hardware vendor:

* The Windows 10 operating system
* Drivers

During deployment, the clients are enrolled into Microsoft Intune and mandatory software is pushed to the device. This includes the following applications:

* Device management software like the Application Portal agent and User Environment Monitoring agent;
* Productivity software:
  + - MicrosoftOffice 365 ProPlus, including Microsoft Teams
    - Adobe Reader DC.
* Tools:
  + - Chrome browser
    - 7-Zip File archiver
* Runtimes and middleware:
  + - Visual C++ runtime libraries
    - Citrix Receiver

# Design

## Client Hardware Requirements

This section defines the minimum hardware requirements to run Windows 10 and the 2016 Office system.

### Windows 10

These are the Microsoft minimum hardware recommendations for systems that will be running the Windows 10 released version. These recommendations are specific to the latest release (1909) and may be subject to change.

|  |  |
| --- | --- |
| Hardware | Requirement |
| CPU | 1 GHz or faster 32-bit (x86) or 64-bit (x64) processor |
| RAM | 1 GB RAM (32-bit) / 2 GB RAM (64-bit) |
| Disk Drive | 16 GB available disk space (32-bit) / 20 GB (64-bit) |
| Graphics | DirectX 9 graphics processor with Windows Display Driver Model (WDDM) 1.0 or higher driver |
| Display | 800 x 600 screen resolution or better |

Note: Some product features of Windows 10, such as navigation using "touch" and security features may require advanced or additional hardware (see paragraph 3.1.3).

Office 365 ProPlus

The following table details the minimum hardware recommendations for systems that will be running Office 365 ProPlus:

|  |  |
| --- | --- |
| Hardware | Requirement |
| CPU | 1.6 gigahertz (GHz) or faster x86-bit or x64-bit 2-core processor |
| RAM | 2 GB RAM (32 bit) / 4 GB RAM (64bit) |
| Disk Drive | 4 gigabyte (GB) free diskspace |
| Graphics | 1280 x 768 screen resolution or better |
| .NET version | some features may require .NET 3.5 and/or 4.6 to also be installed. |

### PXE, TPM, firmware and other requirements

To start a computer from the network, the network interface card (NIC) must be Windows® Pre-Boot Execution Environment (PXE) capable. PXE allows you to start the build/deployment process without requiring a boot disk.

Implementing Windows 10 security features requires the following hardware components:

|  |  |
| --- | --- |
| Feature | Requirement |
| Secure Boot | Secure boot requires firmware that supports UEFI v2.3.1 Errata B and has the Microsoft Windows Certification Authority in the UEFI signature database |
| BitLocker | Trusted Platform Module (TPM) 1.2 or TPM 2.0  An USB disk can be used as alternative  TPM 2.0 is required for automatic encryption during Azure Active Directory domain join |
| Windows Hello | Windows Hello requires specialized illuminated infrared camera for facial recognition or iris detection, or a fingerprint reader which supports the Window Biometric Framework |
| Exploit Guard & Application Control | Current UEFI firmware, Secure Boot, TPM 2.0 and support for Virtualization-based security (VBS) |

Requirements for other features are described here: <https://www.microsoft.com/en-us/windows/windows-10-specifications>

**Design decision**: All Windows 10 devices should meet the following hardware and firmware requirements:

* UEFI boot;
* At least TPM v2.0 chip, TPM enabled in the firmware;
* Secure Boot enabled in the firmware;
* Virtualization (VTx) enabled in BIOS

### Disk Partitioning

All systems, except those who are not deployed using Wipe & Load, will be equipped with one hard drive with single partition available for the user (OS and applications). Additional partitions may be created to support BitLocker and recovery functionality. Systems that will not be deployed using Wipe & Load, keep their existing partition configuration. An example is an Off the shelf used device. See paragraph 3.3.1 for additional information on different scenarios for deployment.

**Design decision**: A system will be configured with a single disk partition available for the user (OS and applications). Additional system partitions will be used for BitLocker and recovery; these partitions will be created automatically during OS Deployment.

## Client Software Requirements

This section outlines the software requirements for the desktop image. This image includes the Windows 10 operating system, updates, services packs, and the applications required in the master image.

### Operating System

**Windows 10 Editions for the enterprise.**

The Windows 10 Pro edition is targeted towards technicians and business users; this edition includes all the features of Windows 10. Additional features include the ability to receive Remote Desktop connections, the ability to participate in a Windows Server domain, Encrypting File System, Hyper-V, and Virtual Hard Disk Booting, Group Policy as well as BitLocker and BitLocker To Go.

The Enterprise Edition includes several other additional features like Direct Access, Windows to Go Creator, AppLocker, BranchCache, Start Screen Control with Group Policy and the security features Credential Guard and Device Guard. For critical mission systems, the Enterprise edition can make use of the Long-Term Servicing Branch (see upgrades and updates in paragraph 3.4).

**Design decision**: **Smart Workspace** will use the 64-bit version of Windows 10 Enterprise by default.

To support 16-bit or other legacy applications that don’t run on the 64-bits version of Windows 10, the 32-bit version of Windows 10 could be used.

Currently, a 32-bits version of the Windows 10 operating system is not planned to be used.

### Core Applications

Core applications are applications or utilities that are used companywide and should be included in the master image, task sequence or enrollment workflow, deployed to all client computers—for example:

* Microsoft Office ProPlus
* Antivirus software
* LOB applications
* Readers and players (such as Adobe® Acrobat Reader)

**Design decision**: The **Smart Workspace** application set will give a user the basic suite of applications to do basic tasks in an offline mode and to connect to the central workspace for LOB applications. Applications that should be available on all workstations are installed during OS deployment or after enrollment in the corporate management infrastructure (see paragraph 3.2.2).

| Baseline | Application | Version | Included in the Master Image |
| --- | --- | --- | --- |
| OS | Internet Explorer | 11 (Included in Windows 10 OS) | Y |
|  | Edge | Included in Windows 10 OS | Y |
|  | .NET Framework | 3.5 SP1 (includes 2.0, 3.0) | Y |
|  | .NET Framework | 4.x (Included in Windows 10 OS) | Y |
| Management | Intune Management Extension | Latest version, installed on enrollment | N |
|  | Application Portal Agent | Latest version | N |
|  | Citrix Receiver | Latest version | N |
| Software | Windows 10 bundled Apps | Latest version | Y |
|  | Microsoft Office (including proofing tools) | Office 365 ProPlus | N |
|  | Flash Player | Included in Windows 10 OS | Y |
|  | Adobe Reader DC | Latest version | N |
|  | 7-Zip (x64) | Latest version | N |
|  | Chrome Browser | Latest version | N |

### Language Support

This section details how the operating system will be configured to address localization. Providing support for multiple languages during an operating system deployment has been a challenge in the past and often required the release of fully localized versions. Many language packs are available for Windows 10, which can be installed on top of the base language of the operating system.

Language packs contain 100 percent of the UI text resources, as shown in the following figure. Windows 10 using a language pack would appear to have a completely localized UI, with all elements appearing in the specified language.

The English (United Kingdom) version of Windows 10 is a language-neutral version with the en-GB language pack applied. Language packs are also sometimes referred to as parent languages.

Language Neutral OS

Sweden 100%

Fully Localized Language Pack

The use of a language pack has the following advantages:

* Wider distribution on a single image
* Less Complication when deploying images in multilingual companies
* Less post-deployment support required
* Lower number of help desk support calls

However, addition of multiple language packs can have the following disadvantages:

* Addition of languages increases image size
* Larger images cause longer deployment times
* Additional updates must be supported for additional application languages

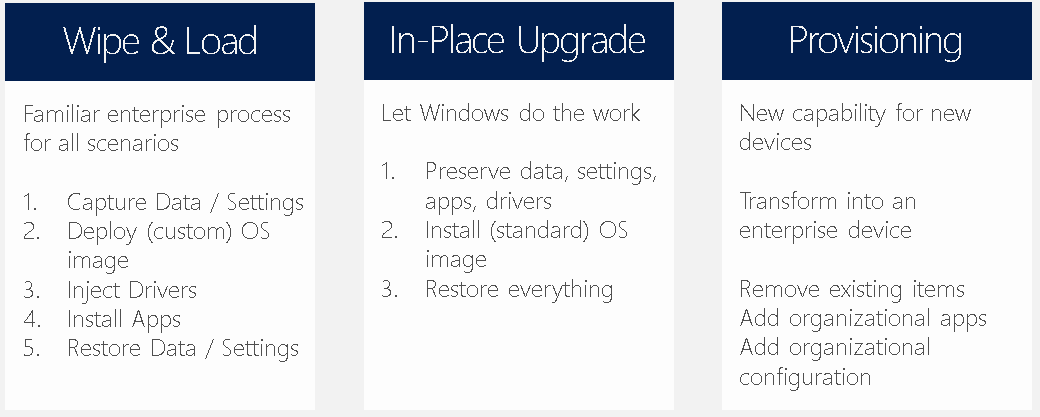
**Design decision**: The **Smart Workspace** image will be created from the English (en-US) OS version. Support for additional languages can be added by installing a language pack from the Microsoft Store for Business. This can be on request, initiated by the user.

## Deployment and management platform

This paragraph describes the options and characteristics for the different options available to deploy and manage devices with the Windows 10 operating system. Paragraphs 3.3.1 through 3.3.3 describe the general options and characteristics, paragraph 3.3.4 describes the design choices made for **Smart Workspace**.

### Scenarios for deployment

With Windows 10, the following scenarios are available for deployment:



The Wipe & Load scenario is the scenario that is traditionally used for provisioning computers with the company standard OS configuration/image. With Windows 10, two additional scenarios are available; In-Place upgrade and Provisioning.

#### Wipe & Load

The wipe & load scenario is well known for deploying the Windows operating systems with SCCM or MDT, used for Windows XP and later versions. This scenario will give IT management the most control as the image is fully customized to company standards. The drawback for this scenario is that the base image must be created and maintained over time which can be time consuming. Wipe and Load deployment also takes a longer time, varying from about 30-90 minutes or longer, depending on the image content and deployment sequence.

#### In-place Upgrade

The In-Place upgrade deployment was introduced with the Windows 8.1 update where it was used to upgrade machines deployed with Windows 8 to Windows 8.1 while preserving installed applications, settings and drivers. The In-Place upgrade scenario can have the following advantages over the Wipe & Load scenario:

* Reduces the time and costs to migrate to Windows 10;
* Migration is automated and managed by Windows. Can be executed through SCCM or MDT tasks;
* Uses the Windows 10 standard image;
* No need to redeploy applications, settings and drivers.

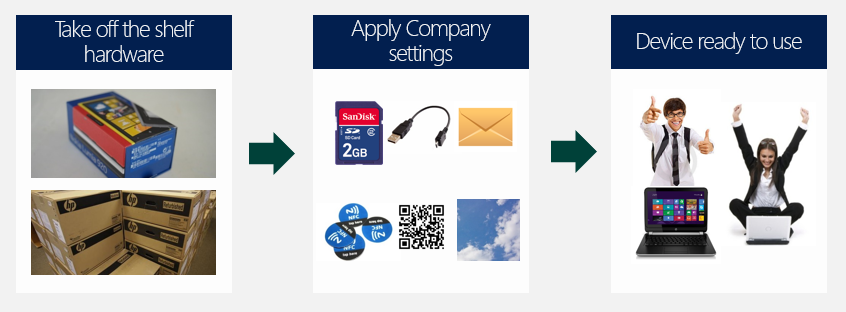
In-Place upgrade can be used to upgrade systems from Windows 7 SP1, Windows 8 or Windows 8.1 to Windows 10. However, the in-place upgrade cannot be used in the following situations:

* Changing BIOS to UEFI
* Changing the disk layout
* When 3rd party disk encryption is used
* Architecture change (x86 -> x64)
* OS Language change
* Domain change
* The use of a Windows 10 custom image is required
* The upgrade to Windows 10 is used to or combined with a bulk change of applications

Furthermore, in-place upgrade does not solve the drift in configurations that may occur over time.

#### Provisioning

Most new devices come with a Windows operating system deployed from the hardware vendor. Until the release of Windows 10, most organizations destroyed the pre-installed / preconfigured OS, replacing it with the company standard operating system using the Wipe & Load scenario. This adds an additional time before the system can be used (typically 1-2 hours) but also requires the company standard image to support the different hardware models and drivers. Instead of re-deploying the device, in this scenario the Windows 10 preinstalled device is re-configured with the company required settings – as shown in the following figure:



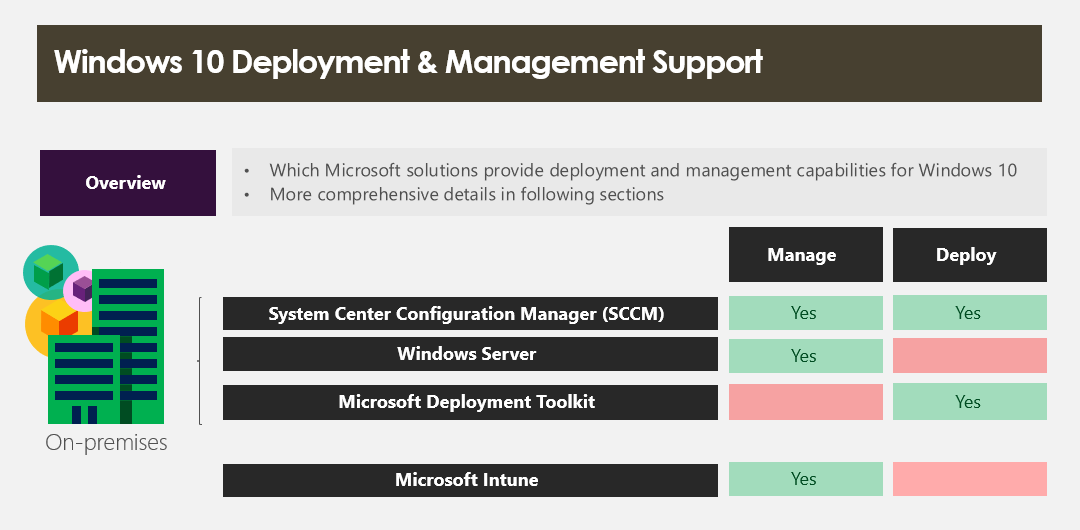
Company specific settings and configurations can be applied through provisioning packages and using management infrastructure solutions like SCCM or Intune (Autopilot). The idea behind the scenario remains the same, in all options.

**Design decision**: Smart Workspace will both reuse existing computers as use new devices. As the target OS and Hardware configuration differs or may differ from the existing configuration, existing devices will be re-deployed using the Wipe & Load scenario. New devices will be onboarded using the provisioning scenario using Autopilot.

The in-place upgrade scenario will be used after the initial installation to keep the Windows 10 systems up to date (Windows Update for Business) with feature updates.

### Deployment and Management infrastructure

The following figure shows the options available for the deployment and management infrastructure capabilities for Windows 10:



#### System Center Configuration Manager

Many companies use System Center Configuration Manager to deploy and manage desktop and laptop computers in the workspace environment. The use of Configuration Manager for Windows 10 devices is fully supported by Microsoft.

After configuring Configuration Manager, the organization is enabled to both deploy and manage Windows 10 on their current and newly deployed devices in the network.

#### Server Infrastructure

The (supported versions of) Windows server infrastructure (Active Directory, File servers, etc.) support managing and working with Windows 10, provided the following changes are applied:

* When KMS is used for Windows activation, the KMS server needs to be updated to support Windows 10 (depending on the OS and version used, an OS version specific hotfix may need to be installed on the KMS host);
* To manage Windows 10 devices with group policies, group policy definitions need to exist in the domain (https://www.microsoft.com/en-us/download/details.aspx?id=48257);

#### Microsoft Deployment Toolkit

Next to SCCM, another option to deploy Windows 10 is the use of the Microsoft Deployment Toolkit (MDT). MDT version 2013 with Update 1 and later fully support deploying Windows 10. Using MDT can be interesting in the following scenario’s:

* When there is no deployment infrastructure available, capable of deploying Windows 10;
* When used instead of SCCM, there is no need to upgrade the current SCCM environment when that environment does not support Windows 10 deployment;
* For mobile or cloud-based scenarios in which devices will be managed using Microsoft Intune;
* MDT is free and available for download without licenses;

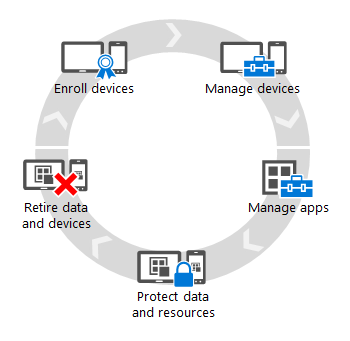
The installation, configuration and use of MDT is very well documented and does not take a lot of time. Furthermore, system administrators already familiar with SCCM should recognize the basics of MDT fast and can be up to speed with MDT in a short time. MDT can only be used to deploy Windows 10 (or other OS versions) and applications but cannot be used to manage these devices once deployed. When using MDT for OS deployment, an additional solution is required to manage those devices.

#### Microsoft Intune

Microsoft Intune is Microsoft’s cloud-based (SaaS) management solution to manage mobile devices like smartphones and tablets running Android or iOS. Intune can also manage Windows desktop devices and laptops running Windows or devices running macOS.

Microsoft Intune can be purchased as a separate licensed product, as part of the Enterprise Mobility + Security suite (EM+S) or included in the Microsoft 365 subscription.

Management with Microsoft Intune is used for:

* Company owned devices that are used in mobile scenario’s; users are underway often and not always – or maybe never – connect to the corporate network. To enable management on these devices, being a cloud service, Intune can be used for these types of scenarios;
* Company owned devices that are used in a cloud-based environment when there is no local IT infrastructure. To enable management on these devices, being a cloud service, Intune can be used for these types of scenarios;
* User’s own devices in BYOD scenario’s which are used to connect to company services and resources. By assigning policies, IT can restrict devices that can connect to the company services. LOB applications that users can install on their own device can be offered through the company portal.

To enable management with Microsoft Intune, the device must first be enrolled. There are different options to enroll a device in Microsoft Intune:

1. The user installs the company portal and enrolls the device;
2. An IT administrator enrolls company owned devices in Microsoft Intune using the Device Enrollment Manager role. This is known as bulk enrollment;
3. A user or administrator joins the device to Azure Active Directory (AAD). AAD is configured to automatically enroll the joined device in Microsoft Intune (see AAD join below);
4. A provisioning package is used to join the device to AAD during deployment. AAD is configured to automatically enroll the joined device in Microsoft Intune (see AAD join below). Using provisioning packages, many devices can be configured in bulk;
5. A user enrolls the device into mobile device management (MDM) using the Work Access settings in Windows 10;

Both the user experience and the management capabilities differ, based on the way the device is enrolled in Microsoft Intune. Basically, this depends on the following choices:

1. The device is enrolled as Intune client managed, Computer device (enrollment options a and b);
2. The device is enrolled as an MDM managed, Mobile device (enrollment options c, d and e);

Using the first option, the Intune client is installed on the device which is used to communicate with the Intune cloud services. This scenario enables the following options:

* Management of the Intune settings using specific computer management policies;
* Management of Windows updates from the Intune management console. This also includes the ability to deploy updates for third party applications like Oracle Java;
* The use of MSI installer and Executable setup packages to install applications on the device;
* Microsoft Intune managed Endpoint protection (anti-virus and anti-malware);
* Management of Firewall policies;
* Inventory of installed software and device attributes;
* Retire devices from Intune;

For enrollment, the user who enrolls the device typically is local administrator on the device. For use, the user can be a standard user. Software can be deployed to devices and users. To deploy software to users, the targeted user must still be a local administrator on the device. When software is deployed to devices, installation is mandatory and thus pushed to the device. Target devices and users can be grouped in Microsoft Intune using Azure Active Directory Groups. When Windows 10 is managed with the Intune client, the build-in MDM client is disabled and the MDM policies available in Intune do not work. With the evolution of Windows 10 and MDM capabilities, this option is rarely used today.

With the second option, the device is managed using existing MDM capabilities of Windows 10. During enrollment, the device is registered in Intune without the need of a client installation on the device as the built-in MDM client is used instead. Typically, this will result in the following capabilities:

* Device Management with built-in and Custom policies. The custom policies consist of OMA-URI settings based on the open standards for mobile device management and Windows 10 capabilities (https://technet.microsoft.com/en-us/library/mt126215.aspx);
* Application deployment using the LOB package type using Windows Installer packages, Win32 Apps\* using (non-)Windows installer setup applications or scripts, modern applications using MSIX packages, applications from the Store for Business and Office 365 ProPlus;
* Running device or user targeted PowerShell scripts\*;
* Retire devices from Intune, remote wipe and remote re-installation;
* Conditional Access policies based on device compliancy;

\*Win32 apps and PowerShell scripts require the device to be Azure AD joined and auto enrolled in Intune.

Intune can be used as a standalone, cloud only management solution. When the organization also is using SCCM for client management, the following options are possible:

* Use Intune and SCCM side by side, operating as two separate management solutions;
* Combination of Intune and SCCM in a co-management environment;

Co-management can have some management advances:

* Management of all devices, whether on premise in the corporate network or mobile outside the corporate network, can take place from a single console;
* Reporting capabilities of SCCM can be used for mobile devices managed by Intune;

#### Azure Active Directory

In traditional corporate environments, devices typically are joined to Windows Active Directory. This enables central management for these devices and provides users with access and SSO experience to resources on the corporate network. For identity and access in cloud-based environments, Azure Active Directory (AAD) is widely used. AAD is used to manage corporate users and groups, including access to cloud services like Office 365 (In fact, Office 365 comes with an AAD tenant).

With Windows 10, also devices can be registered in the company’s directory in Azure. Users then can login on this device using their AAD account providing (SSO-) access to several cloud services. Azure Active Directory is available in four editions: Free, Basic, Premium P1 and Premium P2, AAD Premium P1 is included in the Enterprise Mobility & Security suite (EM+S), which also includes Intune.

With respect to Windows Active Directory, the following must be considered:

* AAD is not the cloud-based version of Windows AD and should not be considered as being the same type of service;
* AAD is not and cannot be used to apply Group Policies to users and/or devices as we know for Active Directory Servers in Windows Server;
* AAD is a separate directory with users and groups. However, the users and groups can be synchronized with Windows AD. This is preferred to provide users to have a single corporate account and password in organizations that also have a Windows Active Directory. For additional functionality, ADFS can be used to federate both directories;
* A device can join either to Windows Active Directory or to Azure Active Directory – not both at the same time. However, a Windows Active Directory domain joined device can be registered to Azure Active Directory to support hybrid scenarios (hybrid join).

A Windows 10 device can be joined to Azure Active Directory:

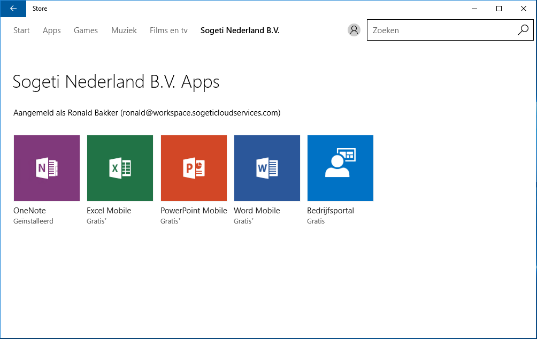
* during the Out of Box Experience (OOBE) phase of the Windows 10 installation cycle;
* using the Windows Settings app in Windows 10;
* using a provisioning package;

To join the device, a user needs to have a valid AAD account and password. AAD can be configured to require Multi Factor Authentication during this process for enhanced security.

When the device is (manually) joined to AAD, it is registered for the user joining the device to AAD. This user typically is added to the local administrator group on the device. Additional users that should have administrator permissions on the AAD joined device can be configured in AAD. These users will be added during the AAD join. After joining AAD, other users can login to the device as well, using their AAD account and password, provided this user is registered in the same AAD domain. These users will be member of the standard Users group on the device.

The Windows 10 Creators update (version 1703) introduced the option to join devices to Azure AD in bulk. This is achieved by new options in the provisioning package which is using a Bulk Token to join the device to Azure Active Directory. Users who use these devices can then be standard users.

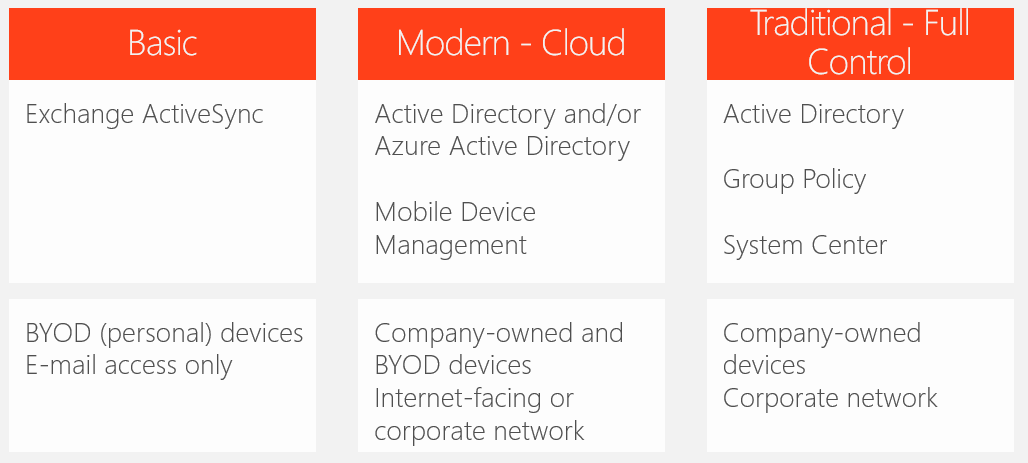
After joining a Windows 10 device to AAD, the following options come available:

* Automatic enrollment in Intune. This setting must be enabled in the AAD configuration (Applications/Microsoft Intune) by providing the Users group for which MDM enrollment applies;
* Business Store. Using the Business Store, users can use their AAD account to install Universal Apps. IT can provision the Business Store with corporate approved public apps and specific LOB apps (see https://businessstore.microsoft.com).

Company applications in the Business store

### Management scenarios

With Windows 10 and the infrastructure options described in paragraph 3.3.1, different scenarios for managing the devices are available. The following figure shows three typical scenarios. These differentiate in control of management for IT and result in different experience and freedom (capabilities) for the user.



#### Modern, Cloud-managed

The cloud-managed scenario typically is used for:

* Corporate devices in a cloud-based environment where there are no local resources available for management (like Windows Active Directory, SCCM, etc.);
* Corporate devices that do not or only in small occasions connect to the company network but still require centralized management;
* Corporate devices on which users have more freedom but still require centralized management. The device is commonly used in the corporate network but can be used outside the network as well;
* User’s own devices which will be used to access corporate resources and services;

Because these devices either do not connect to a corporate network or management infrastructure or are not company owned, these devices are typically Azure Active Directory Joined and/or will be managed with Microsoft Intune.

#### Traditional, Full Control

Currently, this scenario is commonly used for company owned, on premise devices. The device is deployed with a corporate image and applications, and will be fully managed with Windows Active Directory, Group Policies and System Center Configuration Manager. This management scenario is used for company owned devices that will primarily be used while connected to the corporate network to use LOB applications, corporate data and possibly process sensitive information. In this scenario, IT is in full control using a secure corporate standard Windows 10 image and central application management. Users have less freedom to configure the device and/or install applications other than those offered by IT.

#### Basic

The Basic scenario mainly pinpoints to connect user owned devices to corporate services. This scenario often is used to enable users to use company mail services using their own smartphone or tablet, through the corporate network or with an internet connection. With Windows 10 and the Windows 10 mail app, this scenario is also suitable for Windows 10 desktop versions, for instance on the user’s own laptop.

### The best scenario for Smart Workspace

Smart Workspace Line of Business (LOB) applications are available for users on the remote central workspace on the Citrix platform. A small subset of standalone applications, including Office 365, and applications used to connect to the SSW aggregation platform (Citrix receiver and the Application portal agent) are installed in the base installation. Since the SSW is considered a cloud-based environment, management of the computers with Azure Active Directory and Microsoft Intune is the best suited option. With this scenario users will not have to be connected to the **Smart Workspace** network for management purposes. When the device connects to the internet, it can be centrally managed to deploy policies, configuration settings and applications.

**Design decision**: For Smart Workspace we will use Azure AD Join and enrollment in Microsoft Intune, using the Intune MDM scenario, to manage the desktop and laptops. These devices will be managed using the Cloud-managed scenario.

Azure AD Premium P1 and Microsoft Intune are available for Smart Workspace users as part of the EM+S subscription.

Windows Autopilot can be used to join the devices to Azure Active Directory, followed by automatic enrollment in Intune. Apart from the ability to join devices to AAD and entitlement for valid subscriptions, in this scenario users do not need additional permissions on the device to enroll the device.

**Design decision**: Autopilot will be used to join the device to Azure Active Directory, followed by autoenrollment in Intune.

#### Azure AD configuration

The following items are configured in Azure AD to support the deployment of Window 10:

* Selected users can join devices to Azure AD;
* Microsoft Intune is configured for auto enrollment since this will resolve in an MDM managed system;

Per user the following actions are required:

* A user account must exist in Azure AD to allow the user to logon to Azure AD joined devices, connect with Intune and to use other applications that rely on Azure AD like Office 365;
* Assign the user an EM+S license, this allows the user and the device to be managed by Intune and enable Azure AD Premium P1 functionalities;
* Assign the user to an Office 365 license, this allows the user to use Office 365 and Office 365 ProPlus on the Windows 10 device;

#### Intune configuration

The following items are configured in Intune to support the management of Window 10:

* Intune is set as Mobile Device Management Authority;
* Groups are created to encompass devices for management purposes;

#### *Autopilot*

To enable enrollment in the Windows Autopilot program, the device needs to be pre-registered for the organization, in this case Smart Workspace. Users then can use their organization account from Azure Active Directory to login to the onboarded device. After enrollment, Intune is used to install the base application set and to apply default configuration and security profiles.

**Design choice:** Devices used by Smart Workspace in the SSW IT Workplace will be delivered by the hardware vendor preconfigured with Windows 10. Therefore, Auto-pilot will be used to onboard these new devices.

To enable Autopilot, the following two configurations must be set:

* At least one Deployment profile must exist and assigned
* The devices must be pre-registered for Autopilot

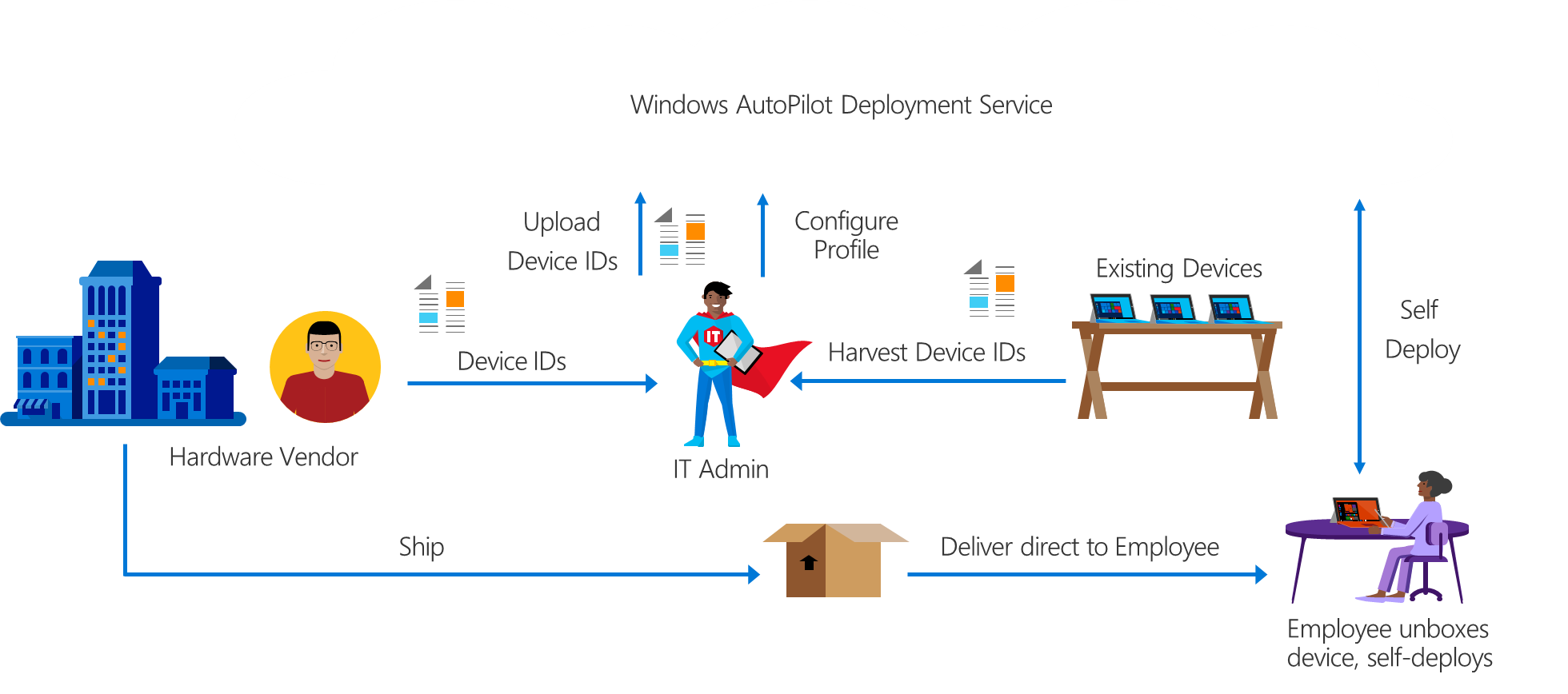
The default deployment profile will be created with the following settings:

|  |  |  |
| --- | --- | --- |
| Setting | Options | Configured Value |
| Deployment Mode | User-Driven  Self-Deploying (Preview) | **User-Driven**  Note: Self Deploying is in preview at this moment in time. When this option is in production (GA), the choice is reconsidered. |
| Join to Azure AD As | Azure AD Joined | **Azure AD Joined** |
| End User license agreement (EULA) | Show  Hide | **Hide** |
| Privacy Settings | Show  Hide | **Hide** |
| User account type | Administrator  Standard | **Standard** |
| White Glove support | Enabled  Disabled | **Enabled** |
| Conversion of existing devices | Enabled  Disabled | **Enabled** |

Devices are registered with a hardware hash, that must be uploaded in Intune or the Microsoft Store for Business. The following options exist to register the devices:

* The organization (in this case ) generates the hashes on the device (so called harvesting of hardware hashes)
* The hardware vendor delivers a list of ID’s for the devices for . This list will be uploaded in **Microsoft Intune.**
* The OEM (hardware vendor) or partner (reseller/distriubutor or CSP partner) registers the devices on behalf of the organization

The process and options are shown in the following figure:



**Design choice:** Devices used by Smart Workspace in the SSW IT Workplace will be pre-registered in the tenant using the OEM/Partner registration process. Agreements for this process already are in place.

The new Windows 10 devices will be joined to Azure Active Directory and enrolled in the existing AAD and Intune tenant. Differentiation between devices that already exist in the tenant and new (SSW-)devices will be created using device group membership. Existing policies will be maintained for those devices, if possible both new and existing policies will be merged at a later moment in time.

In the SSW project, we will consider re-use of laptops and desktops that are able to run the latest version of Windows 10 and support the latest security requirements (TPM 2,0 chip, UEFI boot, etc). Devices that comply with the minimum requirements cannot use the same process as used for new devices. Existing devices need the following activities before they can be used in the SSW workplace:

* Registration in the Autopilot service.
* Installation of Windows 10 using the Wipe & Load scenario
* Enroll using the Autopilot process

To enable the use of Autopilot, these devices need to be registered in Autopilot. As these are not new devices, the vendor does not have the hardware hashes and they need to be harvested first. This requires running a PowerShell script on the device *and* the device must have Windows 10 1703 or later installed. Considering devices will not meet this requirement, the process then would be:

* Install Windows 10 1909
* Harvest hardware hash
* Upload hash in Intune and apply profile
* Reset the device to enforce the Out of the Box (OOBE) cycle where the Autopilot process is initiated

This would take a lot of effort requiring all devices to be touched manually. An alternative scenario is possible in which the Autopilot profile is injected during the installation of Windows 10. This profile is picked up by the OOBE process on first boot and the device is enrolled following the Autopilot process. Once enrolled into Azure AD and Intune, the device is converted into an Autopilot device using the option in the Autopilot profile. This process is described in more details here: <https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/existing-devices> and here <https://osddeployment.dk/2018/12/08/how-to-deploy-autopilot-device-fast-with-mdt/> This second source is using MDT which is excellent for use in an offline scenario and needs far less infrastructure.

**Design choice:** The Autopilot for Existing devices is used to onboard existing devices into the SSW IT Workplace.

Devices can have different use cases, for example based on the persona to which the Windows device is delivered. This may require different policies, settings and applications to be applied on those devices. To identify different device groups, the Group Tag in Autopilot is used. The group tag is set initially upon registration (along with the hardware hash) but can be changed afterwards. Azure AD Dynamic Device groups will be used to identify different groups of devices, using the following query:

(device.devicePhysicalIds -any \_ -eq "[OrderID]:Sweden")

#### *Policies*

Settings on managed devices are configured by applying policies from Intune. In the cloud-based management scenario, where devices are joined to Azure AD, normal Domain Group Policies cannot be used and policies will be managed with Intune. Intune supports different ways of applying policies, based on the chosen managed scenario and goal to achieve with the policy. For MDM managed devices the following policies will be used:

* Device policies.
  + Device Configuration profiles.

Configuration is split in (predefined) configuration profiles, ADMX policies and custom profiles. Predefined profiles have defined settings for which values can be configured. The custom profile is based on OMA-URI settings which must be constructed manually, based on the available policies for MDM client in Windows 10. ADMX templates reflect ADMX backed policies, a subset of the Group Policies available in Windows Active Directory domains that can be managed through the MDM client in Windows 10.

* + Device Compliance policies.

These policies specify the device condition for which a device is marked as compliant. To enable the use of Conditional Access, a Device Compliance policy is required. Devices without a compliance policy assigned will be marked not compliant by default.

* + Device Security.

Using a device security policy, a security baseline is set for the devices to which the policy is assigned. The baseline is a predefined set of about 300 policy settings which Microsoft recommends applying as a best practice. Security baselines are available for Windows 10, Edge (currently preview) and ATP (currently preview).

* Application Policies.
  + Application Configuration Policies

With these settings, applications on mobile devices can be configured. These settings do not apply to Windows 10.

* + Application Protection Policies

These policies can be used to isolate company data from personal data and specify applications that can use company data (Allowed Apps). This feature is built on Windows Information Protection and MAM and can be used on all Windows 10 editions from version 1703 and higher.

* Access policies.
  + Conditional Access.

With conditional access, device characteristics can be set to which a device must comply to enable access to a service for which conditional access is configured. If conditions are not met, access to the service is denied.

Settings configured in the policy are enforced by Intune based on device and/or user group membership.

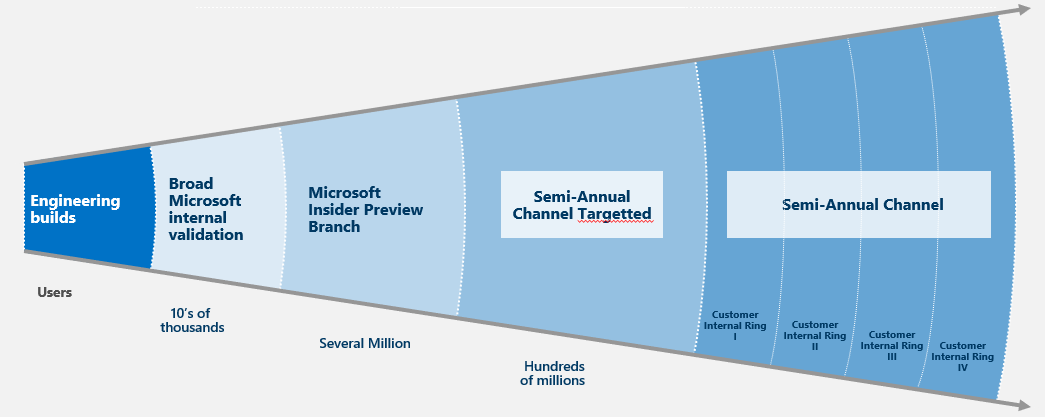
**Design decision**: For Smart Workspace we will apply the Intune policies to configure the device, users and applications. The policies to be configured will be specified in the Windows 10 policy configuration document.

## Upgrades and Updates

An update is a collection of one of more files that can be applied to the operating system or application to correct a known problem or security risk. Before the release of Windows 10, we would install the base operating system version – optionally with a service pack preconfigured. After installation, the system is updated in monthly intervals using Microsoft Update (optionally managed with WSUS, SCCM or Microsoft Intune). This update mechanism still applies for Windows 10. But apart from the monthly update cycle, new versions for Windows 10 will be released regularly – typically on a 6 month interval – known as feature updates (formerly upgrades). This transforms Windows 10 from a product to a service.

### Feature Updates (Upgrades)

Feature updates for Windows 10 are released for different users in different intervals, known as channels (formerly branches), as shown in the following figure:



Enterprise users can speed up the upgrade by applying a different channel. Additionally, Feature and Quality updates can be postponed or deferred. After a defined period, Windows 10 devices on which the current version is not installed, will be no longer supported, unless the device is using the LTSC Edition for Windows 10 Enterprise.

**Design decision**: The base image of Windows 10 will be based on the latest available version. Currently, this is version 1909.

Different rings will be configured to spread the deployment of Feature Updates and (optionally) Quality updates. Quality updates will be deployed as soon as possible, deferral is only allowed for business-critical systems where the update is first tested on a small portion of devices.

### Deployment

Both Feature updates and Quality Updates can be installed using the Windows Update service in Windows 10. Using this out of the box feature IT management has little to no control about the Windows updates installed on the different devices in the workspace environment. Instead of using Windows Updates directly, there are other options to centrally manage the updates for Windows:

* Windows Server Updates Services (WSUS)
* System Center Configuration Manager (SCCM)
* Microsoft Intune

#### Windows Server Update Services (WSUS)

Windows Server Update Services (or WSUS) is a server role included in Windows Server. With this role enabled, Windows updates can be centrally downloaded to the WSUS server and from there be distributed to the Windows client devices. In this scenario, the Windows 10 client device is configured to use updates from the WSUS server instead of directly download and install them from Windows Update. Using WSUS, updates for Windows 10 but also for applications like Microsoft Office or runtimes like Visual C++, and .NET can be centrally managed. Before clients can download and install updates from WSUS, an administrator first needs to approve the updates. WSUS is a good solution for organizations that do not use other client management infrastructure but need control over updates for Windows and other applications.

#### System Center Configuration Manager (SCCM)

SCCM integrates with the WSUS feature to download updates from Windows Update or from a WSUS server. Through SCCM, updates can be deployed manual or automatically. To manually deploy updates, the administrator selects and downloads the required updates, creates an update deployment package and distributes this to the target devices. Normally, this process is repeated once per month. Another option in SCCM is to use Automatic Deployment Rules (ADR) for deploying updates. With ADR, the process of deploying Windows updates can be highly automated. Using filters, the type of updates to be included can be selected. Periodically, updates will be downloaded and when new updates arrive, packages with the latest updates are created and deployed automatically. Using ADR drastically reduces the time administrators need to spend on Windows updates and can increase the number of machines that are up to date with the latest patches. Deploying updates with ADR is the preferred method when SCCM is used in the organization.

#### Microsoft Intune

For devices managed with the MDM client that is built-in into Windows 10 we can configure behavior of Windows updates by defining Windows 10 Update Rings. The update ring is used to specify the following update settings:

* Update Channel
* Updates for Microsoft products
* Updates for Windows drivers
* Automatic update behavior and maintenance window
* Deferral for period for Quality updates
* Deferral for period for Feature updates

An update ring is then assigned to a group of devices to which the settings are applied.

**Design decision**: Deployment of Windows Updates and Upgrades will be managed by Microsoft Intune. Windows 10 Update Rings will be configured to define different groups of devices with different update characteristics.

#### Download optimization

The later versions of Windows 10 contain built-in peering functions to optimize bandwidth used for downloading Windows updates. Instead of letting each device download the Windows updates from internet independently, peering technologies share Windows update sources between computers in the network. Instead of internet connection bandwidth, the local network is used.

**Design decision**: Download optimization profiles are used to optimize the download of Windows updates.

## Licensing Services

Volume Activation fundamentally works in the same way in Windows 10 as it does since the introduction of Windows Vista and later operating systems. You can use Key Management Service (KMS) or Multiple Activation Keys (MAK). The same infrastructure will be used to activate Windows 10 and Windows Server. Virtual machine activations can be counted against activation thresholds.

Starting with Windows Server 2012 and Windows 8, you can avoid designating and configuring an activation server altogether and use Active Directory for activation instead. Whenever you activate a computer running these or later operating systems that is joined to a domain that is using the Windows 8 (or later) schema, an activation object is created and stored in Active Directory, instead of on the local computer. You can accomplish the initial activation of the first computer with Volume Activation Services in Server Manager or Slmgr.vbs Active Directory activation commands.

When MAK keys are used, the Volume Activation Management Tool (VAMT) is required, now included in the Windows Automated Installation Kit (Windows AIK). When KMS keys are used, the KMS client computer must renew their activation by connecting to the KMS host at least once every 180 days to remain activated.

New is the option to purchase Windows Enterprise as a subscription-based license. This can be a separate subscription or part of Microsoft 365. The license can be bought in different models, including E3 and E5. Unlike KMS or MAK licenses, the Windows 10 Enterprise subscription is user based instead of device based. Each user can activate 5 different devices using this license, provided the device is Azure Active Directory domain joined and has an OEM-licensed Windows 10 Pro installation. When a user entitled with a Windows 10 Enterprise subscription license logs in on a device with Windows 10 Pro, the edition will be upgraded to Enterprise automatically.

**Design decision**: tbd.

## Computer Naming

Currently **Smart Workspace** is using computer type and a number to set a specific computer name. The table below will describe the requirements of a **Smart Workspace** computer naming.

|  |  |  |
| --- | --- | --- |
| Type | | Number |
| 6 characters, defined | | 4 numbers |
| *<CC><LLL>*-L | (Laptops) | 0000 – 9999 |
| *<CC><LLL>*-W | (Desktops) | 0000 – 9999 |

**Design decision**: The naming policy for workstations and laptops will be maintained.

## Driver Management

Driver management for new devices used by **Smart Workspace** is covered by the hardware vendor who supplies devices preinstalled with a factory image. The following paragraph is only in scope when custom images are required, for example to use existing devices that will be enrolled in the SSW workplace and need an upgrade or reinstallation of the Operating System through an image.

When creating an OS image, it is important to manage drivers. Master images should be configured to include only the drivers required to successfully create the image. The more generic a master image, the lower the deployment and maintenance costs. Keeping drivers outside of the master image allows them to have their own lifecycle as the master image does not need to be regenerated for a driver update.

**Advice:** To prevent contamination the master image will only contain drivers to create the image. It is advised to create these master images within a virtual environment to minimize the installed drivers.

**Important:** Drivers included in the master image will be present on all systems to which the image is deployed. It is possible that these “in-box” drivers may override other drivers that are installed during the image delivery process.

Most vendors supply driver packs for their current models; using these packs will simplify the addition of new hardware to the deployment infrastructure. By defining a set of drivers to be used for each make and model of client device in the environment, driver mismatch issues can be avoided. By labeling the drivers, cleanup of old and no longer used drivers is also possible.

**Design decision**: The master image will only include the necessary drivers of the used hardware. By default, the driver set included in Windows 10 will be used and will be replaced by vendor drivers only when necessary. MDT will be responsible for the driver management.

MDT will deploy the driver-sets during the deployment using **Auto-Apply Driver Packages**. The sets will be targeted to a specific make and models using WMI.

After onboarding of the device, either from factory installed image or with a custom image, drivers will be managed with Windows Updates. Periodically, drivers will be update using vendor supplied driver packs.

## Windows 10 Security

In keeping with Microsoft’s layered approach to security protection, Windows 10 includes new and enhanced features that help prevent installation of malware, help mitigate the damage that malware can cause if it does infect the computer and remove malware that has already been installed.

The security features discussed in this section include:

* User Account Control (UAC)
* Windows Firewall
* Windows® BitLocker™ Drive Encryption
* BitLocker To Go
* Windows® Defender
* Windows Hello for Business
* Secure Boot
* Device Guard
* Credential Guard
* Applocker

Apart from the above-mentioned features, a lot of settings impact security on the device. A set of standard policies, based on security best practices by Microsoft and several security partners from Microsoft, are combined in the Microsoft Security Baseline. Baselines exist for Windows Active Directory domain joined devices and MDM (Intune) managed devices. Both are based on the same security advisories but the set for MDM managed devices does not contain the settings only valid for devices joined in a Windows Active Directory domain. From the Security Baseline documentation:

The MDM Security is selected based on the following principals.

1. MDM Security Baseline contains all policies part of GP Security Baseline

With Exception of Settings for Legacy technology that are not applicable to Cloud managed devices

- Domain Control / Domain only

- SMBv1

- NTLM

2. Settings of Legacy technology that has alternative solutions with modern technology

3. Policies that manage MS Inbox security technology (not deprecated)

- BitLocker, Smartscreen, DeviceGuard (Virtual Based Security), ExploitGuard, Defender, Firewall

4. Policies that restricts Remote access to device

5. Policies that set Credentials (Password, PIN) requirements

6. Policies that restrict use of Legacy Technology"

**Design decision**: Security Baseline settings for MDM managed devices will be configured and activated in Intune.

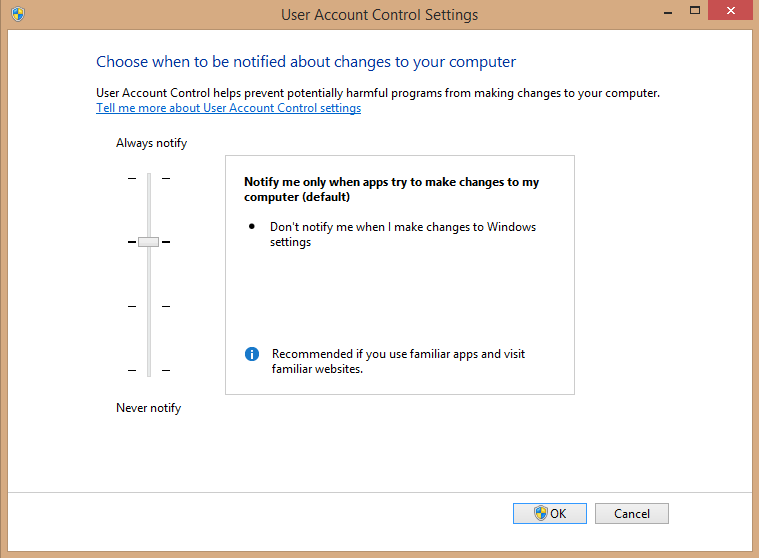
### User Account Control

User Account Control (UAC) was introduced in Windows Vista and was a fundamental change in how security functions at an operating system level. This feature in Windows 7 has brought some significant changes based on customer feedback in order to improve the end-user experience.

The UAC in Windows 7 and later versions offers a scalable level of protection. Whereas Windows Vista only allowed a binary enabling or disabling level of control of the UAC, Windows 10 allows up to four levels of protection or the disabling of the UAC completely.

The four levels of control are:

1. Always notify (equivalent to enabling the UAC in Windows Vista)
2. Default – Notify only when programs try to make changes to my computer.
3. Notify only when programs try to make changes to my computer (do not dim my desktop).
4. Never notify (disable UAC)



Additionally, the number of tasks that a standard user can realize has been increased from Windows Vista. Common standard-user tasks that can now be accomplished without the need for administrative privileges are:

* Install updates and drivers through Windows Update
* View certain system settings, without making changes
* Bluetooth pairing
* Change the screen display text size

UAC reduces or removes the requirement for elevated privileges such as Power User or Local Administrator that was often required in prior Windows versions. If Standard users attempt to perform functions that require elevated privileges, they will be prompted for administrative credentials.

Because of these changes, many software products will require modifications to successfully run without administrative privileges. For application compatibility, Windows 10 includes file system and registry virtualization, which allows applications that require administrative permissions to complete their task, but with the data written to a virtualized area.

UAC also provides increased protection against application-based “shatter” attacks, which use the Windows Messaging System to take over the UI. The Windows Messaging System allows any application to communicate with both the operating system and with any other application. Because all applications on Windows 10 run with user-level permissions by default, this will make it less likely that an application will have the ability to run these types of commands without the user’s knowledge.

**Design decision**: UAC will retain the default out-of-the-box level. The setting is managed through the Baseline Security policy in Intune.

### Windows Firewall

The personal firewall built into Windows 10 builds on the functionality included with Windows Vista and Windows 7. You can use Group Policy to configure every aspect of the firewall, so client computer security settings remain constant. The firewall works closely with Windows Service Hardening to restrict what services can do on the system, providing defense-in-depth and reducing opportunities for attackers to compromise vulnerable computers. Windows Service Hardening restricts critical Windows services from performing abnormal activities in the file system, registry, network, or any other resources that could be used to allow malware to install itself or attack other computers. For example, you can restrict the Remote Procedure Call (RPC) service from replacing system files or modifying the registry.

In Windows 10, IPsec and firewall management are integrated into a single console, known as Windows Firewall with Advanced Security. This console centralizes inbound and outbound traffic filtering along with IPsec server and domain isolation settings in the UI, enabling increased visibility into security settings.

An important new feature that was introduced in Windows 7 and continued in Windows 10 is Multiple Active Firewall Profiles. Windows Vista and Windows Server 2008 allowed one of three firewall profiles to be configured for a network connection—Domain, Public, and Private—but only one of the profiles could be active at any one time. Because of this limitation, if you connected via a Public network to a Domain network, then the most restrictive firewall profile was applied to all communications across all networks. With Windows 10 this restriction has been removed with the inclusion of Multiple Active Firewall Profiles (MAFP).

MAFP requires no additional configuration in order to activate or apply it; in fact, it has no configurable settings at all. Therefore, administrators can continue to use Group Policy, the command line tool netsh, or the Control Panel applet Windows Firewall with Advanced Security to configure, maintain, and control the Windows Firewall settings, profiles, exceptions, and connection rules.

**Design decision**: Windows Firewall will be used as firewall client for client devices within **Smart Workspace**. The firewall is managed with Intune policies.

### BitLocker Drive Encryption

BitLocker Drive Encryption is a hard-disk encryption technology using the Advanced Encryption Standard (AES) that was first introduced with Windows Vista. Use BitLocker Drive Encryption to protect the operating system volume; system files, page file, and hibernation file; as well as user data stored on any volume. Encryption key lengths are either 128 or 256 bits and can be controlled through either Group Policy or WMI. BitLocker-protected drives can be unlocked with smart cards.

Recovery keys can be stored in the Windows Active Directory Domain (for AD joined devices) or Azure Active Directory (for Azure AD joined devices), and domain administrators can use them to unlock a BitLocker-protected drive in the event a user loses his or her key. If recovery key escrow within (Azure-) Active Directory is not available or is not configured, BitLocker Drive Encryption includes a recovery console that you can access on startup and provides a mechanism for entering the recovery key manually.

Supported modes of operation include the use of TPM 1.2 or later and storage of keys on UFDs. For increased security, you can use TPM in conjunction with a PIN or a USB device containing the key. In normal operation, BitLocker Drive Encryption using a TPM is transparent to users; however, certain changes will cause it to lock the drive, requiring recovery. These changes include moving the hard disk to another computer; replacement of the system board, including the TPM chip; or corruption of system files used early in the boot process.

Generally, BitLocker imposes a single-digit percentage performance overhead; making it not noticeable in most scenarios.

BitLocker Drive Encryption requirements include:

* A TPM 1.2 or later (unless USB-key-only mode is used).
* A system basic input/output system (BIOS) compliant with version 1.2 or later Trusted Computing Group.

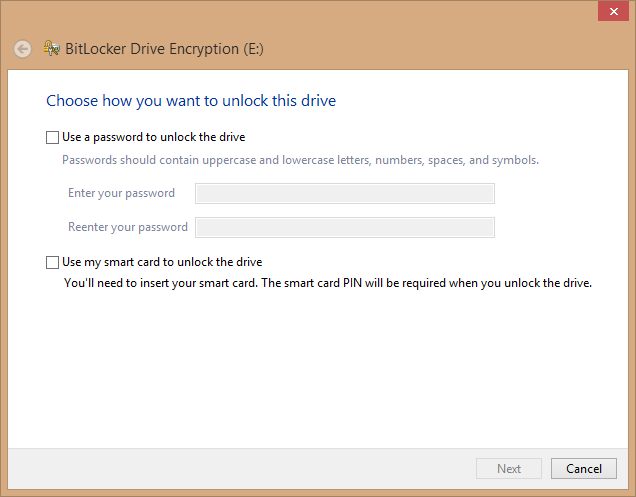
Note that the requirement/recommendation for a 2-GB BitLocker partition has been removed in Windows 7 and higher. Now, upon installing Windows 10, a 350-mb raw partition is created automatically as part of the drive schema.

**Design decision**: BitLocker will be enabled on all Windows 10 devices. BitLocker is enabled using automatic Bitlocker activation in Azure AD join, when the device is enrolled in Autopilot. The recovery key is saved with the device registration in Azure Active Directory.

### BitLocker To Go

BitLocker™ To Go is a new feature introduced with Windows 7 that permits the encryption of removable media using BitLocker. This permits the safe storage and transport of data on portable media, without the inherit risks that are normally associated with storing data on these devices.

Once encrypted, these devices can be unlocked with a password or smart card. Additionally, there is backwards compatibility to Windows XP that allows encrypted devices to be unlocked in read-only mode, if the device has been formatted with the FAT file system.



**Design decision**: **Smart Workspace** will force BitLocker To Go to be used on USB devices when write actions are required. This policy is enforced from Intune.

### Anti-virus and Anti-Malware (Endpoint Protection)

Out of the box, Windows 10 is delivered with Windows Defender to protect Windows clients against viruses and malware.

Using Windows Defender provides the following functionality:

* Protection against viruses and malware
* Periodic updates for anti-virus and anti-malware definitions
* Centralized management for client settings

**Design decision**: Windows Defender will be used for anti-virus and anti-malware protection. The client is included in Windows 10. Configuration is managed from Intune using the Baseline Security policy and checked with the compliance policy.

### Windows Hello for Business

Windows Hello for Business provides strong two-factor authentication (2FA), fully integrated into Windows, and replaces passwords with the combination of an enrolled device and either a PIN or biometric gesture.

Windows Hello for Business is conceptually like smart cards but more flexible. Authentication is performed by using an asymmetric key pair instead of a string comparison (for example, password), and the user’s key material can be secured by using hardware (save in TPM chip). Windows Hello for Business is configured per device, users that use multiple devices need to configure a PIN and optional biometric on each device they want to login to. Therefore, Windows Hello for Business us less suited for shared devices and roaming situations.

To use Windows Hello, the device must be equipped with hardware that is suitable to use facial or fingerprint recognition.

**Design decision**: Users need to configure Windows Hello for Business on all devices. This policy is enabled in the Baseline security policy.

### Device Guard

Device Guard is a combination of enterprise-related hardware and software security features that, when configured together, will lock a device down so that it can only run trusted applications. If the application is not trusted, then it cannot run. It also means that even if an attacker manages to get control of the Windows kernel, he or she will be much less likely to be able to run malicious executable code after the computer restarts because of which decisions are made about what will be able to run and when it will be able to do so.

Device Guard uses the new virtualization-based security in Windows 10 Enterprise to isolate the Code Integrity service from the Microsoft Windows kernel itself, letting the service use signatures defined by your enterprise-controlled policy to help determine what is trustworthy. In effect, the Code Integrity service runs alongside the kernel in a Windows hypervisor-protected container.

The use of Device Guard has several hardware and software requirements, of which the following are the most important:

* Only available in the 64-bits version of Windows 10 Enterprise Edition
* Requires UEFI firmware version 2.3.1 or higher and Secure Boot
* The following Virtualization extensions must be enabled:
  + Intel VT-x or AMD-V
  + Second Level Address Translation
* Requires the following features enabled
  + Hyper-V Hypervisor
  + Isolated User Mode

Device Guard can be deployed and managed using one of the following options:

* Active Directory Group Policies;
* SCCM;
* Windows PowerShell
* Device Guard and Credential Guard hardware readiness tool.

Management through Microsoft Intune is currently not available but is planned for a future release.

**Design decision**: The use of Device Guard is enabled from the Baseline Security policy.

### Credential Guard

Using virtualized based security, Credential Guard in Windows 10 is used to protect secrets (hashes, tickets, credentials) against unauthorized access. Secrets are isolated so only privileged system software is allowed access to circumvent attacks like Pass-The-Hash or Pass-The-Ticket attacks.

Credential Guard provides an additional layer of credential protection specifically for domain users by storing the credentials within the virtualized container, away from both the kernel and user mode operating system. This makes it difficult for even a compromised system to obtain access to the credentials. In addition to the client-side enablement of Credential Guard, you can deploy additional mitigations at both the Certification Authority and domain controller level to prevent credential theft.

The use of Credential Guard has a number of hardware and software requirements, of which the following are the most important:

* Available for Windows 10 Enterprise or Education
* Only available on computers with a 64-bits CPU
* Requires UEFI firmware version 2.3.1.c or higher and Secure Boot
* The following Virtualization extensions must be enabled:
  + Intel VT-x or AMD-V
  + Second Level Address Translation
* Requires the following features enabled
  + Hyper-V Hypervisor
  + Isolated User Mode

Credential Guard can be deployed and managed using one of the following options:

* Active Directory Group Policies;
* Windows Registry settings;
* Device Guard and Credential Guard hardware readiness tool.

**Design decision**: The use of Credential Guard is enabled from the Baseline Security policy.

#### AppLocker

With this feature, admins can control which applications and files can be run by users (App Whitelisting). The feature consists of rules for executables, scripts, DLL files, Windows installer packages and installed packages (‘modern apps’). These rules control whether an app can run based on attributes like location or app publisher. The following default rules will be configured through a custom configuration profile in Intune:

* The use of executables from locations on disk not meant for applications (for example outside C:\Program Files, C:\Program Files (x86) or C:\Windows or locations writable for users) is blocked. This prohibits the ability to copy and launch applications that do not require installation, for example portable apps.
* Preinstalled Store apps that are not desired are blocked from use.

## Privacy

Privacy controls in Windows 10 is divided in two areas of control:

* Device permissions
* App Permissions

Device permissions are required to control the information gathered by services and providers like webservices (browsing) and for Windows diagnostic and feedback. Permissions can be controlled using Intune policies.

An important setting is the setting that controls diagnostic data sent to Microsoft. The default setting is Base but can be set to Enhanced or Full as well. If used with cloud features like Update Compliance, Telemetry settings must be set to at least Basic and preferably to Enhanced or Full and combined with the device name (the device name is left out by default).

**Design decision**: The Diagnostic level (Telemetry) is set to *Basic*.

App Permissions control whether apps can use device peripherals or information from the device. Permissions can be set on the device level (for all apps) or on a per-app level (per app overrides). Both settings can be managed with Intune policies.

**Design decision**: App Settings for privacy will be configured in the device restriction policy for Intune

## Windows Features

The Windows 10 operating system has many features and components that you can enable or disable. This section outlines many of these features for you to make decisions about the default installation state.

**Design decision**: The following table details the recommended Windows Feature configuration. These will be enabled and disabled in the master image file for deployment. Any non-business features have been removed.

| Windows Feature | Default State | Proposed State |
| --- | --- | --- |
| Microsoft .NET Framework 3.5.1 | N | **Y** |
| * Windows Communication Foundation HTTP Activation | N | N |
| * Windows Communication Foundation non-HTTP Activation | N | N |
| Microsoft .NET Framework 4.5 Advances Services |  |  |
| * ASP.NET 4.5 | N | N |
| * WCF Services |  |  |
| * HTTP Activation | N | N |
| * Message Queuing (MSMQ) Activation | N | N |
| * Named Pipe Activation | N | N |
| * TCP Activation | N | N |
| * TCP Port Sharing | Y | Y |
| Active Directory Lightweight Directory Services | N | N |
| Embedded Boot Experience | N | N |
| Embedded Logon | N | N |
| Embedded Shell Launcher | N | N |
| Hyper-V | N | N |
| * Hyper-V Management Tools | N | N |
| * + Hyper-V GUI Management Tools | N | N |
| * + Hyper-V Module for Windows PowerShell | N | N |
| * Hyper-V Platform | N | N |
| Internet Explorer 11 | Y | Y |
| Internet Information Services | N | N |
| * FTP Server: | N | N |
| * + FTP Extensibility | N | N |
| * + FTP Service | N | N |
| * Web Management Tools: | N | N |
| * + IIS 6 Management Compatibility: | N | N |
| * + IIS 6 Management Console | N | N |
| * + IIS 6 Scripting Tools | N | N |
| * + IIS 6 WMI Compatibility | N | N |
| * + IIS Metabase and IIS 6 configuration compatibility | N | N |
| * + IIS Management Console | N | N |
| * + IIS Management Scripts and Tools | N | N |
| * + IIS Management Service | N | N |
| * World Wide Web Services: | N | N |
| * + Application development features: | N | N |
| * + .NET Extensibility | N | N |
| * + ASP | N | N |
| * + ASP .NET | N | N |
| * + CGI | N | N |
| * + ISAPI | N | N |
| * + ISAPI filters | N | N |
| * + Server-side includes | N | N |
| * Common HTTP features: | N | N |
| * + Default document | N | N |
| * + Directory browsing | N | N |
| * + HTTP errors | N | N |
| * + HTTP redirection | N | N |
| * + Static content | N | N |
| * + WebDAV Publishing | N | N |
| * + Health and diagnostics: | N | N |
| * + Custom logging | N | N |
| * + HTTP logging | N | N |
| * + Logging tools | N | N |
| * + ODBC logging | N | N |
| * + Request Monitor | N | N |
| * + Tracing | N | N |
| * Performance features: | N | N |
| * + HTTP compression dynamic | N | N |
| * + Static content compression | N | N |
| * + Security: | N | N |
| * + Basic Authentication | N | N |
| * + Client Certificate Mapping Authentication | N | N |
| * + Digest Authentication | N | N |
| * + IIS Client Certificate Mapping Authentication | N | N |
| * + IP Security | N | N |
| * + Request filtering | N | N |
| * + URL authorization | N | N |
| * + Windows Authentication | N | N |
| Internet Information Services Hostable Web Core | N | N |
| Isolated User Mode | N | N |
| Keyboard Filter | N | N |
| Legacy Components | N | N |
| * Direct Play | N | N |
| Media Features | Y | Y |
| * Windows Media Player | Y | Y |
| Microsoft Message Queue (MSQM) Server | N | N |
| * Microsoft Message Queue (MSQM) Server core: | N | N |
| * + MSMQ Active Directory Domain Services Integration | N | N |
| * + MSMQ HTTP support | N | N |
| * + MSMQ triggers | N | N |
| * + Multicasting support | N | N |
| * MSMQ DCOM proxy | N | N |
| Microsoft Print to PDF | Y | Y |
| Multipoint Connector | N | N |
| Print and Document Services: | Y | Y |
| * LPD Print Service | N | N |
| * LPR Port Monitor | N | N |
| * Scan Management | N | N |
| * Windows Fax and Scan | N | N |
| * Internet Printing client | Y | Y |
| RAS Connection Manager Administration Kit (CMAK) | N | N |
| Remote differential compression API Support | Y | Y |
| RIP Listener | N | N |
| Services for NFS | N | N |
| Simple Network Management Protocol feature | N | N |
| Simple TCPIP Services | N | N |
| SMB 1.0/CIFS Filesharing support | Y | Y |
| Telnet client | N | N |
| Telnet server | N | N |
| TFTP client | N | N |
| Unified Write Filter | N | N |
| Windows Identity Foundation 3.5 | N | N |
| Windows PowerShell 2.0 | Y | Y |
| * Windows PowerShell 2.0 Engine | Y | Y |
| Windows Process Activation Service | N | N |
| Windows TIFF Filter | N | N |
| Work Folders client | Y | Y |
| XPS Services | Y | Y |
| XPS Viewer | Y | Y |

## Proxy configuration

Windows 10 supports three methods to configure a proxy server:

* Auto detect: Windows 10 automatically detects the proxy server based on DNS records;
* Setup script: Windows 10 can use a script, normally a proxy.pac file, to configure when to use a proxy server.
* Manually: The user can manually fill in a proxy server and turn this on and off.

A Windows 10 device, connected to the Smart Workspace corporate network, must use a proxy server to access on the internet. When connected to other networks no proxy server is required.

**Design decision**: Smart Workspace will use DNS records to support auto detection of the proxy server.

# Additional Configuration

## Local administration

By default, users will not be granted administrative rights on their workstations. For administration purposes, an additional account can be created and added to the Administrators group when users require administration permissions.

The following users are member of the Administrators group on all Intune Managed and Azure AD joined devices by default:

* Members of the Global Administrators
* Users given the Device Administrators role permission in AAD

The following users are added to the Administrators group when the device is joined to AAD:

* The user doing a manual Azure AD join
* The user enrolling the device with Autopilot when the profile is configured with Administrator permissions for the enrolling user

**Design decision**: By default, users will not be granted administrative permissions on their workstations. For administration purposes, an additional account can be created and added to the Administrators group when users require administration permissions.

## Folder Redirection

Folder Redirection changes the target location of key folders associated with a given user profile. These local folders are redirected to a remote file share in a seamless manner. Folder Redirection makes use of Offline Files functionality, which allows access to data despite moving between machines or if the remote file share is unavailable.

**Design decision**: Smart Workspace will use no file servers, instead OneDrive will be used to store user data. Default locations will be redirected where possible.

As a result, no roaming profiles will be used as well.

## Branding

Organizational branding allows a consistent user experience from the branding that is normally seen in the environment. Organizational branding allows ensure a standard user experience on every workstation.

Common Branding Items Include:

* Custom Desktop Background
* Custom Windows Lock Screen Image
* Custom User Icons
* Custom Windows Theme Coloring
* OEM/Support Branding

Depending on the setting, branding can be applied to the image or using Group Policy settings.

**Design decision**: Smart Workspace will give the users a free choice in background and theme selection.

A custom lock screen image will be set displaying the Smart Workspace logo.

## Browser configuration

Windows 10 introduces a new web browser; Microsoft Edge. Microsoft Edge, written as a Windows Universal Application, is built for the modern web and a work in progress – IE 11 is the main browser for many enterprises today.

Microsoft Edge’s new rendering engine is built around the idea that the Web “just works,” while being faster, more secure and more reliable. Edge provides several new possibilities:

* **Cortana is built-in and ready to assist;**Cortana in Microsoft Edge is a personal assistant that helps make Web browsing easier. Cortana offers help at just the right moment, based on what she knows about the Web, about the user and what the user might be trying to do. She remains in the background but provides additional information when the user needs it, making browsing easier and more efficient. Cortana in Microsoft Edge will be available in the US versions of this build, and available more broadly later.
* **Inking and sharing;**With the new **inking** capabilities, Microsoft Edge enables the user to write or type directly on the page, comment on what’s interesting or clip what they want – then easily **share** this “Web Note” via mail, or a social network. Researching and collecting information from the Web is just as easy, as they can save their notes directly to OneNote.
* **Distraction-free reading with Reading List and Reading View:**Microsoft Edge offers a new **Reading List** to collect everything the user wants to read, including the ability to save any webpage or PDF for convenient access later. An integrated, distraction-free **Reading View** that keeps the user focused on the content.

Not all websites will work in the Microsoft Edge browser; sites requiring plugins will need to use Internet Explorer or an alternate browser. By using Enterprise Site Mode List, sites can be redirected Internet Explorer. A list of URLs’ can be defined using Group Policy configuration or through Intune.

**Design decision**: Edge will be used as default browser. The Internet Explorer browser is available to users as an alternative. Additional third-party browsers (Chrome and Firefox) can be installed upon user request.

Enterprise Site Mode List will be used when required.

## Cortana

Cortana is an intelligent personal assistant created by Microsoft for multiple platforms, including Windows 10. Cortana's features include being able to set reminders, recognize 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).

**Design decision**: Cortana will be disabled.

## Microsoft Store

The Microsoft Store can be used by end-users to purchase and install public applications in the same way they are used to on their smartphones. The user requires a Microsoft Account (MSA) or a Work-or-School Account (AAD) to access the store. As an alternative, the Microsoft Store for Business can be used.

The Store for Business provides access to a subset of the public Store applications, only approved (purchased) applications are available in the Store for Business. Available apps can be assigned to Azure Active Directory User(-groups) to let users install these apps from the Store for Business or let them be installed with Intune.

**Design decision**: The Microsoft Store for Business will be used to offer only allowed (whitelisted) applications.