Chapter 1

Overview of System Center Configuration Manager and Microsoft Intune

System Center Configuration Manager and Microsoft Intune focus on the management of PCs, servers, and mobile devices, all from a single management console. Microsoft Intune supports both a hybrid scenario as well as a standalone configuration, which will not be covered in this book.

As technology continues to change at an ever increasing rate and with the increased demand to support scenarios such as Bring Your Own Device (BYOD), many organizations are faced with the challenge of finding the right balance between allowing their employees to choose which devices they use versus the management of devices that will need to have access to corporate systems and potentially store corporate data as well as employee personal data.

To support scenarios like BYOD, technologies such as Configuration Manager and Intune are required to provide a comprehensive, cross-platform, and user-centric way to deploy applications and manage user devices, whether they are corporate connected or cloud based.

In this chapter you will learn about the different features of Configuration Manager and Intune, which is a key foundation given future chapters go into far greater detail on each feature available in these products.

A Brief History of Configuration Manager

Before we go much further, let’s take a brief look at the history of Configuration Manager and how it has evolved over the years (see Table 1.1).

<table>
<thead>
<tr>
<th>Release Name</th>
<th>Release Version</th>
<th>Release Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Management Server</td>
<td>1.0</td>
<td>1994</td>
</tr>
<tr>
<td>System Management Server</td>
<td>1.1</td>
<td>1995</td>
</tr>
<tr>
<td>System Management Server</td>
<td>1.2</td>
<td>1996</td>
</tr>
</tbody>
</table>
As you can see from Table 1.1, Configuration Manager has evolved over the years to the latest version, which is known as System Center Configuration Manager (Current Branch).

**NOTE** For now don’t worry about the version numbers such as 1511, 1602, 1606, and so on. We’ll discuss this topic in the “Overview of the New Servicing Model for Configuration Manager” section later in this chapter.

Configuration Manager is a very powerful product with many years of improvements, support, and commitment from Microsoft, the Microsoft Most Valuable Professionals (MVPs), and the community, all of which has resulted in the product that is available today.

### Configuration Manager Features

Before you can begin planning to deploy Configuration Manager, you need a basic understanding of the features it provides. Configuration Manager has its own administrator console, as shown in Figure 1.1.

The major features of Configuration Manager Current Branch are covered next.

#### Application Management

The Application Management feature of Configuration Manager allows you to create, manage, and deploy applications in your environment. This feature also provides monitoring capabilities that allow you to monitor application deployments and take appropriate action in the event of any issues.

The concept of packages and programs from previous versions of Configuration Manager is still supported in Configuration Manager Current Branch, and there may be occasions where you should use these rather than applications (which are explored in Chapter 7, “Application Deployment”).

---

**Table 1.1:** Configuration Manager versions and release dates (continued)

<table>
<thead>
<tr>
<th>RELEASE NAME</th>
<th>RELEASE VERSION</th>
<th>RELEASE DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Management Server</td>
<td>2.0</td>
<td>1999</td>
</tr>
<tr>
<td>System Center Configuration Manager 2007</td>
<td>2007</td>
<td>2007</td>
</tr>
<tr>
<td>System Center Configuration Manager 2012</td>
<td>2012</td>
<td>March 2012</td>
</tr>
<tr>
<td>System Center 2012 R2 Configuration Manager</td>
<td>2012 R2</td>
<td>2013</td>
</tr>
<tr>
<td>System Center Configuration Manager (Current Branch)</td>
<td>1511</td>
<td>December 2015</td>
</tr>
<tr>
<td>System Center Configuration Manager (Current Branch)</td>
<td>1602</td>
<td>March 2016</td>
</tr>
<tr>
<td>System Center Configuration Manager (Current Branch)</td>
<td>1606</td>
<td>July 2016</td>
</tr>
<tr>
<td>System Center Configuration Manager (LTSB)</td>
<td>1606</td>
<td>October 2016</td>
</tr>
</tbody>
</table>
This is probably the most used feature of all the previous versions of Configuration Manager, and it’s probably the most dangerous if not used carefully. It is likely that just about all Configuration Manager admins have accidentally deployed a piece of software that they shouldn’t have (if you haven’t, then keep up the great work!). This isn’t a fault of this feature but something that can happen if you don’t test, test, test, and then test again. Anything you plan on deploying to client computers must be carefully managed, and you must pay close attention to the details of what you are doing.

**Collections**

Collections are simply a way of grouping resources together that share a common criterion such as “Which resources are running Windows 8 with more than 2 GB of RAM, with more than 1 GB of free disk space, and with a certain BIOS version?” Typically collections are based on queries, allowing them to be updated dynamically based on a configurable schedule or by directly assigning resources. Collections can consist of computers, users, user groups, or any discovered resources in the Configuration Manager site database. Collections, as a fundamental feature, have not changed much since previous versions, but they are now the necessary building blocks used to enable other features such as maintenance windows and collection variables, which will be explored in later chapters.

**Company Resource Access**

Using the Company Resource Access feature, you can create and deploy profiles to control access to your company’s resources. Profiles that you can create and deploy include

- Certificates
- Email
Compliance Settings
The Compliance Settings feature is designed to address configuration drift within the enterprise. Enterprise administrators (for workstations and servers) as well as security teams need a tool that enables them to set configuration baselines (based on the Sarbanes–Oxley Act, the Health Insurance Portability and Accountability Act, the Gramm-Leach-Bliley Act, or other compliancy regulations), that contain configuration items detailing how a specific item should be configured (for example, the local guest account should be disabled, Windows Integrated Security for SQL Server should be enabled, and so on). These configuration baselines are then deployed to the appropriate resources and the results reported back to provide details of any configuration drift, thus allowing the appropriate action to be taken.

Microsoft delivers configuration packs that jump-start an organization in the compliance areas mentioned and help you set up a baseline of standards for your workstations and servers, allowing you to audit your environment against that baseline.

You can configure your baselines from scratch, or you can use best practices from Microsoft and their partners in the form of Configuration Manager Configuration Packs, which can be modified if needed. The ability to configure, monitor, and remediate the systems based on specific needs is key to IT operations management and operations on Information Technology Infrastructure Library (ITIL) and Managed Object Format (MOF), respectively. This feature will be covered in Chapter 13.

Endpoint Protection
The Endpoint Protection feature allows you to manage antimalware policies and Windows Firewall security for your Configuration Manager client computers. Endpoint Protection requires a separate license because it installs its own client that is separate from the Configuration Manager client.

Endpoint Protection is covered in Chapter 14, “System Center Endpoint Protection.”

Inventory
Configuration Manager offers you the ability to inventory the hardware and software of devices in your enterprise. Hardware inventory can gather information from your systems such as processor information, the computer manufacturer, and the amount of installed memory. Software inventory can gather lists of file types and their versions installed on your computers, with EXE files as the default. Combine this with extensive information in the Asset Intelligence (AI) knowledge base, and you can use Configuration Manager to get a good handle on what hardware and software is being used in your environment.

Inventory is the backbone of Configuration Manager. Although you can install and run Configuration Manager without enabling Inventory, you wouldn’t be able to do much, since so many other features, such as software updates, require Inventory. We will go into more detail about Inventory in Chapter 10, “Inventory and Software Metering.”
Mobile Device Management
Configuration Manager Current Branch includes two types of mobile device management:

- Mobile Device Management with Windows Intune
- On-premises Mobile Device Management

The following sections provide an overview of these; they are discussed in greater detail in Chapter 19, “Enterprise Mobility and Security.”

Mobile Device Management with Windows Intune
Mobile Device Management (MDM) with Windows Intune allows you to use Configuration Manager to manage Windows Phone, iOS, Android (including Samsung KNOX), and even Windows devices using the Microsoft Intune service over the Internet.

However, even though Intune is used, the actual management tasks are completed by the service connection point, which is a new site system role in Configuration Manager Current Branch.

Using MDM provides the following management capabilities on devices:

- Retire and wipe
- Deployment of line of business applications to devices
- Collect hardware inventory
- Collect software inventory by using built-in reports
- Deploy applications to devices that connect to Windows Store, Windows Phone Store, App Store, or Google Play
- Configure compliance settings such as passwords, security, roaming, encryption, and wireless communication

On-premises Mobile Device Management
As its name suggests, this type of mobile device management allows you to enroll and manage Windows 10 Enterprise PCs and Windows 10 mobile devices using the Configuration Manager infrastructure without the need for a Windows Intune subscription.

Management of these devices is performed by the management functionality built in to supported devices and does not require the Configuration Manager client to be installed.

Operating System Deployment
Operating System Deployment (OSD), as its name suggests, is the ability to deploy an operating system to a machine. Configuration Manager Current Branch includes several improvements to OSD, especially in the distribution of Windows 10 with the inclusion of a new in-place upgrade scenario that can significantly reduce the time and complexity of deploying Windows 10.

As in previous versions, OSD allows you to create and distribute operating system images that include any required updates and applications, to computers both managed and unmanaged by Configuration Manager using PXE boot or bootable media such as USB flash drives, DVD, or CD set.

OSD is discussed in greater detail in Chapter 9, “Operating System Deployment.”
**Power Management**

Saving energy and preserving the environment are important goals for IT professionals and organizations. The Power Management feature allows you to create different power plans that configure Windows’ power management settings on your computers based on your organization’s needs. These plans can then be applied to collections of computers where they will be enforced. Configuration Manager includes various reports relating to power management that allow you to ensure the power settings have been deployed correctly and are in place on the relevant computers.

**Queries**

Queries allow you to retrieve information from the Configuration Manager site database about the resources in your environment that meet certain criteria, such as all machines running a certain version of Windows, or all users running a certain piece of software. Queries can be used to answer questions quickly or make mini-reports that might not be used often enough to be imported into the reporting interface. Of course, queries can be used to create reports, but their primary use is as the basis for *collections*, which we looked at earlier in the “Collections” section.

**Remote Connection Profile**

The Remote Connection Profile feature allows you to create profiles that contain Remote Desktop Connection settings that you can deploy to users in your Configuration Manager hierarchy.

Users can then use the company portal to use Remote Desktop using the Remote Desktop Connection settings deployed to them via the remote connection profile to remotely connect from their Windows, iOS, or Android corporate device to their work computer when they are not connected over the Internet or connected to your domain.

**NOTE** You only need a Microsoft Intune subscription if you want users to be able to connect to their work PC using the company portal. If you don’t have Intune, users can still use a VPN connection to connect to their work PC using Remote Desktop using the settings configured in the remote connection profile.

This feature is discussed in more detail in Chapter 19.

**Remote Control**

The Remote Control feature allows computer support staff to remotely troubleshoot problems with users’ computers just like they are sitting in front of the computer. This feature is still integrated with Remote Assistance and Remote Desktop, and it works pretty much the same as it did in previous versions of Configuration Manager.

This feature is discussed in more detail in Chapter 10.

**Reporting**

The Reporting feature allows you to create and run reports to show data from the Configuration Manager site database for all of the various features, whether it be client installation, inventory, software deployment/updates, or even status or alert messages.
Configuration Manager Current Branch ships with over 400 out-of-the-box reports that you can edit. You can even create your own custom reports using SQL Reporting Services to meet your specific needs.

Reporting is discussed in several chapters and is covered fully in Chapter 12, “Reporting.”

**Software Metering**

Software metering (covered in Chapter 10) allows you to collect information on software usage to assist in managing software purchases and licensing. Using software metering, you can do the following:

- Report on the software that is being used in your environment and on which users are running the software
- Report on the number of concurrent users of a software application
- Report on software license requirements
- Find software that is installed but isn’t being used

The twist to software metering is that the metering rules are automatically populated, or created, but disabled by default, based on the software inventory. This allows you to rapidly meter applications and gain insights into usage. Software metering is part of the Service Measurement process in ITIL and Change and Configuration SMF in MOF. Based on the utilization of software, you can measure when applications are properly used in the environment for better inventory of the current assets.

Software metering is discussed in more detail in Chapter 10.

**Software Updates**

Using this feature, you can manage the daunting task of deploying updates to Microsoft applications and operating systems. Not only does this apply to Microsoft security patches and updates, but having this flexible and extensible environment has allowed partners (such as HP, Dell, IBM, Citrix, and others) to create custom catalogs to update server and desktop BIOS, firmware, and drivers as well as to create internal catalogs. This enables customers to create their line-of-business application update catalogs and update them through the same streamlined process as Microsoft uses for patch management.

Deploying updates require a Windows Server Update Services (WSUS) server. Configuration Manager leverages WSUS with its functionality and provides a higher level of granularity than is available with WSUS alone. Software updates are an important phase in the Incident Management process and IT Operations Management function of ITIL and the Operate Phase in MOF. We will cover software updates in more detail in Chapter 8, “Software Updates.”

**User Data and Profiles Configuration Items**

The user data and profile configuration items in Configuration Manager Current Branch allow you to manage roaming profiles, offline files, and folder redirection on computers running Windows 8.

This feature is discussed in more detail in Chapter 13.
Wake on LAN
The Wake on LAN feature, added to software distribution, was available in SMS 2003 only by purchasing third-party software. It allows you to leverage technology built into computer hardware to wake up computers that have been turned off so they can run assigned deployments. Chapter 7 shows how to enable it.

Asset Intelligence
Asset Intelligence, which was included within Configuration Manager 2007, now comes with its node within the admin console. This is not the only new aspect of Asset Intelligence; AI also became part of the Software + Services initiative within Microsoft. The services component of AI is not a fee-based feature but is just another extension of the holistic approach; it includes the following functionality:

◆ New catalog and license management UI in the Configuration Manager admin console
◆ The ability to customize the local catalog—in other words, create new categories and families
◆ On-demand or scheduled catalog update synchronization through the Configuration Manager console
◆ The ability to tap software assets unknown to the catalog and pass them up to the online service for async identification
◆ The ability to import licensing data from Microsoft and compare it to installed inventory

Asset Inventory is one of the reporting structures used to analyze and ensure that every asset on the system is being used properly and report this to management. We’ll discuss this further in Chapter 11, “Asset Intelligence.”

Application Virtualization Management
With the newest release of App-V, Configuration Manager leverages its existing infrastructure and extends its reach to deliver virtual applications:

◆ It integrates Microsoft App-V 5.0 with Configuration Manager.
◆ Application Virtualization Management (AVM) allows you to use Configuration Manager to manage and deploy virtual applications, when possible, to make managing virtual applications for the Configuration Manager administrator the same experience as managing standard or physical software.
◆ AVM has version checking, user-based targeting, and streaming functionality.
◆ This new version of Configuration Manager integrates with other presentation servers such as Remote Desktop Services’ RemoteApp capability or Citrix XenApp.

Client Health and Monitoring
Configuration Manager displays client health evaluations results and client activities directly in the console, providing alerting and remediation capabilities if health statistics fall below
established thresholds. In this version, you can see several improvements related to client health activities and how the client remediates each of them. Now with the in-place upgrade, you can always have the latest client running in your organization. We will discuss more on this topic in Chapter 6, “Client Health.”

**Microsoft Intune Features**

There are many ways you can benefit from Microsoft Intune. This book will be dedicated to the Cloud Extension with Configuration Manager. However, you can use Microsoft Intune stand-alone as part of your Microsoft Office 365 subscription, or as part of the Microsoft Enterprise Mobility Suite.

The primary features the Intune provides are

- Mobile device management (MDM) that allows you to enroll devices so that they can be provisioned, configured, monitored, and managed
- Mobile application management (MAM) that allows you to publish, push, configure, secure, monitor, and update mobile applications for your users
- Mobile application security that helps you secure mobile data by segregating corporate data from personal data and facilitating just the corporate data to be wiped if required

**Overview of the New Servicing Model for Configuration Manager**

Previous versions of Configuration Manager had a version number such as 2007 or 2012 indicating that they were a major release and the year of their release. In line with Microsoft update policy at the time, service packs, cumulative updates, and “R” releases were typically released throughout the life cycle of the product.

With the advent of Windows 10, things have now changed in Microsoft. Windows 10 will be the last version of Windows with planned updates released every three months, which will be denoted in YYMM format—for example, the November 2015 release of Windows 10 is known as 1511, the February 2016 release is known as 1602, and so forth.

In addition Windows 10 has the following three servicing branches:

- Current Branch (CB)
- Current Branch for Business (CBB)
- Long-Term Servicing Branch (LTSB)

In a nutshell these different branches allow users to control how often they want to update their version of Windows 10 going from every three months in the case of CB through to once a year in the case of LTSB.

More information can be found here:


Does this affect Configuration Manager? Yes and no. Configuration Manager has adopted the Windows 10 servicing model partially. For example, Configuration Manager now does not use
version numbers but instead uses the YYMM format, with 1511 being the first release of the new version.

As of this writing, there is also only one servicing branch for Configuration Manager and that is Current Branch (CB), which is designed to keep pace with Windows 10 and its CB releases.

**Baseline vs. Incremental Update Versions**

Microsoft will periodically release what is known as a *baseline* release. In other words, for a new installation this is the minimum version you will need to start with (as of this writing, the latest baseline version for Configuration Manager CB is 1606).

Then every three to four months Microsoft will release an update known as an *incremental update version* that you install on top of the baseline version. These updates will still have the YYMM format, so in the case of Configuration Manager CB the first incremental update, known as 1602, was completed in February 2016. The next scheduled release as of this writing (known as 1610) is due for completion in December 2016.

Incremental updates have the following features:

◆ They replace service packs and cumulative updates used in previous versions.

◆ They contain both fixes and new features, giving you the flexibility to control which new features you use and when.

◆ You decide which updates you install and when.

◆ Once you decide to install an update, Configuration Manager will automatically upgrade all of the relevant components such as the site server and its components, consoles, and clients. If you are running a remote console, the next time you load it and it connects to a site running a later version, you will receive a notification that an updated console is available and you will be offered the opportunity to install it.

◆ You no longer need to download and install the updates manually. Incremental updates now appear automatically in the new “Updates and Servicing” node of the Configuration Manager console (located in the Administration workspace under Cloud Services). A key benefit of this is that you will know when an update is available rather than encountering an issue and then discovering a fix was released for it that you weren’t aware of.

You will learn more about the Configuration Manager Current Branch servicing model in Chapter 18, “Hierarchy Planning.”

**Overview of the Servicing Model for System Center Configuration Manager**

Two versions of Configuration Manager are available today: the Current Branch and the Technical Preview. Those in the Technical Preview space will receive monthly releases—for example, 1512, 1601, 1602, and 1603 (see Figure 1.2). This will give Technical Preview users the ability to test and validate new product capabilities that may be released to the Current branch.
The Current Branch will receive updates that have been tested and declared ready for enterprises; this release may follow a different path than the Technical Preview. In this example, the releases may look like this: 1602, 1606, and 1610 (see Figure 1.3). These updates will be available for enterprises to upgrade to those Current Branch releases and be able to update their infrastructures to those builds.

The Software as a Service (SaaS) model will give customers an edge on the latest capabilities of the product and will show what is coming next and how can they be ready for a Current Branch release. You should have both versions in your infrastructure so that you can understand what is coming next.

The Update Process
To access the latest build, you must go to Configuration Manager Console ➤ Administration Workspace ➤ Cloud Services and click on Updates and Servicing. Once there, you will be able to see the latest update of Current Branch that you can choose. From here, you can right-click or use the ribbon to run the prerequisites check, as you can see in Figure 1.4. Doing so will validate that the site meets the requirements to perform the upgrade; this is key to ensure the site will be updated to the Current Branch, as shown in Figure 1.5.
Once the tool finishes validating the requirements, you will be able to install the update. Download the updates using the DMPDownloader and store this information in the EasySetupPayload folder (see Figure 1.6).

To validate the progress of the prerequisites check from the servicing, you can choose Monitoring Workspace > Site Servicing Status and you will be able to see the status there, as in Figure 1.7.
Once the prerequisites check is completed, in the console under Updates and Servicing, Yes will appear under Prereq Only, as you can see in Figure 1.8.

**Figure 1.8**
Prereq Only

Now you are ready to install the Current Branch to your site. All you have to do is right-click on the Current Branch update and click Install Update Pack. Doing so will launch the Configuration Manager Updates Wizard, as you can see in Figure 1.9.

**Figure 1.9**
Configuration Manager Updates Wizard in the Technical Preview

Once in this wizard, click Next once. In the Features Included In Update Pack page, you will see what is available in that pack (Figure 1.10); then click Next.
You will then see the Options For Client Update page (Figure 1.11). Here you will have to decide if you want to continue the upgrade without validation or if you want to choose Validate In Pre-Production Collection. For a production environment, we recommend that you select Validate In Pre-Production Collection before releasing the new client version to production.
Then you will accept the licensing and review the update in the Summary section. Finally, click Next to finish the update wizard. This process will take some time; you can monitor the progress on the monitoring workspace as shown in Figure 1.7.

This update process is simpler than earlier updates or cumulative updates process.

**Summary**

With this understanding of Configuration Manager Current Branch, you have a foundation for the upcoming chapters. In the next chapter, you will learn about planning a Configuration Manager infrastructure.