Mastering System Center Configuration Manager

Master how to configure, back up, and secure access to System Center Configuration Manager with this practical guide

Vangel Krstevski
In this package, you will find:

- The author biography
- A preview chapter from the book, Chapter 2 'Assets and Compliance'
- A synopsis of the book’s content
- More information on Mastering System Center Configuration Manager

About the Author

**Vangel Krstevski** is an IT engineer with 5 years of experience in engineering IT Systems based on Microsoft guidelines. He is a strong team player with an affinity for details. His strengths include excellent communication skills, hands-on experience with various Microsoft products, and the ability to manage conflicts and accomplish demands to the agreed standards and timelines. He is currently employed by Re-Aktiv, a software development and consultancy company from Skopje, Macedonia, which specializes in the area of electronic services and company public registry solutions. His main areas of expertise are server virtualization, hybrid cloud scenario design and implementation, and Business Continuity along with System Center. He has worked on many projects, both internal and commercial, as a consultant for Microsoft server-side platforms. He has already written a book titled *Hyper-V Replica Essentials*, Packt Publishing, which helps organizations to implement business continuity and disaster recovery strategies.

I would like to thank my family, friends, and colleagues for supporting me, especially my girlfriend, Monika, who stood by me and gave me support and motivation during the process of writing of this book.
Mastering System Center Configuration Manager

Microsoft System Center Configuration Manager is a powerful System Management product that helps IT administrators with better asset management and organization by grouping them into logical containers. These logical containers allow you to make the deployment of applications easier, software and security updates, antimalware definitions, and so on. Configuration Manager assists you in operating system deployment, allowing you to deploy OS images to multiple target systems at the same time. It also empowers users to be more productive from anywhere on any device by implementing state-of-the-art mobile device management functionalities.

What This Book Covers

Chapter 1, Introduction to System Center Configuration Manager 2012 R2, is all about the initial setup of Configuration Manager 2012 R2. It shows you how to install and set up all the prerequisites and requirements. In the end, there is an explanation on System Center Configuration Manager sites and site hierarchy and all of the site features and functionalities.

Chapter 2, Assets and Compliance, is more about compliance settings and Endpoint Protection. Compliance settings, with knowledge and creativity, can give you feedback about the configuration and compliance of your Windows-based systems and mobile devices.

Chapter 3, The Software Library, explains the different ways in which you can deploy software and also explains how you can use System Center Configuration Manager to do this. It gives you an overview of what applications are and how to create them in Configuration Manager, how to make deployment types, and how to create different detection rules.

Chapter 4, Reporting in Configuration Manager, explains how SQL Server Reporting Services give you the opportunity to show the information contained in the Configuration manager database using SSRS reporting.

Chapter 5, Administration and Monitoring, describes the way in which the System Center Configuration Manager hierarchy is organized. Towards the end, it discusses all the aspects of client settings and how to use these settings to make an optimal configuration for your business needs.
Chapter 6, *Cloud Integration*, describes the benefits of a public cloud, specifically Windows Azure, and explains how you can use System Center Configuration Manager 2012 R2 to deliver application packages to your clients that run on different mobile device operating systems.

Chapter 7, *Security and Backup*, describes the infrastructure security for Configuration Manager and the delegation of administrative access. This chapter includes a detailed description of a new role-based administration model and an overview of the Configuration Manager controls and security accounts.

Chapter 8, *Troubleshooting*, presents the different aspects of how to troubleshoot issues related to the functionalities of Configuration Manager. It begins with common network-related issues and continues by explaining common Configuration Manager console issues.
The Asset Intelligence section of System Center Configuration Manager 2012 R2 gives you the ability to build inventories of your software licenses and also lets you manage them. It gives you an overview of the software installed on your infrastructure by keeping an Asset Intelligence catalog. Asset Intelligence uses Windows Management Instrumentation (WMI) to extract more detailed information from the hardware and software that is being used. SCCM 2012 R2 gives the users more than 60 different reports about the gathered asset information and displays them in a format that is easy to read. Most reports lead to more specific reports, where you can create custom queries to get detailed information. You can add custom information, such as custom software categories, software families, software labels, and hardware requirements, to the Asset Intelligence catalog.

SCCM 2012 R2 delivers an integrated, intelligent, and comprehensive overview of your company's software installations. It helps reduce the total cost of ownership of your application management life cycle, making software inventories by scanning all the hardware resources and translating inventoried data into useful information. You can limit software license usage by importing software license information into the Configuration Manager site's database. Asset Intelligence is very useful for keeping track of all the assets in your infrastructure, including software and hardware. The Asset Intelligence functionality in SCCM 2012 R2 can be used to inventory and report software that is in use in your infrastructure.
The benefits of centralized system management

System Center Configuration Manager 2012 R2 provides various means to manage and deliver different types of user experience, which might be based on identity, connectivity, and types of devices, all of this without having to give up control over protecting your assets. The following are the benefits of implementing System Center Configuration Manager 2012 R2:

• Workstation management: Online System Center offers a solution to the challenge of consumerization by enabling the management and monitoring of workstations and mobile devices, irrespective of whether they belong to the employer or the employee, regardless of their location. Device management is based on Microsoft System Center 2012 Configuration Manager using clients that can be installed from the management portal. Management features include asset inventory, software distribution, patch management, and deployment of images. In addition to these, Online System Center offers a comprehensive software packaging service with an option to automatize workstation preinstallations. You can read more about Online System Center at [http://www.onlinesystemcenter.com](http://www.onlinesystemcenter.com).

• Mobile device management: Mobile device management enables the management of diverse mobile operating systems and smartphones, irrespective of whether they belong to the employer or the employee and the location. You can see all the included functions for mobile device management at [http://technet.microsoft.com/en-us/library/dn376523.aspx#bkmk_comps](http://technet.microsoft.com/en-us/library/dn376523.aspx#bkmk_comps).

• Enables users to be productive from anywhere on any device: This is done through a mechanism to manage a wide range of mobile devices using a single administration console. The product provides optimized and personalized application delivery, based on user identity, device type, and network capabilities. It also allows users to self-provision the application with the help of an online web-based application catalog. To use this function, you require a Windows Intune subscription.
• A unified management of the infrastructure, integrating client management functionalities and protecting against threats: Configuration Manager provides a single tool to manage all your client environments. It consolidates inventory management, software delivery, vulnerability prevention and remediation, and compliance reporting with a single infrastructure. It also offers remote controls, metering, operating system deployment, and so on.

• Simplified administration

In addition, System Center Configuration Manager 2012 R2 continues to get more integrated and comes with a common look and feel between the consoles of the various components. Combined with data integration between those components, both operationally and in a consolidated data warehouse, it gets more intertwined with cloud computing.

Managing compliance

Compliance settings provide you with the ability to define, monitor, enforce, and report a configuration's compliance. Compliance settings can handle the following scenarios, which all IT organizations have to deal with:

• Regulatory compliance: Regulatory compliance is a key scenario in many IT organizations. Regulatory compliance requires IT organizations to specify the security and privacy policies for corporate and user data as well as for IT systems. The difficult part for IT is to enforce and report on the enforcement of the set standards. Some IT companies find it difficult to enforce these policies and rely on scripts and tools that provide results on demand.

• Change verification: This scenario is used to verify a system's configuration before and after the planned changes have occurred. It allows you to confirm whether you are applying the changes to the specified systems.

• Configuration drift: This scenario is very common and known to IT personnel, but most IT companies do not consider the configuration drift. The drift starts when a system goes into production; as soon as multiple IT administrators start to deploy applications, troubleshoot issues, and so on, the system begins its drift from the standard. Over time, this drift can become unpredictable and can cause technical issues.
Assets and Compliance

• Time to resolution: Most problems in the IT world occur due to human errors. These problems become the problem ticket that administrators have to handle. Stopping human errors is impossible, but identifying the human error quickly so that it can be resolved is the key to reducing the impact of such errors.

These scenarios come one by one or in combination, and they place a great overhead on IT. There is a small reward when they are successfully handled because they do not impact the business demand directly, and that is why they are liked less by the IT administrators. Compliance management doesn't eliminate these scenarios, but it makes them more manageable.

System Center Configuration Manager 2012 R2 has many new features, such as the following:

• A unified compliance and settings management across servers, desktops, laptops, and mobile devices
• Simplified administrator experience
• Role-based administration
• Simplified baseline creation experience
• Deployment of baselines
• The user and device targeting of baselines
• Defines compliance service-level agreements (SLAs) for baseline deployments and alert generation
• Monitors the baseline deployment compliance status
• Updated reports to include remediation, conflicts, and error reporting
• An automatic remediation for registry values, Windows Management Instrumentation (WMI) values, and script-based compliance checks
• Configuration item revisioning
• The migration of the existing Configuration Manager 2007 baselines and compliance items (configuration items)
Configuring compliance settings

Compliance settings are very easy to configure, unlike some other Configuration Manager features. The only prerequisites are the Configuration Manager installation and the client setting configuration, which will be discussed later. The client does all the processing and returns results to the server. The only requirements on the client side are as follows:

- Clients must have the Configuration Manager 2012 R2 Client agent installed
- Clients must have the .NET framework 2.0 installed

To enable compliance settings, proceed with the following steps:

1. Go to the Administration section and select client settings. Here, you can edit the existing settings or create a new set of client settings.
2. To edit the existing set, right-click on it and select properties. If you want to create a new set of settings, select Create Custom Client Device Settings.
3. After the client settings are deployed, the client's compliance settings are enabled on the client. This is all that is required to configure Configuration Manager compliance management.

Configuration items and baselines

Compliance is configured by creating two object types:

- Configuration items: This is a set of settings and criteria that define what is compared, checked, and evaluated.
- Configuration baselines: This is a group of multiple configuration items. Configuration items must be part of a configuration baseline for them to be subjected to evaluation by a collection of systems.

There are many combinations of compliance settings because each organization is unique and requires a specific configuration of the system. Compliance settings give you the tools that help you create configuration items and baselines from scratch, according to your specific needs and wants. The following two topics explain the details of baselines and configuration items and the editor used to create and modify them.
**Configuration items**

Configuration items are used to encapsulate all the checks that compliance settings perform against the target system to determine its compliance. These checks are also called the evaluation criteria. To view or edit the configuration items on a particular site, click on the **Assets and Compliance** section of the Configuration Manager console and select **Compliance Settings**.

You can use search filters and saved searches to find specific configuration items, or you can just limit the results from the search that is displayed. Some of the most used search criteria are the following:

- **Revision**: This field shows the highest number of revisions of the configuration item
- **Child**: This field shows that a configuration item is a child item
- **Relationship**: This field shows that the configuration item is a parent of another configuration item
- **Categories**: This field shows the categories that the item belongs to
- **Device type**: This can be either a Windows configuration item or a mobile configuration item

In addition, there are four configuration item types:

- **Applications**: This configuration item checks whether an application exists on a target machine and checks the corresponding settings.
- **Software updates**: This configuration update checks the patch and update levels of a target system. The evaluation criteria are the installation statuses of the patch or the update. To use this configuration item, you first need to configure the Configuration Manager Software Update feature.
- **Operating system**: This configuration item looks for a specific operating system's version and settings. The version is selected from a preconfigured drop-down list.
- **General**: This configuration item is used for mobile devices.

In order to create a new configuration item, you have to select **Create Configuration Item** from the ribbon at the top or right-click on the context menu. This will start a wizard that will guide you through the rest of the process. The following are the steps that you need to perform for all the options:

- **General**: In this page, specify the name of the configuration item and its description. The choice you make determines which pages will be shown.
Configuration item: In addition, you have to select the type of configuration item that you want to create:

- **Windows**: This is applied only to Windows systems.
- **Mobile device**: This is applied to fully supported mobile devices, but it does not include devices managed by the Exchange ActiveSync Connector. To see the full list of supported devices, go to [http://technet.microsoft.com/en-us/library/gg682077.aspx](http://technet.microsoft.com/en-us/library/gg682077.aspx).

Detection methods: This page is only for Windows configuration items and is only shown if the This configuration item contains application settings checkbox is checked in the general tab. Here, you specify the criteria for application detection. There are three ways to do this:

- **Always assume that the application is installed**: This means that the client always assumes that the application is installed.
- **Use Windows installer detection**: This setting uses the Windows installer list of products to determine whether the application exists on the target system. If the application is not installed with MSI, then this method cannot be applied. You can also use WMI to determine the application's version and GUID. Here is the command-line syntax to do that:
  
  ```cmd
  wmic product where "caption like '%Live%'" get name, IdentifyingNumber, version
  ```

- **Custom scripts**: This method uses a custom script (VBScript, Jscript, or PowerShell-based) to detect the installation of an application. The script should return some text to indicate the successful detection of an installed application and should not return text to indicate failure. A simple example of VBScript to detect the installation of the Internet Explorer Administration Kit 7 is given as follows:

  ```vbs
  folderPath = "C:\Program Files\Microsoft IEAK 7"
  Set fso = CreateObject("Scripting.FileSystemObject")
  If fso.FolderExists(folderPath) Then
    WScript.Echo "IEAK 7 Found"
  End If
  ```
• **Settings:** In this page, you can configure the settings that the client will evaluate. You can specify the following:
  - Name
  - Description
  - Setting type
  - Data type

• **Compliance rules:** These rules determine how the client will evaluate each setting in a configuration item. Without compliance rules, settings are meaningless.

• **Supported platforms:** In this page, you can select the platforms that this configuration item applies. All the supported versions of Windows and all mobile device platforms are listed. If the client platform is not listed, the configuration item is not evaluated.

• **Mobile device settings:** Here, you specify a group of settings that the client will evaluate on the target mobile device system. Each selected group will add new pages to the wizard.

• **Platform applicability:** This page shows all the mobile device settings chosen and configured on the mobile device settings page.

• **Summary:** This is a list of all the choices you made in the wizard.

• **Progress:** This shows the progress in creating the configuration item.

• **Completion:** This is the results page that lists the errors that occurred and the warnings that were given during the item creation process.

### Configuration baselines

Configuration baselines are groups of configuration items. Configuration baselines are always deployed to collections that need evaluation. You can add any number of items to a baseline. Also, you can add a baseline in a baseline. The result is a group of settings of the configuration items it contains. To start configuring baselines, go to the **Compliance Settings** menu in the **Assets and Compliance** section of the Configuration Manager console and select **Baselines**. You can limit the displayed baselines using the following search filters:

• **Revision:** This shows the highest number of revisions of the configuration baseline

• **Compliance count:** This shows the number of systems that comply with the baseline
• **Noncompliance count**: This shows the number of systems that do not comply with the baseline

• **Failure count**: This shows the number of systems that encountered an error during evaluation

• **Categories**: This shows the defined categories for the configuration baseline

To create a new baseline, you have to select **Create Configuration Baseline** from the ribbon bar or right-click on the context menu. On the first page, specify the name and description of the baseline. In the bottom of the page, select all the categories that this baseline will belong to. Categories don't have any function out of the Configuration Manager console.

The main activity in baseline creation is to select the configuration data that it will contain. This can be done using the **Add** button from the configuration data listbox. Three options are available:

• **Configuration items**

• **Software updates**

• **Configuration baselines**

Application configuration items can have one of the following purposes:

• **Requires**: The application defined in the configuration item must exist on the target system

• **Optional**: Settings are evaluated only if the application exists on the target system

• **Prohibited**: The application in the configuration item must now exist on the target system

Software updates are always set as required, and they must always exist on the target system. Like software updates, baselines are also set as required, but this means nothing because the important aspect here is the evaluation condition of the configuration items it contains. To modify a baseline, select the baseline and choose **Properties** from the ribbon or right-click on the context menu. You can also disable a baseline from the ribbon or by right-clicking on the context menu.
Baseline deployment
Baselines are deployed on a set of target client systems defined by a collection. Each baseline has a different evaluation schedule defined in the default client settings for the hierarchy. To deploy a baseline, select the configuration baselines node or any other configuration baseline and choose Deploy from the ribbon bar or right-click on the context menu. This opens up the Deploy Baseline dialog, which contains the following information:

- Included configuration baselines
- Remediation for noncompliant rules
- Console alert generation
- System Center Operations Manager alerts
- Target collection
- The baseline evaluation schedule

You can deploy baselines to either user or device collections. If a baseline contains user evaluation criteria, only these criteria will be evaluated. This means that when you deploy a baseline make sure that you have at least one valuation criteria for a user or a device.

System Center Configuration Manager keeps track of all the baseline deployments. To view all the deployments for a baseline, select the baseline; at the bottom, you will see a details pane. This pane has a Deployment tab. If you select this tab, you will see all the deployments for the selected baseline. In order to examine or modify a deployment, you can go to the Monitoring section of the Configuration Manager console and click on the Deployments node. You will find all the deployments here, not just the baseline deployments. There is a console search and filtering functionality that you can use to find deployments that you want to view or modify. One thing that needs to be mentioned here is that you cannot delete a deployment from the Monitoring section. You must delete the baseline from the Assets and Compliance section. To modify a deployment, select it and choose Properties from the ribbon bar or right-click on the context menu.

Compliance evaluation
Clients receive compliance baseline deployments from the Management Point, which is set in the client policy. The information needed for configuration settings' compliance scans often takes more than one client-policy refresh cycle to be staged on the client side. During this, the status of the scan will not match the expectations.
According to baseline deployment, clients evaluate configuration items from the baseline using compliance rules and evaluation schedules. The evaluation usually starts a couple of hours after the start defined in the schedule. There are four different compliance states for a baseline deployment:

- **Compliant**: This means that the target system is in line with the compliance rules in the baseline evaluation conditions
- **Error**: This means that an error occurred on the client system while evaluating the baseline
- **Noncompliant**: This means that the target system is not in line with the compliance rules in the baseline evaluation condition
- **Unknown**: This means that the target system has not reported its status for the baseline

When a compliance rule fails, the configuration item, as a whole, is marked as noncompliant and one of the following noncompliance messages is reported:

- None
- Information
- Warning
- Critical
- Critical with an event

Compliance rules that fail with the critical event's noncompliant message add an entry to the Windows application event log. Based on these entries, you can configure actions in the scheduled tasks or you can use System Center Operations Manager to generate alerts. Baseline and configuration item evaluations are client-side tasks. Results are sent to the site using the state message mechanism inside the Configuration Manager. You can read more about this mechanism at the following blog:


Configuration Manager clients keep a baseline evaluation cache of 15 minutes. The client will not evaluate the baseline until this 15-minute interval expires, unless the baseline deployment has changed. Even if it is configured for a shorter evaluation period or for a manual trigger, the evaluation using System Center Configuration Manager control panel applet.
Configuration packs
System Center Configuration Manager has a large number of predefined configuration baselines that can be used as a starting point. This is because the requirements between different IT organizations are similar. They are contained in a configuration pack, which is analogous to a management pack in System Center Operations Manager. Configuration packs such as management packs can be downloaded for free from the following link:


The types of configuration packs available for download are:

- **Regulatory compliance**: These configuration packs are for regulatory compliance, such as SOX, HIPAA, or EUDPD.
- **Best practices**: These configuration packs are made from the best practices followed by Microsoft's internal IT departments.
- **Third-party software and hardware**: Similar to the management packs in System Center Operations Manager, which include many packs developed for third-party software and hardware, there are configuration packs designed and developed for configuration enforcement for third-party application software.

There are many configuration packs for Configuration Manager 2007 that are compatible with System Center Configuration Manager 2012 R2. When you download the configuration pack, the next thing you have to do is to install it. To do this, you have to perform the following steps:

1. Open the **Assets and Compliance** section from the console.
2. Select configuration items or configuration baselines and then select **Import Configuration Data** from the ribbon or right-click on the context menu.
3. This will start the import configuration wizard, and on the **Select Files** page, click on the **Add** button to browse the CAB file of the configuration pack. You can also import multiple CAB files.
4. Click on **Next** to proceed to the **Summary** page, where you can go through the configuration items and baselines included in the configuration pack that is being imported.
5. Complete the wizard.
Exporting configuration items and baselines

Exporting configuration items and baselines gives you the ability to share them with a different Configuration Manager site; you can edit them or view them in a native XML format.

The export created a CAB file in a specified folder during the export. The CAB file is an XML file, so if you are familiar with it you can edit the XML file. The XML file can also be viewed from the console by clicking on View xml definition.

Compliance authoring

Configuration Manager is responsible for creating, organizing, editing, and deploying compliance settings. The biggest challenge is when you have to translate business requirements into Configuration Manager items.

Organization

The organization of configuration items in configuration baselines is very important, just as in the case of organizing individual policies within Group Policy Objects. Actually, you don't need any organization. If you put all the settings in one configuration item and baseline, you are done. However, the problem is when something goes wrong and you have to troubleshoot an issue. Organize similar settings into a single configuration item; for example, put all the settings for Internet Explorer into one configuration item. For more isolation, you can create a baseline with just one configuration item.

Although this is a good practice and creates isolation, it creates a lot of configuration items and more overhead for administration. Think of the configuration items as building blocks representing atomic units of functionality. Combining these in different ways results in a diverse and comprehensive set of baselines that are easier to maintain and troubleshoot.

Evaluation is mostly quick and has no major impact on the client system. However, it is possible to create complex configuration items or baselines with a lot of configuration settings, but this will affect the target system. Software updates' compliance terms have a great impact on the client performance, especially when many are packed in one baseline. Test the baseline before deploying it so that you ensure that it won't affect performance on the target system. Scripts also have a great impact on target systems and because of this Configuration Manager 2012 R2 has a 1-minute timeout for scripts.
Using Microsoft tools
A great way to start configuring compliance settings is with the help of Microsoft configuration packs. They provide great examples and are good to use as a reference because they can teach you about compliance settings. Many of the evaluation checks are performed by custom scripts, and you can use them in your own configuration settings as well as easily modify them.

Security Compliance Manager
Security Compliance Manager is a Microsoft tool that is free for download. You can download it from the following link:


This tool can help you to create and manage configuration baselines. The difference is that it cannot apply baselines to target systems and that is why it relies on Configuration Manager and group policies to do that. This tool includes a lot of baselines that cover the Windows, Microsoft Office, and Internet Explorer configurations. SCM has the capability to import a Group Policy Object, and this is a great way to start your baseline creation. When you have defined your baseline configuration, you can export it and import the Configuration Manager compliance settings.

CP Studio
This is a third-party application from Silect Software (http://www.silect.com). It is similar to SCM because it offers the authoring of configuration baselines and configuration items. This allows IT administrators to create baselines without the Configuration Manager console. CP Studio provides a rich and intuitive environment for baseline creation. This is important because it shortens the development life cycle of configuration baselines and decreases the time needed for baselines to be put into production.
The compliance strategy

All of the functionalities regarding compliance settings are relatively straightforward. You have to create the settings and deploy them. However, the main thing is what should be done after that. Configuration manager clients will accumulate data, and you have to decide what is to be done with this data. Some of the goals might be satisfying business goals, creating reports, troubleshooting, correcting nonstandard configurations, and so on. Every baseline that you create can address some of these goals. So, that is why the first thing to do is to identify the baseline's purpose, target, and delivery method. The following three parameters define what you put inside a baseline:

- **Reporting**: This consists of another way to view and distribute the compliance results of the deployed baselines.
- **Alerting**: This consists of raising real-time alerts of the evaluation results of a baseline.
- **On-demand results**: This deals with client-side report generation. You can trigger the evaluation on the clients of selected baselines.

Endpoint Protection

Configuration Manager 2007 provided Endpoint Protection as an add-on. In the newest release of Configuration Manager 2012 and 2012 R2, this is a built-in feature. Endpoint Protection allows IT administrators to monitor and control the security state of the client workstations from one console and perform easy administration tasks.

Integrating client management and client security in one console cuts down costs. IT administrators now focus on end-to-end security tasks and manage, report, and react to issues with clients from a common console. The best features of Endpoint Protection are as follows:

- **Licensing**: To implement Endpoint Protection, you need to have a license to use it. The license is called Core Client Access License or CAL.
- **Customizable**: You can create custom client settings and target different device collections. You can find preconfigured malware policies to speed up the deployment process.
• **Separate client:** Endpoint Protection uses a different client from the one that the Configuration Manager uses. The functionalities of the System Center Endpoint Protection client are:

  o Easy to deploy
  o Autouninstallation of third-party software
  o Malware and spyware detection and remediation
  o Rootkit detection and remediation
  o Vulnerability assessment and automatic definition updates
  o Integrated with the Windows firewall
  o Network vulnerability detection using a network inspection system

In System Center Configuration Manager 2012 and 2012 R2, in order to configure Endpoint Protection, you need to enable the site system role. You do not have to run a separate installer, and you also don’t need a different console. You can go to the Monitoring section and see the **Endpoint Protection** menu. The administration of Endpoint Protection is very simple because it is role-based. You can create security roles and assign them to specific users from your company. System Center Endpoint Protection, on a target client machine, is installed together with the Configuration Manager client. If no other malware policy exists, the default malware policy is included in it. This happens when System Center Endpoint Protection is enabled in the default client settings. Endpoint Protection uses the same database as the Configuration Manager, so you do not need to install a separate database. Endpoint Protection uses real-time e-mail notifications.

**Prerequisites for Endpoint Protection**

Before installing Endpoint Protection, you have to fulfill these prerequisites:

• **Windows Server Update Services** are required if you are using the Configuration Manager software update point role to deliver antimalware definition updates.

• If you want to deploy firewall policies to Windows Server 2008 or Windows Vista SP1, you must install this hotfix:

  [http://support.microsoft.com/kb/971800](http://support.microsoft.com/kb/971800)

• One of the options for client computers to synchronize antimalware definition updates is to have Internet access.

• The Endpoint Protection site system role must be running on your central administration site or on a primary site and on a site system server only.
• A software update point must be installed and configured in order to deliver definitions and updates.
• You must install reporting services and the reporting services point to display Endpoint Protection reports.
• Security permissions must be defined to manage Endpoint Protection. There is a built-in security role called Endpoint Protection Manager; this grants permissions to define and monitor security policies.

Planning for Endpoint Protection
Enabling Endpoint Protection point site system role is very easy, but you should carefully plan how you will deploy agents in your hierarchy. It is strongly recommended that you don’t use the default client settings, as this will propagate them to all the clients.

Creating client settings and antimalware policies
A best practice is to create custom client settings for Endpoint Protection and to deploy them to a collection that is created only for Endpoint Protection. You can create many custom client settings for Endpoint Protection to target computers with settings suited for function and purpose. Also, a good practice is to create different policies for servers and clients because you want to configure them in a way such that you can ignore or bypass certain Windows processes, processors, and disk load that would degrade the server's performance. You should create different antimalware policies for the different server platforms they target. Microsoft also provides server-specific antimalware policies that you can import and customize according to your needs. A good example of one of these policies is the built-in policy for Configuration Manager 2012, which is SCEP12_Default_ConfigMgr2012.xml. This policy combines the default server's workload policy settings with settings that are optimized for System Center 2012 Configuration Manager, in particular the settings for file and folder exclusions. The logic here is that server-specific roles do certain things repeatedly and consistently, and you want your antimalware solution to exclude certain processes and files that are regularly used by that specific server role.

A failure to add these exclusions can affect the server performance and cause additional issues, such as loss of communication and network issues.
Deploying to a test collection

Prior to the initial setup of Endpoint Protection in your hierarchy, you should always deploy the agent to a test collection in order to test the settings. This will verify that your custom client settings and antimalware policies function properly on the target system. A definition or an engine update can cause problems on the client computer. Usually, these problems manifest with a blue screen of death or some hardware scenarios. Some updates even block files that might be vital to the business. When you face this kind of a scenario, you can deploy a script through packages/programs. The script should run the following code:

    mpcmdrun.exe –removedefinitions [All]

This will remove any updates and will revert to the previous definition. Also, make sure that you prevent the client from installing the updates again. Endpoint Protection in System Center Configuration Manager 2012 does not contain any of the collections that Manager 2007 came with. Those collections were used to sort computers with malware-related issues into predefined locked-query based collections. You could not edit or view the queries in such collections; however, third parties later released the contents of these queries online in an Excel format, just in case you want to recreate the collections. You don't have to create these collections in System Center 2012 Endpoint Protection; the Endpoint Protection status dashboard replaces this functionality by letting you see the malware and operational state of the entire selected collection. These items are clickable, allowing the administrator to drill down into reports or take recommended actions. Here are the malware remediation status items that are viewable in the dashboard:

- Remediation failed
- Full scan required
- Restart required
- Offline scan required
- Client settings modified by malware
- Malware remediated in the last 24 hours

In addition to the functionality in the dashboard, you can easily build collections based on the new Endpoint Protection classes; these are the same classes as the ones used in the predefined FEP 2010 collections, making those collections unnecessary as you can easily build your own. You have to create separate custom client and antimalware policies and then target device collections. To do this, you can create folders specific to Endpoint Protection, such as:

- Endpoint Protection managed client computers
- Endpoint Protection managed server
After this, you can put a device collection into these folders and target them with different custom client settings and antimalware policies. Servers are critical to the organization, so you should create multiple server device collections to separate different server roles. This is a best practice because SQL Server should be treated differently than Hyper-V hosts or other types of servers, for example, a Web server.

The suggested device collection name for Windows client computers is Endpoint Protection Managed Desktop and Laptops, which can be created in the Endpoint Protection managed client computers' folder that we talked about earlier. Use these device collections only for Endpoint Protection, and create other device collections for other deployments. Here is a list of the suggested collections:

- Endpoint Protection Managed Servers – Domain Controller
- Endpoint Protection Managed Servers – Exchange
- Endpoint Protection Managed Servers – Operations Manager
- Endpoint Protection Managed Servers – Configuration Manager
- Endpoint Protection Managed Servers – SQL 2008
- Endpoint Protection Managed Servers – File Server
- Endpoint Protection Managed Servers – Service Manager
- Endpoint Protection Managed Servers – Data Protection Manager
- Endpoint Protection Managed Servers – IIS Web Server
- Endpoint Protection Managed Servers – Hyper-V
- Endpoint Protection Managed Servers – Terminal Server
- Endpoint Protection Managed Servers – Other Servers

You should place all of the device collections in the Endpoint Protection Managed Servers folder and target them with antimalware policies that best suit them. The key point here is to target specific server roles with customized antimalware rule sets configured to allow optimum performance and availability, even when they are protected via Endpoint Protection. The SCEP client can handle servers in multiple device collections targeted by multiple antimalware policies; however, the policy with the highest priority takes precedence. You can also mix policies for different server roles and combine them into one.
Installing the Endpoint Protection role

Prior to installing the Endpoint Protection role, you must determine its place in the Configuration Manager hierarchy. If you have multiple sites in your hierarchy, you have to install the role on top of these sites in your Central Administration site. If you have a standalone primary site, you have to install the role on it. The Endpoint Protection role can be installed only on one site system server in the Configuration Manager hierarchy. When you enable the Endpoint Protection role, the following actions are performed:

- You are presented with the EULA or the end user’s license agreement
- The default Microsoft active protection service configuration is set
- The System Center Endpoint Protection client is installed on the server hosting the role

When you enable the Endpoint Protection role, the Endpoint Protection client is installed on the machine hosting this role. This client is used to download and host the definition file. The server then pools this client and gets the malware data into the database. The client doesn’t have scans and services enabled, so it can run together with other antimalware solutions on the server. The following example is for a hierarchy containing multiple sites:

1. Go to the Administration section. In the navigation tree on the left-hand side, select Overview and expand Site Configuration. Then, select Servers and Site System Roles. Here, you will be able to see all the installed site systems:

2. Select the CAS site server or the standalone primary server and right-click on it. Select Add Site System Roles.
3. When you reach the system role page of the add site system role wizard or create site system server wizard, select **Endpoint Protection point**. The wizard looks for the Software Update Point role. If it is not installed, you need to install it. If you choose to go through without the software update point, then you have to adjust the default antimalware policy to prevent it from retrieving updates from Configuration Manager:

4. On the Endpoint Protection page, you must accept the license terms and continue with the wizard.
5. On the Microsoft active protection service page, you can choose from the following three options available:

   - I do not want to join Microsoft active protection service
   - Basic membership
   - Advanced membership

Microsoft active protection service or MAPS, formerly known as SpyNet, allows you to send information to Microsoft about the software you detect. This data is used for the creation of new definitions that improve the security and protection levels of your infrastructure. The second option allows you to join the information exchange. With advanced membership, MAPS sends more detailed information about the detected software and alerts the user. A best practice is to choose basic membership because it provides you with a higher level of security.

6. Go through the remaining steps of the wizard. You can change MAPS's membership settings if you go to the Administration section and navigate to Overview | Site Configuration | Server and Site Systems. Select the site server from the list, right click on the Endpoint Protection point, and select Properties in the details pane at the bottom. You can verify the successful installation of the Endpoint Protection role by taking a look at the EPsetup.log file contained in the server's logfile directory for any errors. Here, you should see lines similar to the following:

   SMSEP Setup Started....
   Installing the SMSEP
   Unable to query registry key
   (SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Microsoft Security Client),
   return (0x00000002) means EP client is NOT installed
   Installation was successful.
Chapter 2

Setting up a software update point for Endpoint Protection

If you want to use the software update point role to synchronize and use software updates in order to automatically download and deploy definition updates to your Endpoint Protection client, you must configure it properly. It allows you to synchronize with the Microsoft Windows update on a predefined schedule in order to enable protection for your client machines. It downloads the latest antimalware and engine updates in an automated way. After the download, the updates need to be deployed. This can be done by creating automatic deployment rules. This is an optional way of doing it; you can also perform the tasks manually.

Configuring the SUP to synchronize definition updates

In order to deliver the Endpoint Protection engine and definition updates from the software update point, you must ensure that it is configured to synchronize Definition Updates, as shown in the following screenshot:
Here, you can configure which updates will be synchronized by the SUP. Also, select the Forefront Endpoint Protection 2010 product, which is listed in the Products tab, as shown in the following screenshot:

Don't get confused by the version mismatch between System Center Configuration Manager 2012 and Endpoint Protection 2010 because the Endpoint Protection 2010 Version is included in the Configuration Manager 2012 Version.

Endpoint Protection definition updates are released several times per day, so you should configure them for download at least once per day. To configure SUP with these changes on the Central Administration site or the standalone primary site, perform the following steps:

1. Go to the Administration workspace.
2. Navigate to Overview | Site Configuration | Sites and from the list, select CAS. Click on Settings in the ribbon bar. Select configure site components from the drop-down menu and click on software update point.

3. Select the Classification tab, check Definition Updates, and click on Apply.

4. Select the Products tab and check Forefront Endpoint Protection 2010 from the list.

5. Select the Sync Schedule tab and adjust the schedule to Simple Schedule for every 1 days. To set the actual time, go to Custom Schedule.

6. Click on OK to initiate the synchronization as soon as possible.

Creating autodeployment rules for definition updates

The software update point is used for the new autodeployment rules feature. This eliminates the need to approve updates in WSUS. They can also be easily scaled. This feature gives instructions to automatically download and deploy specific software updates on a predefined schedule. To configure Automatic Deploy Rules (ADR) for Endpoint Protection, perform the following steps:

1. Go to the Software Library workspace.

2. Select Software Updates and expand all the software updates. Right click on it and choose Run Synchronization. You can verify that the synchronization is complete at the site by the following methods:

   ° Review Software Update Point Synchronization Status in the Monitoring workspace. Verify that the synchronization status is completed.

   ° Review SMS_WSUS_SYNC_MANAGER and look for the message ID 6702, WSUS. Verify that the synchronization status is completed.

   ° Review the WSUSsyncmgr.log file and look for Sync Succeeded.

3. Expand Software Updates and select Automatic Deployment Rules.

4. In the ribbon bar, click on Create Automatic Deployment Rule. This starts the automatic deployment rule wizard.
Here, you can give the rule a name, such as ADR: Endpoint protection managed client computers, and point it to a collection you want to target. As you will update this collection regularly, select Add to an existing Software Update Group, as shown in the following screenshot:

5. The Deployment Settings page of the wizard lets you select Use Wake-on-LAN to wake up the client machines for the required deployments. This is useful when you need to deploy updates during the night, when the client machines are turned off. Starting with Configuration Manager R2, you can define templates. These templates have preconfigured settings for Definition Updates:
   
   - On the Software Updates page, you can choose the parameters you want to check when ADR runs.
In the Evaluation Schedule section, click on Customize and set it run every 1 days. Also, make sure that the ADR schedule does not exceed the SUP schedule because you will evaluate for new definitions and your SUP synchronizes once per day.

In the Deployment Schedule screen, you can set the time based on UTC. This allows clients to install updates at the same time. This setting is a recommended best practice.

On the User Experience page, you can hide the definition update notifications because they can occur frequently. Select Hide in the software center, and select all the notifications from the drop-down menu.

On the Alerts page, you can enable options to generate alerts according to your SLA agreement.

On the Download Settings page, you can specify the download settings for these definition updates.

On the Deployment Package page, there are two options:

Select deployment package: You can use this option when you have a deployment package already created

Create a new definition package: You can use this option when you want to create a new deployment package

6. Go through the rest of the wizard and review the summary. You can wait for the ADR to run automatically or you can run it manually. If it runs successfully, it will display Last Error Description of Success and Last Error Code 0x00000000. This can also be disabled and enabled at any time.

Working with antimalware policies

Antimalware policies define how the SCEP client is configured for key security behaviors, such as scheduled scans, scan settings, actions to be taken if malware is found, real-time protection, behavior monitoring, exclusion settings, where to get the definition updates from, and much more. These topics are discussed in the following sections.
Understanding the default antimalware policy

The default client antimalware policy is the policy applied to the client at initial installation. The settings that are contained in this policy are divided into sections. Each section has the following configurable options:

- **Scheduled scans**: This option allows you to specify whether to run scans on target computers or not. There are two options under this setting: full scan and quick scan. A full scan takes more time to complete because it scans everything and everywhere. You can set the day and time for the full scan setting. You can also configure the target computer to look for updates before the full scan and to perform the full scan only when the client is idle.

- **Scan settings**: Here, you can define whether you want to scan e-mails, attachments, archived files, or removable devices. You can also scan network drives, but make sure that they are on a fast network because the scan will take longer to finish.

- **Default actions**: In Endpoint Protection, four levels are defined for the malware: severe, high, medium, and low. When malware is detected, it is rated with one of these levels. When malware with a severe risk level is detected, you can set a default action to be applied.

- **Real-time protection**: This setting lets you scan files and processes in real time. To enable real-time protection, just set it to true in the default antimalware policy.

- **Exclusion settings**: These are very important because they let you mark folders that will not be part of the scanning process. These folders are used by a known application and processes that perform read and write operations in them so that you know that they are not suspicious and you can exclude them from the scan.

- **Advanced**: The advanced settings allow you to create a system restore point before the target computer is cleaned of the malware. You can set up notifications for the end users, when users need to perform certain actions.

- **Threat overrides**: Regarding threat overrides, there are three options: allow, remove, or quarantine. These actions are applied when certain types of malware or virus is detected.
• **Definition updates**: This setting defines how frequently the System Center Endpoint Protection agent will update definitions. You can set different update intervals for definition updates, such as in specific hours or at a specific time of the day. You can also set the source for the updates. It can be Configuration Manager, UNC file share, WSUS, Microsoft update, or Microsoft Malware Protection Center.

**Creating a custom antimalware policy**

In every section of the antimalware policy, you will find the statement *custom policies override the default policy*. This is a reminder that a best practice is to always create a custom policy and configure it according to your needs. After you create the policy, be sure to test it on some device collection containing computers.

**Importing and merging antimalware policies**

As mentioned earlier, there are several examples of antimalware policies provided by Microsoft. You can import them and combine them together to create a new policy. To import a policy, you have to do the following:

1. Go to the **Assets and Compliance** section. From the navigation tree, navigate to **Overview | Endpoint Protection | Antimalware Policies**.
2. From the ribbon bar, select **Import**.
3. Select the policy you want to import.
4. When the import is complete, the policy is opened for editing. When you finish editing, click on **OK**. The imported policy is now available and appears in the console.

**Merging policies**

Merging policies can be very useful. Consider a server that has several functions and that each of these functions has a different antimalware policy. If you merge all of these policies, you will get one policy for this kind of server. To merge policies, do the following:

1. Go to **Assets and Compliance** and from the navigation tree, expand **Overview**. Select **Endpoint Protection** and then click on **Antimalware Policies**.
2. Select all the policies you want to merge and click on Merge from the ribbon bar, as shown in the following screenshot:

![Merge ribbon bar screenshot]

3. You will have to enter a new policy name.

4. You have to select a base policy. This is the policy from which the overall antimalware policy settings are taken and are merged with the exclusion of the other policies selected.

5. The merged policy appears in the console and is ready for deployment. The original policies also remain in the console.

**Configuring alerts for Endpoint Protection**

Alerts can be very useful when specific events occur in the hierarchy, and you can notify responsible users when malware is detected. Alerts are displayed in the Monitoring section under the alerts node. A best practice is to set up e-mail notifications because IT administrators might not always be in front of the Configuration Manager console. Most IT administrators have mobile phones that can send and receive e-mails directly from the phone. This is important because they can receive the e-mail in real time and respond accordingly.
Configuring e-mail notifications

In order to configure e-mail notifications, you must have an SMTP server in your infrastructure. In a multisite hierarchy, you only need to specify the e-mail server at the top, that is, the CAS. An e-mail notification by itself will not alert IT administrators if malware is detected. You also need to configure alert subscriptions to be notified by e-mail for specific alerts. Different e-mail addresses can be specified, and this is a recommended practice to receive e-mail notifications. By having more than one person receive the e-mail alerts, you have more chances to minimize the effects of the malware. To configure e-mail notifications, do the following:

1. Go to the Administration workspace.
2. Navigate to Overview | Site Configuration | Sites. Select Settings from the ribbon bar, click on Configure Site Components, and choose Email Notification:

![Configuration interface screenshot](image)
3. Enter the FQDN or the IP address of the SMTP server and specify the SMTP port. Select None if the server doesn't require authentication; if it requires authentication, enter an account to authenticate. You need to specify the sender address, which might not exist; however, if you want people to reply to it, you need a real e-mail address:

![Image of Email Notification Component Properties]

4. To test the SMTP server, click on Test SMTP Server…. Enter a test e-mail recipient address and click on Send Test Email. If everything is configured properly, the e-mail will reach the destination address and the message Testing email was sent successfully please check your mailbox will be displayed.
An e-mail notification alert consists of the following:

- The from address: This is the address that you specify in the sender address for e-mail alerts
- The subject of the e-mail, which consists of three pieces of information:
  - Description
  - Type of alert
  - Collection name
- Depending on the alert, the body of the e-mail will contain information about the breakout and might include information about the collection name, malware name, and successful remediation

**Alert subscriptions**

Alert subscriptions allow you to specify users who will receive e-mails when malware breakout occurs, but only if e-mail notifications are configured. For each subscription, you can specify multiple e-mail addresses. Each subscription can contain one or more criteria. To set up an alert subscription, do the following:

1. Go to the **Monitoring** section.
2. From the navigation tree, go to **Overview** | **Alerts** | **Subscriptions**.
3. From the ribbon bar, select **Create Subscription and Give it a Name**.
4. Select the e-mail language from the drop-down menu.
5. Choose **Alert** from the list. There are four types of alerts available:
   - Generate an alert when malware is detected
   - The same malware is detected on multiple computers
   - The same malware is detected repeatedly on a computer
   - Multiple types of malware are detected on a computer

You need to select the type of alert and determine whether it is applicable to the device collection you want to monitor.
Configuring custom client device settings for Endpoint Protection

As a best practice, it is recommended that you create custom settings and not use the default settings. This is because default client settings apply to all the clients in the hierarchy. Any modification of the default settings will apply to all the clients. So, it is better to create custom client device settings for target device collections. Custom client settings always have a greater priority than the default client settings. To configure custom client device settings, do the following:

1. Go to the Administration section of the console.
2. In the navigation tree on the left, go to Overview | Client Settings.
3. Right click on it and select Create Custom Client Device Settings.
4. In the Create Custom Client Device Settings wizard, give the settings a name and select Endpoint Protection from the settings list.
5. Select Endpoint Protection on the left-hand side of the window, and on the right-hand side, configure the options as appropriate. A minimum configuration will include the first two options, which means that Endpoint Protection will manage the client computer and the System Center Endpoint Protection client will be installed.
6. Click on OK when you are done.

Deploying Endpoint Protection for custom client agent settings

After you finish configuring the custom client device settings, you have to deploy these settings and target device collections. Perform the following steps in order to deploy client settings to collections:

1. Go to the Administration workspace. From the navigation tree, go to Overview | Client Settings.
2. Right click on the previously created custom client device settings and select Deploy.
3. Select a device collection to which you will deploy the custom device settings and click on OK.

After this, any computer in the target device collection will receive the policy on the next policy update and the client will be installed. If the client is installed, it will not be reinstalled.
Monitoring the status of Endpoint Protection

The Endpoint Protection dashboard consists of three parts:

- **Collection**: This displays the object collection targeted by some antimalware client policy
- **Security state**: This shows the statistics of the Endpoint Protection client's status and displays information about the number of active protected clients and the number of active clients that are at risk
- **Operational state**: This shows the status of the malware definition update status on the clients

These sections give you information related to the last Endpoint Protection status on the currently selected collection. You can summarize this data if you click on **Run Summarization**, or you can schedule a recurring summarization if you click on **Schedule Summarization**. You can find both the options on the ribbon bar of the Configuration Manager console.

Configuring collections to appear in the collection view

To display information on the dashboard, you must configure collections to be viewed. To configure a collection to appear on the dashboard, go to the **Configuring Alerts for Device Collections** topic. When you finish configuring the collection, you can select it from the drop-down list. There are seven checkboxes provided:

- Client check
- Client remediation
- Client activity
- Malware detection
- Malware outbreak
- Repeated malware detection
- Multiple malware detection

Only malware alerts can be e-mailed, but all the seven checkboxes listed in the previous list can be viewed in the Endpoint Protection dashboard. To configure alerts for device collections, follow these steps:

1. Open the **Configuration Manager** console and go to the **Assets and Compliance** section.
2. From the navigation tree, go to Overview | Device Collections and select the Endpoint Protection Managed Desktops and Laptops collection.

3. Choose Properties, click on the Alerts tab, and check View this collection in the Endpoint Protection Dashboard.

4. Click on Add and select the multiple alerts you want to be notified for.

**Security state view**

This view gives you security information about the Endpoint Protection client's status and about any status regarding malware remediation. In the left-hand side pane, there are six clickable options:

- **Clients protected with endpoint protection**
  This option gives the number and percentage of clients from the device collection managed by Endpoint Protection that are not in a malware-pending remediation, don't have operation issues, and have up-to-date antivirus definitions.

- **At risk from malware or operational issue**
  This option gives a list of malware with pending remediation status, operational issues, and antivirus definitions that are older than one week.

- **Endpoint protection client not yet installed**
  This option shows the computers from the device collection that still haven't reported their statuses or don't have a SCEP client installed on them.

- **Endpoint protection client is not supported on the platform**
  This option shows the clients that have an OS that is not supported.

- **Configuration manager client inactive**
  This option lists whether Configuration Manager is inactive. This is defined in the activity settings. You can find them by navigating to Monitoring | Overview | Client Status | Client Status Settings.

- **Configuration manager client not installed**
  This option shows all the clients that do not have a SECP client installed on them.
Malware remediation status
When you go to the security area of the dashboard, in the right-hand side pane, there are several sections related to malware remediation. If a target system is found in a state that matches the items in this list, a link is added. This link leads to the Assets and Compliance section, and it gives you more details about the object. The items in the list are as follows:

- Remediation failed
- Full scan required
- Restart required
- Offline scan required
- Client settings modified by malware
- Malware remediated in the last 24 hours

Top malware
In the security area of the dashboard, in the bottom-right pane, there is information about the top malware by number of client computers in the last 24 hours. If no malware was found, the results are also listed. When you click on a specific type of malware, you can get more details about it.

Monitoring malware details
If you go to the Assets and Compliance section, you can get more information about the malware. To get more details regarding the malware, do the following:

1. Go to the Assets and Compliance section.
2. Click on a device collection, select a computer, and click on the Malware Details tab.

This tab will give you information about the threat name, detection time, category, severity, default action, state name, detection mode, and so on. You can also customize the view by adding and removing columns.

Monitoring Endpoint Protection details
IT administrators need to be able to quickly find out whether a computer is managed by the SCEP and the Endpoint Protection's policy name. To get this information, do the following:

1. Go to the Assets and Compliance section.
2. Click on a device collection, select a computer, and click on the Endpoint Protection tab.
Here, you can get very important information such as:

- Deployment information
- Remediation information
- Policy application information

**Performing on-demand actions for the malware**

Another very important functionality of Endpoint Protection is the on-demand scanning, that is, full or quick scanning. This gives commands to the SCEP client to first update the malware definition files and then initiate actions. To perform on-demand actions, do the following:

1. Go to the **Assets and Compliance** section.
2. From the navigation tree, choose **Overview** and select **Device Collections**.
3. Select the device collection managed by Endpoint Protection, and then select the client that you want to scan.
4. Right click on the client, select **Endpoint Protection**, and then you can select the full, quick, or download definitions.

The actions will not start right away but instead, they will start when the client receives the next policy. The default interval is defined in the client settings policy and is 60 minutes.

**Reporting in Endpoint Protection**

Endpoint Protection has six built-in reports. The reports allow IT administrators to go deep and gain more information regarding the malware. With the help of role-based authentication, you can assign reports to management personnel. These are the Endpoint Protection built-in reports:

- **Top users by threats**
  
  This is a list of users with the greatest number of detected threats. The report asks for a collection name and optionally asks for a start and end date. The report lists users by threat, incident count, number of computers, and when the threat was detected. You can go deep into the report by clicking on the username. This lists the computer name and the threat with the severity level of the malware, category, incident count, and detection date. If you want to get more information about the malware, click on the threat’s name. This will display a report describing that particular threat.
• User threat list
This is a list of the threats found under a particular user account. It is important and also useful to find the user who put a risk on the organization through their activities. You can also print the report that displays their account name and show it to the involved users and their managers.

• Antimalware activity report
To view this report, you need to enter a device collection name for which you want to view information and also choose a start and end date. This report is an overview of the antimalware that is either removed from the computers in the collection or is quarantined.

• Infected computers
This is a list of the computers that have had malware on them in a specific time frame. You can also enter the threat's name, the default action taken, and the infection status. Infection status is one of the three remediation states. The possible selections are:
  - Remediation fail
  - Remediation with pending actions
  - Remediated
  - Null

• Infected computers report
For this report, you need to select a collection name and also choose the start and end dates. Moreover, you can select which cleaning action took place—whether it is cleaned, quarantined, removed, allowed, user specified, no action, blocked, or null. You can also select the previously mentioned remediation status. To go further into the report, you can enter the malware's name.

• Dashboard report
For this report, you need to enter a device collection name first and the start and end dates. This report shows different pieces of Endpoint Protection information about the computers in the selected device collection. It also gives you a graphical overview of the state of Endpoint Protection for the collection.
The Endpoint Protection client
The Endpoint Protection client is the application found in the system tray, which is used by users to view the malware that is detected on their computer. When the client and the computer is in a healthy state, the icon is green. When malware is detected, the client changes color; it becomes red and it also flashes in the system tray to alert the user. Depending on the malware and its severity, a user can be asked to take action by clicking on **Clean Computer**. If the user doesn't take an action, the client itself determines what action is appropriate and applies it based on the antimalware policy.

Installing the Endpoint Protection client
You must distinguish the Configuration Manager client from the Endpoint Protection client. When you deploy the Configuration Manager client, the Endpoint Protection client is prestaged. The files are locally cached and the SCEP is installed only when the client settings are configured to enable the System Center Endpoint Protection client.

Understanding Endpoint Protection client settings
When you install System Center Endpoint Protection, you can choose from six configurable options. Multiple custom client settings can be created, multiple collections can be targeted, and you can give them different priorities and functionalities. The custom client settings always take priority over the default client settings. If a computer is a member of multiple collections targeted by different custom client policies, the custom policy with the highest priority wins. Here are the settings that you can configure:

- **Manage Endpoint Protection client on client computers**: This allows Configuration Manager to manage the SCEP client that is found on the computer. If the machine has an Endpoint Protection client and you set this setting to **True**, it will allow Configuration Manager to manage this SCEP client.

- **Install Endpoint Protection client on client computers**: This is used to control the installation of the Endpoint Protection client on client machines. If you set this to **False** and the setting from the first bullet to **True**, it will allow you to uninstall third-party antimalware software. If you set this to **True**, it will force the installation of the Endpoint Protection client agent.
• **Automatically remove previously installed antimalware software before Endpoint Protection is installed:**

If you set this to **True**, it will uninstall antimalware software, such as McAfee, Symantec, and TrendMicro.

• **Suppress any required computer restarts after the Endpoint Protection client is installed:**

Sometimes, the installation of the SCEP client agent requires a restart. If this is the scenario, you can set this to **True** in order to suppress a restart. This can be very useful for servers.

• **Allowed period of time users can postpone a requires restart to complete the Endpoint Protection client installation:**

This setting defines how long the client can postpone the restart needed after the client installation.

• **Disable alternate sources for the initial definition update:**

When this is set to **True**, it will force the first update of Endpoint Protection definitions to come from Configuration Manager rather than from other sources. When the Endpoint Protection client is installed before receiving its first policy, it doesn't know where to get its definition updates from; so, setting this option ensures that it polls only Configuration Manager for the definition updates.

---

**Automatic removal of antimalware software**

When you install the SCEP client, you can uninstall third-party antivirus software. It will allow the following antivirus software to be uninstalled:

- All Microsoft antimalware products, except Windows Intune and Security Essentials
- Symantec Antivirus Corporate Edition 10
- Symantec Endpoint Protection 11
- Symantec Endpoint Protection Small Business Edition 12
- MacAfee Virus Scan Enterprise Version 8
- Trend Micro OfficeScan

The antivirus software that is not listed must be uninstalled with a custom uninstaller. If you do not uninstall it first, it will leave your computer with two antivirus solutions, which can cause instability and performance loss.
Removing the Endpoint Protection client
If you need to remove the Endpoint Protection client, you have to apply a script to the machines where it is installed. The removal of SCEP is not automatic and if you disable the Endpoint Protection client agent settings, it will not remove the client. Even if you remove the Configuration Manager client, it will not remove the SCEP client. To remove the SCEP client, you must uninstall it manually from Programs and Features or execute this script:

```
scepinstall.exe /u /s
```

Delivering definition updates
When you configure a custom antimalware policy for Endpoint Protection, you must specify the definition update's source. There are five sources that you can choose from:

- Updates distributed from WSUS
- Updates distributed from Microsoft Update
- Updates distributed from Microsoft's malware protection center
- Updates distributed from Configuration Manager
- Updates from UNC file shares

Summary
In this chapter, we learned more about compliance settings and Endpoint Protection. With knowledge and creativity, compliance settings can give you feedback on the configuration and compliance of your Windows-based systems and mobile devices. Together with the remediation features, compliance settings can enforce compliance standards through the hierarchy. Compliance settings have a big impact on the companies in the area of configuration and compliance verification and enforcement from one single tool. Integrating System Center Endpoint Protection into Configuration Manager is a great feature that it offers. It consolidates security tasks together with client management and reduces cost. You can now simply enable the Endpoint Protection role within Configuration Manager and configure client and antimalware settings. In the next chapter, we will take a look at the Software Library section of the Configuration Manager console and see how to create packages and applications and how to distribute them to clients.
Where to buy this book
You can buy Mastering System Center Configuration Manager from the Packt Publishing website.
Alternatively, you can buy the book from Amazon, BN.com, Computer Manuals and most internet book retailers.
Click here for ordering and shipping details.