Department of Information Systems
Arkansas. A State of Technology.

Microsoft®

System Center 2012 Endpoint Protection

Contents

Endpoint Protection in Configuration Manager

Before you can use Endpoint Protection to manage security and malware on System Center 2012 Configuration Manager client computers, you must perform the configuration steps detailed in this topic.

Configure Endpoint Protection in Configuration Manager

Use the following table for the steps and details about how to configure Endpoint Protection.

Steps	Details
Step 1: Create an Endpoint Protection point site system role.	The Endpoint Protection point site system role must be installed before you can use Endpoint Protection. It must be installed on one site system server only, and it must be installed at the top of the hierarchy on a central administration site or a stand-alone primary site.
Step 2: Configure alerts for Endpoint Protection.	Alerts inform the administrator when specific events have occurred, such as a malware infection. Alerts are displayed in the **Alerts** node of the **Monitoring** workspace, or optionally can be emailed to specified users.
Step 3: Configure definition update sources for Endpoint Protection clients.	Endpoint Protection can be configured to use various sources to download definition updates.
Step 4: Configure the default antimalware policy and create any custom antimalware policies.	The default antimalware policy is applied when the Endpoint Protection client is installed. Any custom policies you have deployed are applied by default, within 60 minutes of deploying the client. Ensure that you have configured antimalware policies before you deploy the Endpoint Protection client.
Step 5: Configure custom client settings for Endpoint Protection.	Use custom client settings to configure Endpoint Protection settings for collections of computers in your hierarchy. **Important** Do not configure the default Endpoint Protection client settings unless you are sure that you want these settings applied to all computers in your hierarchy.

Use the following information when the steps in the preceding table require supplemental procedures.

Create an Endpoint Protection Point Site System Role

Use one of the following procedures depending on whether you want to install a new site system server for Endpoint Protection or use an existing site system server.

Important

When you install an Endpoint Protection point, an Endpoint Protection client is installed on the server hosting the Endpoint Protection point. Services and scans are disabled on this client to enable it to co-exist with any existing antimalware solution that is installed on the server. If you later enable this server for management by Endpoint Protection and select the option to remove any third-party antimalware solution, the third-party product will not be removed. You must uninstall this product manually.

Install and configure the Endpoint Protection point site system role: New site system server

1. In the Configuration Manager console, click **Administration**.
2. In the **Administration** workspace, expand **Site Configuration**, and then click **Servers and Site System Roles**.
3. On the **Home** tab, in the **Create** group, click **Create Site System Server**.
4. On the **General** page, specify the general settings for the site system, and then click **Next**.
5. On the **System Role Selection** page, select **Endpoint Protection point** in the list of available roles, and then click **Next**.
6. On the **Endpoint Protection** page, select the **I accept the Endpoint Protection license terms** check box, and then click **Next**.

   Important You cannot use Endpoint Protection in Configuration Manager unless you accept the license terms.
7. On the **Microsoft Active Protection Service** page, select the level of information that you want to send to Microsoft to help develop new definitions, and then click **Next**.

   Note This option configures the Microsoft Active Protection Service settings that are used by default. You can then configure custom settings for each antimalware policy you create. Join Microsoft Active Protection Service, to help to keep your computers more secure by supplying Microsoft with malware samples that can help Microsoft to keep antimalware definitions more up-to-date. Additionally, when you join Microsoft Active Protection Service, the Endpoint Protection client can use the dynamic signature service to download new definitions before they are published to Windows Update.
8. Complete the wizard.

Install and configure the Endpoint Protection point site system role: Existing site system server

1. In the Configuration Manager console, click **Administration**.
2. In the **Administration** workspace, expand **Site Configuration**, click **Servers and Site System Roles**, and then select the server that you want to use for Endpoint Protection.
3. On the **Home** tab, in the **Server** group, click **Add Site System Roles**.
4. On the **General** page, specify the general settings for the site system, and then click **Next**.
5. On the **System Role Selection** page, select **Endpoint Protection point** in the list of available roles, and then click **Next**.
6. On the **Endpoint Protection** page, select the **I accept the Endpoint Protection license terms** check box, and then click **Next**.

   Important You cannot use Endpoint Protection in Configuration Manager unless you accept the license terms.
7. On the **Microsoft Active Protection Service** page, select the level of information that you want to send to Microsoft to help develop new definitions, and then click **Next**.

   Note This option configures the Microsoft Active Protection Service settings that are used by default. You can configure custom settings for each antimalware policy you configure.
8. Complete the wizard.

Configure Alerts for Endpoint Protection in Configuration Manager

You can configure Endpoint Protection alerts in Microsoft System Center 2012 Configuration Manager to notify administrative users when specific security events occur in your hierarchy. Notifications display in the Endpoint Protection dashboard in the Configuration Manager console, in reports, and you can configure them to be emailed to specified recipients.

Use the following steps and the supplemental procedures in this topic to configure alerts for Endpoint Protection in Configuration Manager.

Important

You must have the **Enforce Security** permission for collections to configure Endpoint Protection alerts.

Use the following table for the steps, details, and more information about how to configure alerts for Endpoint Protection.

Steps	Details
Step 1 (Optional): Configure email settings for alerts.	Before you can configure email subscriptions for alerts, you must configure an SMTP server in your hierarchy. An SMTP server can only be specified at the top-level site of your Configuration Manager hierarchy.
Step 2: Configure alerts by collection.	Configure the properties of a device collection and specify settings for alerts.
Step 3 (Optional): Configure email subscriptions for specific alerts.	Select the Endpoint Protection alerts in the **Monitoring** workspace, and create subscriptions by specifying email addresses to send the Endpoint Protection alerts.

Use the following information when the steps in the preceding table require supplemental procedures. These procedures configure the alerts for Endpoint Protection.

Note

In Configuration Manager with no service pack, you could only configure email subscriptions for Endpoint Protection alerts. Beginning with System Center 2012 Configuration Manager SP1, you can configure email subscriptions to all alerts generated by Configuration Manager.

Use the following table to find information about how to configure alerts and alert subscriptions in Configuration Manager:

For information about how you can monitor the alerts that are generated by Configuration Manager, see the Monitor Alerts in Configuration Manager section in the Monitor Configuration Manager Sites and Hierarchy topic.

Management Tasks for Alerts

Use the information in this section to help you manage alerts in Configuration Manager.

1. In the **Monitoring** workspace, click **Alerts** and then select a management task.
   Use the following table for more information about the management tasks that might require some information before you select them.

Management task	Details
Configure	Opens the *<alert name>***Properties** dialog box where you can modify the name, severity, and thresholds for the selected alert. If you change the severity of the alert, this configuration affects how the alerts are displayed in the Configuration Manager console.
Edit Comment	Enter a comment for the selected alerts. These comments display with the alert in the Configuration Manager console.
Postpone	Suspends the monitoring of the alert until the specified date is reached. At that time, the state of the alert is updated. You can only postpone an alert when it is enabled.
Create subscription	Opens the **New Subscription** dialog box where you can create an email subscription to the selected alert. **Note** Prior to Configuration Manager SP1, you can create email subscriptions only for Endpoint Protection and client status alerts.

Configure Email Subscriptions for Alerts

Use the procedures in this section to help you configure email subscriptions to alerts in Configuration Manager.

Important

In Configuration Manager with no service pack, you can only configure email subscriptions for Endpoint Protection alerts.

Configure email notification settings in Configuration Manager with no service pack

1. In the Configuration Manager console, click **Administration**.
2. In the **Administration** workspace, expand **Site Configuration**, and then click **Sites**.
3. On the **Home** tab, in the **Settings** group, click **Configure Site Components** and then click **Email Notification**.
4. In the **Email Notification Component Properties** dialog box, specify the following information:
    a. **Enable email notification for Endpoint Protection alerts**: Select this check box to enable Configuration Manager to use an SMTP server to send email alerts.
    b. **FQDN or IP Address of the SMTP server to send email alerts**: Enter the fully qualified domain name (FQDN) or IP address and the SMTP port for the email server that you want to use for these alerts.

c. **Endpoint Protection SMTP Server Connection Account**: Specify the authentication method for Configuration Manager to use to connect the email server.
d. **Sender address for email alerts**: Specify the email address from which alert emails are sent.
e. **Test SMTP Server**: Sends a test email to the email address specified in **Sender address for email alerts**.

5. Click **OK** to save the settings and to close the **Email Settings Component Properties** dialog box.

Configure email notification settings in Configuration Manager SP1 and System Center 2012 R2 Configuration Manager

1. In the Configuration Manager console, click **Monitoring**.
2. In the **Monitoring** workspace, expand **Alerts**, and then click **Subscriptions**.
3. On the **Home** tab, in the **Create** group, click **Configure Email Notification**.
4. In the **Email Notification Component Properties** dialog box, specify the following information:
    a. **Enable email notification for alerts**: Select this check box to enable Configuration Manager to use an SMTP server to send email alerts.
    b. **FQDN or IP Address of the SMTP server to send email alerts**: Enter the fully qualified domain name (FQDN) or IP address and the SMTP port for the email server that you want to use for these alerts.
    c. **SMTP Server Connection Account**: Specify the authentication method for Configuration Manager to use to connect the email server.
    d. **Sender address for email alerts**: Specify the email address from which alert emails are sent.
    e. **Test SMTP Server**: Sends a test email to the email address specified in **Sender address for email alerts**.
5. Click **OK** to save the settings and to close the **Email Settings Component Properties** dialog box.

Subscribe to alerts

1. In the Configuration Manager console, click **Monitoring**.
2. In the **Monitoring** workspace, click **Alerts**.
3. In the **Alerts** list, select an alert and then, on the **Home** tab, in the **Subscription** group, click **Create subscription**.
4. In the **New Subscription** dialog box, specify the following information:
    a. **Name**: Enter a name to identify the email subscription. You can use up to 255 characters.
    b. **Email address**: Enter the email addresses that you want the alert sent to. You can separate multiple email addresses with a semicolon.
    c. **Email language**: In the list, specify the language for the email.
5. Click **OK** to close the **New Subscription** dialog box and to create the email subscription.

Note

You can delete and edit subscriptions in the **Monitoring** workspace when you expand the **Alerts** node, and then click the **Subscriptions** node.

Configure Alerts by Collection

1. In the Configuration Manager console, click **Assets and Compliance**.
2. In the **Assets and Compliance** workspace, click **Device Collections**.
3. In the **Device Collections** list, select the collection for which you want to configure alerts, and then on the **Home** tab, in the **Properties** group, click **Properties**.

   Note

   You cannot configure alerts for user collections.

4. On the **Alerts** tab of the <*Collection Name*>**Properties** dialog box, select **View this collection in the Endpoint Protection dashboard** if you want to view details about antimalware operations for this collection in the **Monitoring** workspace of the Configuration Manager console.

   Note

   This option is unavailable for the **All Systems** collection.

5. On the **Alerts** tab of the <*Collection Name*>**Properties** dialog box, click **Add**.
6. In the **Add New Collection Alerts** dialog box, in the **Generate an alert when these conditions apply** section, select the alerts that you want Configuration Manager to generate when the specified Endpoint Protection events occur, and then click **OK**.
7. In the **Conditions** list of the **Alerts** tab, select each Endpoint Protection alert, and then specify the following information:
   a. **Alert Name** – Accept the default name or enter a new name for the alert.
   b. **Alert Severity** – In the list, select the alert level to display in the Configuration Manager console.

      Depending on the alert that you select, specify the following additional information.

Alert name	Additional information required
Malware detection	This alert is generated if malware is detected on any computer in the collection that you monitor. Specify the following information to configure this alert: **Malware detection threshold:** - specifies the malware detection levels at which this alert is generated. In the list, select one of the following:

	○ **High – All detections** - The alert is generated when there are one or more computers in the specified collection on which any malware is detected, regardless of what action the Endpoint Protection client takes. ○ **Medium – Detected, pending action** - The alert is generated when there is one or more computers in the specified collection on which malware is detected, and you must manually remove the malware. ○ **Low – Detected, still active** - The alert is generated when there are one or more computers in the specified collection on which malware is detected and is still active.
Malware outbreak	This alert is generated if specified malware is detected on a specified percentage of computers in the collection that you monitor. Specify the following information to configure this alert: ○ **Percentage of computers with malware detected** – The alert is generated when the percentage of computers with malware that is detected in the collection exceeds the percentage that you specify. Specify a percentage from **1** through **99**. **Note** The percentage value is based on the number of computers in the collection, but excludes computers that do not have a Configuration Manager client installed. It includes computers that do not yet have the Endpoint Protection client installed.
Repeated malware detection	This alert is generated if specific malware is detected more than a specified number of times over a specified number of hours on the computers in the collection that you monitor. Specify the following information to configure this alert: ○ **Number of times malware has been detected:** - The alert is generated when the same malware is detected on computers in the collection more than the specified number of times. Specify a number from **2** through **32**. ○ **Interval for detection (hours):** Specify the detection interval (in hours) in which the number of malware detections must occur. Specify a number from **1** through **168**.
Multiple malware detection	This alert is generated if more than a specified number of malware types are detected over a specified number of hours on computers in the collection that you monitor.

	Specify the following information to configure this alert: ○ **Number of malware types detected:** The alert is generated when the specified number of different malware types are detected on computers in the collection. Specify a number from **2** through **32**. ○ **Interval for detection (hours):** Specify the detection interval, in hours, in which the number of malware detections must occur. Specify a number from **1** through **168**.

8. Click **OK** to close the <*Collection Name*>**Properties** dialog box.

Configure definition update sources for Endpoint Protection clients.

With Endpoint Protection in Microsoft System Center 2012 Configuration Manager, you can use any of several available methods to keep antimalware definitions up to date on client computers in your hierarchy. The information in this topic can help you to select and configure these methods.

To update antimalware definitions, you can use one or more of the following methods:

- **Updates distributed from Configuration Manager** – This method uses Configuration Manager software updates to deliver definition and engine updates to computers in your hierarchy.
- **Updates distributed from Windows Server Update Services (WSUS)** – This method uses your WSUS infrastructure to deliver definition and engine updates to computers.
- **Updates distributed from Microsoft Update** – This method allows computers to connect directly to Microsoft Update in order to download definition and engine updates. This method can be useful for computers that are not often connected to the business network.
- **Updates distributed from Microsoft Malware Protection Center** – This method will download definition updates from the Microsoft Malware Protection Center.
- **Updates from UNC file shares** – With this method, you can save the latest definition and engine updates to a share on the network. Clients can then access the network to install the updates.

You can configure multiple definition update sources and control the order in which they are assessed and applied. This is done in the **Configure Definition Update Sources** dialog box when you create an antimalware policy.

Configure Definition Update Sources

Use the following procedure to configure the definition update sources to use for each antimalware policy.

To configure definition update sources

1. In the Configuration Manager console, click **Assets and Compliance**.
2. In the **Assets and Compliance** workspace, expand **Endpoint Protection**, and then click **Antimalware Policies**.
3. Open the properties page of the **Default Antimalware Policy** or create a new antimalware policy.
4. In the **Definition updates** section of the antimalware properties dialog box, click **Set Source**.
5. In the **Configure Definition Update Sources** dialog box, select the sources to use for definition updates. You can click **Up** or **Down** to modify the order in which these sources are used.
6. Click **OK** to close the **Configure Definition Update Sources** dialog box.

Using Windows Server Update Services (WSUS) to Deliver Definitions

If you use WSUS to keep your antimalware definitions up to date, you can configure it to auto-approve definition updates. Although using Configuration Manager software updates is the recommended method to keep definitions up to date, you can also configure WSUS as a method to allow users to manually initiate definition updated. Use the following procedures to configure WSUS as a definition update source.

Configuring Update Synchronization

Use the following procedure to configure Endpoint Protection updates when your WSUS server is not integrated into your Configuration Manager environment.

To synchronize Endpoint Protection definition updates in standalone WSUS

1. In the WSUS administration console, expand **Computers**, click **Options**, and then click **Products and Classifications**.
2. On the **Products** tab of the **Products and Classifications** dialog box, select the **Forefront Endpoint Protection 2010** check box.
3. On the **Classifications** tab of the **Products and Classifications** dialog box, select the **Definition Updates** and **Updates** check boxes.

Approving Definition Updates

Endpoint Protection definition updates must be approved and downloaded to the WSUS server before they are offered to clients that request the list of available updates. Clients connect to the WSUS server to check for applicable updates and then request the latest approved definition updates.

To approve definitions and updates in WSUS

1. In the WSUS administration console, click **Updates**, and then click **All Updates** or the classification of updates that you want to approve.
2. In the list of updates, right-click the update or updates you want to approve for installation, and then click **Approve**.

3. In the **Approve Updates** dialog box, select the computer group for which you want to approve the updates, and then click **Approved for Install**.

In addition to manual approval, you can also set an automatic approval rule for definition updates and Endpoint Protection updates. This will configure WSUS to automatically approve Endpoint Protection definition updates downloaded by WSUS.

To configure an automatic approval rule

1. In the WSUS administration console, click **Options**, and then click **Automatic Approvals**.
2. On the **Update Rules** tab, click **New Rule**.
3. In the **Add Rule** dialog box, under **Step 1: Select properties**, select the **When an update is in a specific classification** check box.
4. Under **Step 2: Edit the properties**, click **any classification**.
5. Clear all check boxes except **Definition Updates**, and then click **OK**.
6. In the **Add Rule** dialog box, under **Step 1: Select properties**, select the **When an update is in a specific product** check box.
7. Under **Step 2: Edit the properties**, click **any product**.
8. Clear all check boxes except **Forefront Endpoint Protection**, and then click **OK**.
9. Under **Step 3: Specify a name**, enter a name for the rule, and then click **OK**.
10. In the **Automatic Approvals** dialog box, select the check box for the newly created rule and then click **Run rule**.

Note To maximize performance on your WSUS server and client computers, decline old definition updates. To accomplish this task, you can configure automatic approval for revisions and automatic declining of expired updates.

Using Microsoft Update to Download Definitions

When you select to download definition updates from Microsoft Update, clients will check the Microsoft Update site at the interval defined in the **Definition updates** section of the antimalware policy dialog box.

This method can be useful when the client does not have connectivity to the Configuration Manager site or when you want users to be able to initiate definition updates.

Important Clients must have access to Microsoft Update on the Internet to be able to use this method to download definition updates.

Using the Microsoft Malware Protection Center to Download Definitions

You can configure clients to download definition updates from the Microsoft Malware Protection Center. This option is used by Endpoint Protection clients to download definition updates if they have not been able to download updates from another source. This update method can be useful if there is a problem with your Configuration Manager infrastructure that prevents the delivery of updates.

Important

Clients must have access to Microsoft Update on the Internet to be able use this method to download definition updates.

Downloading Definitions from a Share on the Network

You can manually download the latest definition updates from Microsoft and then configure clients to download these definitions from a shared folder on the network. Users can also initiate definition updates when you use this update source.

Note

Clients must have read access to the shared folder to be able to download definition updates.

For more information about how to download the definition and engine updates to store on the file share, see Install the latest Microsoft Forefront Security definition updates.

To configure definition downloads from a file share

1. In the Configuration Manager console, click **Assets and Compliance**.
2. In the **Assets and Compliance** workspace, expand **Endpoint Protection**, and then click **Antimalware Policies**.
3. Open the properties page of the **Default Antimalware Policy** or create a new antimalware policy.
4. In the **Definition updates** section of the antimalware properties dialog box, click **Set Source**.
5. In the **Configure Definition Update Sources** dialog box, select **Updates from UNC file shares**.
6. Click **OK** to close the **Configure Definition Update Sources** dialog box.
7. Click **Set Paths**. Then, in the **Configure Definition Update UNC Paths** dialog box, add one or more UNC paths to the location of the definition updates files on a network share.
8. Click **OK** to close the **Configure Definition Update UNC Paths** dialog box.

Configure the default antimalware policy and create any custom antimalware policies.

You can deploy antimalware policies to collections of Microsoft System Center 2012 Configuration Manager client computers to specify how Endpoint Protection protects them from malware and other threats. These antimalware policies include information about the scan schedule, the types of files and folders to scan, and the actions to take when malware is detected. When you enable Endpoint Protection, a default antimalware policy is applied to client computers. You can also use additional policy templates that are supplied or create your own custom antimalware policies to meet the specific needs of your environment.

Note

Configuration Manager supplies a selection of predefined templates that are optimized for various scenarios and can be imported into Configuration Manager. These templates are available in the folder *<ConfigMgr Install Folder>*\AdminConsole\XMLStorage\EPTemplates.

Important

If you create a new antimalware policy and deploy it to a collection, this antimalware policy overrides the default antimalware policy.

Use the procedures in this topic to create or import antimalware policies and assign them to System Center 2012 Configuration Manager client computers in your hierarchy.

Note

Before you perform these procedures, ensure that Configuration Manager is configured for Endpoint Protection.

Modify the default antimalware policy

1. In the Configuration Manager console, click **Assets and Compliance**.
2. In the **Assets and Compliance** workspace, expand **Endpoint Protection**, and then click **Antimalware Policies**.
3. Select the antimalware policy **Default Client Antimalware Policy** and then, on the **Home** tab, in the **Properties** group, click **Properties**.
4. In the **Default Antimalware Policy** dialog box, configure the settings that you require for this antimalware policy, and then click **OK**.

Create a new antimalware policy

1. In the Configuration Manager console, click **Assets and Compliance**.
2. In the **Assets and Compliance** workspace, expand **Endpoint Protection**, and then click **Antimalware Policies**.
3. On the **Home** tab, in the **Create** group, click **Create Antimalware Policy**.
4. In the **General** section of the **Create Antimalware Policy** dialog box, enter a name and a description for the policy.
5. In the **Create Antimalware Policy** dialog box, configure the settings that you require for this antimalware policy, and then click **OK**.
6. Verify that the new antimalware policy is displayed in the **Antimalware Policies** list.

Import an antimalware policy

1. In the Configuration Manager console, click **Assets and Compliance**.
2. In the **Assets and Compliance** workspace, expand **Endpoint Protection**, and then click **Antimalware Policies**.
3. In the **Home** tab, in the **Create** group, click **Import**.
4. In the **Open** dialog box, browse to the policy file to import, and then click **Open**.

5. In the **Create Antimalware Policy** dialog box, review the settings to use, and then click **OK**.
6. Verify that the new antimalware policy is displayed in the **Antimalware Policies** list.

Deploy an antimalware policy to client computers

1. In the Configuration Manager console, click **Assets and Compliance**.
2. In the **Assets and Compliance** workspace, expand **Endpoint Protection**, and then click **Antimalware Policies**.
3. In the **Antimalware Policies** list, select the antimalware policy to deploy. Then, on the **Home** tab, in the **Deployment** group, click **Deploy**.

   Note The **Deploy** option cannot be used with the default client malware policy.
4. In the **Select Collection** dialog box, select the device collection to which you want to deploy the antimalware policy, and then click **OK**.

List of Antimalware Policy Settings

Many of the antimalware settings are self-explanatory. Use the following sections for more information about the settings that might require more information before you configure them.

Scheduled Scans

Setting name	Description
Scan type	You can specify one of two scan types to run on client computers: • **Quick scan** – This type of scan checks the in-memory processes and folders where malware is typically found. It requires fewer resources than a full scan. • **Full Scan** – This type of scan adds a full check of all local files and folders to the items scanned in the quick scan. This scan takes longer than a quick scan and uses more CPU processing and memory resources on client computers. In most cases, use **Quick scan** to minimize the use of system resources on client computers. If malware removal requires a full scan, Endpoint Protection generates an alert that is displayed in the Configuration Manager console. The default value is **Quick scan**.
Randomize the scheduled scan start times (within 30 minutes)	Select **True** (Configuration Manager with no service pack) or **Yes** (Configuration Manager SP1) if you want to help avoid flooding the network, which can occur if all computers send their antimalware scans results to the Configuration Manager database at the same time.

	This setting is also useful when you run multiple virtual machines on a single host. Select this option to reduce the amount of simultaneous disk access for antimalware scanning. **Note** In Configuration Manager SP1, this setting appears in the **Advanced** section of the antimalware policy settings.

Scan Settings

Setting name	Description
Scan network drives when running a full scan	Set to **True** (Configuration Manager with no service pack) or **Yes** (Configuration Manager SP1) if you want to scan any mapped network drives on client computers. **Important** If you enable this setting, it might significantly increase the scan time on client computers.

Default Actions

Select the action to take when malware is detected on client computers. The following actions can be applied, depending on the alert threat level of the detected malware.

- **Recommended** – Use the action recommended in the malware definition file.
- **Quarantine** – Quarantine the malware but do not remove it.
- **Remove** – Remove the malware from the computer.
- **Allow** – Do not remove or quarantine the malware.

Real-time Protection

Setting name	Description
Enable real-time protection	Set to **True** (Configuration Manager with no service pack) or **Yes** (Configuration Manager SP1) if you want to configure real-time protection settings for client computers. We recommend that you enable this setting.
Monitor file and program activity on your computer	Set to **True** (Configuration Manager with no service pack) or **Yes** (Configuration Manager SP1) if you want Endpoint Protection to monitor when files and programs start to run on client computers and to alert you about any actions that they perform or actions taken on them.
Scan system files	This setting lets you configure whether incoming, outgoing, or incoming and outgoing system files are monitored for malware. For performance reasons, you

	might have to change the default value of **Scan incoming and outgoing files** if a server has high incoming or outgoing file activity.
Enable behavior monitoring	Enable this setting to use computer activity and file data to detect unknown threats. When this setting is enabled, it might increase the time required to scan computers for malware.
Enable protection against network-based exploits	Enable this setting to protect computers against known network exploits by inspecting network traffic and blocking any suspicious activity.
Enable script scanning	For Configuration Manager with no service pack only. Enable this setting if you want to scan any scripts that run on computers for suspicious activity.

Exclusion Settings

Setting name	Description
Excluded files and folders	Click **Set** to open the **Configure File and Folder Exclusions** dialog box and specify the names of the files and folders to exclude from Endpoint Protection scans. If you want to exclude files and folders that are located on a mapped network drive, specify the name of each folder in the network drive individually. For example, if a network drive is mapped as F:\MyFolder and it contains subfolders named Folder1, Folder2 and Folder 3, specify the following exclusions: • F:\MyFolder\Folder1 • F:\MyFolder\Folder2 • F:\MyFolder\Folder3

Advanced

Setting name	Description
Enable reparse point scanning	For System Center 2012 Configuration Manager SP1 and later: Set to **Yes** if you want Endpoint Protection to scan NTFS reparse points. For more information about reparse points, see Reparse Points in the Windows Dev Center.

Threat Overrides

Setting name	Description
Threat name and override action	Click **Set** to customize the remediation action to take for each threat ID when it is detected during a scan. **Note** The list of threat names might not be available immediately after the configuration of Endpoint Protection. Wait until the Endpoint Protection point has synchronized the threat information, and then try again.

Definition Updates

Setting name	Description
Set sources and order for Endpoint Protection client updates	Click **Set Source** to specify the sources for definition and scanning engine updates, and to also specify the order in which they are used. If Configuration Manager is specified as one of the sources, then the other sources are used only if software updates fails to download the client updates. If you use any of the following methods to update the definitions on client computers, then the client computers must be able to access the Internet. • Updates distributed from Microsoft Update • Updates distributed from Microsoft Malware Protection Center **Important** Clients download definition updates by using the built-in system account. You must configure a proxy server for this account to enable these clients to connect to the Internet. If you have configured a software updates automatic deployment rule to deliver definition updates to client computers, these updates will be delivered regardless of the definition updates settings.

Configure Custom Client Settings for Endpoint Protection

This procedure configures custom client settings for Endpoint Protection which can be deployed to collections of computers in your hierarchy.

Important Do not configure the default Endpoint Protection client settings unless you are sure that you want them applied to all computers in your hierarchy.

Enable Endpoint Protection and configure custom client settings

1. In the Configuration Manager console, click **Administration**.
2. In the **Administration** workspace, click **Client Settings**.
3. On the **Home** tab, in the **Create** group, click **Create Custom Client Device Settings**.
4. In the **Create Custom Client Device Settings** dialog box, provide a name and a description for the group of settings, and then select **Endpoint Protection**.
5. Configure the Endpoint Protection client settings that you require.

   Important You must install the Endpoint Protection site system role before you can configure client settings for Endpoint Protection.
6. Click **OK** to close the **Create Custom Client Device Settings** dialog box. The new client settings are displayed in the **Client Settings** node of the **Administration** workspace.
7. Before the custom client settings can be used, you must deploy them to a collection. Select the custom client settings you want to deploy and then, in the **Home** tab, in the **Client Settings** group, click **Deploy**.
8. In the **Select Collection** dialog box, choose the collection to which you want to deploy the client settings and then click **OK**. The new deployment is shown in the **Deployments** tab of the details pane.

Client computers will be configured with these settings when they next download client policy. To initiate policy retrieval for a single client, see the Initiate Policy Retrieval for a Configuration Manager Client section in the How to Manage Clients in Configuration Manager topic.

Create and Deploy Windows Firewall Policies for Endpoint Protection in Configuration Manager

Firewall policies for Endpoint Protection in System Center 2012 Configuration Manager let you perform basic Windows Firewall configuration and maintenance tasks on client computers in your hierarchy. You can use Windows Firewall policies to perform the following tasks:

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

Use the following procedures in this topic to help create and assign Windows Firewall policies to Configuration Manager client computers in your hierarchy:

- To create a Windows Firewall policy
- To deploy a Windows Firewall policy

Create a Windows Firewall policy

1. In the Configuration Manager console, click **Assets and Compliance**.
2. In the **Assets and Compliance** workspace, expand **Endpoint Protection**, and then click **Windows Firewall Policies**.
3. On the **Home** tab, in the **Create** group, click **Create Windows Firewall Policy**.
4. On the **General** page of the **Create Windows Firewall Policy Wizard**, specify a name and an optional description for this firewall policy, and then click **Next**.
5. On the **Profile Settings** page of the wizard, configure the following settings for each network profile:

   Important If you want to deploy Windows Firewall policies to computers running Windows Server 2008 and Windows Vista Service Pack 1, you must first install Hotfix KB971800 on these computers.

   Note For more information about network profiles, see the Windows documentation.
   a. **Enable Windows Firewall**

      Note If **Enable Windows Firewall** is not enabled, the other settings on this page of the wizard are unavailable.
   b. **Block all incoming connections, including those in the list of allowed programs**
   c. **Notify the user when Windows Firewall blocks a new program**
6. On the **Summary** page of the wizard, review the actions to be taken, and then complete the wizard.
7. Verify that the new Windows Firewall policy is displayed in the **Windows Firewall Policies** list.

Deploy a Windows Firewall policy

1. In the Configuration Manager console, click **Assets and Compliance**.
2. In the **Assets and Compliance** workspace, expand **Endpoint Protection**, and then click **Windows Firewall Policies**.
3. In the **Windows Firewall Policies** list, select the Windows Firewall policy that you want to deploy.
4. On the **Home** tab, in the **Deployment** group, click **Deploy**.
5. In the **Deploy Windows Firewall Policy** dialog box, specify the collection to which you want to assign this Windows Firewall policy, and specify an assignment schedule. The Windows Firewall policy evaluates for compliance by using this schedule and the Windows Firewall settings on clients to reconfigure to match the Windows Firewall policy.
6. Click **OK** to close the **Deploy Windows Firewall Policy** dialog box and to deploy the Windows Firewall policy.

   Important When you deploy a Windows Firewall policy to a collection, this policy is applied to computers in a random order over a 2 hour period to avoid flooding the network.

How to Manage Antimalware Policies and Firewall Settings for Endpoint Protection in Configuration Manager

Use the information in this topic to help you manage Endpoint Protection antimalware policies and Windows Firewall policies in Microsoft System Center 2012 Configuration Manager, to perform on-demand scans, to force computers to download the latest available definitions, and to remediate detected malware.

Manage Antimalware Policies

In the **Assets and Compliance** workspace, expand **Endpoint Protection**, click **Antimalware Policies**, select the antimalware policy that you want to manage, and then select a management task.

Use the following table for more information about the management tasks that might require some information before you select them.

Task	Details
Increase Priority	If multiple antimalware policies are deployed to the same computer, they are applied in order. Use this option to increase the priority by which the selected antimalware policy is applied. Use the **Order** column to view the order in which the policies are applied. The antimalware policy that has the highest numbered priority is always applied first.
Decrease Priority	If multiple antimalware policies are deployed to the same computer, they are applied in order. Use this option to decrease the priority by which the selected antimalware policy is applied. Use the **Order** column to view the order in which the policies are applied.
Merge	Merges the two selected antimalware policies. In the **Merge Policies** dialog box, enter a name for the new, merged policy. The **Base policy** is the antimalware policy that is merged with this new antimalware policy. **Note** If two settings conflict, the most secure setting is applied to computers.
Deploy	Opens the **Select Collection** dialog box. Select the collection to which you want to deploy the antimalware policy, and then click **OK**.

Manage Windows Firewall Policies

In the **Assets and Compliance** workspace, click **Endpoint Protection**, click **Windows Firewall Policies**, select the Windows Firewall policy that you want to manage, and then select a management task.

Use the following table for more information about the management tasks that might require some information before you select them.

Task	Details
Increase Priority	If multiple Windows Firewall policies are deployed to the same computer, they are applied in order. Use this option to increase the priority by which the selected Windows Firewall policy is applied. Use the **Order** column to view the order in which the policies are applied.
Decrease Priority	If multiple Windows Firewall policies are deployed to the same computer, they are applied in order. Use this option to decrease the priority by which the selected Windows Firewall policy is applied. Use the **Order** column to view the order in which the policies are applied.
Deploy	Opens the **Deploy Windows Firewall Policy** dialog box from where you can deploy the firewall policy to a specified collection.

Perform an On-demand Scan of Computers

You can perform a scan of a single computer, multiple computers, or a collection of computers in the Configuration Manager console. This scan occurs outside any scheduled scans that you configured. Use the following procedure to perform an on-demand scan.

Important

If any of the computers that you select do not have the Endpoint Protection client installed, the on-demand scan option is unavailable.

Perform an on-demand scan of computers

1. In the Configuration Manager console, click **Assets and Compliance**.
2. In the **Devices** or **Device Collections** node, select the computer or collection of computers that you want to scan.
3. On the **Home** tab, in the **Collection** group, click **Endpoint Protection**, and then click **Full Scan** or **Quick Scan**.

The scan will take place when the computer or collection of computers next downloads client policy. To monitor the results from the scan, use the procedures in How to Monitor Endpoint Protection in Configuration Manager.

Force Computers to Download the Latest Definition Files

You can force a single computer, multiple computers, or a collection of computers to download the latest definition files from the Configuration Manager console by using the following procedure.

Important
If any of the computers that you select do not have the Endpoint Protection client installed, the **Download Definition** option is unavailable.

Force computers to download the latest definition files

1. In the **Devices** or **Device Collections** node, select the computer or collection of computers for which you want to download definitions.
2. On the **Home** tab, in the **Collection** group, click **Endpoint Protection**, and then click **Download Definition**. The definition download will take place when the computer or collection of computers next downloads client policy.

   Note
   Use the **System Center 2012 Endpoint Protection Status** node in the **Monitoring** workspace to discover clients that have out-of-date definitions.

Remediate Detected Malware

When malware is detected on client computers, this will be displayed in the **Malware Detected** node under **Endpoint Protection Status** in the **Monitoring** workspace of the Configuration Manager console. Select an item from the **Malware Detected** list, and then use one of the following management tasks to remediate or allow the detected malware:

Task	Details
Allow this threat	Creates an antimalware policy to allow the selected malware. The policy is deployed to the **All Systems** collection and can be monitored in the **Client Operations** node of the **Monitoring** workspace.
Restore files quarantined by this threat	Opens the **Restore quarantined files** dialog box where you can select one of the following options: • **Run the allow-threat or exclusion operation first to assure that files are not put back into quarantine** – Restores the files that were quarantined because of the detected malware and also excludes the files from malware scans. If you do not exclude the files from malware scans, they will be quarantined again when the next scan runs. • **Restore files without a dependency on the allow or exclusion job** – Restores the quarantined files but does not add them to the exclusion list.

View infected clients	Displays a list of all clients that were infected by the selected malware.
Exclude selected files or paths from scan	When you select this option from the malware details pane, the **Exclude files and paths** dialog box opens where you can specify the files and folders that you want to exclude from malware scans.

Monitor Endpoint Protection in Configuration Manager

You can monitor Endpoint Protection in your Microsoft System Center 2012 Configuration Manager hierarchy by using the **System Center 2012 Endpoint Protection Status** node in the **Monitoring** workspace, the **Endpoint Protection** node in the **Assets and Compliance** workspace, and by using reports.

Monitor Endpoint Protection by Using the System Center 2012 Endpoint Protection Status Node

1. In the Configuration Manager console, click **Monitoring**.
2. In the **Monitoring** workspace, click **System Center 2012 Endpoint Protection Status**
3. In the **Collection** list, select the collection for which you want to view status information.
   Important
   Collections are available for selection in the following cases:
   a. When you select **View this collection in the Endpoint Protection dashboard** on the **Alerts** tab of the <*collection name*>**Properties** dialog box.
   b. When you deploy an Endpoint Protection antimalware policy to the collection.
   c. When you enable and deploy Endpoint Protection client settings to the collection.
4. Review the information that is displayed in the **Security State** and **Operational State** sections. You can click any status link to create a temporary collection in the **Devices** node in the **Assets and Compliance** workspace. The temporary collection contains the computers with the selected status.

   Important

   Information that is displayed in the **System Center 2012 Endpoint Protection Status** node is based on the last data that was summarized from the Configuration Manager database and might not be current. If you want to retrieve the latest data, on the **Home** tab, click **Run Summarization**, or click **Schedule Summarization** to adjust the summarization interval.

Monitor Endpoint Protection in the Assets and Compliance Workspace

1. In the Configuration Manager console, click **Assets and Compliance**.
2. In the **Assets and Compliance** workspace, perform one of the following actions:
    a. Click **Devices**. In the **Devices** list, select a computer, and then click the **Malware Detail** tab.
    b. Click **Device Collections**. In the **Device Collections** list, select the collection that contains the computer you want to monitor and then, on the **Home** tab, in the **Collection** group, click **Show Members**.
3. In the <*collection name*> list, select a computer, and then click the **Malware Detail** tab.

Monitor Endpoint Protection by Using Reports

Use the following reports to help you view information about Endpoint Protection in your hierarchy. You can also use these reports to help troubleshoot any Endpoint Protection problems. The Endpoint Protection reports are in the Endpoint Protection folder.

Report name	Description
Antimalware Activity Report	Displays an overview of antimalware activity for a specified collection.
Infected Computers	Displays a list of computers on which a specified threat is detected.
Top Users By Threats	Displays a list of users with the most number of detected threats.
User Threat List	Displays a list of threats that were found for a specified user account.

Malware Alert Levels

Use the following table to identify the different Endpoint Protection alert levels that might be displayed in reports, or in the Configuration Manager console.

Alert level	Description
Failed	Endpoint Protection failed to remediate the malware. Check your logs for details of the error.
Removed	Endpoint Protection successfully removed the malware.
Quarantined	Endpoint Protection moved the malware to a secure location and prevented it from running until you remove it or allow it to run.
Cleaned	The malware was cleaned from the infected file.
Allowed	An administrative user selected to allow the software that contains the malware to run.
No Action	Endpoint Protection took no action on the malware. This might occur if the computer is restarted after malware is detected and the malware is no longer detected; for instance, if a mapped network drive on which malware is detected is not reconnected when the computer restarts.
Blocked	Endpoint Protection blocked the malware from running. This might occur if a process on the computer is found to contain malware.