



The Antimalware Policy Setting Overview

We need to understand the settings before we can build custom policies. With that in mind in we will present an overview of the various policy settings available to us in Endpoint Protection.

Open the SCCM console

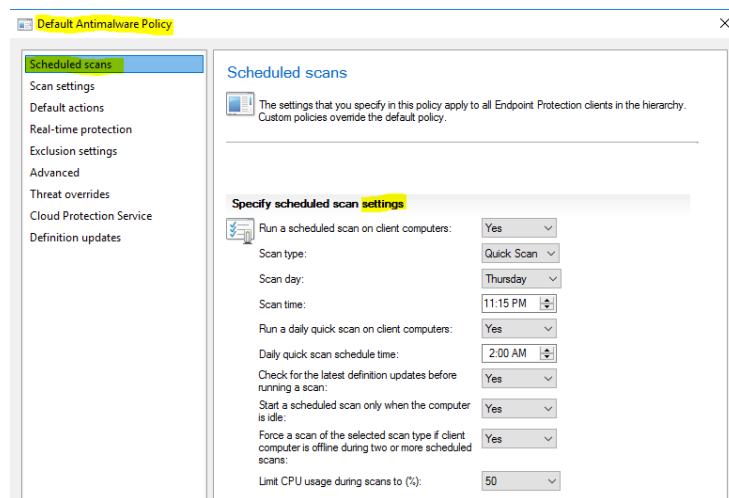
- From the Workspace click **Assets and Compliance**, from the **navigation pane** click Endpoint Protection, then **click Antimalware Policies**. Displayed are **two policies**, the SCEP Standard Desktop custom policy and the Default Antimalware Policy.

Antimalware Policies 2 items

Icon	Name	Type	Order	Deployments	Description
	SCEP Standard Desktop	Custom	1	1	SCEP Standard Desktop
	Default Client Antimalware Policy	Default	10000	0	Settings that apply to all clients in the hierarchy, and can be modified by custom client settings

From the List View, right click on Default Client Antimalware Policy, then select properties.

We see the categories on the left and the options or settings for each category on the right.



The screenshot shows the 'Default Antimalware Policy' properties window. On the left is a navigation pane with categories: Scheduled scans (selected), Scan settings, Default actions, Real-time protection, Exclusion settings, Advanced, Threat overrides, Cloud Protection Service, and Definition updates. The main area is titled 'Scheduled scans' and contains a description: 'The settings that you specify in this policy apply to all Endpoint Protection clients in the hierarchy. Custom policies override the default policy.' Below this is a section 'Specify scheduled scan settings' with the following options:

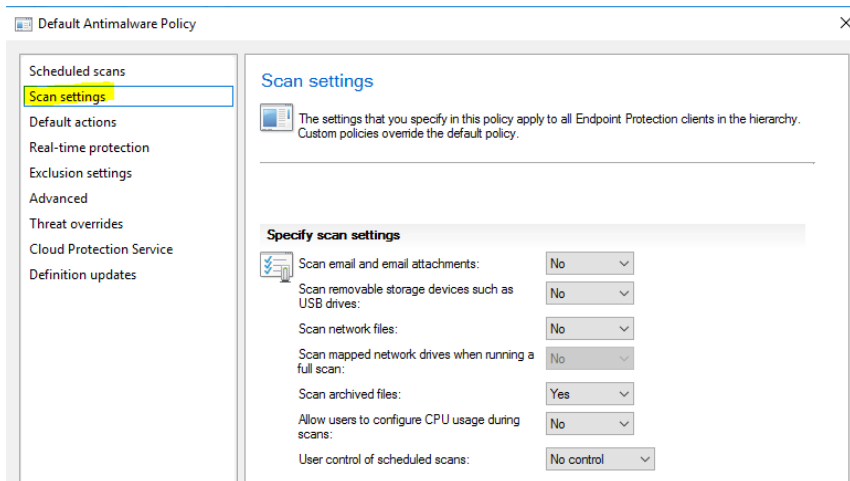
- Run a scheduled scan on client computers: Yes
- Scan type: Quick Scan
- Scan day: Thursday
- Scan time: 11:15 PM
- Run a daily quick scan on client computers: Yes
- Daily quick scan schedule time: 2:00 AM
- Check for the latest definition updates before running a scan: Yes
- Start a scheduled scan only when the computer is idle: Yes
- Force a scan of the selected scan type if client computer is offline during two or more scheduled scans: Yes
- Limit CPU usage during scans to (%): 50

Scheduled Scans – These settings customize the schedule that you will utilize in your organization

- Run a scheduled scan – the choices are Yes or no
- Scan type – The choices are Quick Scan or Full Scan
- Scan day – Select Daily or select one of the days Sunday through Saturday
- Set the Scan Time

- Check for the latest definition updates before running a scan
- You can Limit the amount of CPU utilization that should be used during the scan so that the system is still usable.

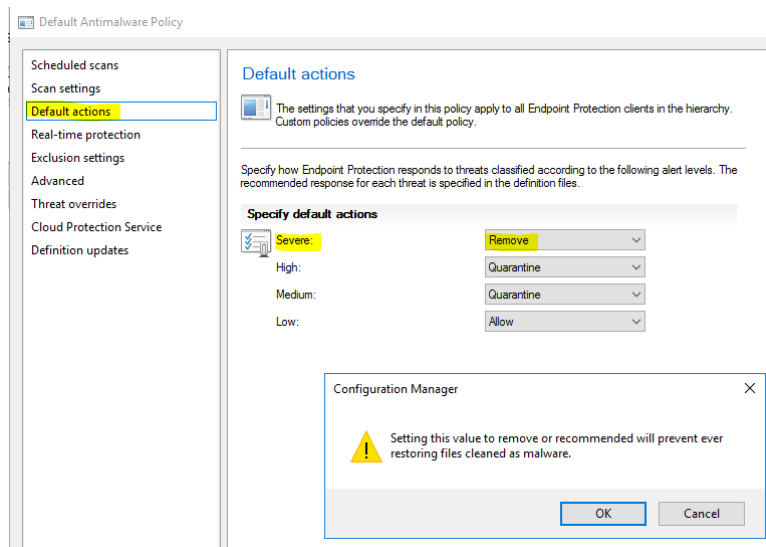
Scan Settings - These settings determine what will be scanned



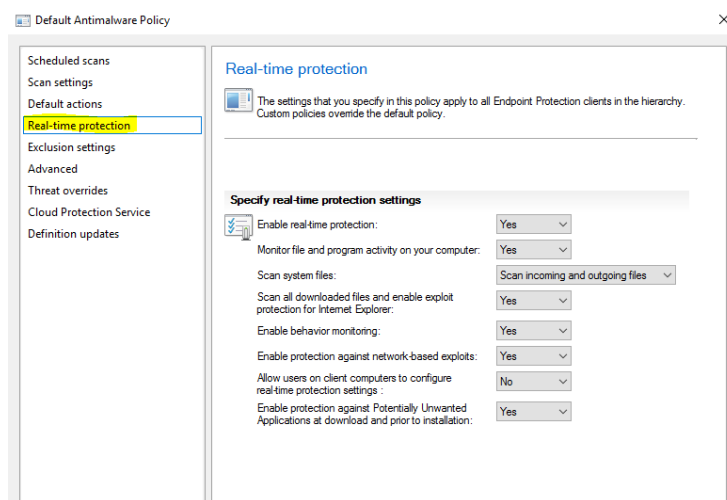
- Scan email and attachments
- Scan USB thumb drives
- Scan network files
- Scan mapped network drives
- Allow users to configure CPU usage during scans
- Allow users control of scheduled scans – Normally set to no control

Default Actions - Specifies how Endpoint Protection responds based upon the rated severity Levels

- Severe – We can choose remove, which will remove the malware.
- High - We can choose remove, which will remove the malware.
- Medium and Low – We can choose Quarantine

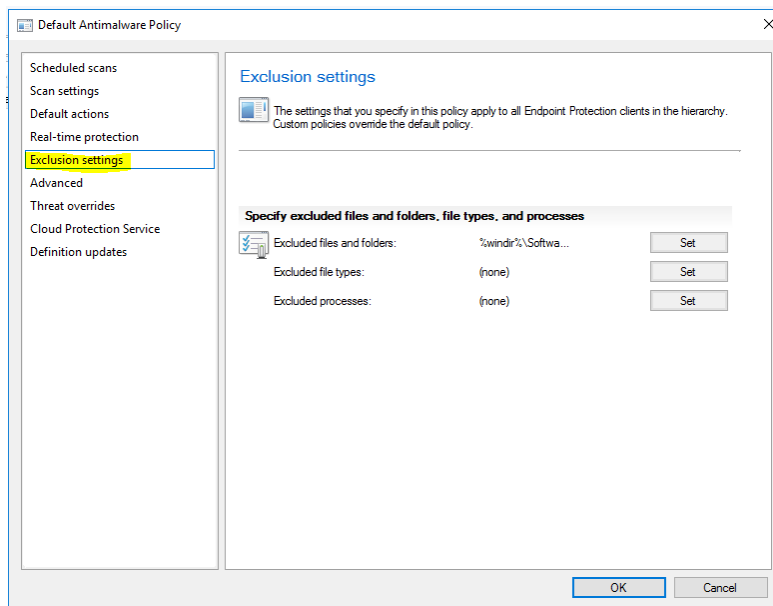


Real Time Protection – These settings enable you to configure the continuous monitoring capabilities on an Endpoint Protected client.



- Enable real-time protection – Set to Yes
- Scanning system files - Options are the scanning of incoming and outgoing files, or incoming or outgoing files only
- Enable behavior monitoring – Not just relying on known malware, but we are looking for suspicious activity to set alarms.
- Enable protection against network-based exploits – Helps protect you against zero-day vulnerabilities.

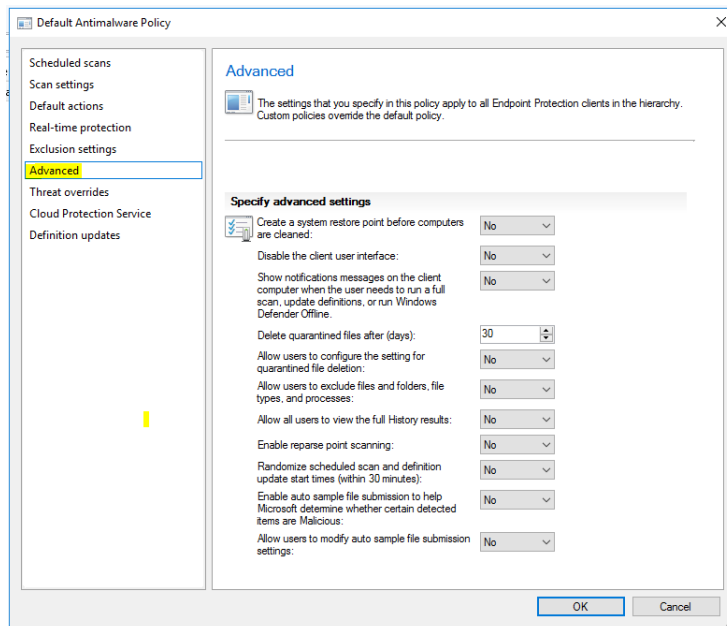
Exclusion Settings - You can exclude files and folders because those files continually set off false alarms



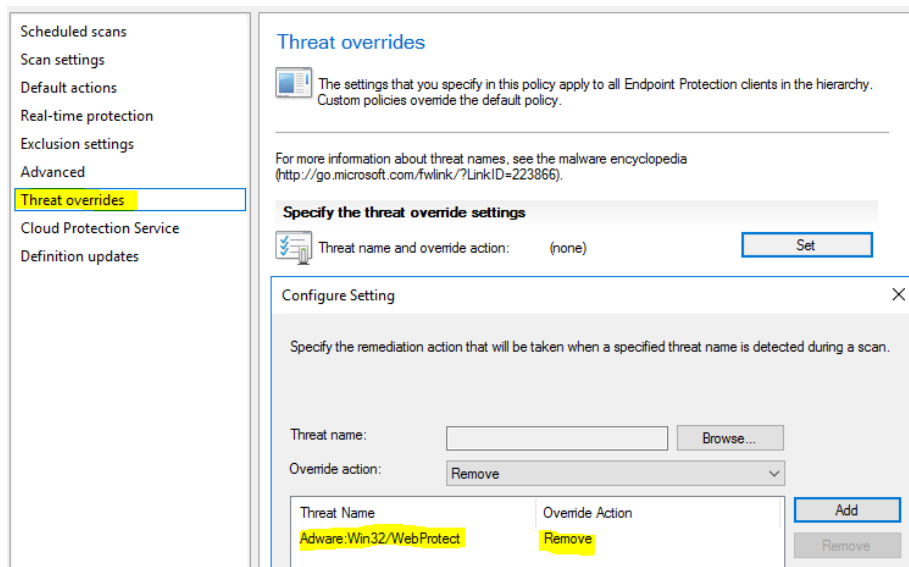
- Files, folders – Set the path to the files and folders
- Files types – You can set file types like .jpeg or .bat
- Excluded Processes – Here you can exclude processes like spoolsv.exe, which manages printing in the background without tying up your computer. You may not need to scan that process.

Advanced Settings – Contains things that you can allow the users to do.

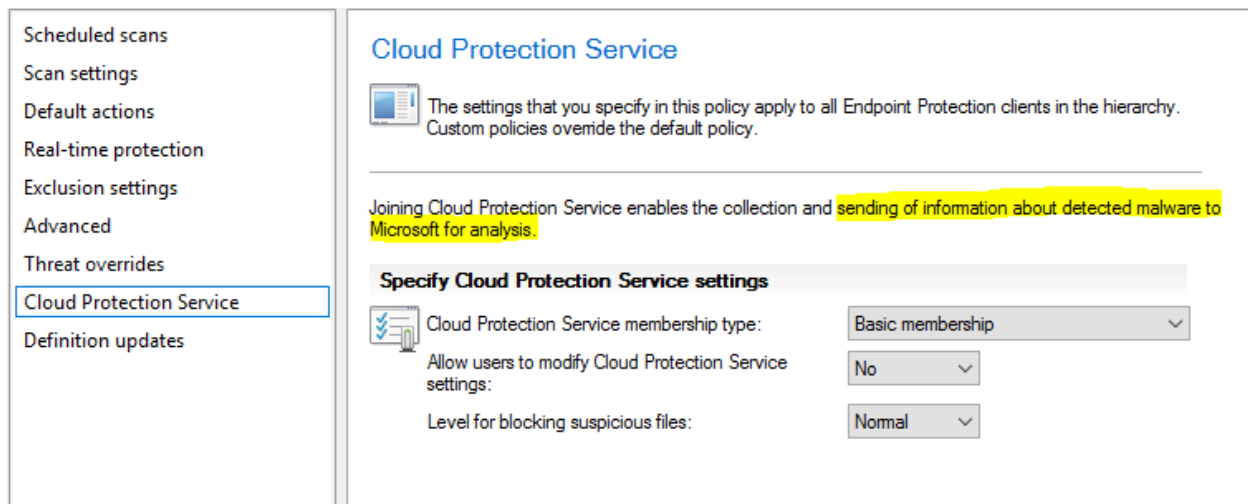
- Most of these settings I normally set to no
- Delete quarantined files after (days) you can set this to whatever is appropriate.



Threat Overrides - Here you can set a specific threat name like Adware:Win32/WebProtect, then select an Override action like allow, remove, quarantine

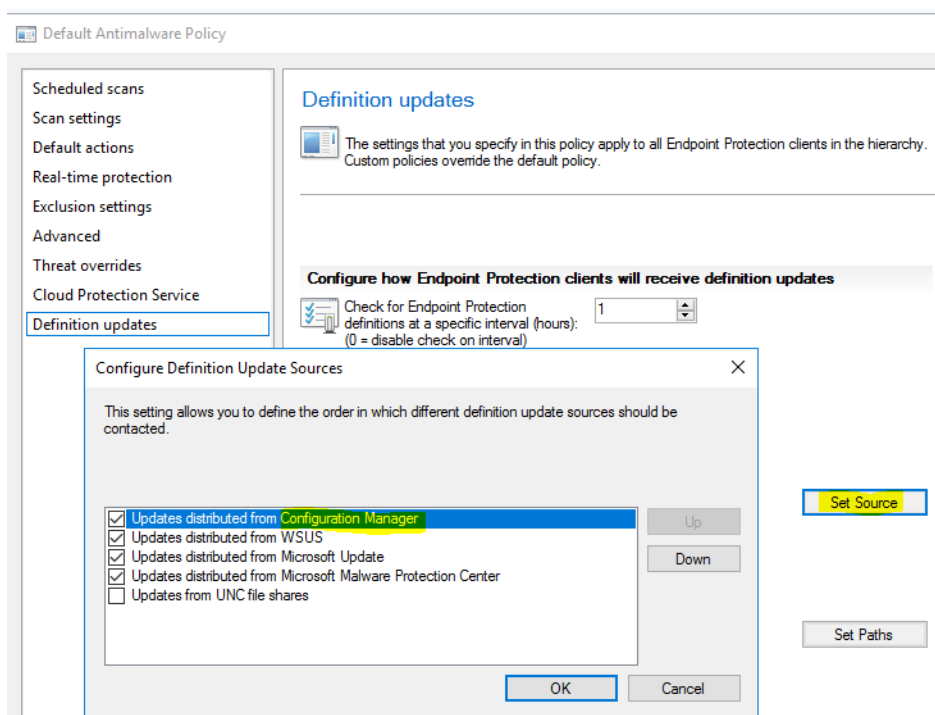


Cloud Protection Service – This setting enables the client to send information about detected malware to Microsoft for analysis.



Definition Updates – Determines how often EP clients should check updates for the endpoint protection engine, as well virus definitions

- You can setup an hourly time interval that the client will check for Endpoint Protection definitions.
- Check for EP definitions at a specified time



Set Source – You can set one or more settings in order, that will pull down updates depending upon what is checked. This is saying that the client will receive it's updates from one or more of these locations in the order that you select.

- Updates distributed from Configuration Manager
- Updates distributed from WSUS
- Updates distributed from Microsoft Update
- Updates distributed from Microsoft Malware Protection Center
- Updates distributed from UNC shares

Set Paths – If UNC file shares are selected as a definition updates source, specify the UNC paths. The path will be [\\servername\folder](#) name

Custom Policy Import and Export – You can import and export custom policies in and out of Configuration Manager. You might do that for backup purposes, or you may re-use custom policies between different environments so that you don't have to reconfigure all the setting over again.

From the List view right click the SCEP Standard Desktop Custom policy, click export, type in a file and choose a location, then press save.

Congratulations, you have completed this lecture. Thanks for watching and we will see you in the next lecture.