Welcome to the Endpoint Protection Client Installation

Prerequisites for the Endpoint Protection Client Installation

- The SCCM client must be **installed first** on the computer **before the client can be managed.**
- The SCCM client is installed for central management purposes
- This step was covered in the Client Push Installation lecture, so we will not be repeating those steps here.
- After the client installation step has been completed, the Endpoint Protection client can be deployed to the computer.

Installation of Endpoint Protection on Windows 8.1 and earlier

- On Windows 8.1 and earlier the EP client is installed in **addition** to the SCCM client

Windows 10

- If you have a Windows 10 client, then you have the Windows 10 Defender antimalware client already installed, so you don't need to install the EP client.
- You can configure and **manage** EP settings on windows 10 clients with the System Center Endpoint Antimalware Policy.
- You can install EP using Configuration Manager's **Client settings.**
- Windows 10 Defender updates must be kept up to date. This can be accomplished by creating and deploying an Automatic Deployment Role.

Pre-Windows 8.1 EP Client Installation

For this lecture, we will be configuring Endpoint Protection Windows 10 clients. I have included a written manual installation for Windows 8.1 and below in case you still have earlier versions of Windows in your organization. Checkout the manual that accompanies this lecture for details.

Manual Installation of Endpoint Protection

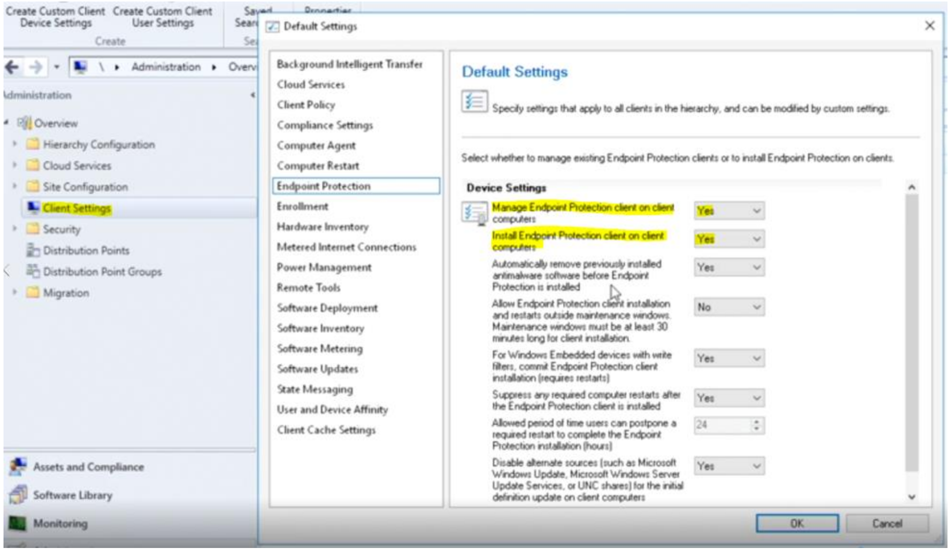
Windows 7

- From your SCCM server open **C:\Program Files\Microsoft Configuration Manager\Client.** Copy the **scepinstall.exe and the ep_defaultpolicy.xml** file to your installation folder on your Windows 7 client.
- Double click **scepinstall.exe** file and go through the installation wizard.

- Click **next**, click **I accept** on the Software license screen
- Click **I do not wat to join** the Customer Experience Improvement Program
- Click **next**, check the **turn firewall on**, click **next**
- Click **Install,** check Scan my computer for potential threats after getting the latest updates, click finish
- **Install updates.**

Windows 10 EP Installation

Configure the Client Settings



Default Settings

Specify settings that apply to all clients in the hierarchy, and can be modified by custom settings.

Select whether to manage existing Endpoint Protection clients or to install Endpoint Protection on clients.

Device Settings

Manage Endpoint Protection client on client computers	Yes
Install Endpoint Protection client on client computers	Yes
Automatically remove previously installed antimalware software before Endpoint Protection is installed	Yes
Allow Endpoint Protection client installation and restarts outside maintenance windows. Maintenance windows must be at least 30 minutes long for client installation.	No
For Windows Embedded devices with write filters, commit Endpoint Protection client installation (requires restarts)	Yes
Suppress any required computer restarts after the Endpoint Protection client is installed	Yes
Allowed period of time users can postpone a required restart to complete the Endpoint Protection installation (hours)	24
Disable alternate sources (such as Microsoft Windows Update, Microsoft Windows Server Update Services, or UNC shares) for the initial definition update on client computers	Yes

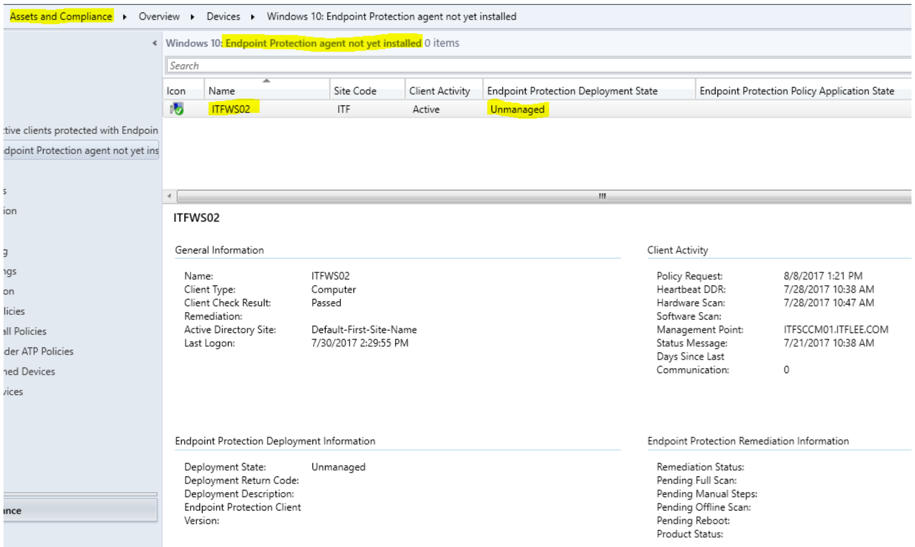
- In the Configuration Manager console from the workspace click **Administration,** from the Navigation Pane, right click **Client settings** and click on **Create Custom Client Device Settings**.
- From the **General** tab to the right type a Name – **EP Client Settings**. From below click Endpoint Protection, click **ok.**
- From the list view in the console double click **EP Client Settings**
- On the left pane click **Endpoint Protection**
- From Device Settings **change** all the settings to **Yes** except Allow Endpoint Protection client installation and restarts outside maintenance window. Leave this set **to no.**
- Manage EP client on client computers enables you to use Configuration Manager to manage windows clients.
- Install EP client on client computers – When this setting is enabled to a device collection, Endpoint Client will be deployed to all the computers in that collection.

Take Note:

- EP will not install right away, the installation could take up to an hour.
- You can remove other previously installed antimalware software by selecting Yes for Automatically remove previously installed software

Right click on **EP Client Settings, click deploy,** now select a collection click **Windows 10,** then click **ok.**

This slide shows ITFWS02 that the SCCM client has been installed but the EP client has not been installed yet.



Assets and Compliance ▸ Overview ▸ Devices ▸ Windows 10: Endpoint Protection agent not yet installed

Windows 10: Endpoint Protection agent not yet installed 0 items

Icon	Name	Site Code	Client Activity	Endpoint Protection Deployment State	Endpoint Protection Policy Application State
	ITFWS02	ITF	Active	Unmanaged	

ITFWS02

General Information

```
Name:                   ITFWS02
Client Type:            Computer
Client Check Result:    Passed
Remediation:
Active Directory Site:  Default-First-Site-Name
Last Logon:             7/30/2017 2:29:55 PM
```

Client Activity

```
Policy Request:         8/8/2017 1:21 PM
Heartbeat DDR:          7/28/2017 10:38 AM
Hardware Scan:          7/28/2017 10:47 AM
Software Scan:
Management Point:       ITFSCCM01.ITFLEE.COM
Status Message:         7/21/2017 10:38 AM
Days Since Last
Communication:          0
```

Endpoint Protection Deployment Information

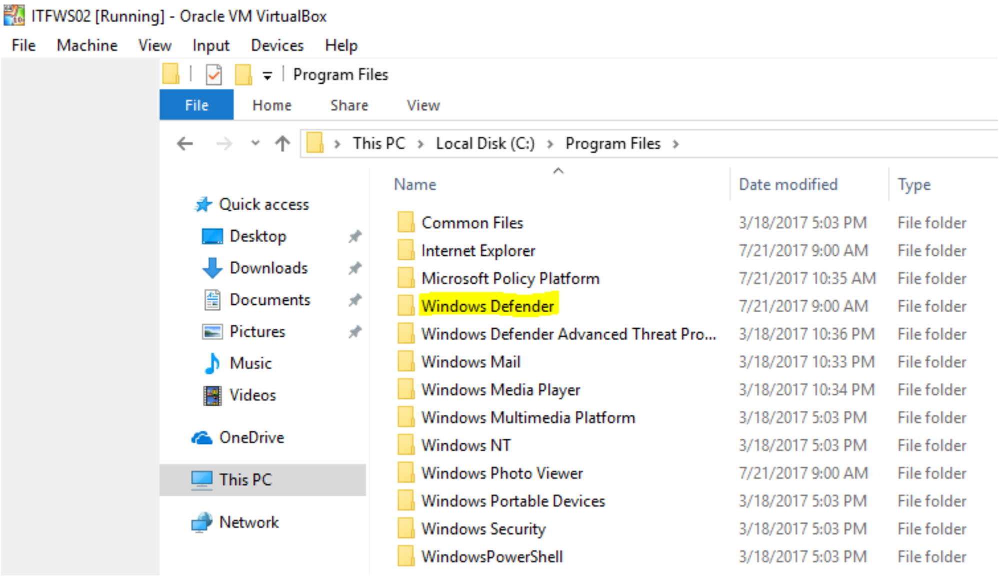
```
Deployment State:            Unmanaged
Deployment Return Code:
Deployment Description:
Endpoint Protection Client
Version:
```

Endpoint Protection Remediation Information

```
Remediation Status:
Pending Full Scan:
Pending Manual Steps:
Pending Offline Scan:
Pending Reboot:
Product Status:
```

Search
:tive clients protected with Endpoin
dpoint Protection agent not yet ins
s
ion
g
ngs
on
licies
all Policies
der ATP Policies
ned Devices
vices
ance

- **From ITFWS02 this slide shows that the Windows 10 client is unmanaged as well**



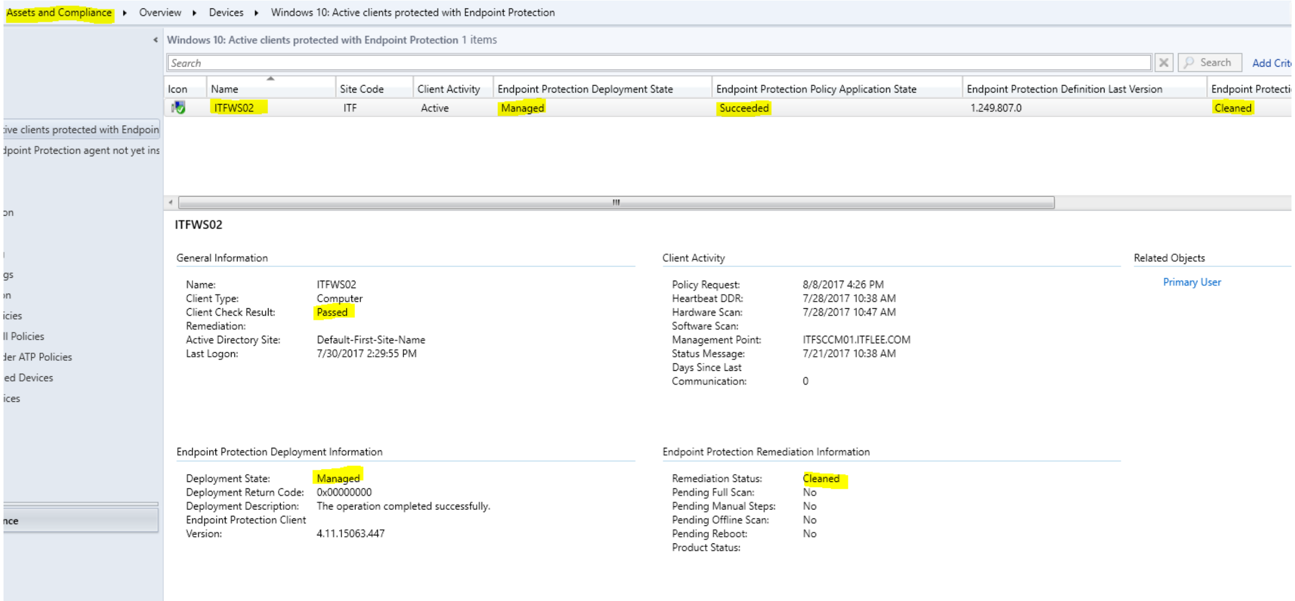
ITFWS02 [Running] - Oracle VM VirtualBox

Program Files

This PC › Local Disk (C:) › Program Files ›

Name	Date modified	Type
Common Files	3/18/2017 5:03 PM	File folder
Internet Explorer	7/21/2017 9:00 AM	File folder
Microsoft Policy Platform	7/21/2017 10:35 AM	File folder
Windows Defender	7/21/2017 9:00 AM	File folder
Windows Defender Advanced Threat Pro...	3/18/2017 10:36 PM	File folder
Windows Mail	3/18/2017 10:33 PM	File folder
Windows Media Player	3/18/2017 10:34 PM	File folder
Windows Multimedia Platform	3/18/2017 5:03 PM	File folder
Windows NT	3/18/2017 5:03 PM	File folder
Windows Photo Viewer	7/21/2017 9:00 AM	File folder
Windows Portable Devices	3/18/2017 5:03 PM	File folder
Windows Security	3/18/2017 5:03 PM	File folder
WindowsPowerShell	3/18/2017 5:03 PM	File folder

- **After about an hour the console show that ITFWS02 in now managed.**


Assets and Compliance ▸ Overview ▸ Devices ▸ Windows 10: Active clients protected with Endpoint Protection
Windows 10: Active clients protected with Endpoint Protection 1 items
Search
Search
Add Crit
ive clients protected with Endpoin
dpoint Protection agent not yet ins
on
gs
on
icies
ll Policies
der ATP Policies
ed Devices
ices
nce
Primary User

Icon	Name	Site Code	Client Activity	Endpoint Protection Deployment State	Endpoint Protection Policy Application State	Endpoint Protection Definition Last Version	Endpoint Protecti
	ITFWS02	ITF	Active	Managed	Succeeded	1.249.807.0	Cleaned

ITFWS02

General Information

Name:	ITFWS02
Client Type:	Computer
Client Check Result:	Passed
Remediation:	
Active Directory Site:	Default-First-Site-Name
Last Logon:	7/30/2017 2:29:55 PM

Client Activity

Policy Request:	8/8/2017 4:26 PM
Heartbeat DDR:	7/28/2017 10:38 AM
Hardware Scan:	7/28/2017 10:47 AM
Software Scan:	
Management Point:	ITFSCCM01.ITFLEE.COM
Status Message:	7/21/2017 10:38 AM
Days Since Last Communication:	0

Related Objects

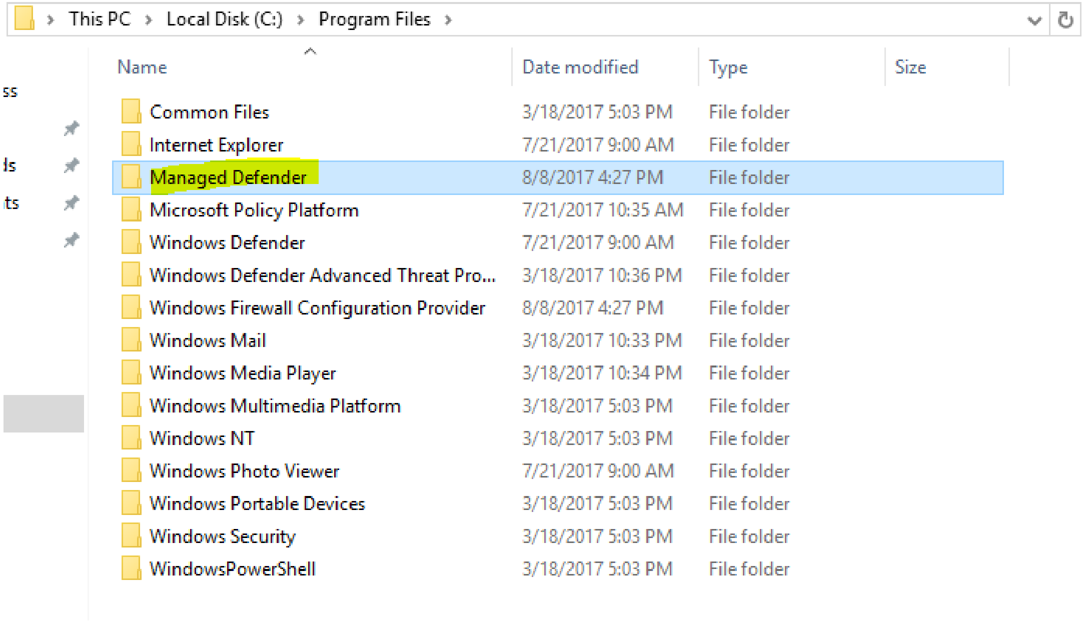
Endpoint Protection Deployment Information

Deployment State:	Managed
Deployment Return Code:	0x00000000
Deployment Description:	The operation completed successfully.
Endpoint Protection Client Version:	4.11.15063.447

Endpoint Protection Remediation Information

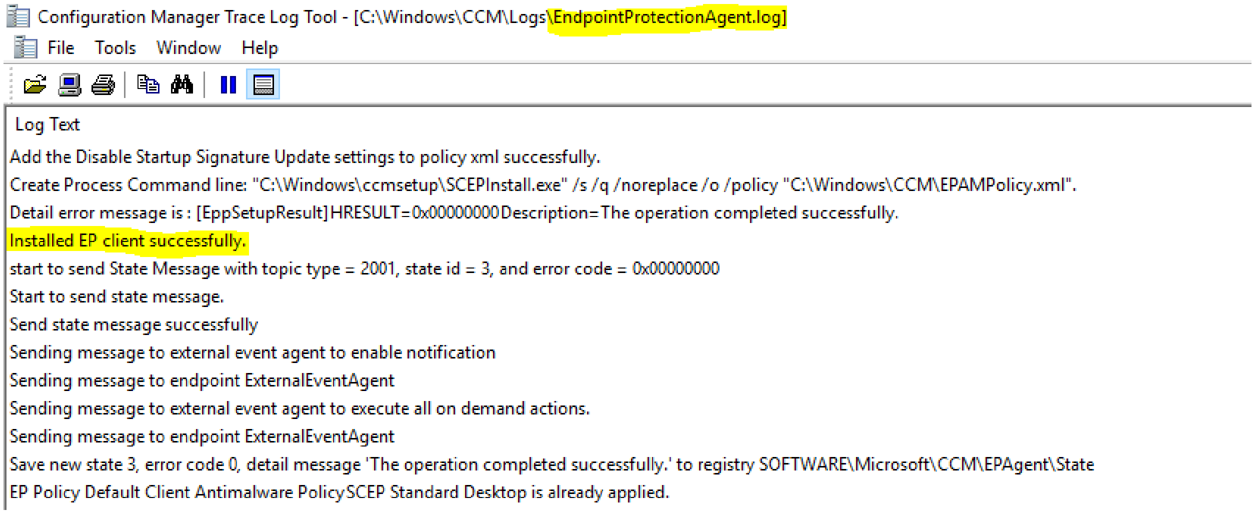
Remediation Status:	Cleaned
Pending Full Scan:	No
Pending Manual Steps:	No
Pending Offline Scan:	No
Pending Reboot:	No
Product Status:	

- **This is what the Client should look like after the installation has been successful.**



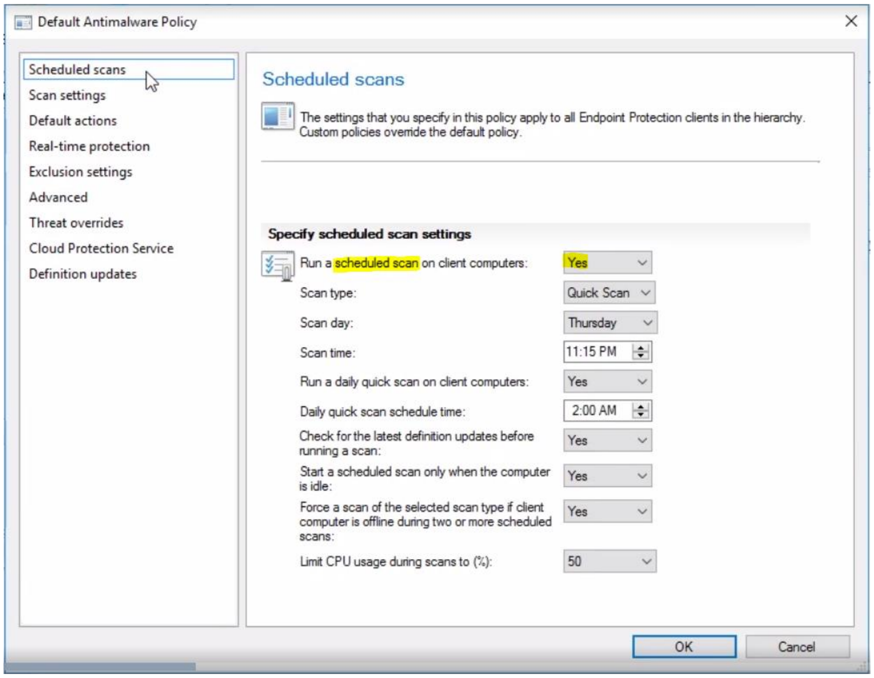
Name	Date modified	Type	Size
Common Files	3/18/2017 5:03 PM	File folder	
Internet Explorer	7/21/2017 9:00 AM	File folder	
Managed Defender	8/8/2017 4:27 PM	File folder	
Microsoft Policy Platform	7/21/2017 10:35 AM	File folder	
Windows Defender	7/21/2017 9:00 AM	File folder	
Windows Defender Advanced Threat Pro...	3/18/2017 10:36 PM	File folder	
Windows Firewall Configuration Provider	8/8/2017 4:27 PM	File folder	
Windows Mail	3/18/2017 10:33 PM	File folder	
Windows Media Player	3/18/2017 10:34 PM	File folder	
Windows Multimedia Platform	3/18/2017 5:03 PM	File folder	
Windows NT	3/18/2017 5:03 PM	File folder	
Windows Photo Viewer	7/21/2017 9:00 AM	File folder	
Windows Portable Devices	3/18/2017 5:03 PM	File folder	
Windows Security	3/18/2017 5:03 PM	File folder	
WindowsPowerShell	3/18/2017 5:03 PM	File folder	

On the Windows 10 Computer, open the EndpointProtectionAgent.log file with the CMtrace.exe command. You should see Installed EP client installed Successfully.


Configuration Manager Trace Log Tool - [C:\Windows\CCM\Logs\EndpointProtectionAgent.log]
File Tools Window Help

```
Log Text
Add the Disable Startup Signature Update settings to policy xml successfully.
Create Process Command line: "C:\Windows\ccmsetup\SCEPInstall.exe" /s /q /noreplace /o /policy "C:\Windows\CCM\EPAMPolicy.xml".
Detail error message is : [EppSetupResult] HRESULT=0x00000000Description=The operation completed successfully.
Installed EP client successfully.
start to send State Message with topic type = 2001, state id = 3, and error code = 0x00000000
Start to send state message.
Send state message successfully
Sending message to external event agent to enable notification
Sending message to endpoint ExternalEventAgent
Sending message to external event agent to execute all on demand actions.
Sending message to endpoint ExternalEventAgent
Save new state 3, error code 0, detail message 'The operation completed successfully.' to registry SOFTWARE\Microsoft\CCM\EPAgent\State
EP Policy Default Client Antimalware Policy SCEP Standard Desktop is already applied.
```

Antimalware Policy Creation



Scheduled scans

The settings that you specify in this policy apply to all Endpoint Protection clients in the hierarchy. Custom policies override the default policy.

Specify scheduled scan settings

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

- Open Configuration Manager console, From the Workspace click **Assets and Compliance, from the Navigation Pane** expand **Endpoint Protection**, right click **Antimalware Policies** and click **Create Antimalware Policy.**

- From the General tab type a name – Type **Windows 10 Desktop**
- At the bottom **Check all** the selections, click **ok**
- From the Navigation Pane, click Antimalware Policies
- From the Lists View right click **Windows 10 Desktop**, click **properties**
- Here we see the categories on the left and the options or settings for each category on the right. Choose these settings to match your organization's needs. For this lecture, I chose the following:

Scheduled Scans

- Run a scheduled scan – Choose Yes
- Scan type – Choose Quick Scan
- Scan day – Select Daily
- Set the Scan Time - 6:00 AM
- Set the reset to the default settings
- Scan Settings
- Scan email and attachments - Yes
- Scan USB thumb drives - Yes
- Scan network files - No
- Scan mapped network drives - No
- Allow users to configure CPU usage during scans - No
- Allow users control of scheduled scans – Normally set to no control
- Default Actions
- Severe – Choose remove
- High - Choose remove
- Medium and Low – Choose Quarantine

Real Time Protection

- Enable real-time protection – Set to Yes
- Scanning system files - Scan incoming and outgoing files
- Enable behavior monitoring – Set to Yes
- Enable protection against network-based exploits – Set to Yes
- The rest set to default

Exclusion Settings

- Accept the defaults

Advanced

- Accept the default settings

Threat Overrides

- Accept the defaults, then move on.

Cloud Protection Services

- Accept default Basic membership

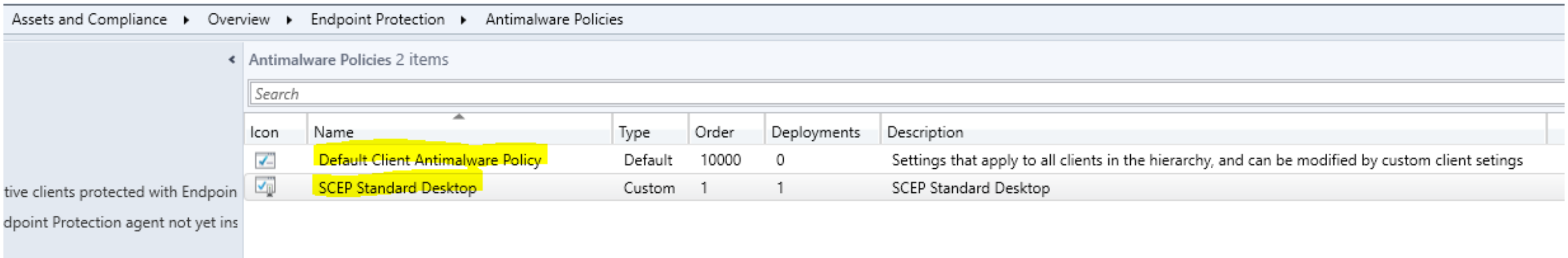
Definition Updates

- Set time interval to 1 hour, accept the defaults
- Set Source – Uncheck all except Updates distributed from Configuration Manager, click **ok**

Deploy the Custom Antimalware Policy to a Collection

- From the List View, right click on the Windows 10 Desktop Policy, click Deploy, Choose a device Collection.

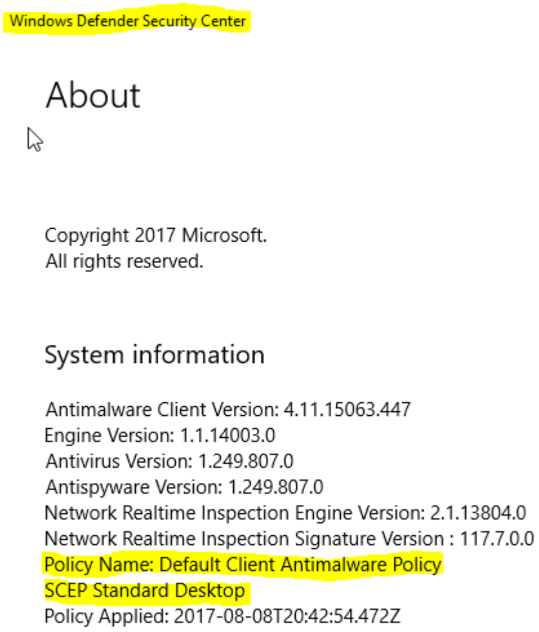
How can we prove that the Windows 10 client has received the default and the custom malware policy as shown in this slide?


Assets and Compliance ▸ Overview ▸ Endpoint Protection ▸ Antimalware Policies
tive clients protected with Endpoin
dpoint Protection agent not yet ins
Search

Antimalware Policies 2 items

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

Depending upon the version of Windows Defender that you have. If you open settings, help, about, if your windows 10 WS is managed you should see the three antimalware policies listed at the bottom of the screen.



Windows Defender Security Center

About

Copyright 2017 Microsoft.
All rights reserved.

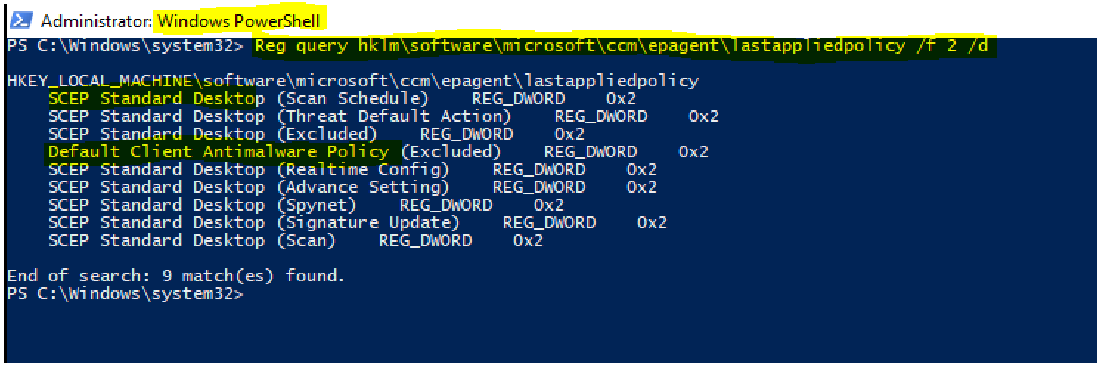
System information

Antimalware Client Version: 4.11.15063.447
Engine Version: 1.1.14003.0
Antivirus Version: 1.249.807.0
Antispyware Version: 1.249.807.0
Network Realtime Inspection Engine Version: 2.1.13804.0
Network Realtime Inspection Signature Version : 117.7.0.0
Policy Name: Default Client Antimalware Policy
SCEP Standard Desktop
Policy Applied: 2017-08-08T20:42:54.472Z

Another method to verify the EP client installation is to use Windows Powershell to search the registry for the last applied policy statement.

Open Windows Powershell and type

- Reg Query hklm\software\microsoft\ccm\epagent\lastappliedpolicy /f 2 /d – double check
- You can see the SCEP standard desktop policy the Default Client Antimalware Policy and the Windows 10 Desktop Policy have all been applied to this computer.



Administrator: Windows PowerShell

```
PS C:\Windows\system32> Reg query hklm\software\microsoft\ccm\epagent\lastappliedpolicy /f 2 /d

HKEY_LOCAL_MACHINE\software\microsoft\ccm\epagent\lastappliedpolicy
    SCEP Standard Desktop (Scan Schedule)    REG_DWORD    0x2
    SCEP Standard Desktop (Threat Default Action)    REG_DWORD    0x2
    SCEP Standard Desktop (Excluded)    REG_DWORD    0x2
    Default Client Antimalware Policy (Excluded)    REG_DWORD    0x2
    SCEP Standard Desktop (Realtime Config)    REG_DWORD    0x2
    SCEP Standard Desktop (Advance Setting)    REG_DWORD    0x2
    SCEP Standard Desktop (Spynet)    REG_DWORD    0x2
    SCEP Standard Desktop (Signature Update)    REG_DWORD    0x2
    SCEP Standard Desktop (Scan)    REG_DWORD    0x2

End of search: 9 match(es) found.
PS C:\Windows\system32>
```

Setting up Alerts

- From the Workspace click Assets and Compliance, from the Navigation Pane click Device Collections

- Right click the **target collection** on which you deployed the **antimalware policy**, click **properties**, then click **Alerts**, check the box that says **View this collection in the Endpoint Protection Dashboard**. Click **Add.**
- In the Add New Collection Alerts check **all the options except the last option**, click **ok,** then **ok again.**

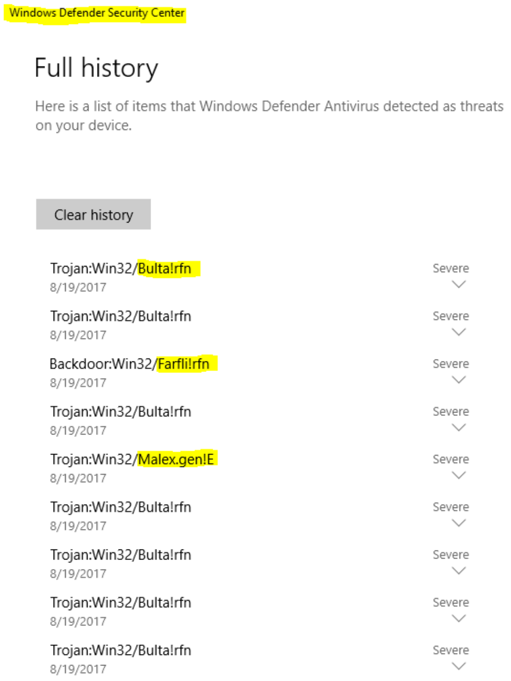
Windows Firewall Policies

- For this lecture here are the settings, your settings may be different. The settings are based upon the needs of your organization.
- From the Workspace, click Assets and Compliance, then from the Navigation Pane click Endpoint Protection.
- Right click Windows Firewall Policies, click Create Windows Firewall Policy
- For a name type ITFLEE Firewall Policy, click next
- Categories to the left, options to the right.
- Enable Windows Firewall
- Under Profile Settings, Domain Profile, change to Yes.
- For Private profile, change to Yes
- change to Yes
- Block all incoming connections – With these settings below, any inbound traffic originating from outside of our machine would be blocked.
- Domain Profile, change to Yes.
- For Private profile, change to Yes
- Public Profile change to Yes
- Notification
- Domain Profile, change to Yes.
- For Private profile, change to Yes
- Public Profile change to Yes

Testing the Effectiveness of Endpoint Protection and Windows Defender

- I purposely downloaded a number of Malware, Trojans and various other nasty computer viruses just to test the effectiveness of Windows Defender.
- I have to say this!! I would definitely not recommend downloading and installing Malware and viruses on your production network.
- If you would like to test the capabilities of EP and Windows Defender, I would recommend that you disconnect the target computer from your labs network so that the Malware has no opportunity to spread to the other VM's in your lab.
- From the Windows 10 computer ITFSW02 open Windows Defender, open Scan History, See full history

Displayed is the list of Trojans and Malware that Windows Defender detected.



Windows Defender Security Center

Full history

Here is a list of items that Windows Defender Antivirus detected as threats on your device.

Trojan:Win32/Bulta!rfn 8/19/2017	Severe
Trojan:Win32/Bulta!rfn 8/19/2017	Severe
Backdoor:Win32/Farfli!rfn 8/19/2017	Severe
Trojan:Win32/Bulta!rfn 8/19/2017	Severe
Trojan:Win32/Malex.gen!E 8/19/2017	Severe
Trojan:Win32/Bulta!rfn 8/19/2017	Severe
Trojan:Win32/Bulta!rfn 8/19/2017	Severe
Trojan:Win32/Bulta!rfn 8/19/2017	Severe
Trojan:Win32/Bulta!rfn 8/19/2017	Severe

Bultarfn is a Trojan that can steal your personal information and send it off to a hacker or give a malicious hacker access to your PC. (Rated as severe)
I installed this Trojan seven times on this computer.

- Farfli!rfn – This threat can give a malicious hacker unauthorized access and control of your PC. (Rated as severe)
- Malex.gen!E – This is a malicious file that attempts to copy itself in certain folders without the users consent or knowledge. This trojan is able to open a backdoor to allow remote hackers access to your PC. This trojan can change your PC settings, block Anti-virus software, and cause identity theft. Considered a serious threat.

Now let’s use the SCCM SQL Server Reporting Services to check out the effectiveness of Windows Defender

- From the SCCM server open Configuration Manager, from the Workspace click Monitoring.
- From the Navigation Pane click **Reporting**, from Report Manager, click the reports server, in this case itfsccm01.
- Login to Windows Security, click configMgr_ITF
- Click Endpoint Protection, then click Infected Computers
- From Collection Name, click **Windows 10**

- From Start Date type **8/20/2017**
- Then click View Report
- Double click ITFWS02, scroll down and there is the list of malware and trojans that were installed on the Windows computers.
- To the right under action, you can see that Windows Defender was successful in each case to remove these serious threats.

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