COMODO
Creating Trust Online®

Comodo
Endpoint Security Manager
Professional Edition

Software Version 3.3

Administrator Guide

Guide Version 3.2.031115

Table of Contents

COMODO
Creating Trust Online®

1.Introduction to Comodo Endpoint Security Manager - Professional Edition

Comodo Endpoint Security Manager (CESM) Professional Edition is designed to help administrators of corporate networks deploy, manage and monitor Comodo Endpoint Security software on networked computers.

Total Protection for networked computers

The most powerful & intuitive all-purpose Endpoint manager in its class, CESM PE manages not only the security of your workstations, laptops and netbooks, but now also manages their system status. Once installed through the simplified wizards, endpoints are quickly and efficiently discovered via Active Directory query or IP address range. They can then be grouped as required and administrative policies applied. CESM will automatically reapply those policies to endpoints not compliant with their required configurations.

More efficient, effective and easier management

This ability to roll out and centrally manage security policies to a network that is protected with a proven and fully integrated security suite can save thousands of man-hours per year. Administrator time that would otherwise be lost to repetitive configuration and vendor interoperability problems can be re-directed towards more productive and profitable core business interests. Furthermore, because CESM policies can be deployed immediately across all protected nodes, administrators can respond more quickly to protect an entire network against the latest, zero hour threats. CESM's intuitive interface provides fingertip access to task wizards, important network and task related data and support resources.
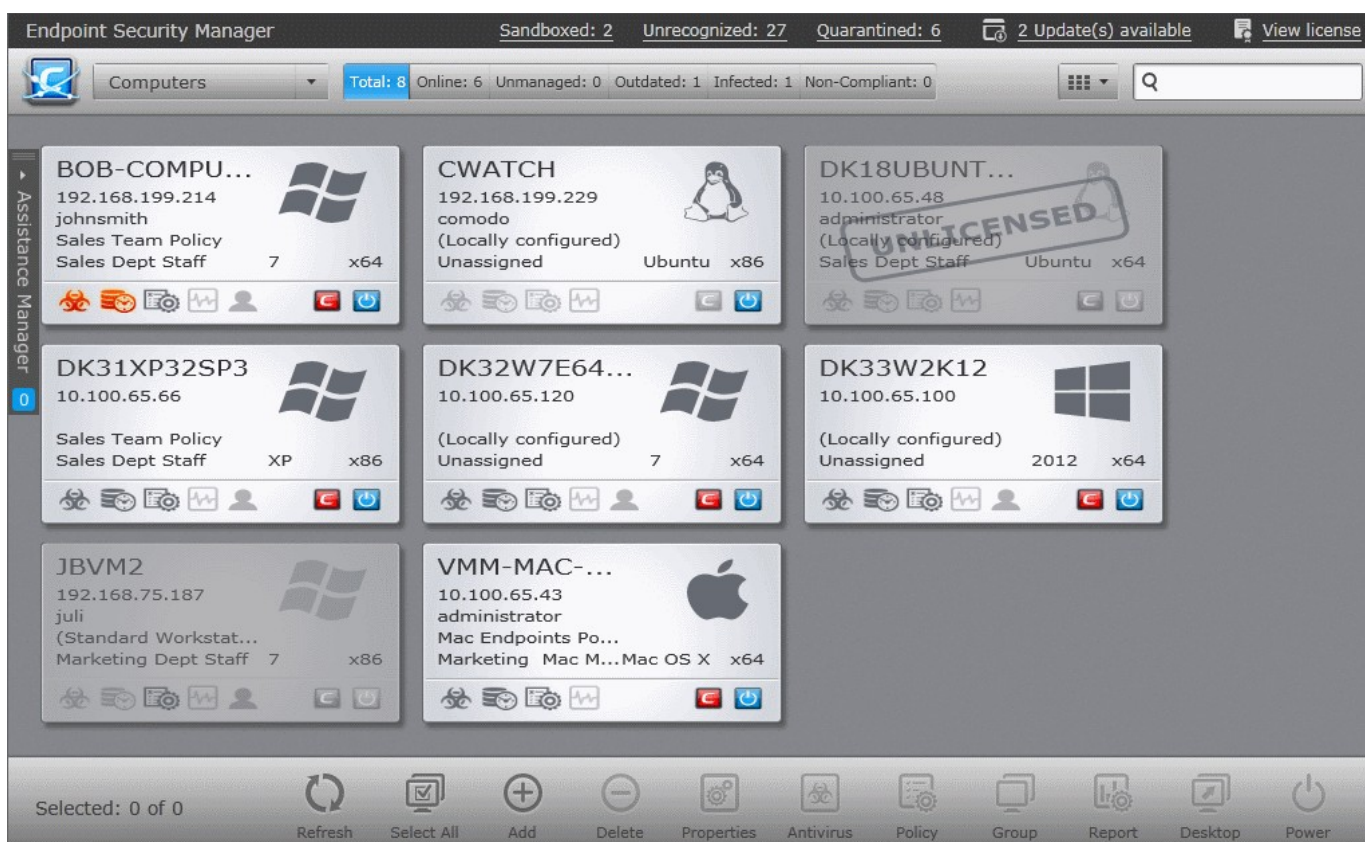
Features:

• Total visibility and control over endpoint security through a centralized, web-based console. New, panorama-style, interface compatible with touch-screen computers.

• Seamless import and control of Microsoft Active Directory Domain into the CESM Administrative Console.

- Proven endpoint protection from Comodo Endpoint Security software - including real-time antivirus, packet-filtering firewall, website filtering, automatic sand-boxing of untrusted files and strict host intrusion prevention.

- Provides granular software and hardware details for each endpoint including OS version, installed applications, CPU and RAM usage and more.

- Effortless endpoint management. Remotely restart endpoints, manage running applications, processes and services. initiate remote desktop sessions through the CESM interface and more.

- Highly configurable policies allow admins to enforce power options and device availability controls on endpoints.

- New 'Internet policy' supports different CES configuration for devices when inside or outside of the network.

- Real time notifications lower emergency response time to emerging threats.

- Protects Mac OS based computers with proactive Antivirus and centralized management.

- Supports Linux based computers and Windows Embedded systems like Point of Sales (POS) terminals.

- New reports with built in drill down to computers and in-report remediation.

- Integrated chat window to interact with endpoint users for resolving issues immediately.

Guide Structure

This guide is intended to take you through the configuration and use of Comodo Endpoint Security Manager Professional Edition and is broken down into the following main sections.

The Computers Area - Plays a key role in the CESM Administrative Console interface by providing system administrators with the ability to import, view and manage networked computers.

- Add/Import computers to CESM for centralized management.

- View complete details of the endpoints that are managed by CESM.

    - Assign and re-assign endpoints to groups.
    - Manage quarantined items, currently running applications, processes and services in remote endpoints.
    - Managing drives and storage at the endpoints.

- Run on-demand antivirus scans on individual or a bunch of selected endpoints.

- Start shared remote desktop session with remote endpoints.

The Groups Area - Allows administrators to create endpoint groups in accordance with your organization's structure and apply appropriate security policies.

- Create computer Groups for easy administration.

- Apply security policies to groups.

- Run on-demand antivirus scans on individual or multiple endpoints.

- Generate granular reports for grouped endpoints.

The Policies Area - Allows administrators to create, import and manage security policies for endpoint machines.

- View and modify the configuration of any policy - including name, description, security product components, target computers and whether the policy should allow local configuration.

- Create new policies by importing settings from another computer or by modifying an existing policy.

- Apply policies to entire endpoint groups.

The Quarantine area - View all the suspicious programs, executables, applications and files moved to quarantine by CES and CAS installations at the managed endpoints and manage them.

The Sandbox area - View all the unrecognized programs, executables, applications that are currently run inside the sandbox at the managed endpoints and manage them.

Files Management - View all the executable files which are not identified as safe on checking with Comodo certified safe files database and manage them.

The Applications area - View all applications installed on endpoints and uninstall unwanted applications.

The Processes area - View the processes running currently on all the endpoints in real time and terminate unnecessarily running processes at selected endpoints.

The Services Area - View the Windows Services, Unix Daemons and Mac Services that are loaded on all the managed

endpoints and start or stop services on selected endpoints.

The Reports Area - Generate highly informative, graphical summaries of the security and status of managed endpoints.

- Drill-down reports can be ordered for anything from a single machine right up to the entire managed network.

- Each report type is highly customizable according to administrator's requirements.

- Reports can be exported to .pdf and .xls formats for printing and/or distribution.

- Available reports include endpoint security product configuration, policy compliance, malware statistics, policy delta, security product logs, quarantined items and more.

The Help Area - Allows the administrator to view CESM version and update information, view and upgrade licenses, and view support information.

- View the version and update information. View the license information and activate/upgrade licenses.

- View details of the server upon which CESM is installed.

- View support contact information and different ways to get help on CESM.

The Preferences Area - Allows the administrators to configure language settings, report archives, email notifications and dependent CESM servers and to download CESM agents for offline installation on remote endpoints.

- Download CESM Agent for installation on to remote endpoints, to manually add them to CESM

- Configure the lifetime of the generated reports generated and retained in CESM server.

- Select the language in which CESM interfaces should appear.

- Configure automated email notifications from CESM. CESM can send notification mails to administrator on the occurrence of certain events like virus outbreaks, malware found and more.

- Configure 'dependent' CESM servers. Centrally manage and configure any subordinate CESM server currently managing endpoints on a different network.

- Configure the auto discovery feature to identify unmanaged endpoints in Active Directory.

1.1. Software Components and System Requirements

Software Components

CESM Professional Edition consist of three interdependent software components:

- **The Administrative Console**
- **The Central Service**
- **The Remote Agent**

Administrative Console
The Administrative Console provides access to all functionality of Comodo Endpoint Security Manager through a friendly and highly configurable interface. Administrators can use the console to deploy, manage and monitor Comodo Endpoint security software on networked computers.

- **Click here** to go to the Admin console help pages.

- **Click here** for system requirements for endpoint machines that run the administrative console.

- **Click here** to read about logging into the console.

Central Service
The Central Service is the main functional module responsible for performance of all CESM system tasks. Central Service also keeps and updates information on all current and past system's activities.

- **Click here** for a guide that explains how to install Central Service.

- **Click here** for system requirements for machines that run the central service.

- **Click here** to read about the central service configuration tool.

Remote Agents

Remote Agents are intermediaries between remotely managed PC's and CESM Central Service and must be installed on every managed PC. CESM Remote Agents are responsible for receiving tasks and requests from the Central Service and executing those tasks on the Managed Computers. ('Tasks' from Central Service include operations such as installing or uninstalling software, fetching report information and applying security policy). Endpoints imported into a CESM service can be managed only by the same CESM service - meaning the agent cannot be reconfigured to connect to any other CESM service - a feature which increases security.

- **Click here** for system requirements for endpoint machines that run the CESM agent and the security software CES/CAS or CAV for Mac.

- **Click here** to read how to install and deploy the agent.

System Requirements

CESM Central Service Computer (the PC that will run the Endpoint Security Manager software)

CENTRAL SERVICE COMPUTER - SYSTEM REQUIREMENTS		
Hardware		
Component	**32 bit**	**64-Bit**
Processor	Dual-Core 1.8 GHz processor or better	Dual-Core 1.8 GHz processor or better
Memory	2 GB RAM (4GB recommended)	2 GB RAM (4GB recommended)
Hard Disk	16 GB (15 GB free disk space if using SQL Express 2008/2012)	20 GB (15 GB free disk space if using SQL Express 2008/2012)
Display	Super VGA (1024x768) or higher resolution video adapter and monitor	Super VGA (1024x768) or higher resolution video adapter and monitor
Software		
Operating System	The following operating systems are supported: **Microsoft Windows Server Family**: Windows 2003 Server (SP2 or higher) Windows 2003 Small Business Server Windows 2003 Small Business Server R2 Windows 2008 Server (SP2 or higher) Windows 2008 Small Business Server Windows 2008 Server R2 Windows 2011 Small Business Server Windows 2012 Server **Microsoft Windows Client Family:** Windows XP (SP3 or higher) Windows Vista (SP1 or higher) Windows 7 Windows 8 Windows 8.1	The following operating systems are supported: **Microsoft Windows Server Family:** Windows 2003 Server (SP2 or higher) Windows 2003 Small Business Server Windows 2003 Small Business Server R2 Windows 2008 Server (SP2 or higher) Windows 2008 Small Business Server Windows 2008 Server R2 Windows 2011 Small Business Server Windows 2012 Server **Microsoft Windows Client Family:** Windows Vista (SP1 or higher) Windows 7 Windows 8 Windows 8.1

CENTRAL SERVICE COMPUTER - SYSTEM REQUIREMENTS		
Software Environment	Microsoft® .NET Framework 4.0/4.5 Microsoft ReportViewer 2010 SP1 (**Note** - The above components will be installed automatically if not present. If Microsoft .Net Framework 4.0 is present in the system, it will be updated to Microsoft .Net Framework 4.5 automatically. During the update the system will require to restart the server. If you want to avoid restarting the server, close all the applications that use .NET Frame work before installing CESM. However, if some system applications could not be closed, the restart cannot be avoided.)	Microsoft® .NET Framework 4.0/4.5 Microsoft ReportViewer 2010 SP1 (**Note** - The above components will be installed automatically if not present. If Microsoft .Net Framework 4.0 is present in the system, it will be updated to Microsoft .Net Framework 4.5 automatically. During the update the system will require to restart the server. If you want to avoid restarting the server, close all the applications that use .NET Frame work before installing CESM. However, if some system applications could not be closed, the restart cannot be avoided.)
Database	Microsoft SQL Server 2012 Express LocalDB (Note - The above component will be installed automatically if not present)	Microsoft SQL Server 2012 Express LocalDB (Note - The above component will be installed automatically if not present)
Other Requirements	The CESM program modules (Console, Service and Agent) may require Windows Firewall and/or personal firewall configuration changes in order to operate successfully. By default, the CESM Central Service is assigned: • TCP Port 9901 open to the Internet for inbound connections from Agents on portable computers • TCP Ports 57193, 57194 open to the Internet for inbound http: and https: console connections • TCP port 57195 open to the Internet for remote desktop sessions of managed computers through the console These ports can be opened in Windows Firewall by opening the control panel, selecting 'Windows Firewall > Exceptions > Add Port...' then specifying each of the ports above in turn.	

CESM Administrative Console computer - (PCs that will run the browser-based interface for configuring and managing the CESM Central Service (this computer may also be the Central Service PC)

ADMINISTRATIVE CONSOLE COMPUTER - SYSTEM REQUIREMENTS		
Hardware		
Component	**32 bit**	**64-Bit**
Display	Minimum 1024x768 display with windowed browser Touch capable display interface and operating system (optional)	Minimum 1024x768 display with windowed browser Touch capable display interface and operating system (optional)
Software		
Operating System	The following operating systems are supported: **Microsoft Windows Server Family:** Windows 2003 Server (SP2 or higher) Windows 2003 Small Business Server Windows 2003 Small Business Server R2 Windows 2008 Server (SP2 or higher)	The following operating systems are supported: **Microsoft Windows Server Family:** Windows 2003 Server (SP2 or higher) Windows 2003 Small Business Server Windows 2003 Small Business Server R2 Windows 2008 Server (SP2 or higher)

ADMINISTRATIVE CONSOLE COMPUTER - SYSTEM REQUIREMENTS		
	Windows 2008 Small Business Server Windows 2008 Server R2 Windows 2011 Small Business Server Windows 2012 Server **Microsoft Windows Client Family:** Windows XP (SP3 or higher) Windows Vista (SP1 or higher) Windows 7 Windows 8 Windows 8.1	Windows 2008 Small Business Server Windows 2008 Server R2 Windows 2011 Small Business Server Windows 2012 Server **Microsoft Windows Client Family:** Windows Vista (SP1 or higher) Windows 7 Windows 8 Windows 8.1
Browsers and software	Microsoft Silverlight 5.1 Microsoft Internet Explorer 10.0 or higher Mozilla Firefox 21.0 or higher Google Chrome 27.0 or higher Comodo Dragon 27.0 or higher	Microsoft Silverlight 5.1 Microsoft Internet Explorer 10.0 or higher Mozilla Firefox 21.0 or higher Google Chrome 27.0 or higher Comodo Dragon 27.0 or higher
Other Requirements	• TCP Ports 57193,57194 will be used for http: and https: connections	

Endpoint Computer (Windows) - (a managed Window based PC that will run CESM Agent and Endpoint security software CES/CAS)

ENDPOINT COMPUTER - SYSTEM REQUIREMENTS		
Hardware		
Component	**32 bit**	**64-Bit**
Processor *recommended*	1.2 GHz 32 bit processor or higher	1.2 GHz 64 bit processor or higher
Memory *recommended*	512 MB RAM (1GB recommended)	512 MB RAM (1GB recommended)
Hard Disk recommended	420 MB free hard drive space	420 MB free hard drive space
Software		
Operating System	The following operating systems are supported: **Microsoft Windows Server Family:** Windows 2003 Server (SP2 or higher) Windows 2003 Small Business Server Windows 2003 Small Business Server R2 Windows 2008 Server (SP2 or higher)	The following operating systems are supported: **Microsoft Windows Server Family:** Windows 2003 Server (SP2 or higher) Windows 2003 Small Business Server Windows 2003 Small Business Server R2 Windows 2008 Server (SP2 or higher)

ENDPOINT COMPUTER - SYSTEM REQUIREMENTS		
	Windows 2008 Small Business Server Windows 2008 Server R2 Windows 2011 Small Business Server Windows 2012 Server **Microsoft Windows Client Family:** Windows XP SP3 or higher Windows Vista Windows 7 Windows 8 Windows 8.1	Windows 2008 Small Business Server Windows 2008 Server R2 Windows 2011 Small Business Server Windows 2012 Server **Microsoft Windows Client Family:** Windows Vista Windows 7 Windows 8 Windows 8.1
Other Requirements	The CESM program modules (Console, Service and Agent) may require Windows Firewall and/or personal firewall configuration changes in order to operate successfully. By default, the CESM Central Service is assigned: • TCP Port **9901** for connections with the CESM Agent. These ports can be opened in Windows Firewall by opening the control panel, selecting 'Windows Firewall > Exceptions > Add Port...' then specifying each of the ports above in turn. • Also for ESM Agent installation using the Deployment wizard, target computer should be prepared as follows: The registry key HKLM\SYSTEM\CurrentConrolSet\Control\Lsa\forceguest must be set to «0»; On Windows Vista and higher, if the account is not a built-in Administrator, check if HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\LocalAccountTokenFilterPolicy DWORD registry value is set to «1».	

Endpoint Computer (Mac OS X) - (a managed Mac OS X based computer that will run CESM Agent and Endpoint security software CAV for Mac)

ENDPOINT COMPUTER - SYSTEM REQUIREMENTS	
Software	
Operating System	**Mac OS X client family:** Mac OS X 10.6.8 Mac OS X 10.9

Endpoint Computer - (a managed PC/Device will run CESM Agent, device management only)

ENDPOINT COMPUTER - SYSTEM REQUIREMENTS
Software

ENDPOINT COMPUTER - SYSTEM REQUIREMENTS	
Operating System	**Linux .deb family:** Debian (6.0.6 or higher) x86 and x64 editions Ubuntu (12.04 or higher) x86 and x64 editions **Windows Embedded Systems:** Windows 7 only

1.2. Removing Incompatible Products

For Comodo Endpoint Security to operate correctly, incompatible security software must first be removed from endpoint machines.

- During the installation process, CESM PE can detect and automatically remove some brands of incompatible software.

- However, certain software can be detected by CESM PE, but must be removed manually.

- The following table contains a list of incompatible software and states whether CESM PE can detect and remove it or only detect it.

Vendor	Product Name	Uninstall Type	Version Tested	Components
Agnitum	Outpost Security Suite Pro 7.1	Detect only	3415.520.1247	Outpost Security Suite Pro 7.1
AVAST Software	avast! Free Antivirus	Detect only	6.0.10.91	avast! Free Antivirus
AVG Technologies	AVG Internet Security	Detect only	10.0.1325	AVG 2011
Avira GmbH	Avira AntiVir Premium	Detect only	10.2.0.278	Avira AntiVir Desktop
Comodo Group	Comodo Internet Security 4.1, 5.8	Automatic	4.1, 5.8	Comodo Internet Security
Doctor Web, Ltd.	Dr.Web anti-virus for Windows 6.0 (x86/x64)	Detect only	6.0.5.02020	Dr.Web anti-virus for Windows 6.0 (x86/x64)
	Dr.Web Security Space 6.0 (x86/x64)	Detect only		Dr.Web Security Space 6.0 (x86/x64)
ESET	ESET Smart Security	Automatic	4.2.67.10, earlier	ESET Smart Security
Kaspersky Lab.	Kaspersky Antivirus	Detect only		Kaspersky Antivirus
McAfee, Inc.	McAfee Total Protection	Detect only	11.0.572	McAfee SecurityCenter 11.0 McAfee VirusScan 15.0 McAfee Personal Firewall 12.0 McAfee SiteAdvisor 3.3 McAfee Anti-Spam 12.0 McAfee Parental Controls 13.0 McAfee Anti-Theft File Protection 2.0 McAfee Online Backup 3.0 McAfee QuickClean and Shredder 11.0
	McAfee Internet Security	Detect only	11.0.572	McAfee SecurityCenter 11.0

				McAfee VirusScan 15.0
				McAfee Personal Firewall 12.0
				McAfee Anti-Spam 12.0
				McAfee Parental Controls 13.0
				McAfee Online Backup 3.0
				McAfee QuickClean and Shredder 11.0
	McAfee VirusScan Enterprise	Automatic		McAfee VirusScan Enterprise
Sophos Limited	Sophos Endpoint Security and Control	Automatic	9.7, earlier	Sophos AutoUpdate Sophos Anti-Virus Sophos Client Firewall
Symantec Corporation	Symantec Endpoint Protection	Automatic	11.0.6005.562, earlier	Symantec Endpoint Protection
Fortinet	FortiClient Lite	Automatic	4.3.3.0445	FortiClient Lite 4.3.3.445

If your product is detected but not automatically removed, please consult your vendor's documentation for precise uninstallation guidelines.

However the following steps will help most Windows users:

- Click the Start button to open the Windows Start menu.
- Select Control Panel > Programs and Features (Win 7, Vista); Control Panel > Add or Remove Programs (XP).
- Select your current antivirus or firewall program(s) from the list.
- Click Remove/Uninstall button.
- Repeat process until all required programs have been removed.

1.3. Installing and Configuring the Service

1. Downloading and running the installer

Download and save the CESM setup file to the computer that will be used for the Central Service. This unified installer can be used to setup both the Central Service and CESM configuration tool.

You have a choice of two installation files, 'CESM_Setup_3.1.<version>.exe' or 'CESM_Setup_3.1.<version>_Full.exe'.

The '..._FULL.exe' file is a larger file that also contains additional, required software (.net Framework 4,5, SSQL Server 2012 Express LocalDB and Microsoft Report Viewer 2010 SP1).

The other file does not contain this additional software but will download it from the Internet if it is not detected on your server.

To start the installation, double click on the setup file . The installation wizard will start and the 'Select the language' dialog is displayed. CESM is available in several languages.
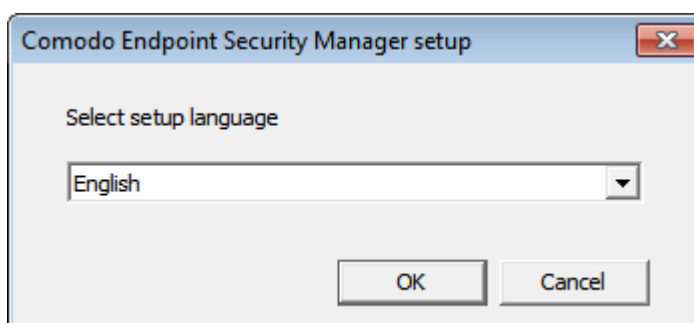
- Select the language in which you want CESM to be installed from the drop-down and click 'OK'.

The installer will first check whether all the required supporting software are installed in the server. If not, it will install the supporting software first. You can continue the installation only after installing the additional software by clicking the setup icon again and selecting the language.
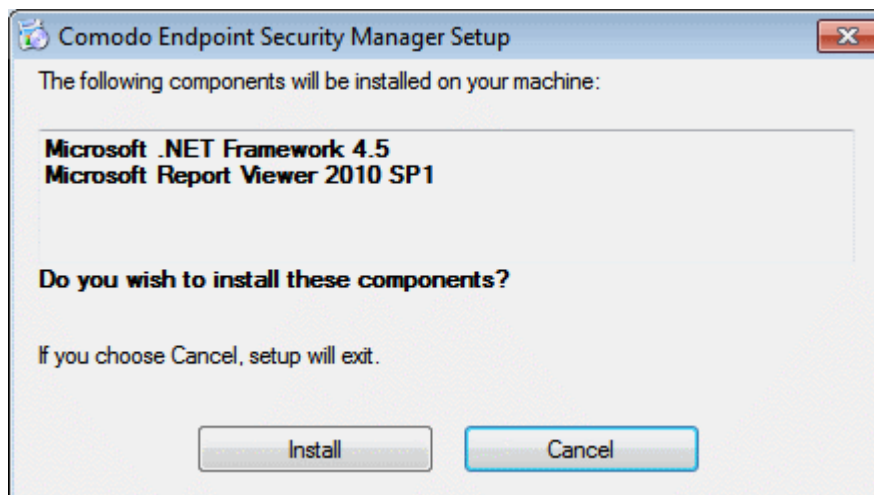
If the additional software are already available, the installation of CESM will start.

2. Welcome Screen
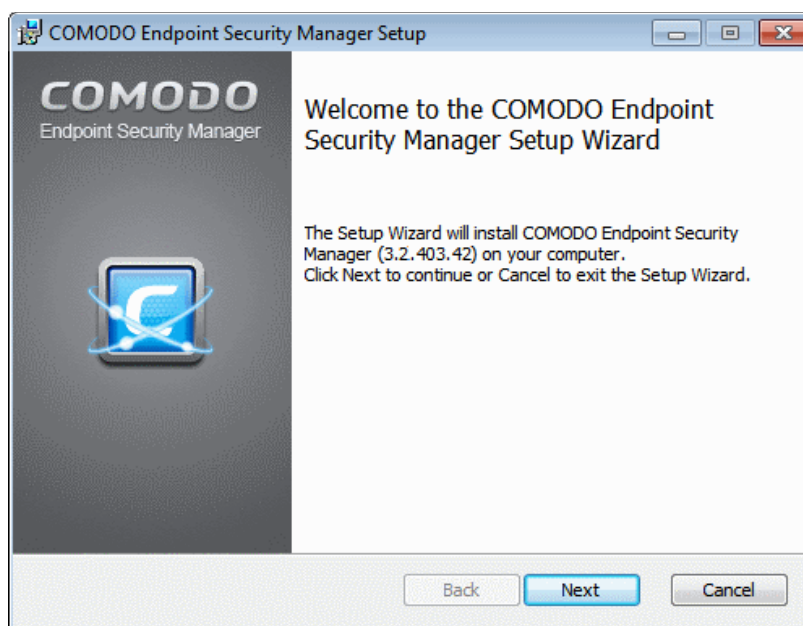
The welcome screen will be displayed.

- Click 'Next'.

3. License Agreement

The End-User License Agreement will be displayed:
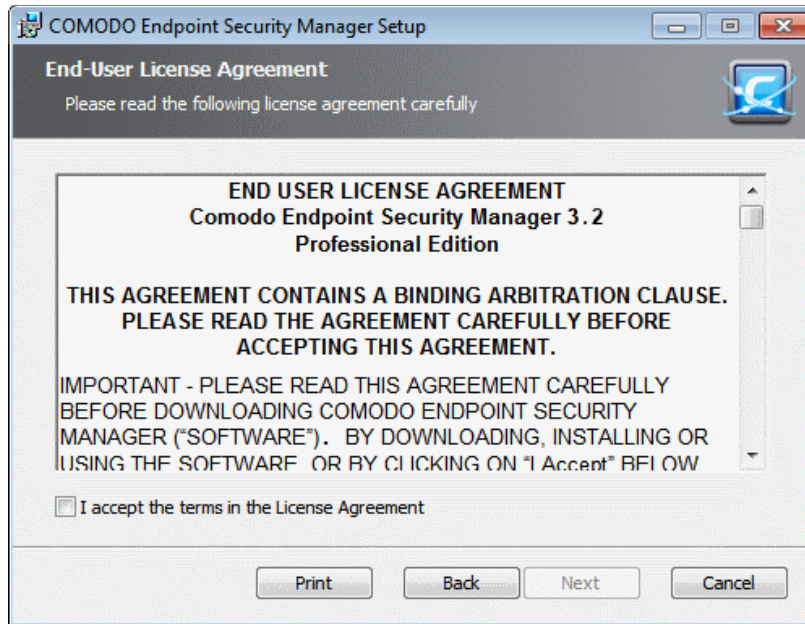
To complete the initialization phase you must read and accept to the License Agreement. After you have read the End-User License Agreement, check the 'I accept the terms in the License Agreement' box and click 'Next' to continue installation. If you decline, you cannot continue with the installation.

The release notes for the current version of CESM will be displayed.
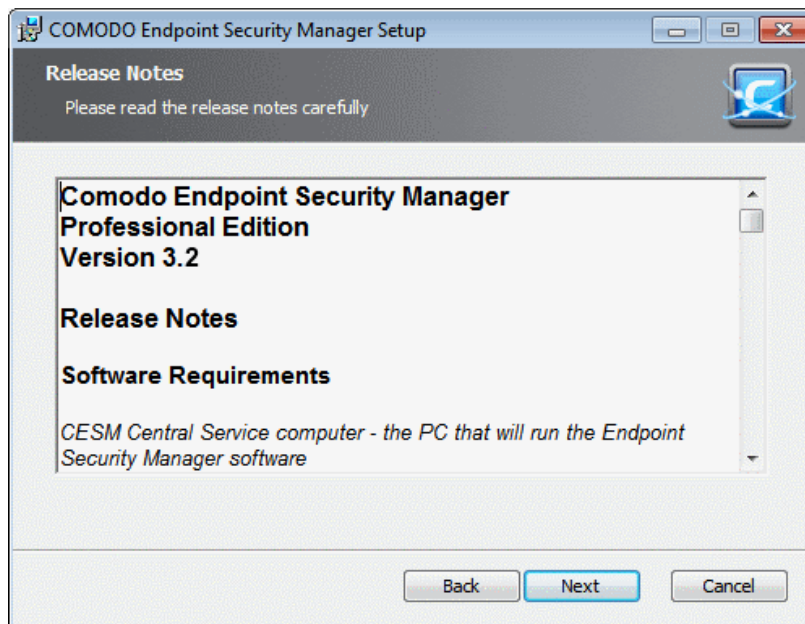
• Read the notes and click 'Next'.

4. Choosing Installation Preferences

The next stage is to choose the setup type:

- **Typical** - Installs all components (CESM Server and Documentation) to the default location of c:\Program Files > Comodo > Endpoint Security Manager. This is the option recommended for most users. After installation you have to enter the license key in the 'License Information' screen. Refer to Help > **License Information** for more details.

  On selecting 'Typical' and clicking 'Next', you need to choose whether or not you want to install Proxy Cache Service.

  - If you want the security product (CES/CAS/CAVM) installations at the managed endpoints to download AV database updates from a proxy server, choose to install 'Proxy Cache Service'
  - If you want the security product installations at the managed endpoints to download AV database updates from the Comodo servers directly, you need not install 'Proxy Cache Service'
  - For more details on setting up a proxy server, refer to the section **Caching Proxy Settings** under **Appendix 1 - The Service Configuration Tool**
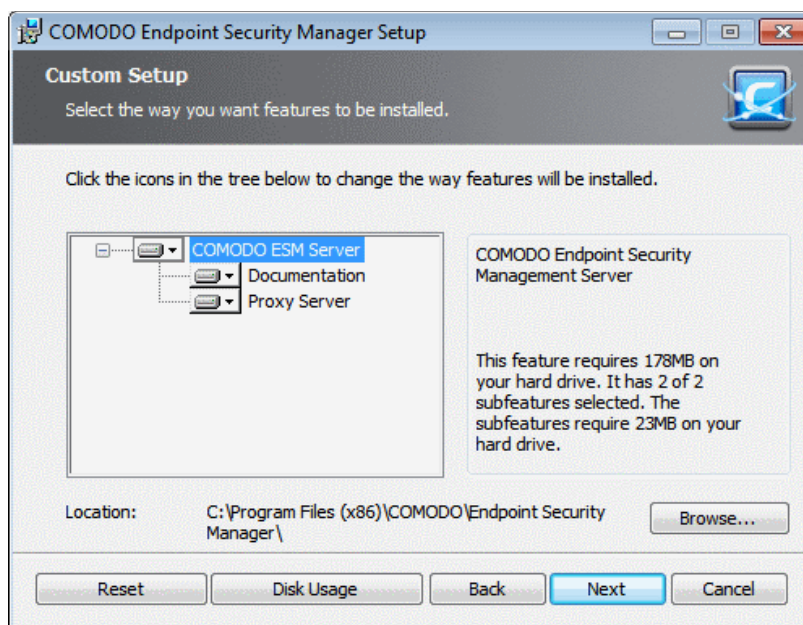
  The setup progress will move to **Selecting Database Server**.

Note: If you choose to install CESM PE in Typical mode, after installation the administrator needs to enter the license key in the Help > **License Information** screen, in order to start using the application.

- **Custom** - Enables the administrator to choose which components are installed and modify the installation path *if required* and to enter the license key. On selecting Custom and clicking 'Next', the Custom Setup dialog will be displayed:

  On selecting 'Custom' and clicking 'Next', the setup progress will move to **Selecting Components**

- **Complete** - Installs all components (CESM Server and Documentation) to the default location of C:\Program Files > Comodo > Endpoint Security Manager. This is the option recommended for most users.

  On selecting 'Complete' and clicking 'Next', the setup progress will move to **Selecting Database Server**.

5. Selecting Components

Choose the components that you want to install.

Custom Setup - Key	
Control	**Description**
	Icons with the ▼ symbol to the right are the currently selected installation option. Clicking this icon will open a menu allowing the user to select alternative installation options. These alternative installation options are explained in the next four rows of this table.
	Indicates that the component named to the right of the icon will be installed on the local drive.
	Indicates that the component named to the right of the icon and all of its associated sub-components will be installed on the local drive.
	Indicates that the component named to the right of the icon will be installed as and when the user requires. Choosing this option will create a shortcut to the Comodo folder on the Windows start menu - allowing the feature to be installed when the shortcut is selected.
	Indicates that the component named to the right of the icon will not be installed.
Browse....	The 'Browse...' button allows to select another location folder for CESM to be installed.
Reset	The 'Reset' button allows to roll back to default installation options.
Disk Usage	The combined disk space that will be taken up if the currently selected components are installed.
Back	The 'Back' button allows to roll back to 'Release Notes' dialog.
Next	The 'Next' button confirms your choices and continues onto the next stage of the installation process.
Cancel	The 'Cancel' button annuls the installation and quits the installation wizard.

- Click the 'Browse...' button to change installation directory (default = 'C:\Program Files\COMODO\Endpoint Security Manager').

- Click 'Next' to move to the next step.

6. Entering the License Key

- Enter the license key you received through email and click Register.
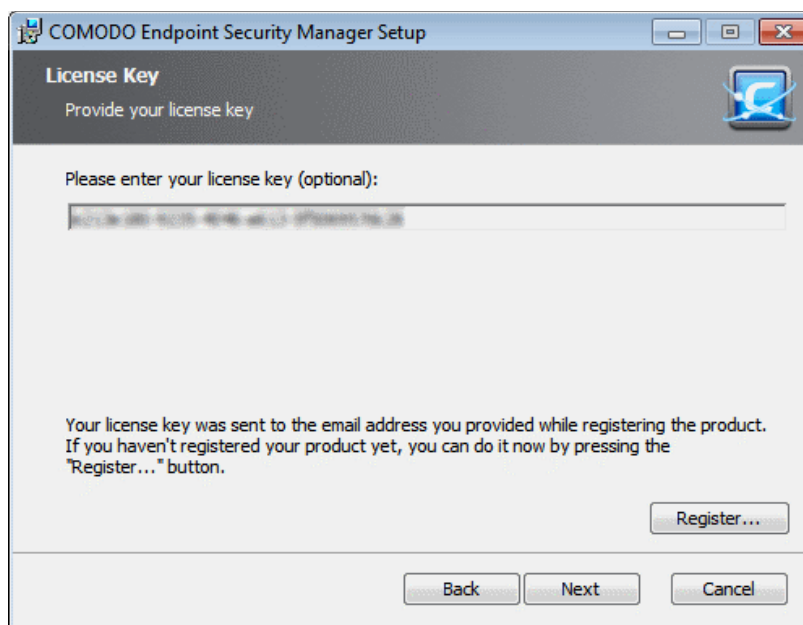
Note: If you do not want to activate the license at this moment or do not have the license key handy, you can skip to next step **Selecting Database Server** by clicking Next without entering the key. You can activate the license at the later time by entering the key in the Help > License Information screen. Refer to the section **License Information** for more details.

The setup will communicate with Comodo in order to register your product. Once the registration process is complete, the license summary will be displayed.
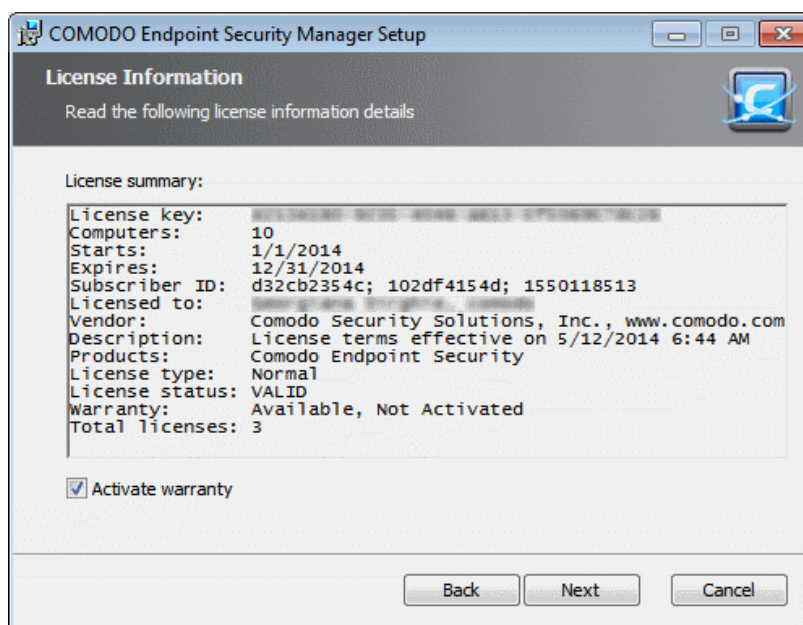
- The warranty is not activated by default. If you want to activate the warranty at this time, select the 'Activate warranty' checkbox. Else leave it blank. You can activate the warranty at a later time from the Upgrade License Wizard. Refer to the section **Upgrading Your License** for more details.

- Click 'Next' to continue the installation.

7. Selecting Database Server

The next step is to select the SQL database server for CESM.

- If you do not have a SQL database configured in your server, select Microsoft SQL Server 2012 Express LocalDB. The setup will automatically install and configure an SQL Database. On clicking Next, the installation will move to **Finalization**.
- If you already have an SQL database configured in your server, select Use an existing Microsoft SQL Server instance and click 'Next'.
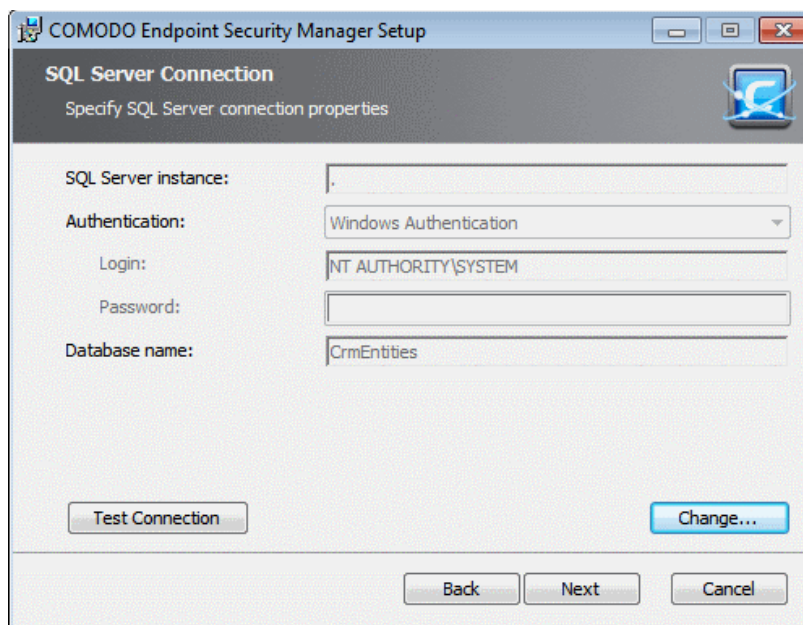
- Enter the parameters of the existing SQL server instance. If you want to test the connection to the SQL server 'Test connection' The result will be displayed immediately.
- Click Next.

8. Finalizing the Installation

On completion of the configuration, the 'Ready to Install' screen will be displayed.
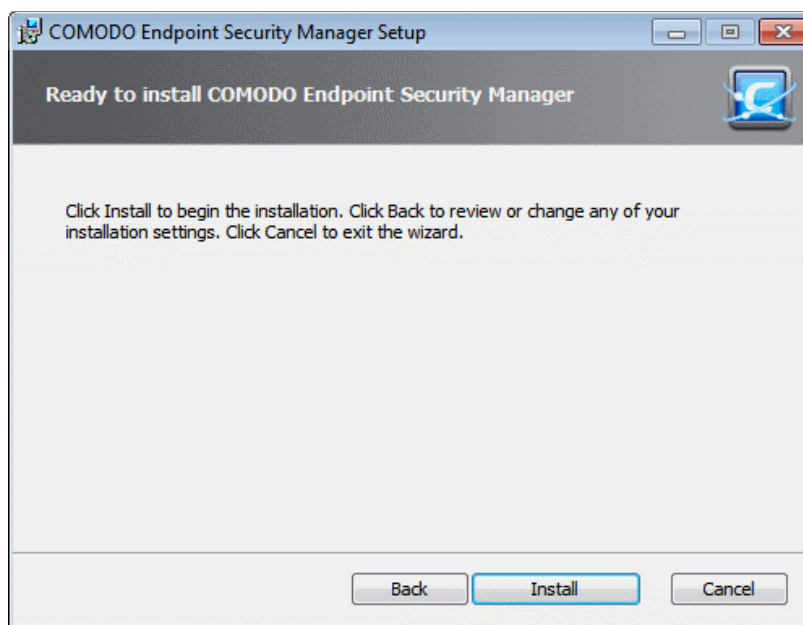
- Click 'Install'. The installation will be started and the progress will be displayed.

Once installation is completed the finish dialog is displayed - offering admins the opportunity to either finish and exit the installer or finish and start the **configuration tool**.
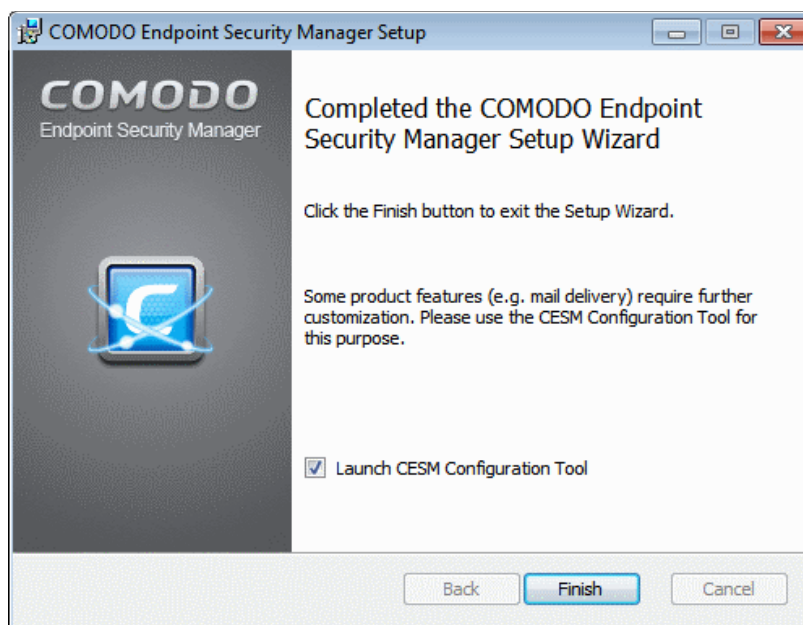
- Select the 'Launch CESM Configuration Tool' check box to open the configuration utility immediately after exiting the installer. This utility will allow admins to:
  - Start or Stop the service.
  - View and configure hostnames or IP addresses that will connect to the server.
  - View and configure console and agent ports.
  - View and configure Internet (proxy) and mail server settings.
  - Manage SSL server certificates for the administrative console.
  - View a log of database events.

  Click here for more details on CESM Configuration Tool.

- Click 'Finish' to complete installation and exit the wizard.

Further reading:

Key Concepts - Definitions of key terms in CESM.

Quick Start Guide - Importing endpoints to central management.

The Administrative Console - Explains how to use the console to manage endpoints, view reports and deploy tasks.

The Configuration Tool - This utility is used to start or stop the CESM service, configure port and address settings and specify internet and mail settings.

1.4. Key Concepts

Endpoint - An endpoint refers to any desktop, laptop, netbook or any other Windows embedded computing device like a Point Of Sales (POS) System that is connected to a corporate network. CESM allows network and system administrators to remotely install, manage and monitor Comodo Endpoint Security (CES), Comodo Antivirus for Servers (CAS) and Comodo Antivirus (CAV) for Mac OS X on endpoints.

Managed Endpoint - Refers to any desktop, laptop or other computing device that is managed the CESM central service. To be successfully managed, an endpoint must have two items installed - the security software (CES, CAS OR CAV for Mac) and the CESM agent (to facilitate communication between the central service and the endpoint).

Dependent Server - A 'dependent server' is another CESM central server in a different network. You may, for example, have different CESM servers in each of your branch offices to handle endpoints located in that office. Administrators can log into a dependent server via the CESM console and so manage endpoints connected to the remote server's network. Setting up dependent servers in remote offices will reduce server workloads and improve operational efficiency.

Agent - A CESM agent is a small application installed on every managed endpoint to facilitate communication between the endpoint and the CESM central server. The agent is responsible for receiving tasks and passing them to the endpoint's

---

installation of Comodo Security Software (CES, CAS OR CAV for Mac). Example tasks include changes in security policy, an on-demand virus scan, updates to the local antivirus database or gathering reports that have been requested by the central service. As an additional security feature, endpoint agents can only communicate with the specific instance of the central service which provisioned the agent. This means the agent cannot be reconfigured to connect to any other CESM service. The agent also acts as a tool for endpoint users to interact with the administrators for resolving any issues in their systems.

Groups - CESM allows administrators to create groups of computers as required by their network and/or corporate structures. Once a group has been created, admins can run tasks on all endpoints in the group in one action.

Remote Mode - CESM can apply security policies and run tasks like AV scans or database updates only if the installation of CES, CAS or CAV for Mac on the endpoint is in Remote Management Mode (i.e. it is being remotely administered through CESM).

Unassigned Group - 'Unassigned' is the name of the default computer group into which newly imported computers are placed. Any computer imported into CESM by installing the agent will be automatically placed in the 'Unassigned' group and will be assigned the 'Locally Configured' Policy. The administrator can then reassign computers from the 'Unassigned' group to the group of their choice.

'Locally Configured' Policy - 'Locally Configured' is a security policy that allows CES/CAV settings to be changed by the local user without being monitored for compliance with a set policy.

Reports - CESM allows administrators to generate highly informative, graphical summaries of the security status of managed endpoints. Each type of report is fully customizable and can be ordered for anything from a single machine right up to the entire managed environment.

Quarantine - Malicious files detected on an endpoint by the antivirus scanner may either be deleted immediately or isolated in a secure environment known as 'quarantine'. Any files moved into quarantine are encrypted so they cannot be run or executed. This prevents infected files from corrupting a computer or the rest of the network.

Sandbox - Installations of CES and CAS with Sandbox component on managed endpoints can run suspicious, unknown/unrecognized or unstable programs and untrusted applications in an isolated environment called the 'Sandbox'.

An application is made to run inside the sandbox when:

- The application is auto-sandboxed based on the Sandbox rules defined in the Policy applied to the individual endpoint or the group to which the endpoint belongs.
- The application is auto-sandboxed based on the Sandbox rules configured at the CES/CAS installation at the endpoint
- The user at the endpoint runs a program inside the Sandbox on a 'one-off' basis. This is helpful to test the behavior of new executables that have they downloaded or for applications that they are not sure that you trust.

Sandboxed applications have restricted access to system hardware and software resources based on the policy applied to the endpoint. Changes made by applications in the sandbox will not affect the data, files or operating system of the rest of the endpoint.

Unmanaged Endpoint - Refers to any desktop, laptop or any other computing device connected to the network but not controlled/managed by CESM. CESM's discovery tools can identify unmanaged endpoints and help administrators import them into the service.

Next:

Best Practices

Quick Start Guide

1.5. Best Practices

1. In CESM, security policies should be applied to 'groups' of computers rather than individual endpoints. So the administrator should first create computer groups that mirror their organization from the administrative console, before importing policy. See **Creating New Endpoint Groups** for explanation on creating new groups.

2. It is recommended to maintain the default group 'Unassigned' with the policy 'Locally Configured' until all the required endpoints in the network are imported. This will prevent CESM from overwriting existing CES security settings on a new endpoint at the instant it becomes managed after deploying the agent.

3. Policy is implemented in a typical PC environment 'imaging' strategy - just as a PC is 'imaged' for replicating it to others. A policy can be created or edited at an endpoint and tested to ensure it works as required before creating an image. The image can then be imposed on other endpoints. The purpose of the administrative console is to alert, centrally deploy software and enforce policy.

4. If the policy of a remote computer is to be changed, it can be pushed to a special test/imaging PC or any nearby PC. The CES on the test/imaging computer can be set to local administration mode in order to edit its configuration. The configuration can be then and imported as a new policy for application to remote computers. If needed the test/imaging computer can be reverted to its original policy.

5. An endpoint serving as a test/imaging computer can be left in 'Local Administration Mode' so that administrators can easily use it to create/modify and import new policies. Even if the PC has an assigned policy other than 'Locally Configured', the endpoint will not be overwritten with policy from the ESM console until it is returned to remote management mode (even if the PC reboots).

6. Regardless of whether the agent and CES, CAS or CAV for Mac are installed automatically from the administrative console or manually at the endpoints using the 'Manage this Endpoint' feature of CESM or **offline deployment**, they should be updated only through CESM.

Next:

Quick Start Guide

1.6. Quick Start Guide

This tutorial briefly explains how an administrator can setup Comodo Endpoint Security Manager Professional Edition (CESM PE) then install and monitor installations of Comodo Endpoint Security (CES), Comodo Antivirus for Servers (CAS) or Comodo Antivirus (CAV) for Mac on networked computers.

We recommend admins to have read the '**Best Practices**' section before putting this tutorial into practice.

The guide will take you through the following processes - click on any link to go straight to that section as per your current requirements.

> **Step 1 - Install**
>
> **Step 2 - Login to the Admin Console**
>
> **Step 3 - Import Endpoints and Install Agents (and optionally Comodo Endpoint Security/Comodo Antivirus for Servers/Comodo Antivirus for Mac)**
>
> **Step 4 - Open the dashboard - check that target endpoints are reporting correctly**
>
> **Step 5 - Create Groups of computers**
>
> **Step 6 - Import security policy from an endpoint and apply to groups**
>
> **Step 7 - View Reports**

Step 1 - Install Comodo Endpoint Security Manager Professional Edition *(see* **Installing and Configuring the Service** *if you need more help with this)*

1. Download and run the CESM PE setup file. A link to this file is provided in your license confirmation email. This file will install the central service on the machine you intend to use as the CESM server. Supported Operating Systems are Win XP SP3, Win Vista SP2, Win 7, Win 8, Windows Server 2003, Windows Server 2003 Small Business Server, Windows Server 2008, Windows Server 2008 R2, Windows Server 2008 Small Business Server and Windows Server 2012.

    There is a choice of two setup files. The '..._FULL.exe' file contains all additional, required software (.net Framework 4.5, SQL Server 2012 Express LocalDB and Microsoft Report Viewer 2010 SP1). The other is a lightweight web installer that does not contain this additional software but will download it from the Internet if it is not detected on your server.

2. Run the setup file. Any missing software components will be automatically installed (CESM requires .NET, SQL Server 2012 Express LocalDB and Microsoft report viewer).

3. Choose the installation type:

    *   Select 'Typical' as the installation type for fastest setup experience; after installation you will need to provide a valid license key in the License Information screen of the console interface to start using the service. The License Information screen can be accessed by selecting 'Help' from the drop-down at the top left and clicking 'License Information' from the left hand side navigation. Refer to **Viewing License Information** for more details.

- Select 'Custom' if you wish to change install location or select which components are installed; you will be required to provide your license during setup.

- Select 'Complete' if you want to install full set of CESM components.

4. At the setup finalization dialog, make sure 'Launch CESM Configuration Tool' is selected before clicking 'Finish'.

5. In the configuration tool, take note of the hostname/IP address of the server and the port settings. You will need these if you wish to access the console from remote machines and if you want to setup protection for laptops and other computers that are outside the local network (you will also need to open these ports to the Internet on your enterprise firewall).

6. This tool also allows you to modify Internet connection settings and specify mail server settings (required for email notifications).

7. Since the ESM console can be accessed via the Internet, you may desire to obtain an SSL certificate and apply it using the Configuration Tool or you can distribute the self-signed certificate already installed to computers that you will use to administer ESM.

Step 2 - Login to the Admin Console *(see* **logging into the console** *if you need more help with this)*

1. After setup is complete, there are two ways that you can access the admin console:

- On the server itself - open the console by clicking 'Start > All Programs > Comodo > Endpoint Security Manager > CESM Console'

  From remote machines via Internet browser - use the following address format to access the console:

- https://<your server hostname or IP address>:57194

> **Tip**: You can find the server hostname/IP and the CESM port numbers by opening the **configuration tool** on the server. Click 'Start > All Programs > Comodo > Endpoint Security Manager > CESM Configuration Tool'.

2. Login to the console using the Windows administrator login and password of the system that CESM was installed on to begin using your software.
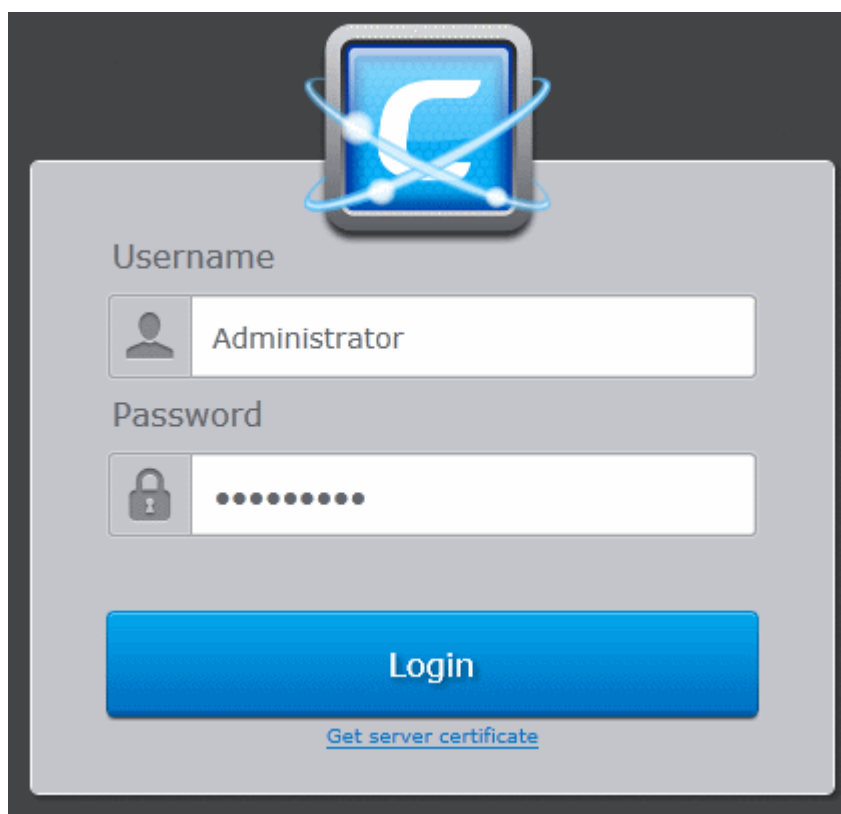
3. To log out of the console, close the browser window or tab containing the console, or press the 'Refresh' button or

---

choose 'Logout' from the drop-down at the top left of the interface.

Step 3 - Import Endpoints and Install Agents (and optionally Comodo Endpoint Security/Comodo Antivirus for Servers/Comodo Antivirus for Mac)

Prerequisite - Before importing the endpoints, you need to download the latest versions of the CESM Agent and the CES/CAS/CAVM packages for remote or manual installation on to the endpoints to be managed. Refer to the section **Preferences** > **Downloading ESM Packages** for more details

---

Next, we need to import endpoints and install the agent and the security software (CES, CAS or CAV for Mac) on them. The agent is a small piece of software that facilitates communication between the endpoint and the CESM server.

There are two ways to accomplish this:

- Remotely, using a console wizard to automatically push the agent and (optionally) the security software onto target machines. This wizard is started by clicking Add from the Computers interface of the console.

- Locally. You can download the agent setup file from the admin console, transfer the file to the endpoints to be managed through any media like DVD, CD, USB memory and install the agent at the endpoints. Detailed explanation on using this method can be found in **Adding Computers by Manual Installation of Agent**.

The remainder of step 3 describes the first method - remote installation.

1. Open the 'Computers' interface by selecting Computers from the drop-down at the top left.

2. Click 'Add' from the 'Computers' interface. The 'Add Computer' wizard will start.
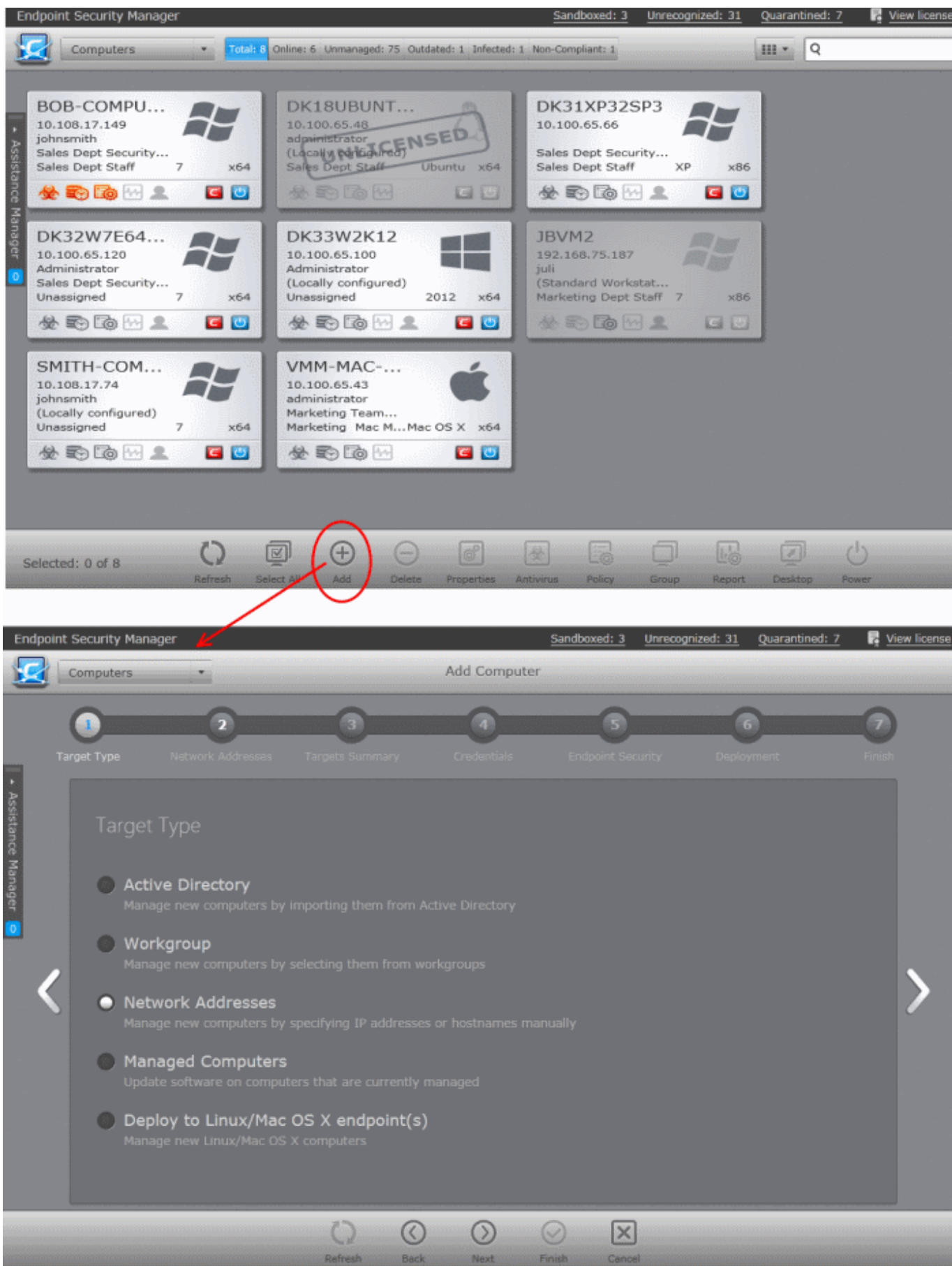
3. The first stage is to choose how you want to import (Target Type). Computers can be imported using one of three methods: Active Directory, Workgroup or by IP Address. Linux and Mac Os computers can be imported by specifying

their IP addresses. Administrators should, of course, repeat this wizard until they have imported all computers in their network.

4. Select the appropriate import method then swipe the screen to the move to the next stage. 'Swiping' is done by holding left-click button down in gray space and dragging the mouse to the left. If you have a touch-sensitive screen then you can swipe between screens with your finger. A third alternative is to click the arrows in the middle on the left and right side of the interface. These arrows turn blue in color when the mouse cursor is placed on them.

   - If you chose 'Active Directory', you next have to choose whether to import from the current domain or a custom domain. The 'current' domain means whichever domain the CESM server is a member of - not the current domain of the endpoint being used to manage the server. If you choose 'custom domain' then you will need to enter the IP or name of the domain controller and the administrator username and password for that domain.

   - If you chose 'Workgroup', you next have to specify which workgroup to import from. You can specify manually by typing the workgroup name or use the 'Find Workgroups' option to have the wizard present you with a choice of workgroups detected on the server machine's local network. You can only import from one workgroup at a time so you may have to repeat this wizard.

   - If you chose 'IP Addresses', you next have to specify the IP, IP range, host name or subnet of the target machines. Click the 'Add' button to confirm your choice. Repeat until you have added all IP addresses or ranges that you wish to scan.

   - If you chose Deploy to Linux/Mac OS X endpoint(s), you next have to specify the secure shell (SSH) port, the IP, IP range, host name or subnet of the Linux and/or Mac OS target machines (CESM will install the appropriate agent facilitating device management). Click the 'Add' button to confirm your choice. Repeat until you have added all IP addresses or ranges that you wish to scan.

   Click the right arrow button to continue.

5. The next stage, 'Select Targets', allows you to choose those imported computers onto which you want to install the Agent and the security product (CES/CAS/CAVM). Select the check-boxes next to your intended targets and swipe the screen left to continue (or click the right arrow button).

6. The next step 'Target Summary' provides you the summary such as status, IP address of the endpoint(s) that you want to install the agent or the security product. Select the check box beside the computer that you want to install the packages. If you want to select all the computers, select the check box beside the 'Target Computer'. Swipe left (or click the right arrow button) to move onto the next step.

7. Credentials. Next up is to choose whether the agent has to be installed under the currently logged in user account or the network administrator account. If you choose 'Custom Credentials', enter the user name and password of an account with administrative privileges on the machine - such as Administrator, hostname\administrator, domain\administrator as the login ID. Swipe left (or click the right arrow button) to move onto the next step.

8. The final step prior to deployment is to decide whether you want to install Comodo Endpoint Security (CES), Comodo Antivirus for Servers /CAS) or Comodo Antivirus for Mac (CAVM) *also* at this time.

   - If you want to continue with this process and install the security software now then make sure 'Install Comodo Endpoint Security' is enabled and:

     (1) Choose the CES/CAS/CAVM version you wish to install from the drop down (most recent is recommended in virtually all cases).

     (2) Select the components that you want to include from the Components drop-down:
     - Full Suite, which contains all the components (Sandbox, Antivirus and Firewall)
     - Sandbox and Antivirus
     - Sandbox and Firewall (Not applicable for CAS/CAVM)
     - Sandbox only
     (3)Select the language in which the CES/CAS is to be installed from the Language drop-down.
     (4) Check 'Suppress Reboot' if you do not want the target endpoint to automatically restart after installation.

     Reboot is required to complete installation, but you may want to postpone this until later.

     (5) 'Uninstall all incompatible third products' - Check this option to uninstall select third party antivirus, firewall and other desktop security software from the endpoints, prior to the installation of the security software. Performing this step will remove potentially incompatible products and thus enable security software to operate correctly. Some incompatible products can be detected, but not automatically uninstalled and must be removed manually. If your product is detected but not uninstalled, please consult your vendor's documentation for precise uninstallation guidelines.

     Click Here to see the full list of incompatible products.

Click the right arrow button to continue to move onto the next step to move to deployment step.
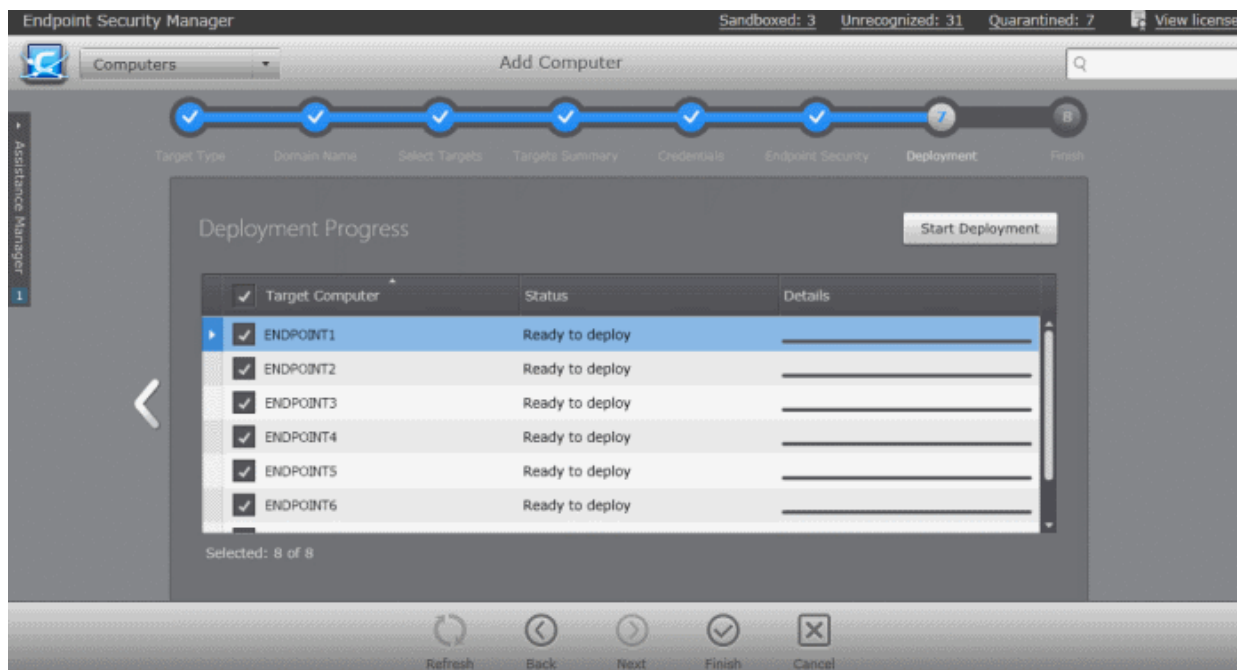
9. Deployment.

    •   Click 'Start Deployment'. You will see installation progress per-endpoint. Once deployment is successful, click the 'Finish' icon at the base of the interface to exit the wizard. After the successful installation of agent, the endpoints will be reporting to CESM.

    •   If deployment fails, click on the words 'Deployment Failed' to discover the reason. The info box also contains advice that may remediate the issue.
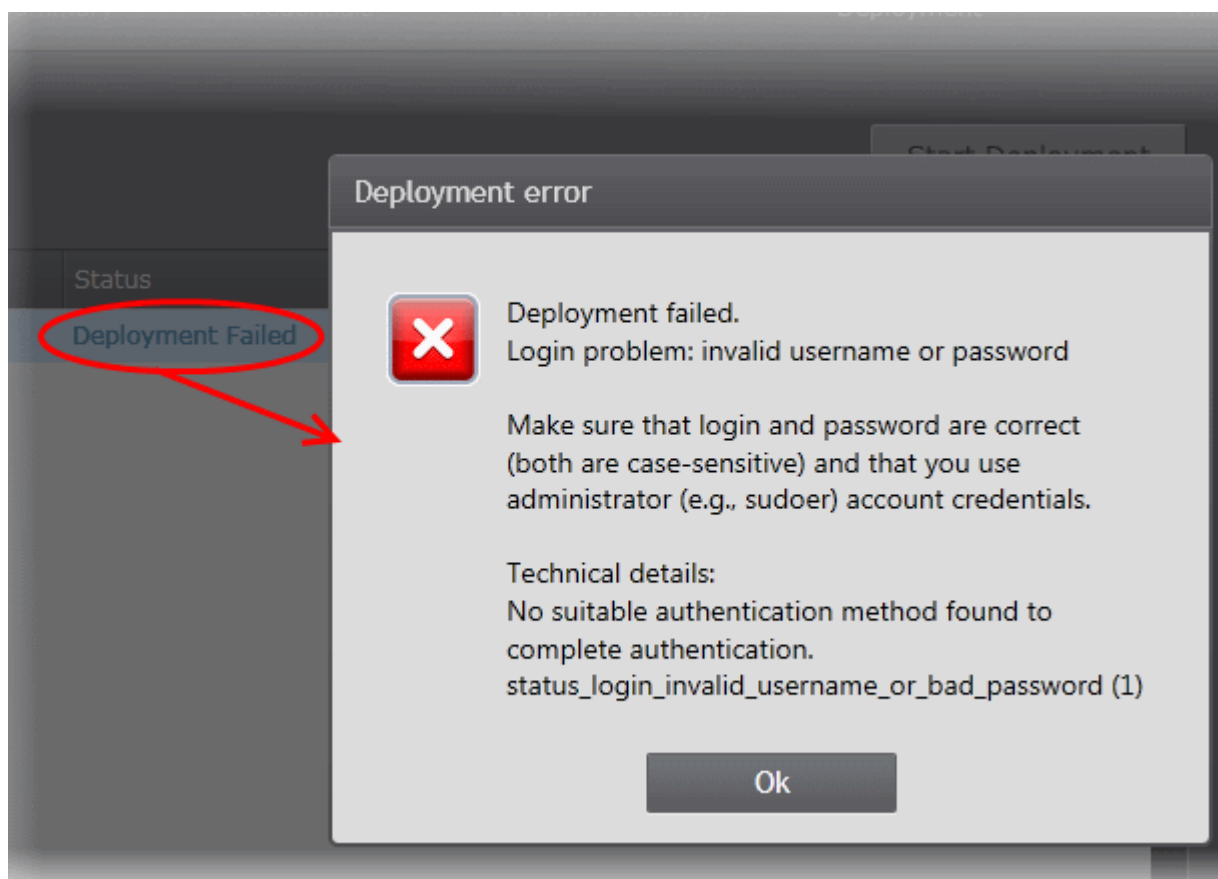
Step 4 - Check that target endpoints are reporting correctly

1.   Open the 'Computers' interface by selecting Computers from the drop-down at the top left.

2.   The details on all the computers added will be displayed in the 'Computers' interface. Check whether all the computers are added from the 'Total' and 'Online' fields in the title bar. The title bar also provides a snapshot information regarding connectivity, virus outbreaks and security policy compliance.

  • After checking that all computers are reporting correctly, it is a good idea to make sure the latest virus database is installed. Select all the computers and click the 'Update AV' at the base of the interface.

  • After updating, we advise running a virus scan on all computers. Select all the computers and click 'Run a scan' at the base of the interface to do this. Note - real-time AV protection is already running on all endpoints. If any malware is discovered, it will be brought to your attention by change in color of status indicators.

  • General advice regarding navigation and other functional areas can be found in **The Administrative Console**.

Step 5 - Create Groups of computers

In CESM, security policies are applied to 'groups' of computers rather than individual endpoints. Once a group has been created, admins can run tasks on entire groups of computers (such as applying policy, running AV scans, deploying agents, updating AV databases and more). 'Policies' are the security configuration of CES/CAS and are imported from specific, already configured, endpoints then applied to groups (we will cover this in step 6).

  • By default, all newly imported computers are placed into a group named 'Unassigned' and inherit that group's security policy of 'Locally Configured'. Effectively, this means remote management is not in operation and the endpoints will continue to use the security policy that is already in effect on the endpoint. If needed, the administrator can assign a policy to 'Unassigned' group so that the policy will be applied to any imported computer and remote management is enabled immediately.

  • We advise admins to create groups corresponding to the structure of their organization THEN import policy (from an endpoint) and apply it to selected groups. Policies can also later be changed for individual computers in a group, overriding group policy defaults.

  • To start,

    • Open 'Groups' area by selecting 'Groups' from the drop-down at the top left.

    • Click 'Add' from the bottom to start the 'Create Group' Wizard,

- Select required computers,
- Leave policy as (Locally Configured),
- Type a name for the group then finish.
- If you wish to create multiple groups, repeat the previous step until all computers have been assigned.
- See '**Creating New Endpoint Groups**' if you need help with this wizard. See '**The Groups area**' for an overview of functionality.

Step 6 - Import security policy from an endpoint and apply to groups

A policy is the security configuration of Comodo Endpoint Security (CES) or Comodo Antivirus for Servers (CAS) deployed on a group of endpoints. Each policy determines the antivirus settings, Internet access rights, firewall traffic filtering rules and Defense+ application control settings for an endpoint. Policies are imported from already tested and configured endpoint machines then applied to groups. In the previous step, you assigned computers into groups but left the policy as 'Locally Configured' - which means remote management is effectively switched off (CESM will not enforce policy compliance and each endpoint in the group will simply continue to use the CES/CAS settings it is currently using).

The next tasks are to import a policy from a tested and configured endpoint, apply the policy to a group and (optionally), switch on remote management for computers in that group.

- To set the parameters of a particular security policy, you need to place the endpoint in 'locally managed' mode by selecting 'Manage Locally' in CES/CAS settings on the endpoint itself - either by physically sitting at the machine or by a remote connection.
- Once you have set and tested the policy at the endpoint, you should return to the CESM console and prepare to import this policy. Note - leave the endpoint in locally managed mode while doing this.
- At the console,
    - Open the 'Policies' interface by selecting 'Policies' from the drop-down at the top left,
    - Click 'Add' from the 'Policies' interface to start the 'Create Policy' wizard,
    - Select 'Create New' and choose the specific computer from which you want to import. Modify 'Settings' and 'Agent Settings' if required.
- For 'Targets', choose which groups you want to apply the policy to and how you want it applied. 'For local policy' and 'For Internet policy' are the policies to be used depending on whether the machine connects from inside or outside of the VPN. Also, select 'Override individual computer's policy' to make sure this policy is applied correctly and select 'Apply Policy after finish' to immediately apply the policy to all the selected endpoints upon completion of policy creation. If you want to apply the policy later, do not select 'Apply Policy after finish'.
- Finally, give the policy a name and description and click 'Finish'.

    Please see **Policies - Key Concepts** for more explanation of policies - including how to create, import, export and deploy.

Step 7 - Viewing Reports

The reports area contains a wealth of valuable information for administrators. Admins can also drill-down to individual endpoints from any report. Reports can be exported, printed and cover the following categories:

- Antivirus Updates
- Assistance Logs
- Security Product Configuration
- Security Product Logs
    - Antivirus Logs
    - Firewall Logs
    - Defense+ Logs
- Computer Details
- Computer Infections
- Hardware Inventory
- Installed Software Inventory
- Malware Statistics
- Policy Compliance

- Policy Delta Report
- Quarantined Items
- Top 10 Malwares
- Warranty Report

Click here to read more about reports.

2. The Administrative Console

The Administrative Console is the nerve center of Comodo Endpoint Security Manager, allowing administrators to deploy, manage and monitor Comodo endpoint security software on networked computers.

Built using the latest Microsoft® Silverlight technology, the interface consists of the following main areas that can be selected from the drop-down menu near the top left - 'Computers', 'Groups' 'Policies', 'Quarantine', 'Sandbox', 'Applications', 'Processes', 'Services', 'Reports', 'Help', 'Preferences' and 'Logout'. Assistance Manager feature that can be accessed at any time by clicking the blue slider at the left of the interface enables administrators to remotely chat and interact with users in order to clarify and resolve problems.

Main Functional Areas
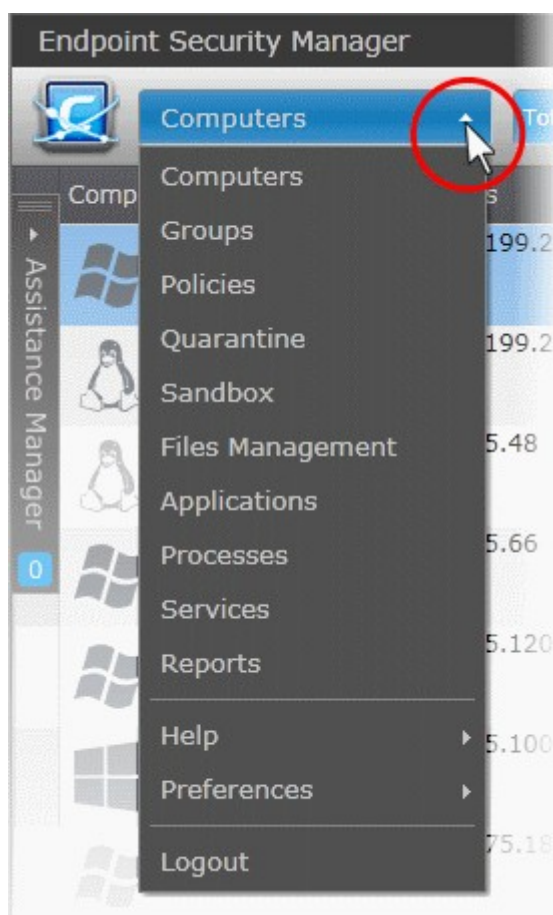
- **Computers** - View, manage and add computers. Add individual computers to groups and apply policies on a per-computer basis. Run an on-demand scan and update virus signature database on target computers. Start a Remote Desktop Sharing session with a remote computer. See **The Computers Area** for more details.

- **Groups** - View, manage and add endpoint groups. Specify policies on a group basis. Run an on-demand scan and update virus signature database on all target computers in a group. See **The Groups Area** for more details.

- **Policies** - View and manage the security policies that apply to managed endpoints. Also contains a step-by-step wizard that enables administrators to create and import a policy from existing endpoints, modify that policy, then re-export to other computers or groups of computers. See **The Policies Area** for more details.

- **Quarantine** - View all the suspicious programs, executables, applications and files moved to quarantine by CES/CAS installations at the managed endpoints and manage them. See **Viewing and Managing Quarantine Items** for more details.

- **Sandbox** - View all the programs, executables, applications that are currently run inside the sandbox at the managed endpoints and manage them. See **Viewing and Managing Sandboxed Applications** for more details.

- **Files Management** - View all the executable files discovered from all the endpoints with their file rating based on Comodo certified safe files database and manage them. See **Viewing and Managing Files List** for more details.

- **Applications** - View the Applications running currently in all the endpoints. Stop the unwanted applications in all the endpoints at-once. See **Viewing and Managing Currently Running Applications** for more details.

- **Processes** - View the Processes running currently in all the endpoints. Terminate the unwanted processes in specific endpoints or in all the endpoints at-once. See **Viewing and Managing Currently Running Processes** for more details.

- **Services** - View the Services that are currently loaded at all the managed endpoints. Start or Stop the services as required at specific endpoints or in all the endpoints at-once. See **Viewing and Managing Services** for more details.

- **Reports** - Allows administrators to generate a wide range of reports for managed endpoints - including malware statistics, policy compliance, activity logs, update status, infections and more. The reports can be downloaded in .pdf or spreadsheet formats for analysis and archival purposes. See **The Reports Area** for more details.

- **Help -** Allows administrators to view version, license, support and server information. Administrators can use the

---

interface to purchase additional endpoint licenses, to get online help and to get product updates. See "**Viewing ESM Information** section for more details.

- **Preferences** - Allows administrators to configure report archives, email notifications and dependent CESM servers. Administrators can also download CESM agents to install on remote endpoints that they wish to manually add to the CESM network. See '**Viewing and Managing Preferences**' section for more details.

- **Logout-** Allows administrators to logout of the CESM Console.

2.1. Logging-in to the Administrative Console

After installing CESM central service on a Windows server, admins can access the console in the following ways:

- On the server itself by opening:

  Start > All Programs > Comodo > Endpoint Security Manager >CESM Console

- Via web-browser from any **other PC**

  Use the following address convention to access the console

  https://<server hostname or IP address>:57194

  - Where <server hostname or IP address> is the server upon which CESM central service is installed.
  - 57194 is the DEFAULT https port configured for the service. If you changed this port number during installation or by using the Configuration Tool then modify the address accordingly.
  - If you wish to check which server names, IP addresses and port numbers are currently in use, please open the **Configuration Tool** on the server by opening.

    Start > All Programs > Comodo > Endpoint Security Manager >CESM Configuration Tool

> **Note:** If you receive a browser security error, you have not **installed an SSL certificate** from a Certification Authority. If you will not be installing a custom certificate, you can download the self-signed certificate in your browser by clicking 'Get server certificate' at the bottom of the login screen. You can then install the certificate in the Trusted Root Certification Authorities section on machines which will be accessing the console to eliminate the browser warning.

- Login to the console using the Windows administrator login and password of the system that CESM was installed on to begin using your software. The context of the login is that of the server computer on which the CESM Server service is running (not the computer running the administrative console). If the CESM Service is running on a domain, use the domain\username syntax to specify the user name (e.g. contoso\administrator).
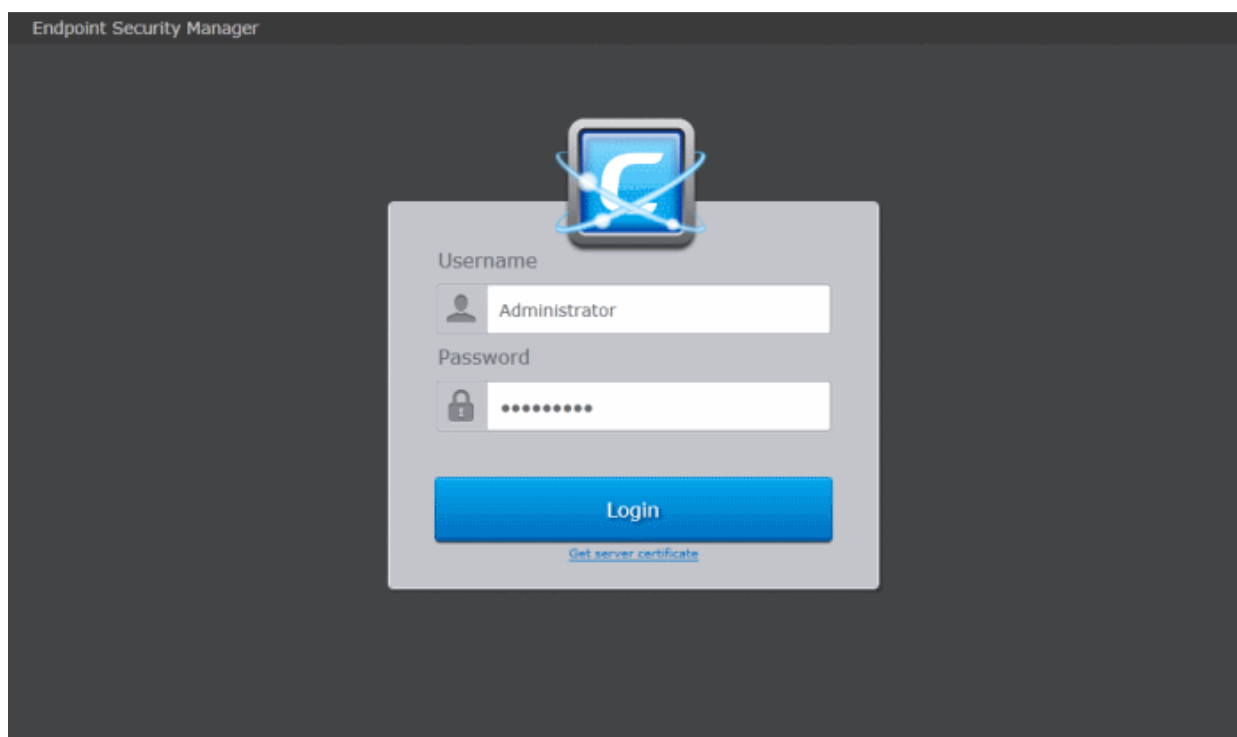
2.2. Using Assistance Manager

The Assistance Manager feature enables administrators to remotely chat and interact with users in order to clarify and resolve issues they are experiencing with their computer. Assistance Manager can be accessed at any time by clicking the blue slider at the left of the interface. The number at the bottom of the slider indicates the number of current users either waiting or in-chat with the administrator.

The chat function is only available to end-users if the CESM agent is installed on their computer. Once installed, the agent icon will be available in their system tray. They can initiate a chat session by double clicking the icon or right-clicking and selecting 'Request Assistance...'.

- For more details on how to install the agent on endpoints, refer to the sections '**Importing Computers by Automatic Installation of Agent**' and '**Adding Computers by Manual Installation of Agent**'.

- For more details on how end-users can start a support chat with the CESM administrator, refer to **Instant User Assistance** in the CES guide.

Managing chat sessions

- Click anywhere on the Assistance Manager slider to expand the window:
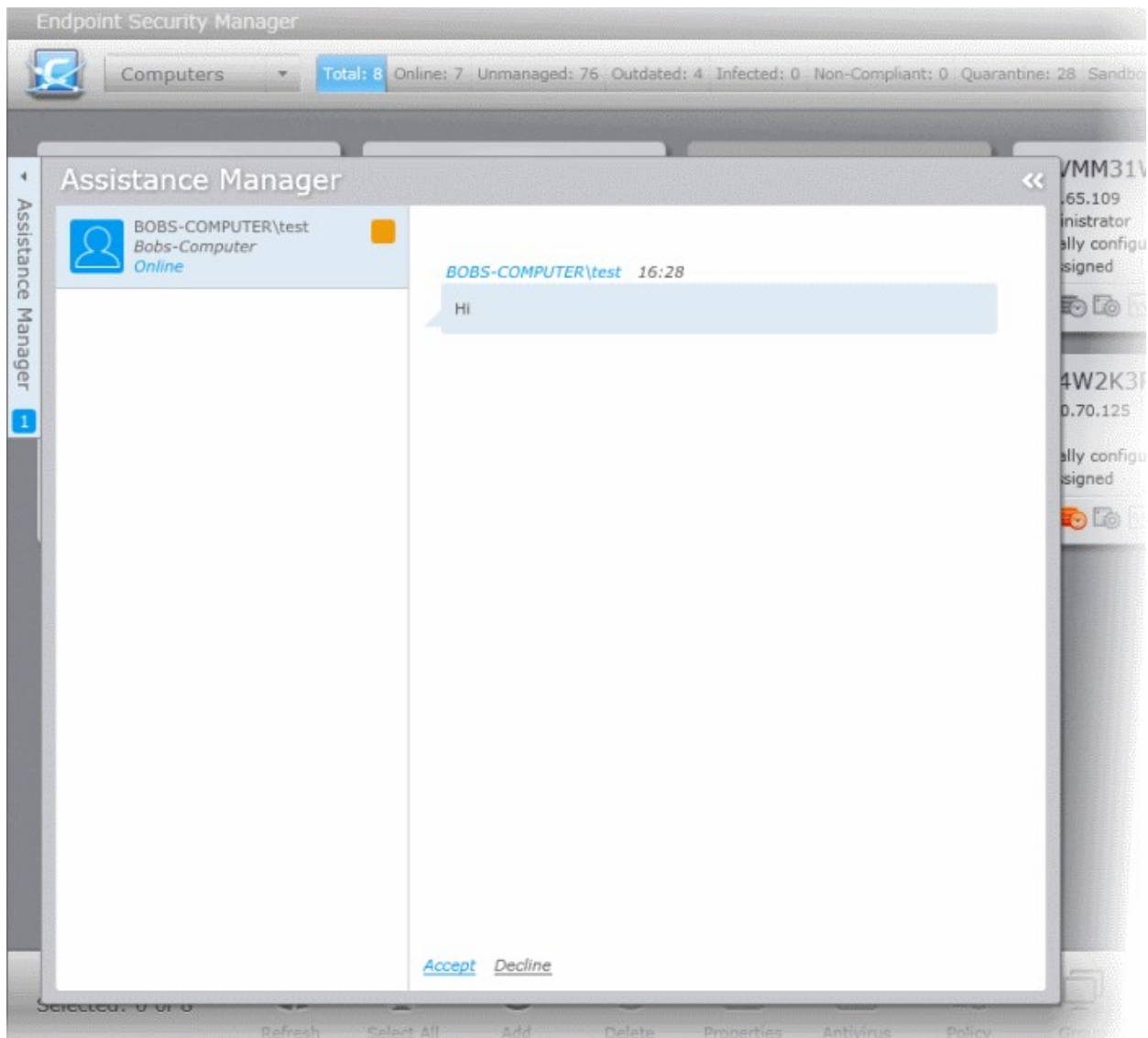
- The left hand pane shows a list of users that require assistance or are waiting for your response. Click on any user name to display their request in the chat pane on the right.

- If you have not yet started a conversation with this user, click 'Accept' at the bottom to proceed with the chat. You can also start chats by right-clicking on the user's computer in the 'Computers' screen then choosing 'Accept Assistance Request' from the context-sensitive menu.
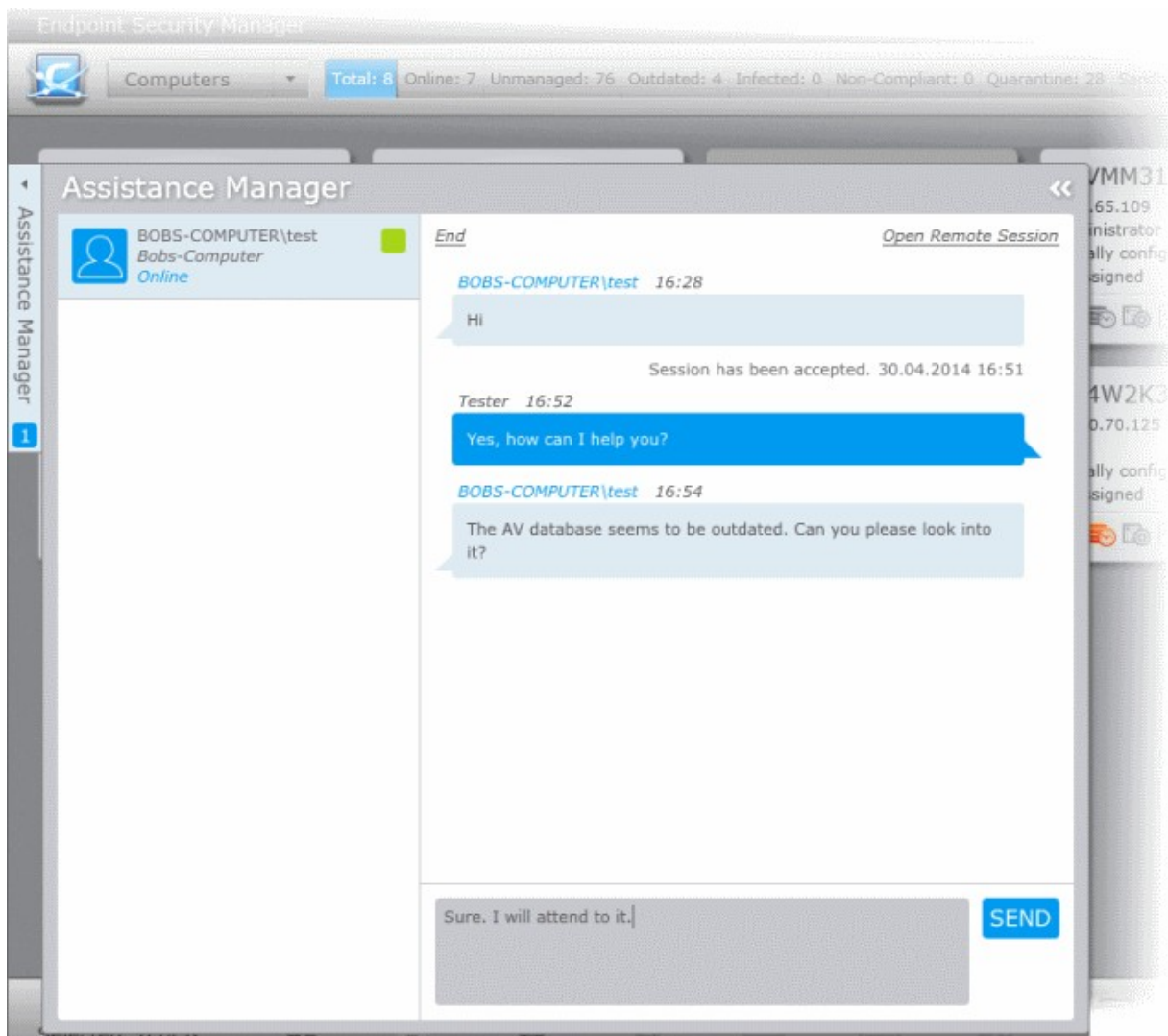
Administrators can use the remote desktop feature in CESM to access the endpoint. Refer to the section **Accessing Endpoints through Remote Desktop Sharing Session** for more details.

- Click 'End' at the top to close the chat session with the endpoint user.
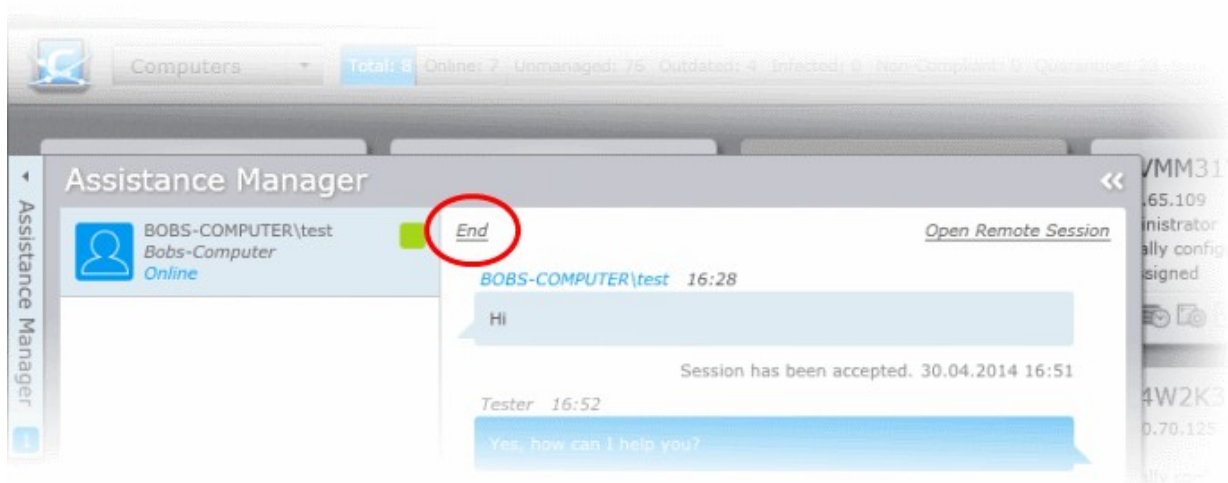
The chat session with the endpoint user will be terminated.

Next - **The Computers Area.**

3. The Computers Area

The 'Computers' area plays a key role in the CESM Administrative Console interface by providing system administrators with the ability to import, view and manage networked computers. In grid and panorama views, each endpoint is represented by a box containing key information about that computer's address, operating system and security status. The title bar displays the numbers of applications that are currently sandboxed, unrecognized and quarantined and enables you to view the list of files under respective category. The filter button at the gray bar provide at-a-glance statistics of number of endpoints in different statuses and enable to filtering them accordingly. You can add endpoints or perform actions on selected endpoints using the options along the bottom of the interface.
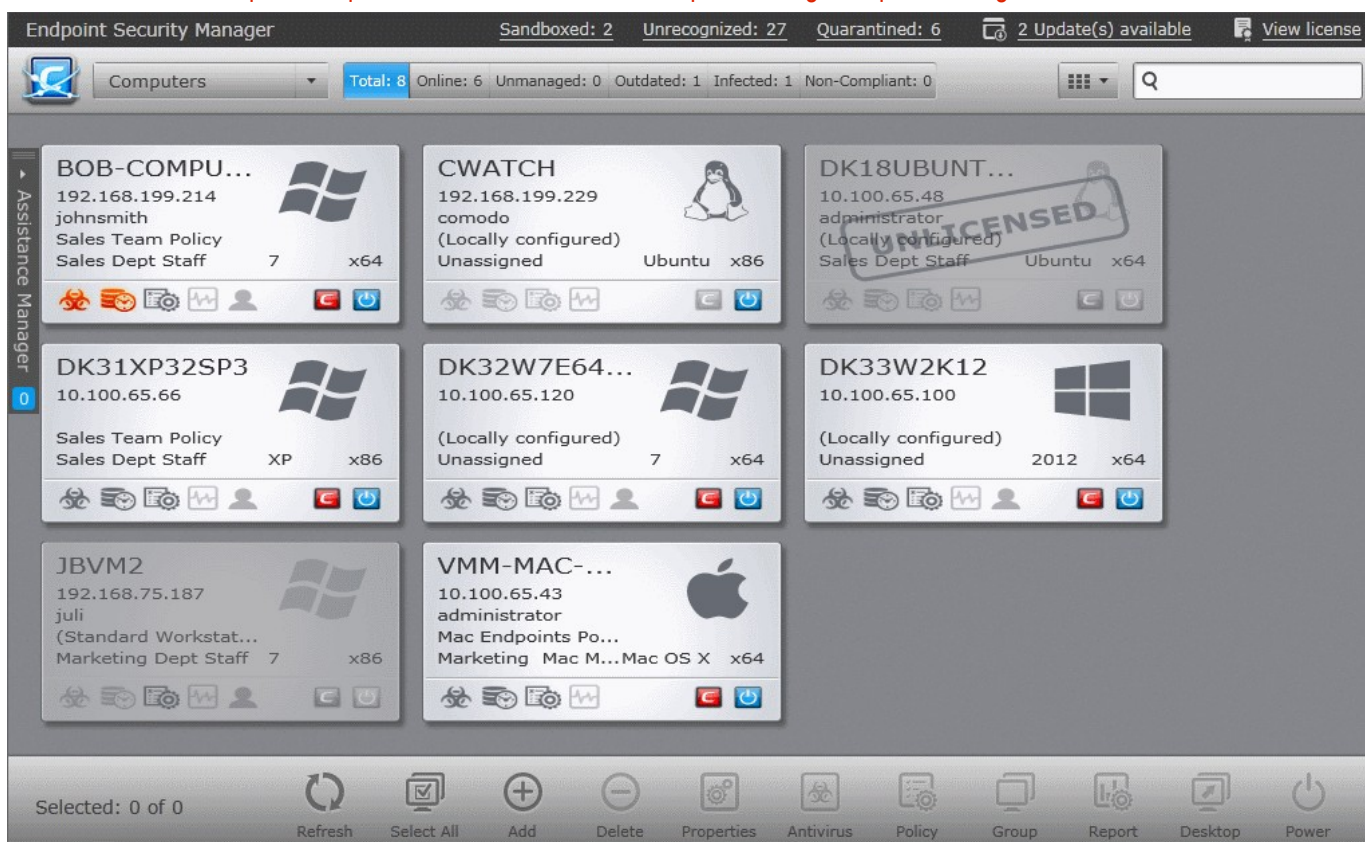
The 'Computers' area allows administrators to:

- View the list of endpoints that are managed by CESM.

- Add/Import computers to CESM for centralized management.

- Identify unmanaged endpoints in the network and bring them under control of CESM

- Assign computers to Endpoint Groups for easy administration.

- View full details of a target computer:

  - CPU/RAM & Drive metrics;

  - Network metrics;

  - Currently running services and processes with ability to stop/start services or terminate running processes;

  - Installed applications with ability to uninstall unwanted .msi based applications;

  - Disk drives with ability to discover 10 largest files consuming disk space and delete selected files;

  - View alerts generated when the hardware/software system resource usage has exceeded set thresholds.

- Apply security policies to computers.

- Run an on-demand scan on target endpoints.

- Update virus signature database on target endpoints.

- Start a Remote Desktop Sharing session with a target endpoint.

- Generate CES/CAS.CAVM Reports for a target endpoint.

- Wake/Reboot/Shutdown endpoints as required.

- View and manage items identified as unrecognized files, quarantined items and programs running inside the sandbox across the network.

Once the agent is installed, the endpoint computer is added into CESM and is ready to be managed through CESM. See the section '**Adding Endpoint Computers to CESM**' for complete instructions.

View Filter and Shortcut Options

The Computers area can display the computers connected to CESM in **tile view** or **list view** or **3D Panoramic view**.

Tile View
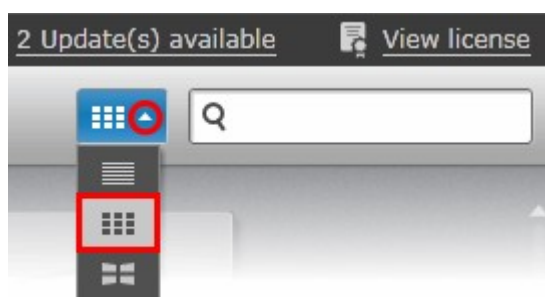
The Computers area displays the computers added to CESM as tiles in tile view. If you wish to switch from other views to tile view, click the

drop-down at the top right and choose the tile view button .

Each computer is represented by a tile with its status details:
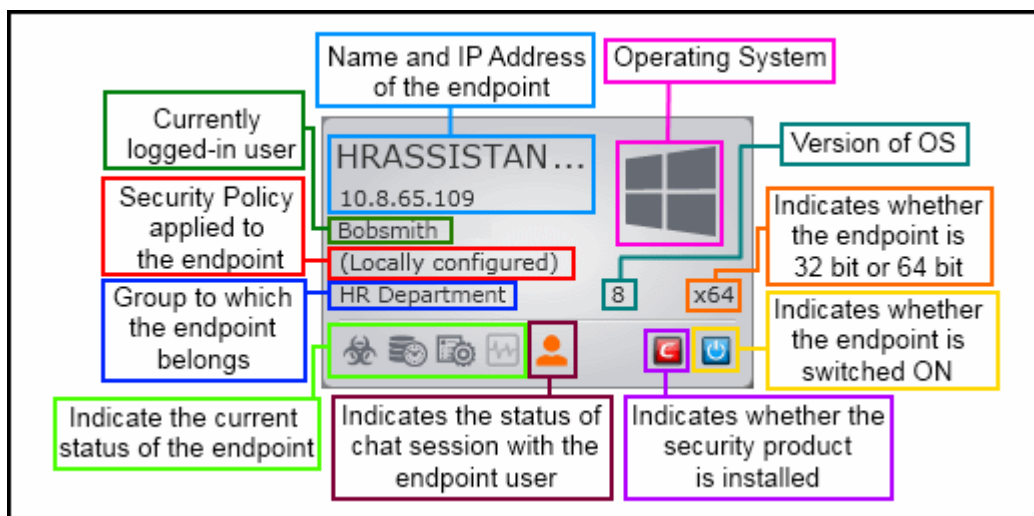
The icons at the bottom indicate the current status of the endpoint.

Status	Icon	Indication
Power		The endpoint is powered ON
		The endpoint is powered OFF
Comodo Endpoint Security		CES is installed
		CES is not installed
Compliancy Status		Endpoint is compliant with the policy applied
		Endpoint is not compliant with the policy applied
Virus Database Status		The virus signature database is up-to-date
		The virus signature database is outdated
Infection Status		The endpoint is not infected
		The endpoint is infected
System Resource Usage Status		The system resources usage is under limits as per the policy applied
		The system is overloaded and the resources usage has exceeded the limits as per the policy applied
Assistance Manager		Endpoint user waiting or in-chat with the administrator.
		No assistance request initiated by the endpoint user.

List View
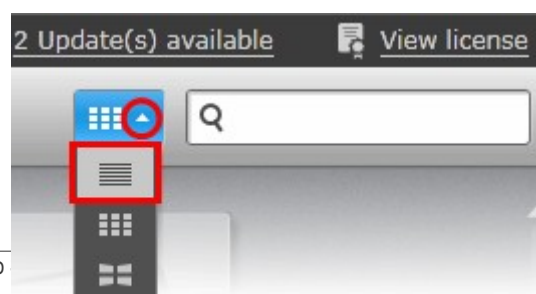
The Computers area displays the computers added to CESM as a list in list view. If you wish to switch from other views to list view, click the drop-down at the top right and choose the list view button ▤ .

Column Heading	Description
Computer	Displays the name of the Endpoint computer and the currently logged-in user.
IP Address	Displays the IP Address of the endpoint.
Group	Displays the Group to which the endpoint belongs.
Status	Indicates the connection status, license status, virus signature database update status and resource usage status of the endpoint. The connection state can be one of the following: • **Online** - The endpoint agent is connected to CESM. • **Offline** - The endpoint agent is not connected to CESM at this moment. • If the endpoint is not covered under license, it will be indicated as 'Unlicensed' below the connection status. • If the virus signature database in the endpoint is not up-to-date, it will be indicated as 'Outdated' below the connection status. • If system resource usage like CPU usage, memory usage, network usage and disk usage exceeds the threshold limits set as per the policy applied to the endpoint, it will be indicated as 'Overloaded' below the connection status.
Security Product	Indicates whether or not Comodo Endpoint Security (CES), Comodo Antivirus for Servers (CAS) or Comodo Antivirus for Mac (CAVM) is installed on an endpoint and whether or not it is

	managed by CESM. CESM cannot manage old versions of security software. The version number of the security software is displayed below the installation state. • **Installed -** CES/CAS/CAVM is installed and managed by CESM. • **Not Installed** - CES/CAS/CAVM is not installed at the endpoint. • **Unsupported** - The security software is installed by not managed by CESM.
Policy	Displays whether or not the security software on a particular endpoint is compliant with its security policy. The local and internet policies which have been applied to the endpoint are displayed beneath the compliance status. The compliance status can be one of the following: • **Non-Compliant** - The CES/CAS/CAVM installation at the endpoint is not compliant to the applied security policy. • **Pending** - The compliance status of the CES/CAS/CAVM installation at the endpoint is yet to be assessed. For further reading on 'Policies', please see '**The Policies Area**'.
Operating System	Indicates the operating system of the endpoint.
Actions	Displays the current action and/or the last action executed of the endpoint like AV scan or AV update.

3D Panoramic View
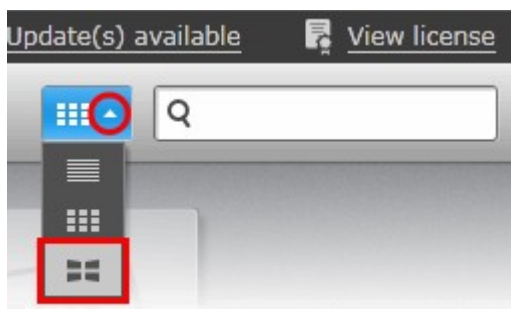
The 3D Panoramic view displays the computer tiles in a 360° canvas, and is helpful to view and manage individual computers, if you have large number of managed endpoints.

If you wish to switch from other views to 3D Panorama view, click the

drop-down at the top right and choose the panorama view button .
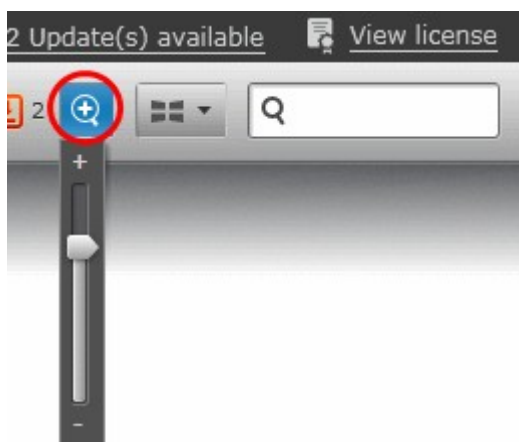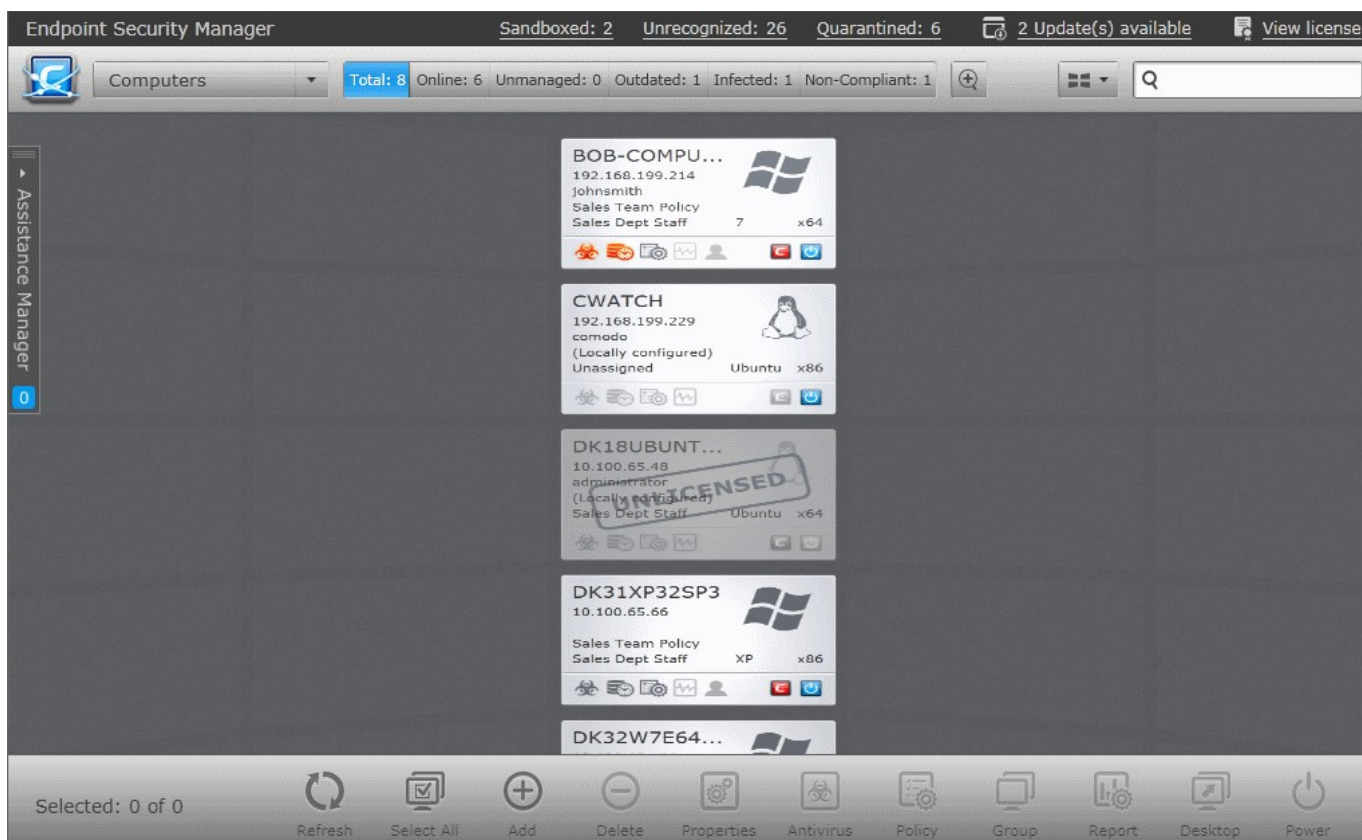
The Administrator can zoom-in or zoom-out the display as required by clicking the zoom button and moving the magnification slider.

Note: For CESM to render the 'Computers' area in 3D Panoramic view, usage of 3D Graphics display drivers should be allowed for CESM server in your Microsoft Silverlight installation.

To enable 3D Graphics display driver

1. Open the Microsoft Silverlight configuration interface by right clicking on the gray stripe and selecting Silverlight from the context sensitive menu or by clicking Start > All Programs > Microsoft Silverlight from your Windows Start menu.

2. Click 'Permissions' tab.
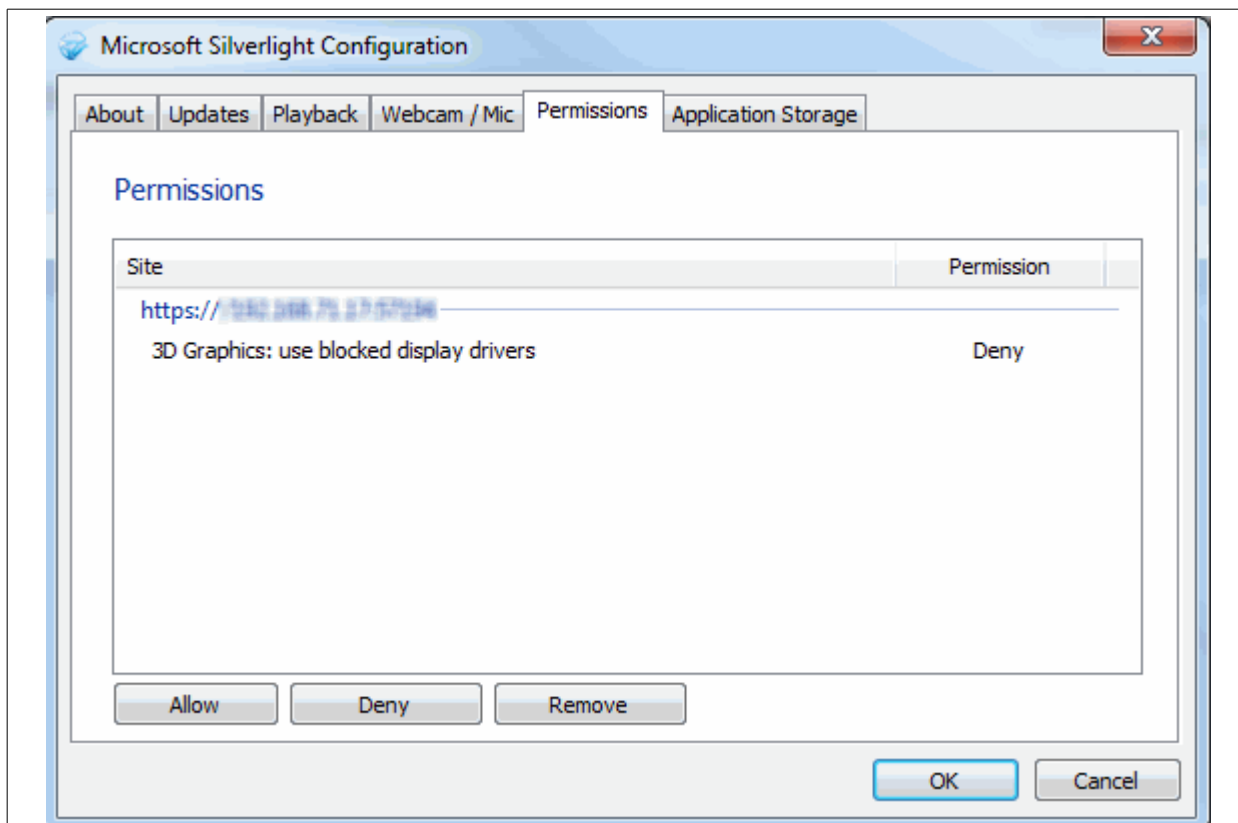
3. Select 3D Graphics: use blocked display drivers and click Allow button.

4. Click OK in the configuration dialog.

5. Restart the browser and login to CESM.

Filter Options and Shortcuts

The title bar displays the numbers of applications currently running inside the sandbox, quarantined and number of executable files with 'Unrecognized' rating, as shortcut links. The filter buttons in the gray stripe, give at-a-glance statistics of the computers in the network. The shortcuts and the buttons enable the administrator to:

• Filter the computers based on the criteria

• Add endpoints from unmanaged computers in the network

• Access 'Quarantine', 'Sandbox' and 'Unrecognized Files' interfaces directly

The search field in the right allows the administrator to search for a specific computer by entering its name or IP address, partially or fully.
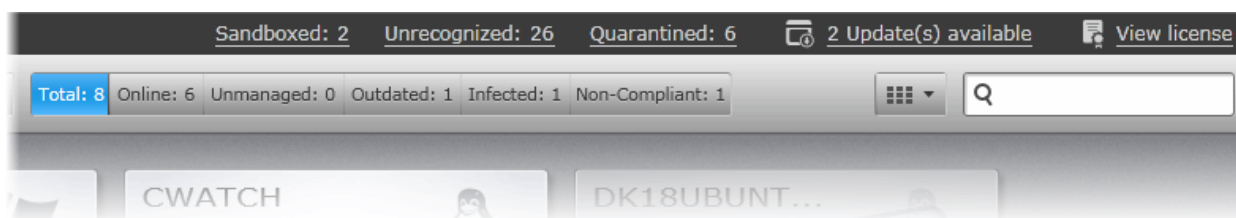
Button/Shortcut icon	Description
Sandboxed Sandboxed: 2	Displays the total count of unidentified programs, executables and applications automatically sandboxed by the behavior blocker component of CES installations and the new applications manually added to run inside sandbox at the managed end[points. Clicking the button opens the

	'Sandbox' interface. Refer to the section **Viewing and Managing Sandboxed Applications** for more details.
Unrecognized Unrecognized: 26	Displays the total count of items identified as Unrecognized files by the CES/CAS installations at the managed endpoints. The number is updated each time a new item is discovered as Unrecognized file. Clicking the icon opens the 'Files Management' interface displaying 'Unrecognized Files' list. Refer to the section **Viewing and Managing Unrecognized Files** for more details.
Quarantined Quarantined: 6	Displays the total count of suspicious files and executables moved to quarantine by the CES/CAS installations at the managed endpoints. The number is updated each time an item is moved to quarantine in a managed endpoint. Clicking the icon opens the 'Quarantine' interface. Refer to the section **Viewing and Managing Quarantined Items** for more details.
Total	Displays the total number of managed computers. Clicking the button displays all the managed endpoints in the 'Computers' interface
Online	Displays the total number of managed computers that are currently online. Clicking the button displays only the computers that are online and connected to the CESM server in the 'Computers' interface
Unmanaged	CESM can discover endpoints which are connected to the network but unconnected to CESM and allows administrators to easily bring them under central management. For CESM to discover endpoints automatically, auto discovery has to be enabled through Preferences > Auto Discovery Settings pane. Please refer to the section '**Auto Discovery Settings**' for more details. If enabled, the 'Unmanaged' button displays the number of unmanaged endpoints discovered from the network. Clicking the button opens the 'Unmanaged' interface that lists the identified endpoints and enables adding them to CESM. Refer to the section '**Importing Unmanaged Endpoints from Network**' for more details.
Outdated	Displays the number of managed endpoints at which the virus signature database of CES/CAS installation is not updated. Clicking the button displays only those endpoints with outdated virus signature databases.
Infected	Displays the number of managed endpoints that are infected by malware. Clicking the button displays only the infected endpoints in the 'Computers' interface.
Non-complaint	Displays the number of managed endpoints that are currently not in compliance with the security policy applied. Clicking the button displays only the non complaint endpoints in the 'Computers' interface.

Refer to the sections below for more information on tasks accomplished from the 'Computers' area.

- **Viewing details and managing computers**
- **Adding Endpoint Computers to CESM**
- **Running on-demand scan on individual Endpoints**
- **Updating virus database on individual Endpoints**
- **Accessing Endpoints through Remote Desktop Sharing Session**

3.1. Viewing Details and Managing Endpoints

From the 'Computer Properties' screen, administrators can view detailed information about each endpoint and directly perform various management tasks on the machine. Tasks include applying/re-applying security policies, managing Endpoint Security configuration, assigning the endpoint to groups, running a virus scan, viewing and modifying currently running applications and services and launching a remote desktop sharing session.

To open the Computer Properties screen

- Open the 'Computers' interface by selecting 'Computers' from the drop down at the top left
- Select an endpoint from the list and either.

- Click 'Properties' from the options at the bottom.

  or

- Right click on the computer and select 'Open' from the context sensitive menu.

  or

- Double click on a computer.
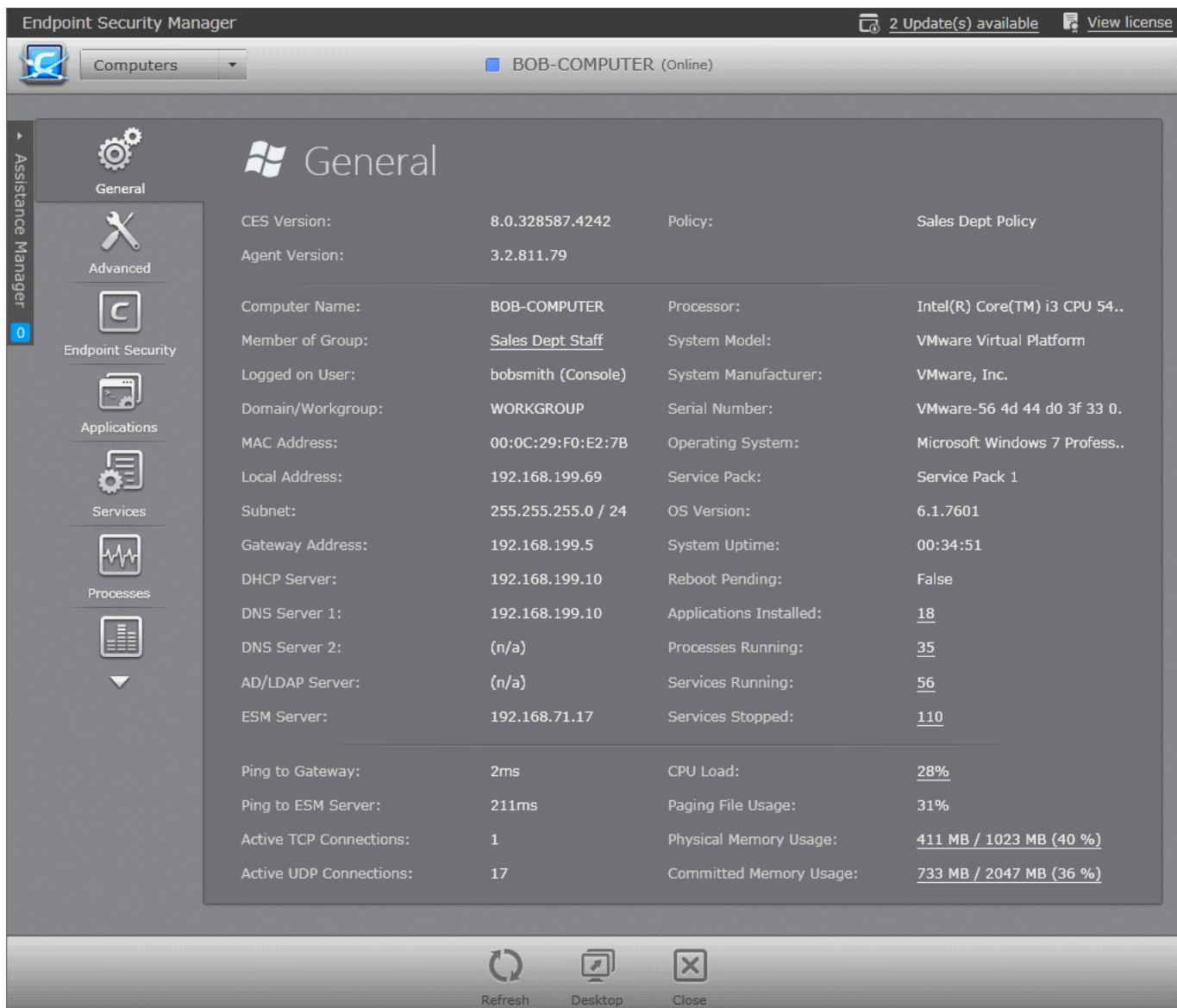
The tabs at the left of the 'Computer Properties' screen allow administrators to view and manage items such as general/advanced properties, CES status, installed applications, currently running processes, services, storage and more. The tabs shown depend on the operating system of selected endpoint.

The Computer Properties screen allows the administrator to perform the following tasks depending on the operating system:

Windows	Mac OS X	Linux
• **View General Properties**	• **View General Properties**	• **View General Properties**
• **View and Manage Group and Security Policy Details**	• **View and Manage Group and Security Policy Details**	• **View and Manage installed applications**
• **View and Manage Internet Security Software**	• **View and Manage Internet Security Software**	• **View and Manage currently loaded Daemons**
• **View and Manage installed**	• **View and Manage installed**	• **View and Manage currently**

applications	applications	loaded processes
• **View and Manage currently loaded services**	• **View and Manage currently loaded Daemons**	• **View and Manage Drives and Storage**
• **View and Manage currently loaded processes**	• **View and Manage currently loaded processes**	
• **View System Monitoring Alerts**	• **View System Monitoring Alerts**	
• **View and Manage Drives and Storage**	• **View and Manage Drives and Storage**	
• **View Event Log**		

3.1.1. Viewing General Properties

'General Properties' displays a detailed summary of information about the selected endpoint. This includes online status, infection status, compliance status, network address, CES version, group membership, policy applied and current user. The summary also contains detailed hardware and operating system/software information about the endpoint.

The General Properties pane is displayed by default when you first open details about a computer.

- Clicking on the name of the group beside 'Member of Group' takes you to the General screen of the group to which the endpoint belongs. Refer to the section **Viewing and Managing Groups** for more details.

- Clicking on the numbers beside 'Processes Running', CPU load, 'Physical Memory Usage' and 'Committed Memory Usage' opens the 'System Processes' pane that allows you to view the currently running processes at the endpoint and to terminate unnecessarily running processes in order to optimize the system's performance. Refer to **Viewing and Managing Currently Running Processes** for more details.

- Clicking on the number beside 'Applications Installed' opens the 'Installed Applications' pane that allows you to view the applications installed in the system and to uninstall unwanted applications (msi based applications only). Refer to **Viewing and Managing installed applications** for more details.

- Clicking on the numbers beside 'Services Running'/'Daemons Running' and 'Services Stopped'/'Daemons Stopped' opens the 'System Services'/'Daemons' pane depending on the OS of the endpoint and allows you to view the currently running Windows services or Linux/Mac OS daemons at the endpoint and to terminate unnecessarily running services/daemons in order to optimize the system's performance. Refer to **Viewing and Managing Currently Running Services or Daemons** for more details.

- To reload the currently viewed screen with updated details, Click 'Refresh'

- To close the 'General Properties' screen of the selected endpoint click 'Close'.

- To start a remote desktop session with the selected endpoint, click 'Desktop"

3.1.2. Viewing and Managing Group, Security Policy and Warranty Details

The Advanced Properties pane displays the details of the group to which the endpoint belongs and the security policy applied. The administrator can reapply the security policy for non-compliant endpoints or even change the security policy as needed.

For Windows based endpoints, the pane also displays the warranty status for the CES installation on the endpoint and enables the administrator to enable or disable the warranty, depending on requirement and number of CES licenses purchased.

- To open the 'Advanced' pane, click 'Advanced' from the left hand side navigation of Computer Properties screen.

Note: The 'Advanced' tab is available only for Windows and Mac OS based endpoints

---

Group and Policy Details

The 'Group and Policy Details' area displays the details of the group to which the endpoint belongs, the security policy in effect on the endpoint and its compliance status. It also allows the administrator to change the security policy applied to the endpoint, if required.

- **Member of Group** - Name of the group to which the endpoint belongs. Clicking on the group name opens the Group properties interface. Refer to **Viewing and Managing Endpoint Groups** for more details.

- **Current Policy** - Displays the current security policy applied to the endpoint as per the current connection mode. Clicking on the policy name opens the Policy Properties interface. Refer to **Editing a Security Policy** for more details.

- **Current Policy Status** - Displays whether the endpoint is in complaint or non-compliant policy mode applied to it. If it is non-complaint, the administrator can click the 'Reapply Policy' button to drive the endpoint to be compliant to the policy.

- **Current Connection Mode** - Indicates whether the endpoint is connected to CESM through local network or Internet, which determines whether the computer will be using the Local Policy or Internet Policy.

- **Last Poll Time** - Indicates the date and time at which CESM has polled the endpoint to check the compliancy status. The policy will be re-applied to non-compliant endpoints to make them compliant, during the next polling.

- **Use group policy for this computer** - If selected, local and Internet connection security policies assigned to the group to which the endpoint belongs are applied to the endpoint. The policies in effect are displayed below:

  - **Group Local Policy** - Displays the Local network connection security policy assigned for the group. Clicking on the policy name opens the Policy Properties interface. Refer to **Editing a Security Policy** for more

details.

- **Group Internet Policy** - Displays the Internet connection security policy assigned for the group. Clicking on the policy name opens the Policy Properties interface. Refer to **Editing a Security Policy** for more details.

- **Use individual policy for this computer** - If selected, administrators can apply local and internet policies to the endpoint on an individual/manual basis, regardless of the group to which it belongs. Policies can be chosen from the respective drop-downs menus.

  - **Local Policy** - The drop-down displays the current local network connection security policy applied to the endpoint. The administrator can change it by selecting the required policy from the drop-down.
  - **Internet Policy** - The drop-down displays the current Internet connection security policy applied to the endpoint. The administrator can change it by selecting the required policy from the drop-down.

Warranty Details

The Warranty Details area displays whether the CES warranty is enabled or disabled for the endpoint. If needed, the administrator can enable or disable the warranty depending on the endpoint requirement and the number of CES licenses purchased, by clicking 'Enable' or 'Disable' button respectively.

> **Note**: The 'Warranty Details' are displayed only for Windows based endpoints installed with CES.

- To reload the currently viewed screen with updated details, Click 'Refresh'

- To close the 'Advanced Properties' screen of the selected endpoint click 'Close'.

- To start a remote desktop session with the selected endpoint, click 'Desktop"

3.1.3. Viewing and Managing Endpoint Security Software

The 'Endpoint Security' pane displays the details of the CES/CAS installation on the Windows based endpoint/CAV for Mac installation on Mac OS X based endpoint.

- **Windows based Endpoints** - The administrator can view the version details of the CES installation and virus signature database, run on-demand antivirus scans on the endpoint, update the database, manage items quarantined by the CES at the endpoint and view a log of Antivirus and Viruscope events and activities of the files identified as malware. Refer to the following section **Viewing and Managing CES on Windows based Endpoint** for more details.

- **Mac OS based Endpoints** - The administrator can view the version details of the CAV product and virus signature database and can update the database at the endpoint, run on-demand antivirus scans on the endpoint, update the database, manage items quarantined by the CAV at the endpoint and view a log of Antivirus events. Refer to the following section **Viewing and Managing CAV on Mac OS X based endpoint** for more details.

Viewing and Managing CES on Windows based Endpoint

- To open the Endpoint Security pane, click the 'Endpoint Security' tab from the left hand side navigation of the Computer Properties screen. The pane has three tabs:

  - **General**
  - **Quarantined Items**
  - **Antivirus Events**
  - **Viruscope Events**

General
The general tab displays the version, virus database update status of the CES installation. The administrator can run antivirus scans from this area.
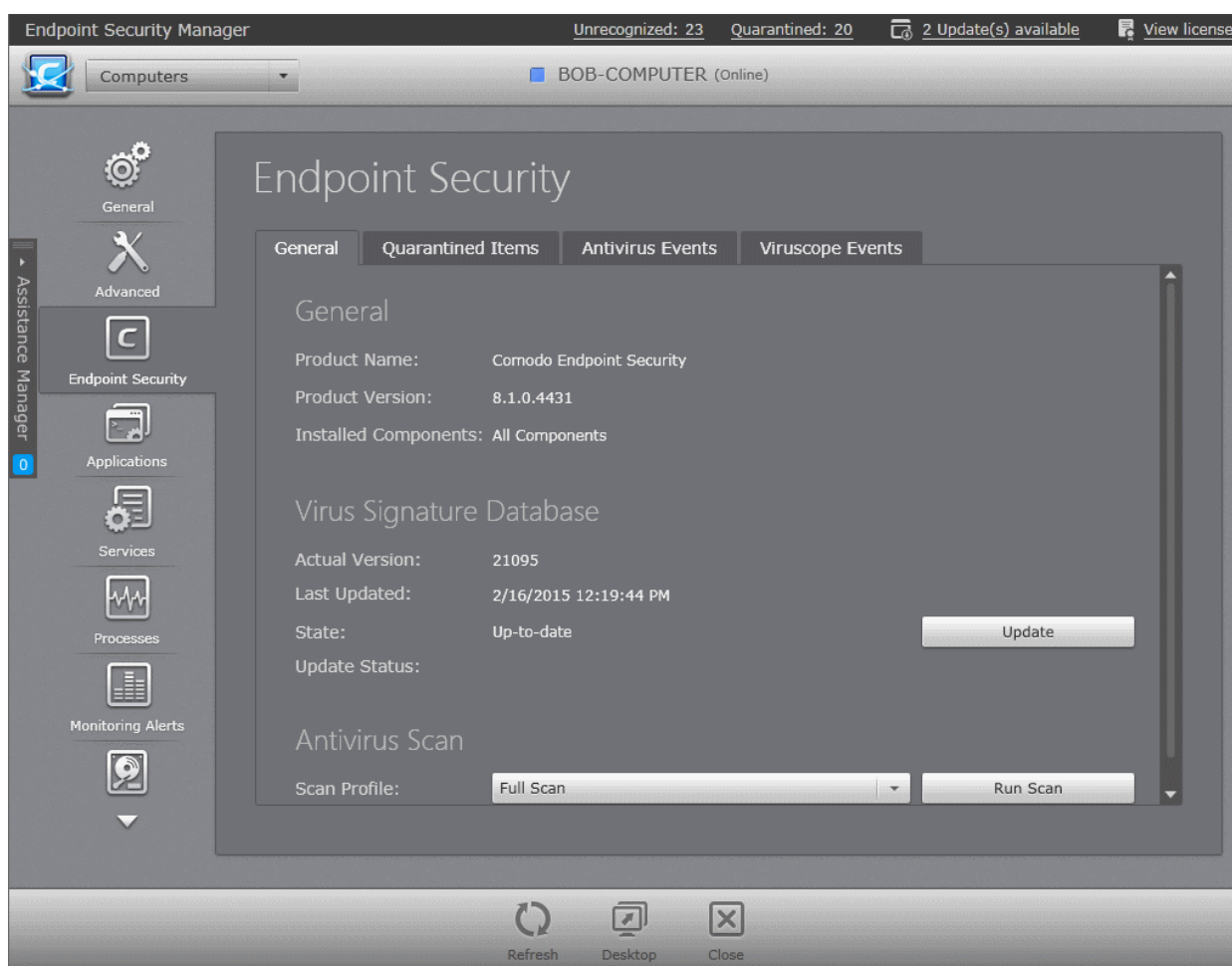
- **Product Version** - Displays the version of CES installed on the endpoint

- **Installed Components** - Displays the components, Antivirus, Firewall or All Components of CES installed on the endpoint.

Virus Signature Database

- **Actual Version** - Displays the version number of virus signature database on the endpoint.

- **Last Updated** - Displays the date and time of last scheduled or manual database update operation.

- **State** - Indicates whether the virus signature database is up-to-date or outdated. It is recommended to keep the virus database up-to-date always to protect your endpoints from zero-hour threats. If the database is out-dated, the administrator can manually run the update operation by clicking the 'Update' button.

- **Update Status** - Displays the result of last update operation.

Antivirus Scan

The Antivirus Scan area allows the administrator to commence on-demand antivirus scans directly on the selected endpoint.

To run an antivirus scan

- Select the Scan Profile from the drop-down, depending on the areas to be scanned on the endpoint. The default scan profiles are:

  - **Full Scan** - This profile covers every local drive, folder and file on the endpoint.

  - **Quick Scan** - Covers critical areas in the endpoint which are highly prone to infection from viruses, rootkits and other malware. This includes system memory, auto-run entries, hidden services, boot sectors, important registry keys and system files. These areas are responsible for the stability of the computer and keeping them clean is essential.

  - More scan profiles can be defined when creating a policy and applying the policy to the group or the endpoint. For more details on scan profiles, please refer to CES online help guide at **http://help.comodo.com/topic-84-1-604-7476-Scan-Profiles.html**

- Click 'Run Scan'.

> **Tip**: Alternatively, you can run a scan on an individual endpoint from the 'Computers' area, by right-clicking on the endpoint and selecting 'Scan' from the context sensitive menu or selecting the endpoint and clicking 'Antivirus' > 'Scan' > 'Full Scan' from the options at the bottom of the interface.

The scan will start immediately and the progress will be displayed beside 'Scan Status'.

- If malware is discovered during the scan that is not handled successfully (deleted, disinfected or quarantined) then the endpoint will be indicated as Infected in the 'Computers' area.

- The results of the scan can be viewed as an Infection report from the Reports area - click 'Reports' then the 'Computer Infections'. The report can also be exported as a pdf file or a spreadsheet file for printing purposes. Refer to **Reports > Computer Infections** for more details.

- To reload the currently viewed screen with updated details, Click 'Refresh'

- To close the 'Endpoint Property' screen of the selected endpoint click 'Close'.

- To initiate a remote desktop session with the selected endpoint, click 'Desktop'

Quarantined Items

The 'Quarantined Items' tab displays the list of items found as malicious and moved to quarantine by CES installation on the endpoint from real-time and on-demand scans. The administrator can analyze the trustworthiness of the items and delete them permanently or restore them to their original location from this interface.

Quarantined Items - Column Descriptions	
Column Heading	**Description**
Malware	The name of the item identified as malware and moved to quarantine
Location	The original file path of the quarantined item at the endpoint.
Quarantined	The precise date and time at which the item was moved to quarantine at the endpoint.
Status	Indicates the progress of actions like restoring or deleting the item, when executed.

Search Options

The administrator can search for specific items by entering the malware name, location or quarantined period in the respective search field that appears on clicking the filter icon ⊤ in the respective column header.

- Click the filter icon in the 'Malware' column header to search for a particular malware by entering the name in full or part and click 'Apply'.
- Click the filter icon in the 'Location' column header to search for a particular entry by specifying the location in full or part and click 'Apply'.
- Click the filter icon in the 'Quarantined' column header to search for an entry based on the period at which the item was quarantined, choose the start date and end date of the period by clicking the the calendar icons and click 'Apply'.
- To restore item(s) which are not malicious, select the item(s) and click 'Restore'. The items will be restored to their original locations in the endpoint.
- To remove item(s) that are malicious, select the item(s) and click 'Delete'. The items will be permanently deleted from the endpoint.

Note: The administrator can view a consolidated list of items moved to the quarantine by the CES installations at all the managed endpoints through the 'Quarantine' Area and manage them. The 'Quarantine' area is accessible by choosing 'Quarantine' from the drop-down at the top left or clicking 'Quarantine' button in the filter options at the top of the 'Computers' interface. Refer to the section **Viewing and Managing Quarantined Items** for more details.

- To reload the currently viewed screen with updated details, Click 'Refresh'
- To close the 'Endpoint Property' screen of the selected endpoint click 'Close'.
- To initiate a remote desktop session with the selected endpoint, click 'Desktop'

Antivirus Events

The 'Antivirus Events' tab displays the log of antivirus events at the endpoints with the details of each event as a table.

Antivirus Events - Column Descriptions	
Column Heading	**Description**
Date	The precise date and time of the event.
Location	The original file path of the item identified as malware.
Malware Name	The name of the item identified as malware.
Action	The action taken by CES/CAS on the item, like Detected or Quarantined.
Status	The result of the action performed on the item

Filter and Search Options:

The administrator can filter the table to search for events based on date, location of malware, the malware name, action or status by entering the search criteria in the search field that appears on clicking the filter icon ▼ in the respective column header.

- Click the filter icon in the 'Date' column header to filter the events occurred on particular date range, specify the date range and click 'Apply'.
- Click the filter icon in the 'Location' column header to search for a particular entry by specifying the location in full or part and click 'Apply'.
- Click the filter icon in the 'Malware Name' column header to filter events related to a particular malware, entering the name of the malware in full or part and click 'Apply'.
- Click the filter icon in the 'Action' column header to filter events by a particular action taken by CAV, enter the action and click 'Apply'.
- Click the filter icon in the 'Status' column header to filter the events based on status, enter the status and

click 'Apply'.

Viruscope Events

The 'Viruscope Events' tab displays the log of viruscope events at the endpoints detected based on malicious activities executed by the applications, with the details of each event as a table.

Antivirus Events - Column Descriptions	
Column Heading	**Description**
Date	The precise date and time of the event.
Location	The original file path of the item that exhibited malicious activities.
Malware Name	The name of the item identified as malware.
Action	The action taken by CES on the item. The possible actions are: • Reverse - Viruscope detected suspicious activity and attempted to reverse any changes made to the file system. • Quarantine - Viruscope placed the suspicious file into quarantine. • Detect - Viruscope detected malicious activity but did not quarantine the executable or reverse its changes. • Ask - Viruscope detected malicious activity and presented a pop-up asking the user whether it should quarantine the executable or reverse the changes.
Status	The result of the action performed on the item.
Activities	The activities of the item at the endpoint before it was identified as malware and an action was taken by CES. The Activities can be viewed only for endpoints installed with CES 8 or above. For other

	endpoints with CES 7 or below or CAS, the 'Activities' column will show 'No Activities'. Refer to the following section **Viewing Activities of a Malware** for more details.

Filter and Search Options:

The administrator can filter the table to search for events based on date, location of malware, the malware name, action and/or status by entering the search criteria in the search field that appears on clicking the filter icon ▼ in the respective column header.

- Click the filter icon in the 'Date' column header to filter the events occurred on particular date range, specify the date range and click 'Apply'.
- Click the filter icon in the 'Location' column header to search for a particular entry by specifying the location in full or part and click 'Apply'.
- Click the filter icon in the 'Malware Name' column header to filter events related to a particular malware, entering the name of the malware in full or part and click 'Apply'.
- Click the filter icon in the 'Action' column header to filter events by a particular action taken by CAV, enter the action and click 'Apply'.
- Click the filter icon in the 'Status' column header to filter the events based on status, enter the status and click 'Apply'.
- Click the filter icon in the 'Status' column header to filter the events based on status, enter the status and click 'Apply'.

Viewing Activities of a Malware

The CES installation at the endpoint can monitor the process activities of an item identified as malware and add to the Viruscope logs forwarded to the CESM server. The administrator can view the activities of the malware, if any, at the endpoint and take corrective actions, if required, at the endpoint.

Note: The ability to monitor the activities and display them in the Antivirus logs is added to CES version 8. Hence the administrator will be able to view the process activities of a malware only for endpoints installed with CES 8 or above. For the endpoints installed with lower versions like CES 7, the Activities column will display 'No Activities' for all the entries.

The Activities column will indicate the number of activities identified for a malware as a hyperlink for the events. If the malware was identified before it could execute any malicious processes at the endpoint, the Activities column will indicate 'No Activities'.

- To view the process activities of a malware click the 'Activities' link in the Activities link
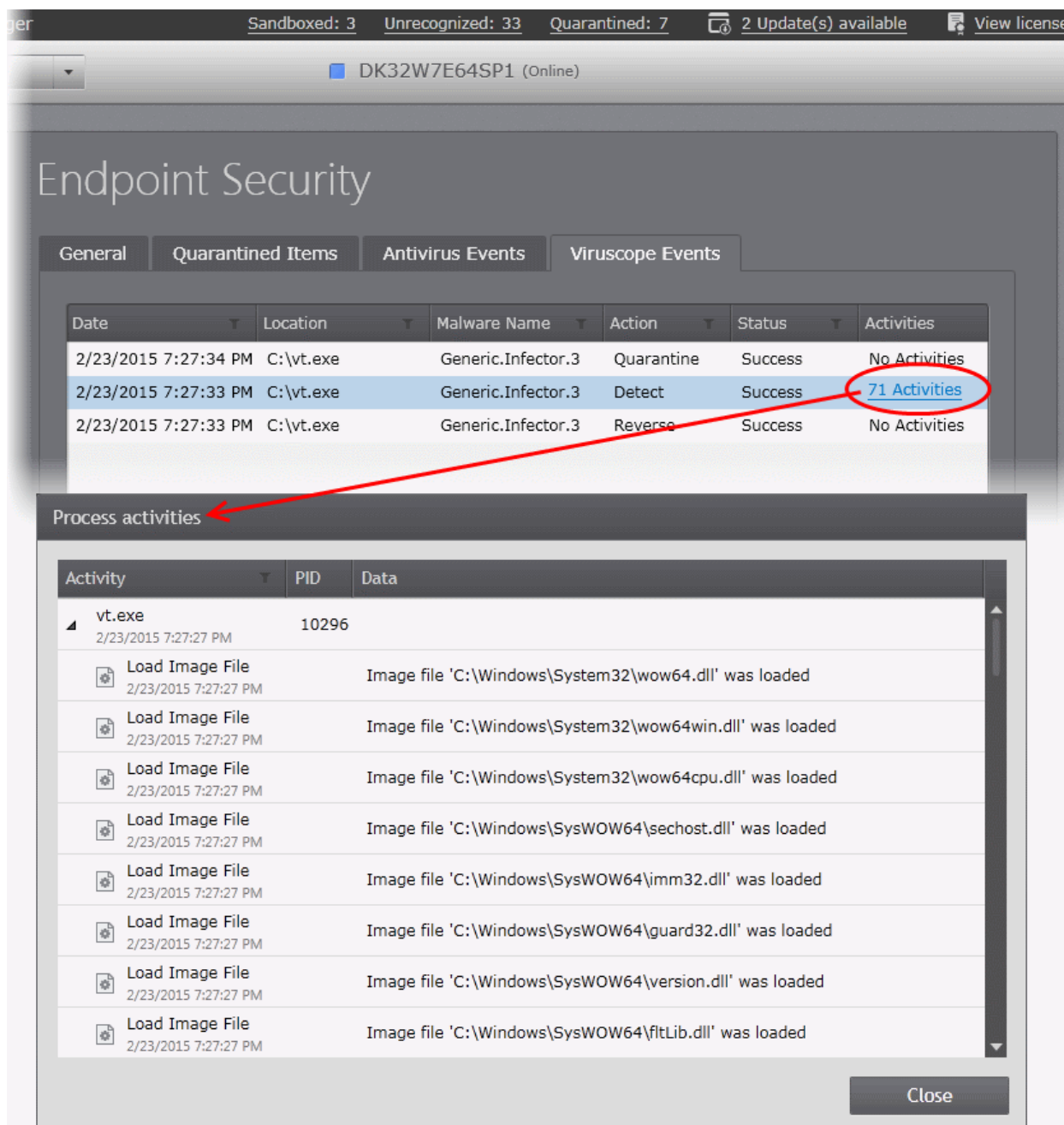
The 'Process Activities' dialog will open, displaying the list of process activities of the malware as a tree structure. The administrator can expand an item by clicking the right arrow ▷ beside a process name.

Process Activities - Column Descriptions	
Column Heading	**Description**
Activity	Indicates the process initiated by the malware
PID	Indicates the process identifier of the process
Data	A short description of the process.

Viewing and Managing CAV on Mac OS X based Endpoint

- To open the Endpoint Security pane, click the 'Endpoint Security' tab from the left hand side navigation of the Computer Properties screen. The pane has three tabs:

- **General**
- **Quarantined Items**
- **Antivirus Events**

General

The general tab displays the version, virus database update status of the CAV installation. The administrator can run antivirus scans from this area.
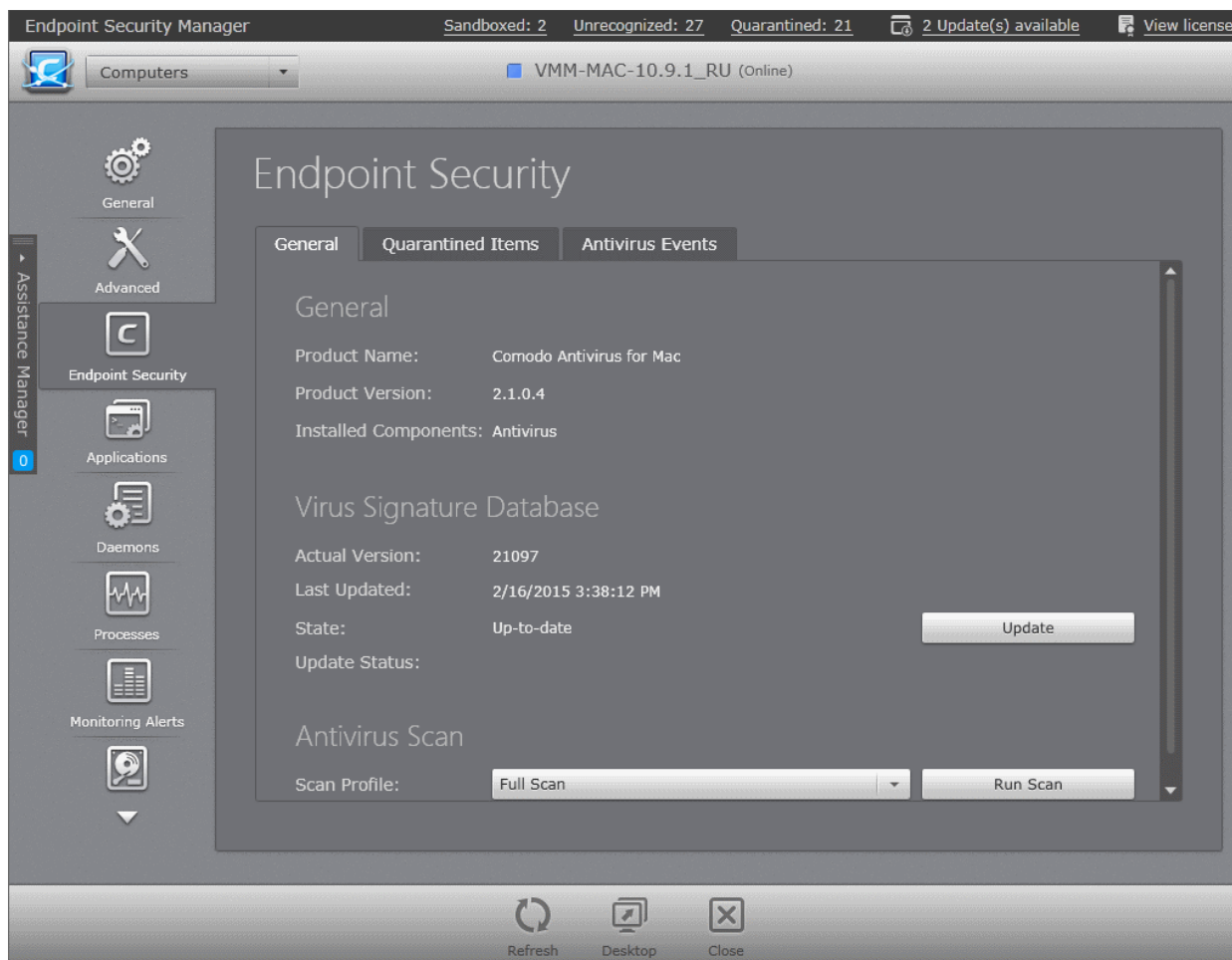
- **Product Name -** Displays the name of the security product installed on the endpoint.

- **Product Version** - Displays the version of CAV for Mac installed on the endpoint

- **Installed Components** - Displays the component, Antivirus installed on the endpoint.

Virus Signature Database

- **Actual Version** - Displays the version number of virus signature database on the endpoint.

- **Last Updated** - Displays the date and time of last scheduled or manual database update operation.

- **State** - Indicates whether the virus signature database is up-to-date or outdated. It is recommended to keep the virus database up-to-date always to protect your endpoints from zero-hour threats. If the database is out-dated, the administrator can manually run the update operation by clicking the 'Update' button.

- **Update Status** - Displays the result of last update operation.

Antivirus Scan

The Antivirus Scan area allows the administrator to commence on-demand antivirus scans directly on the selected endpoint.

To run an antivirus scan

- Select the Scan Profile from the drop-down, depending on the areas to be scanned on the endpoint. The default scan

profiles are:

- • **Full Scan** - This profile covers every local drive, folder and file on the endpoint.
- • **Quick Scan** - Covers critical areas in the endpoint which are highly prone to infection from viruses, rootkits and other malware. This includes system memory, auto-run entries, hidden services, boot sectors, important registry keys and system files. These areas are responsible for the stability of the computer and keeping them clean is essential.
- • More scan profiles can be defined when creating a policy and applying the policy to the group or the endpoint. For more details on scan profiles, please refer to CES online help guide at **http://help.comodo.com/topic-84-1-604-7476-Scan-Profiles.html**

- • Click 'Run Scan'.

Tip: Alternatively, you can run a scan on an individual endpoint from the 'Computers' area, by right-clicking on the endpoint and selecting 'Scan' from the context sensitive menu or selecting the endpoint and clicking 'Antivirus' > 'Scan' > 'Full Scan' from the options at the bottom of the interface.

The scan will start immediately and the progress will be displayed beside 'Scan Status'.

- • If malware is discovered during the scan that is not handled successfully (deleted, disinfected or quarantined) then the endpoint will be indicated as Infected in the 'Computers' area.
- • The results of the scan can be viewed as an Infection report from the Reports area - click 'Reports' then the 'Computer Infections'. The report can also be exported as a pdf file or a spreadsheet file for printing purposes. Refer to **Reports > Computer Infections** for more details.
- • To reload the currently viewed screen with updated details, Click 'Refresh'
- • To close the 'Endpoint Property' screen of the selected endpoint click 'Close'.
- • To initiate a remote desktop session with the selected endpoint, click 'Desktop'

Quarantined Items

The 'Quarantined Items' tab displays the list of items found as malicious and moved to quarantine by CES installation on the endpoint from real-time and on-demand scans. The administrator can analyze the trustworthiness of the items and delete them permanently or restore them to their original location from this interface.

Quarantined Items - Column Descriptions	
Column Heading	**Description**
Malware	The name of the item identified as malware and moved to quarantine
Location	The original file path of the quarantined item at the endpoint.
Quarantined	The precise date and time at which the item was moved to quarantine at the endpoint.
Status	Indicates the progress of actions like restoring or deleting the item, when executed.

Search Options

The administrator can search for specific items by entering the malware name, location or quarantined period in the respective search field that appears on clicking the filter icon ▼ in the respective column header.

- Click the filter icon in the 'Malware' column header to search for a particular malware by entering the name in full or part and click 'Apply'.

- Click the filter icon in the 'Location' column header to search for a particular entry by specifying the location in full or part and click 'Apply'.

- Click the filter icon in the 'Quarantined' column header to search for an entry based on the period at which the item was quarantined, choose the start date and end date of the period by clicking the the calendar icons and click 'Apply'.

- To restore item(s) which are not malicious, select the item(s) and click 'Restore'. The items will be restored to their original locations in the endpoint.

- To remove item(s) that are malicious, select the item(s) and click 'Delete'. The items will be permanently deleted from the endpoint.

> **Note**: The administrator can view a consolidated list of items moved to the quarantine by the security product installations at all the managed endpoints through the 'Quarantine' Area and manage them. The 'Quarantine' area is accessible by choosing 'Quarantine' from the drop-down at the top left or clicking 'Quarantine' button in the filter options at the top of the 'Computers' interface. Refer to the section **Viewing and Managing Quarantined Items** for more details.

- To reload the currently viewed screen with updated details, Click 'Refresh'
- To close the 'Endpoint Property' screen of the selected endpoint click 'Close'.
- To initiate a remote desktop session with the selected endpoint, click 'Desktop'

Antivirus Events

The 'Antivirus ' tab displays the log of antivirus events at the endpoints with the details of each event as a table.

Antivirus Events - Column Descriptions	
Column Heading	**Description**
Date	The precise date and time of the event.
Location	The original file path of the item identified as malware.
Malware Name	The name of the item identified as malware.
Action	The action taken by CAV on the item, like Detected or Quarantined.
Status	The result of the action performed on the item

Filter and Search Options:
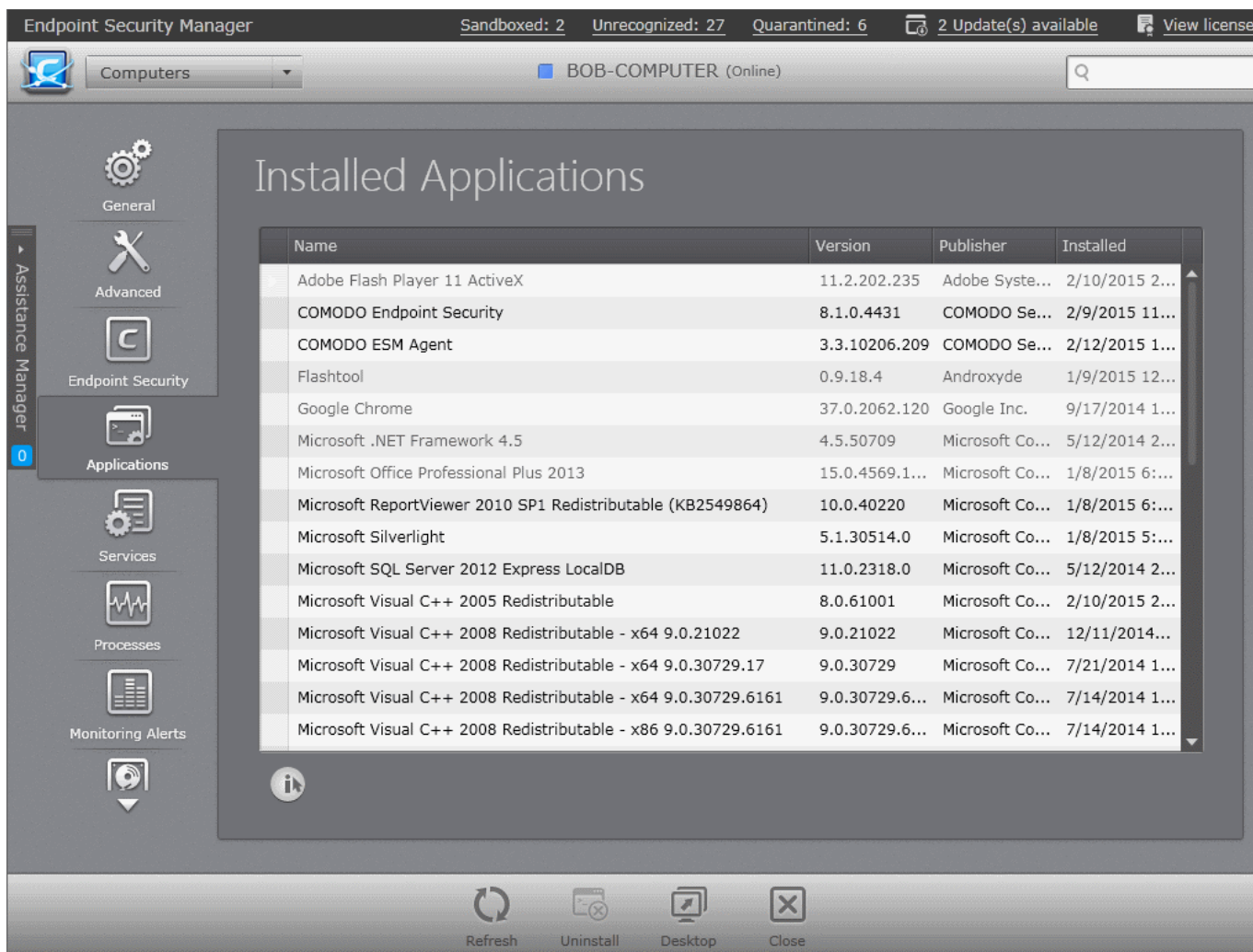
The administrator can filter the table for searching specific events by specifying the date, the malware name, location, action taken or the status in the respective search field that appears on clicking the filter icon ⊤ in the respective column header.

- Click the filter icon in the 'Date' column header to filter the events occurred on particular date range, specify the date range and click 'Apply'.
- Click the filter icon in the 'Location' column header to search for a particular entry by specifying the location in full or part and click 'Apply'.
- Click the filter icon in the 'Malware Name' column header to filter events related to a particular malware, entering the name of the malware in full or part and click 'Apply'.
- Click the filter icon in the 'Action' column header to filter events by a particular action taken by CAV, enter the action and click 'Apply'.
- Click the filter icon in the 'Status' column header to filter the events based on status, enter the status and click 'Apply'.

3.1.4. Viewing and Managing Installed Applications

The 'Installed Applications' pane displays the list of applications that are currently installed in the selected endpoint. The administrator can analyze the list and, if unwanted applications are present, the administrator can uninstall.

- To open the 'Installed Applications' pane, click the 'Installed Applications' tab from the left hand side navigation of the 'Computer Properties' screen.

- To uninstall an application, select it and click 'Uninstall' or right click on the application and select 'Uninstall' . The application will be uninstalled form the endpoint.
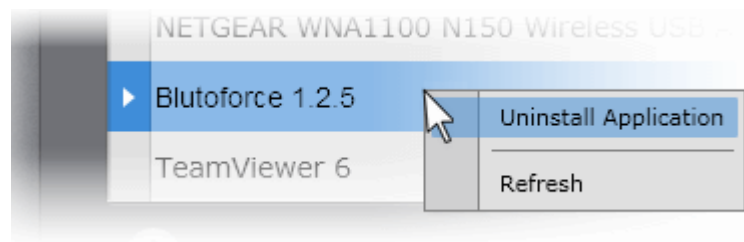
Note: You can uninstall only MSI based applications from this interface.

- To reload the currently viewed screen with updated details, Click 'Refresh'

- To close the 'Installed Applications' screen of the selected endpoint click 'Close'.

- To initiate a remote desktop session with the selected endpoint, click 'Desktop'

3.1.5. Viewing and Managing Currently Loaded Services or Daemons

The 'System Services'/'Daemons' pane displays the list of Windows Services loaded to Windows based endpoints or Mac OS X/Unix Daemons that are currently loaded on to the selected Mac OS or Linux based endpoint with their running status. The administrator can also view a short description of the service and stop/start services/daemons as required.

- To open the 'System Services'/'Daemons' pane, click the 'Services' tab or 'Daemons' tab from the left hand side navigation of the Computer Properties screen.

To view a short description of a service, hover the mouse cursor over the service.
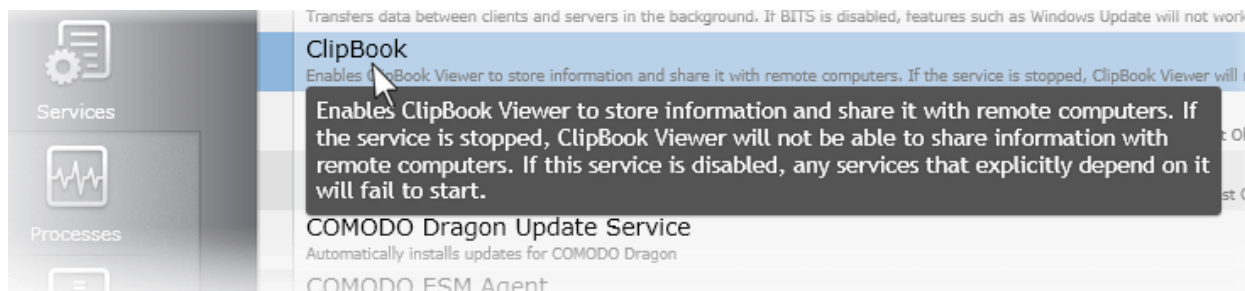
- To stop a running service/daemon, select it and click 'Stop' at the bottom of the interface or right click on it and choose 'Stop Service'/'Stop Daemon'.

- To start a stopped service/daemon, select it and click 'Start' at the bottom of the interface or right click on it and choose 'Start Service'/'Start Daemon'.
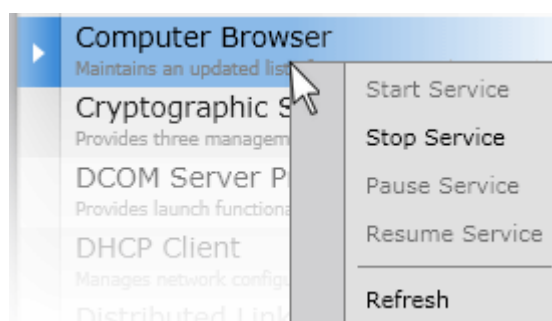
- To temporarily stop a service/daemon, right click on it and choose 'Pause Service'/'Pause Daemon'.

- To restart a temporarily stopped a service/daemon, right click on it and choose 'Resume Service'/Resume Daemon.

- To reload the currently viewed screen with updated details, Click 'Refresh'

- To close the 'System Services'/'Daemons' screen of the selected endpoint click 'Close'.

- To initiate a remote desktop session with the selected endpoint, click 'Desktop'

3.1.6. Viewing and Managing Currently Loaded Processes

The 'System Processes' pane displays the list of Processes that are currently loaded to the selected endpoint with their attributes like process identity, user account that has started the process, its CPU usage, memory usage and peak memory usage. The administrator can analyze the list and terminate unnecessarily running processes if required.

- To open the 'System Processes' pane, click the 'Processes' tab from the left hand side navigation of the Computer Properties screen.

- To stop a currently running process, select it and click 'End Process' or right click on the process and choose 'End Process'.

- To reload the currently viewed screen with updated details, Click 'Refresh'

- To close the 'System Processes' screen of the selected endpoint click 'Close'.

- To initiate a remote desktop session with the selected endpoint, click 'Desktop'

3.1.7. Viewing System Monitoring Alerts

The 'System Monitoring Alerts' pane displays the list of alerts generated whenever the system resource usage exceeds the thresholds set by the policy, applied to the endpoint. The administrator can analyze the history of system resource usages for troubleshooting, if any problems are reported on the endpoint.

- To open the 'System Monitoring Alerts' pane, click the 'Monitoring Alerts' tab from the left hand side navigation of the Computer Properties screen.

Note: The 'Monitoring Alerts' tab is available only for Windows and MacOS based endpoints.

- To reload the currently viewed screen with updated details, Click 'Refresh'

- To close the 'System Monitoring Alerts' screen of the selected endpoint click 'Close'.

- To initiate a remote desktop session with the selected endpoint, click 'Desktop'

3.1.8. Viewing and Managing Drives and Storage

The 'File System' pane displays the list of physical drives that are mounted on the selected endpoint. The contents of each drive can be browsed by double-clicking it. The 'Largest Files' feature allows admins to identify the top 10 largest files in a drive and to delete them if required.

- To open the 'File System' pane, click the 'File System' tab from the left hand side navigation of the Computer Properties screen.
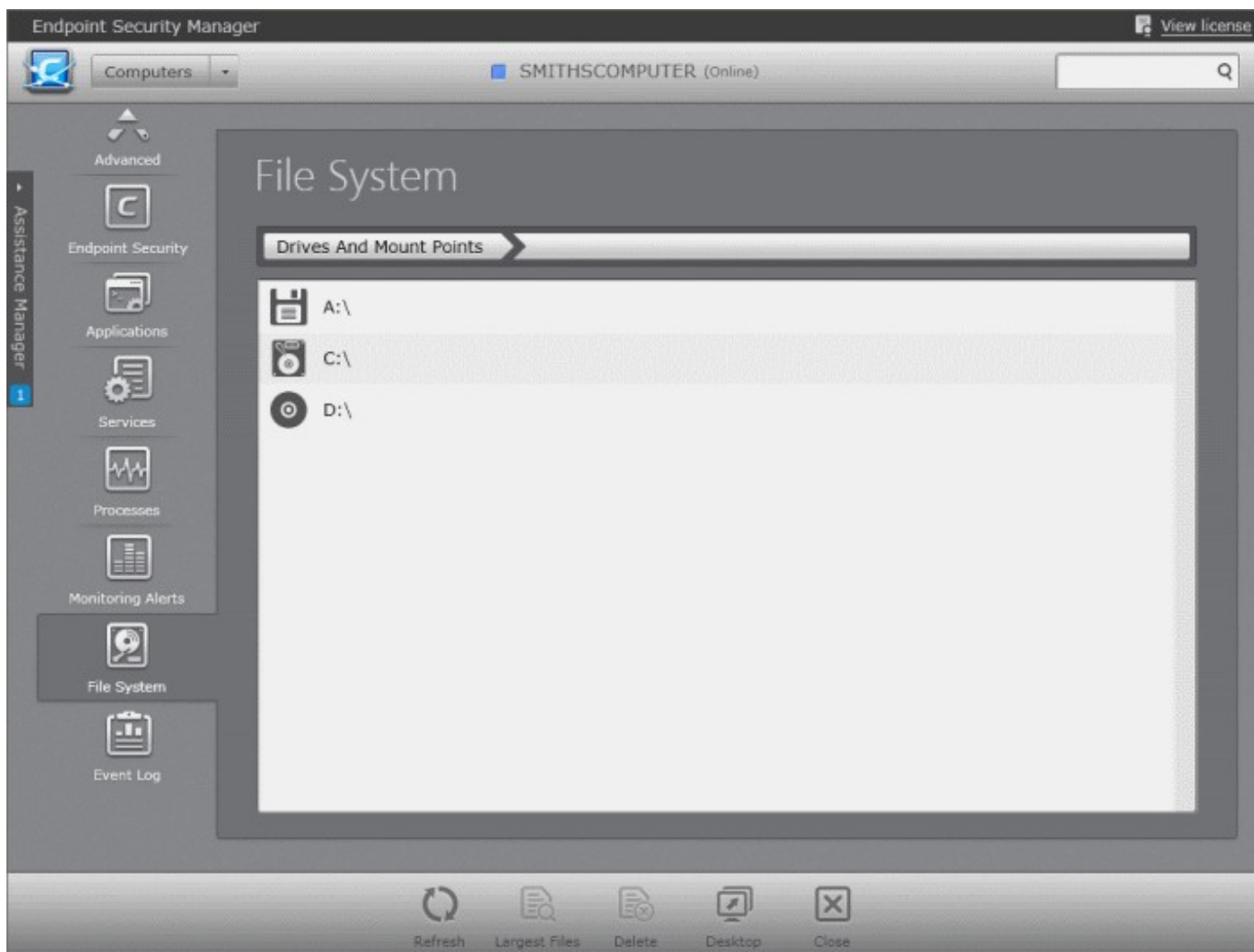
- To browse through the folders and files in a drive, double click on the drive > Folder and so on.
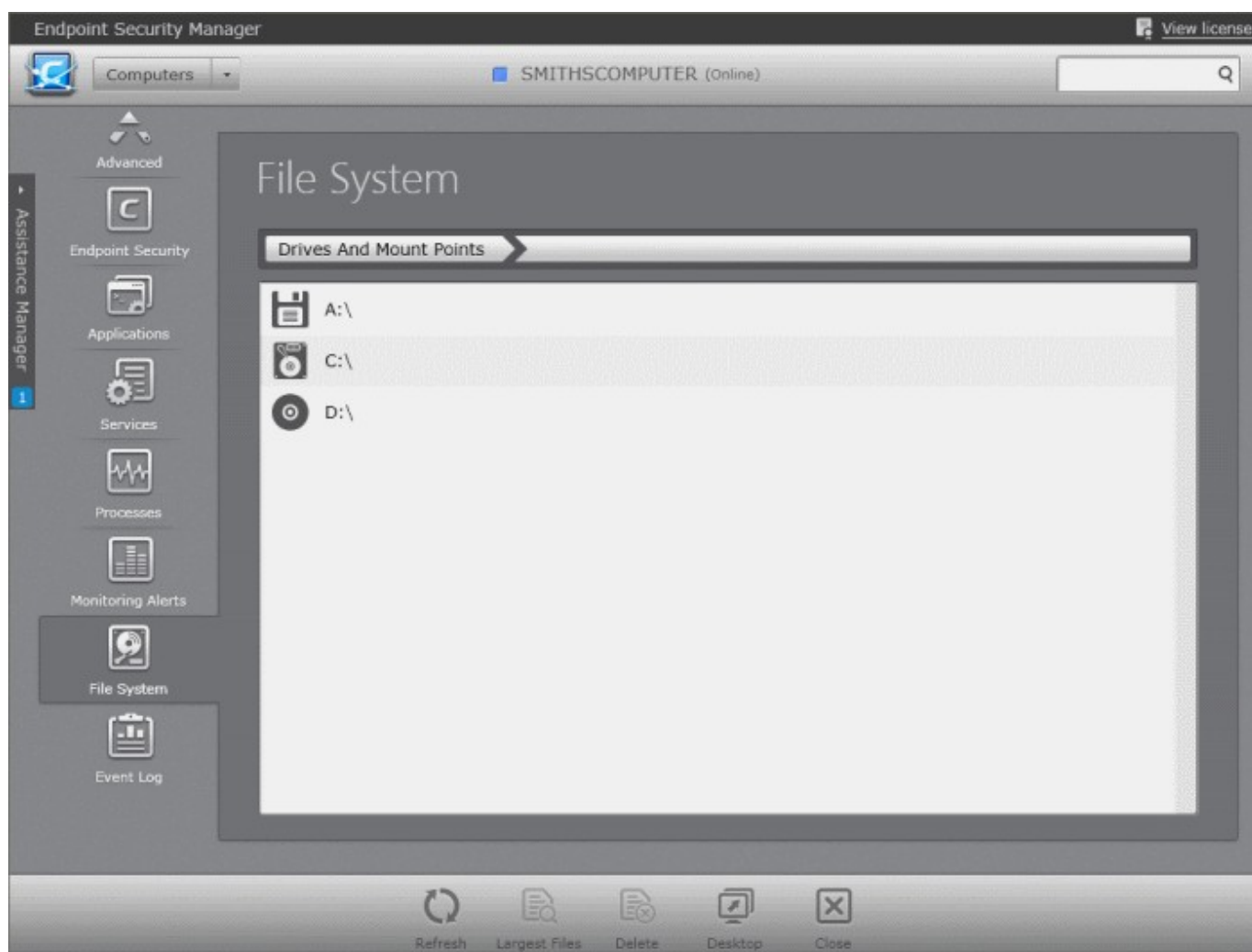
- To delete an unwanted folder or file, select the item and click 'Delete' or right click on the item and choose 'Delete' from the context sensitive menu.

- To identify top ten space consuming files in a drive, select the drive and click 'Largest Files' at the bottom of the interface or right click on a drive and choose 'Largest Files' from the context sensitive menu.
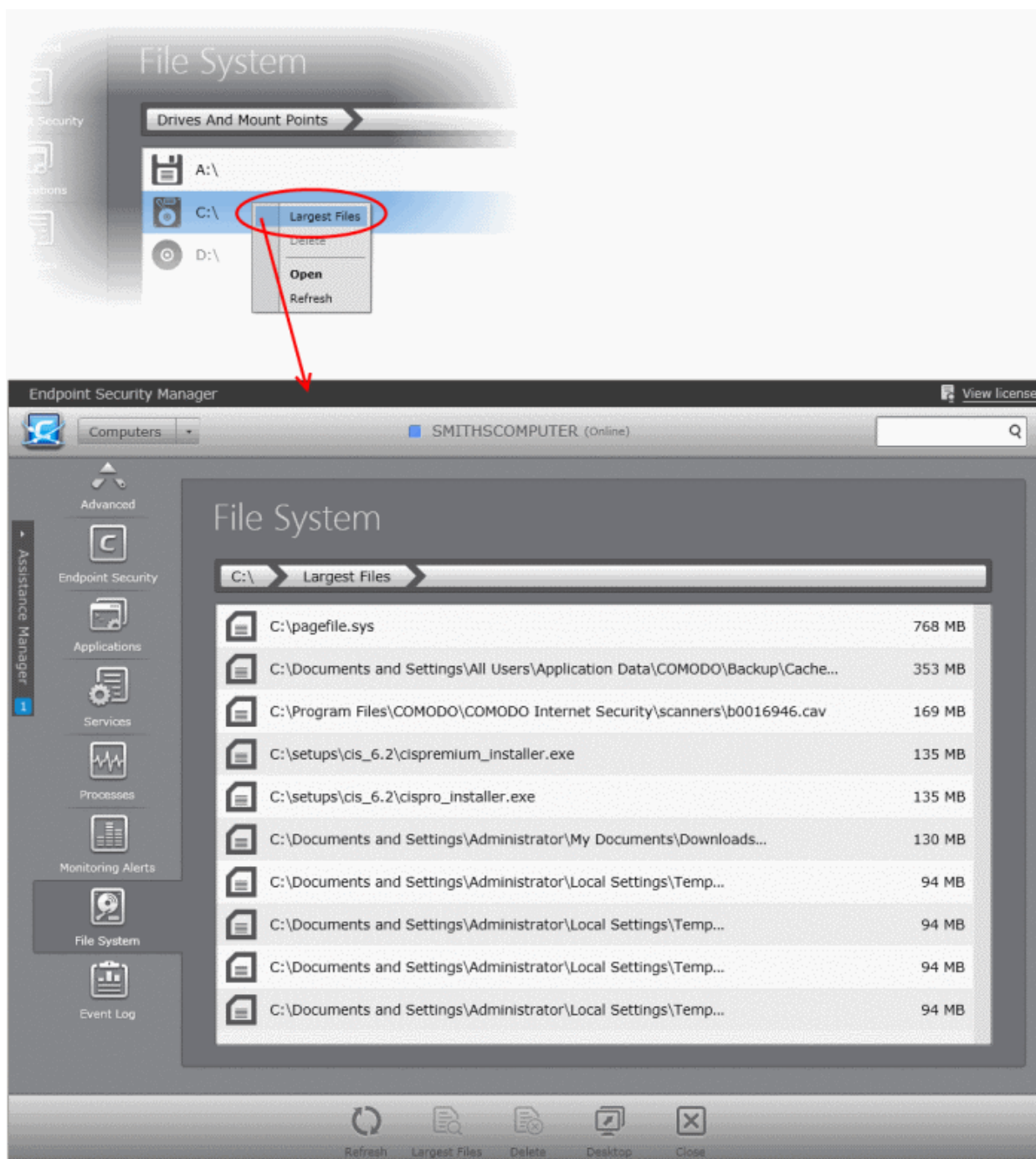
The administrator can delete unwanted files from the large files list, to conserve disk space and improve system performance.

- To reload the currently viewed screen with updated details, Click 'Refresh'

- To close the 'File System' screen of the selected endpoint click 'Close'.

- To initiate a remote desktop session with the selected endpoint, click 'Desktop'

3.1.9. Viewing Event Log

The 'Event Log' pane allows administrators to browse endpoint events, such as a failure to start a component or complete an action at the selected endpoint.

- To open the 'Event Log' pane, click the 'Event Log' tab from the left hand side navigation of the 'Computer Properties' screen.

Note: The 'Event Log' tab is available only for Windows based endpoints.
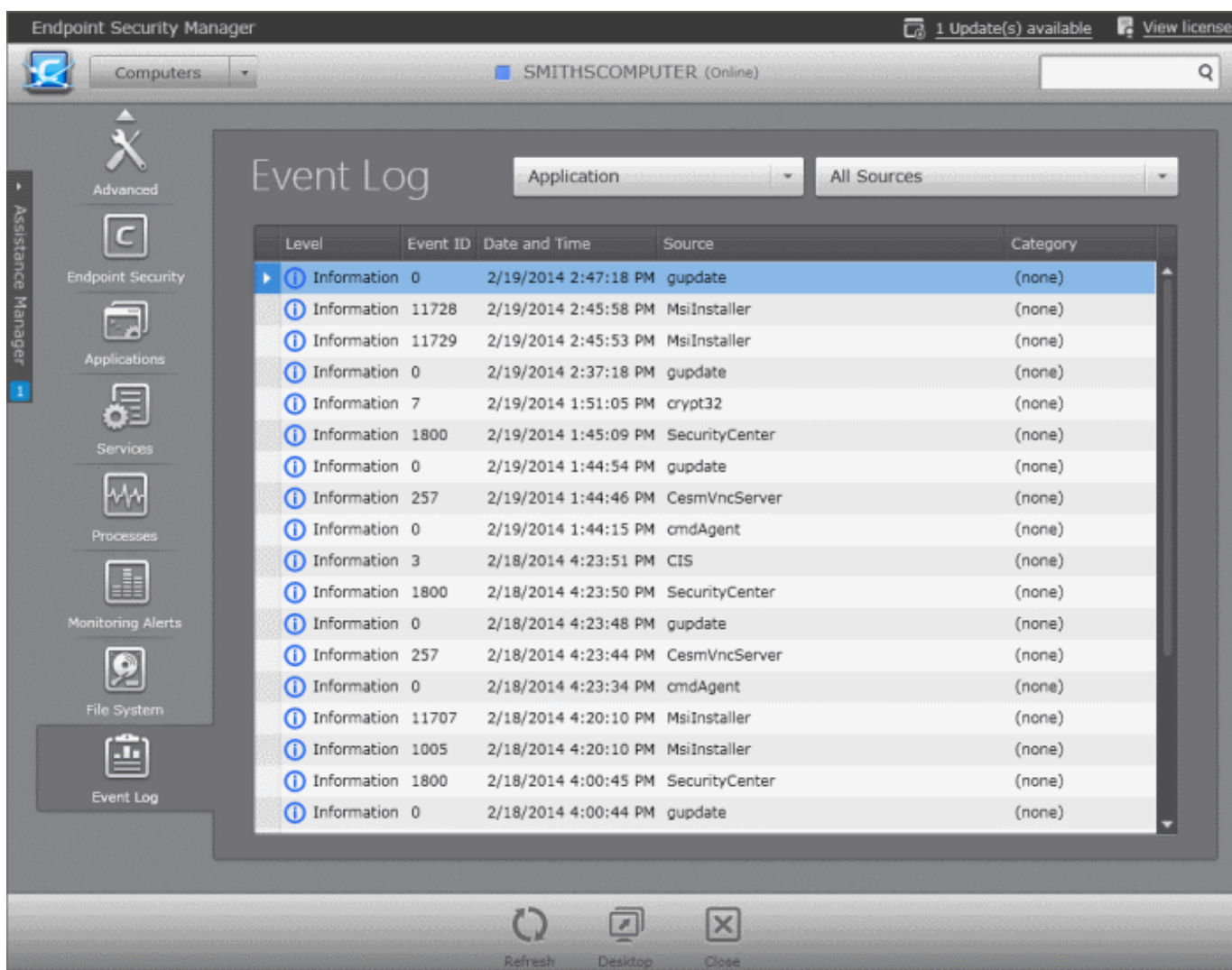
- To view the details of an event, double-click on the event. The 'Event Log Item Details' dialog will open.
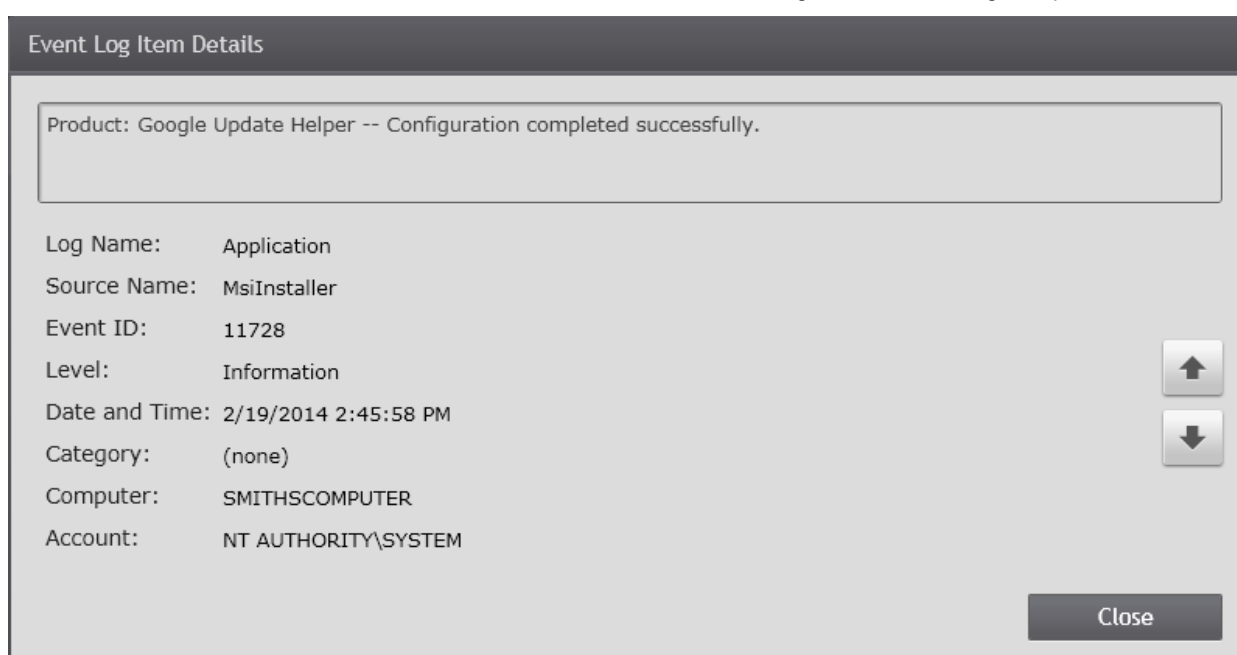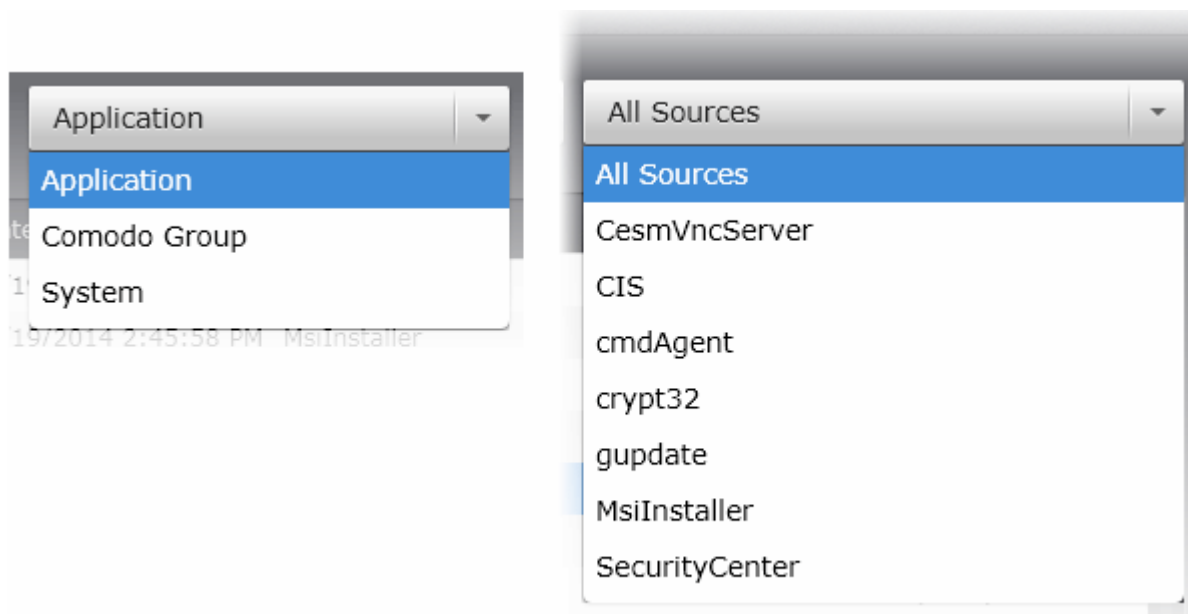

- To navigate through successive log items, and view the details of those, click the up and down arrows at the lower

pane of the 'Event Log Item Details' dialog.
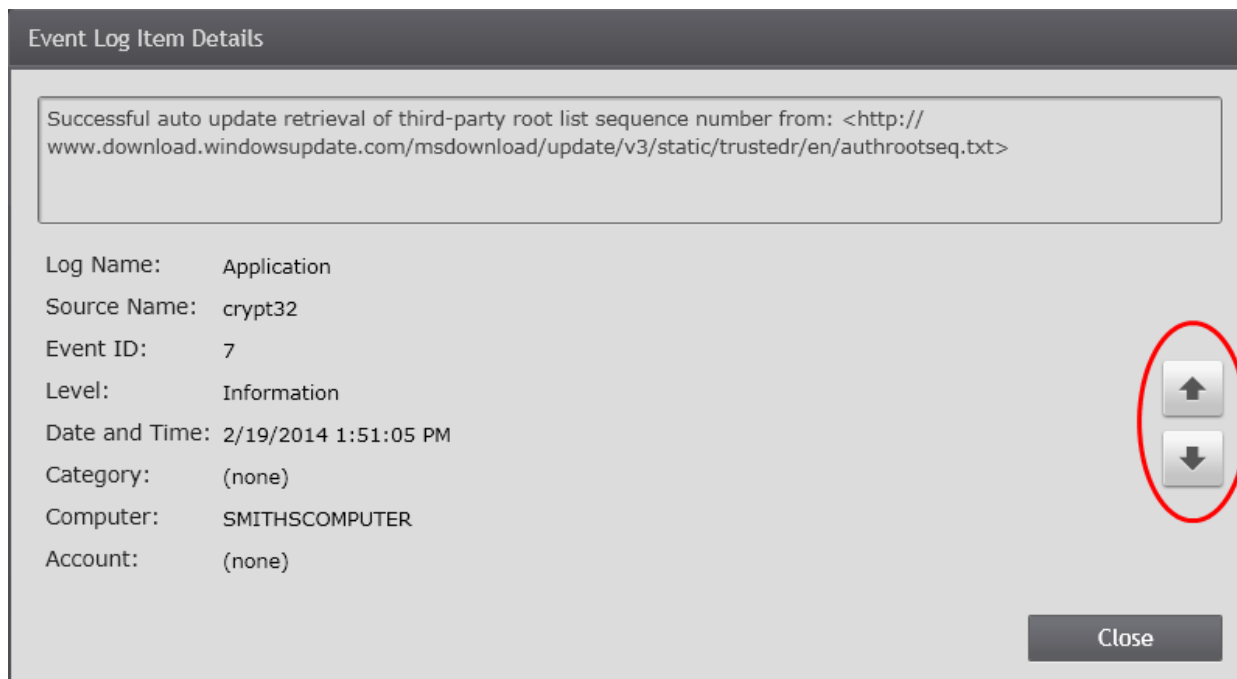
- You can filter the results based on the category of the events from the drop-down at the left.
- You can filter the results based on the sources from the drop-down at the right.

- To reload the currently viewed screen with updated details, Click 'Refresh'
- To close the 'Event Log' screen of the selected endpoint click 'Close'.
- To initiate a remote desktop session with the selected endpoint, click 'Desktop"

3.2. Adding Endpoint Computers to CESM

Each managed endpoint requires a small software agent to be installed to facilitate communication with the CESM console. Depending on the method by which the agent is installed, the endpoints can be imported into CESM in two ways:

- Installing the agent directly from the CESM Admin Console and importing computers from Active Directory, Workgroup or by specifying the IP addresses. This method is suitable for computers in the local network. Refer to **Importing Computers by Automatic Installation of Agent**.

- Downloading the agent as an executable for installing manually, transferring it onto media such as DVD, CD, USB memory or uploading it to a network share then installing onto the endpoint computers. This method is more suitable for computers connected through external networks like the Internet. Refer to **Adding Computers by Manual Installation of Agent**.

Once the agent is installed, the endpoint computer is automatically discovered and added into CESM to the Unassigned group where it will be given the configured policy (see '**The Policies Area**' for more details) and is then ready to be managed.

The 'Computers' area also allows the administrators to arrange the added computers into 'Groups' as per the structure of the organization for easy administration. Once created administrators can run tasks on entire groups of computers (such as applying security policy for CES, running AV scans, deploying agents, updating AV databases and more). Refer to **The Groups Area** for more details.

3.2.1. Importing Computers by Automatic Installation of Agent

Prerequisite - Before importing the endpoints, you need to download the latest versions of the CESM Agent and the CES/CAS and CAV for Mac packages for remote or manual installation on to the endpoints to be managed. Refer to the section **Preferences** > **Downloading ESM Packages** for more details

The 'Add Computer' wizard enables the administrator to:

- Remotely install the CESM agent software and CES software on Windows based network endpoints that can be reached from the CESM service computer. Computers can be imported from Active Directory, from a Workgroup or by specifying individual IP addresses.

- Remotely install CESM agent software and CAV for Mac on Mac OS based network endpoints that can be reached from the CESM service computer. Computers can be imported by specifying individual IP addresses.

- Remotely install CESM agent software on Linux based network endpoints that can be reached from the CESM service computer. Computers can be imported by specifying individual IP addresses.

- Remotely update installed Comodo software in managed computers. See '**Updating Comodo Software on Managed Computers**' for more details.

To import endpoints

- Click the 'Add' from the 'Computers' area to start the wizard:

Step 1 - Select the Target Type

Computers can be imported into CESM in the following ways:

- **Active Directory** - imports computers from an Active Directory Domain.

- **Workgroup** - imports computers from a Workgroup.

- **Network Addresses** - imports Windows based individual computers specified by their IP Addresses.

- **Deploy to Linux/Mac OS X endpoints** - allows you to import Linux and Mac OS based computers specified by their IP Addresses. CESM will automatically detect the Operating system of the computers and remotely install the agent package and endpoint security package appropriate to the OS.

  - For Linux based endpoints - CESM will install the CESM agent for centralized device management
  - For Mac OS X based computers - CESM will install the agent and Comodo Antivirus for Mac

- **Managed Computers** - allows you to update installed Comodo software in managed computers. See '**Updating Comodo Software on Managed Computers**' for more details.

> **Note:** Targets are contacted by the CESM service computer and its network connection, not the computer running the management console.

CESM Professional Edition can manage a large number of networked computers so, administrators should repeat this process until all computers for which management is required have been successfully imported.

> **Note:** In most editions, licenses are required for each computer you wish to manage.

Explanations of importing using the sources can be found below in the sections that follow: **Import from Active Directory**, **Import from Workgroup**, **Import Computers by IP Address** and **Importing Linux and Mac OS based Computers**.

- Select the appropriate method to import the computers from Active Directory or Workgroup or select Network Addresses if you want to import Windows based computers by specifying their IP addresses or DNS names or select 'Deploy to Linux/Mac OS X endpoints' if you want to import Linux or Mac OS based computers by specifying their IP addresses or DNS names.
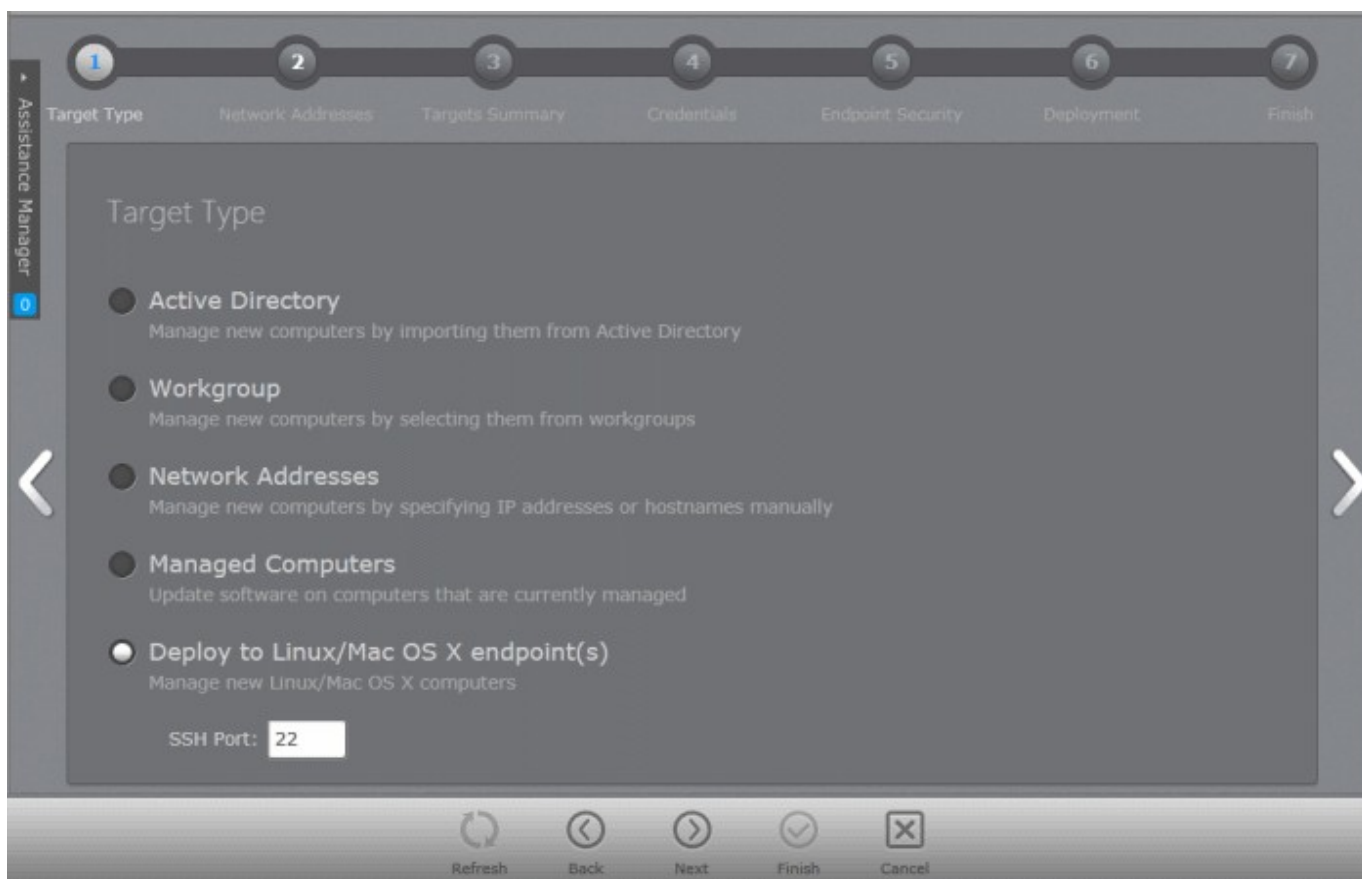
Importing from Active Directory

• Choose 'Active Directory' and move to the next step by clicking the right arrow or swiping the screen to the left.

Step 2 - Domain Name

Select Current Domain or Custom Domain. Current Domain should be chosen if the CESM service computer is currently a member of the domain you wish to use to target for installation. If you select Custom Domain, you have to enter the details of domain controller, an administrator user name and password.


Domain Import Settings - Table of Parameters	
Current Domain (Selected by default)	Selecting this option will import any computers from the Active Directory domain that the CESM server is a member of.
Custom Domain controller	Selecting this option allows the administrator to specify an alternative Active Directory domain from which computers will be imported. Choosing this option requires administrators to specify the following details:
Domain Controller:	Enter the IP address or host name of the Active Directory domain controller from which they wish to import.
User Name:	Enter the user-name of a user with administrative rights to the domain controller.
Password:	Enter the password of the user specified in the 'User Name' field.

• Click the right arrow. The wizard moves to next step to select the target endpoints.

Select Targets

The Active Directory structure for the selected domain will be listed.

___
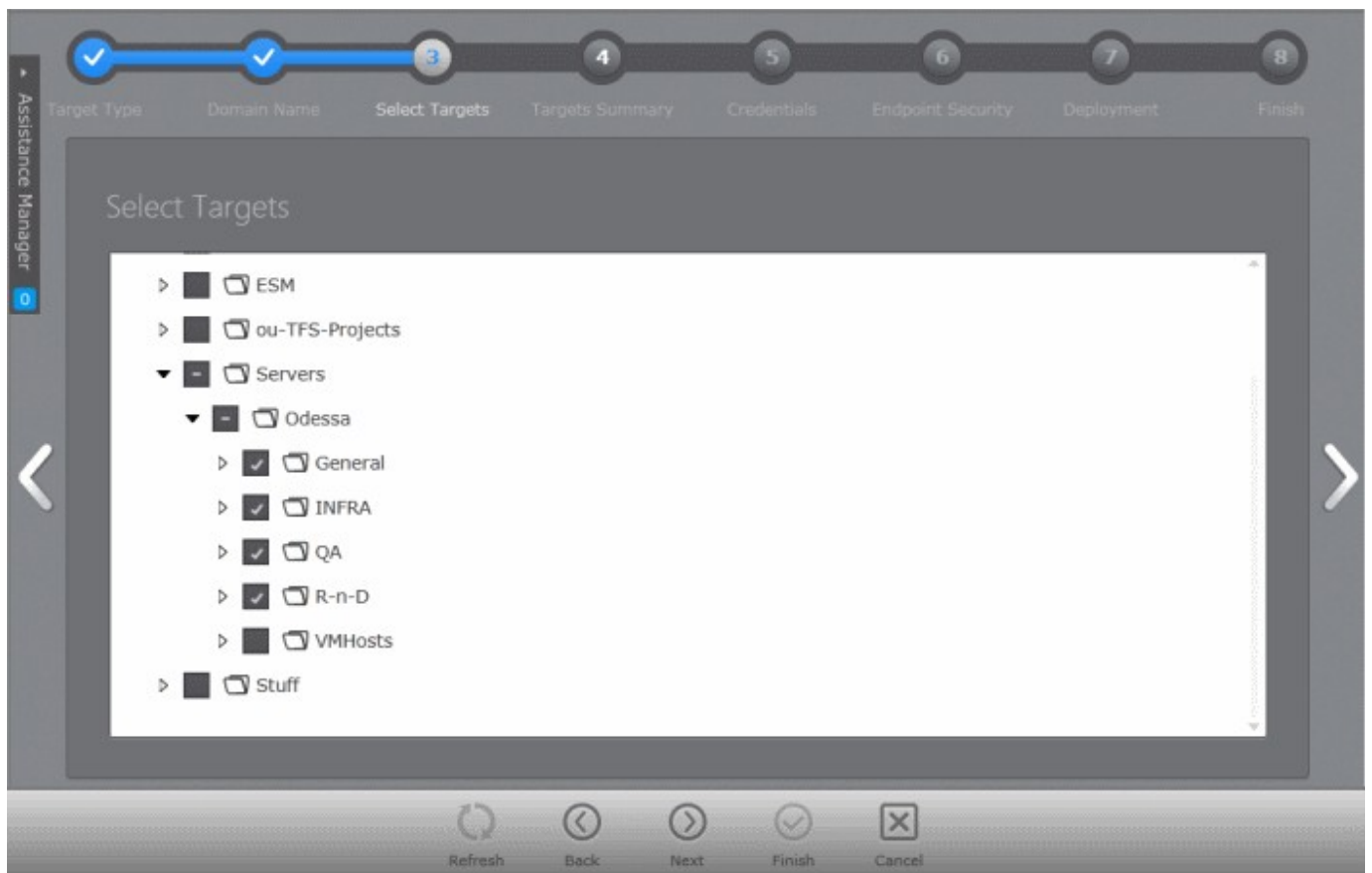
- Click the ▸ icon to expand or collapse the tree structure.

- Select the target endpoints onto which you wish to install the agent and import into CESM.

- Click the right arrow or swipe left to move to **step 3** to select the endpoints.

Importing Computers from Workgroup

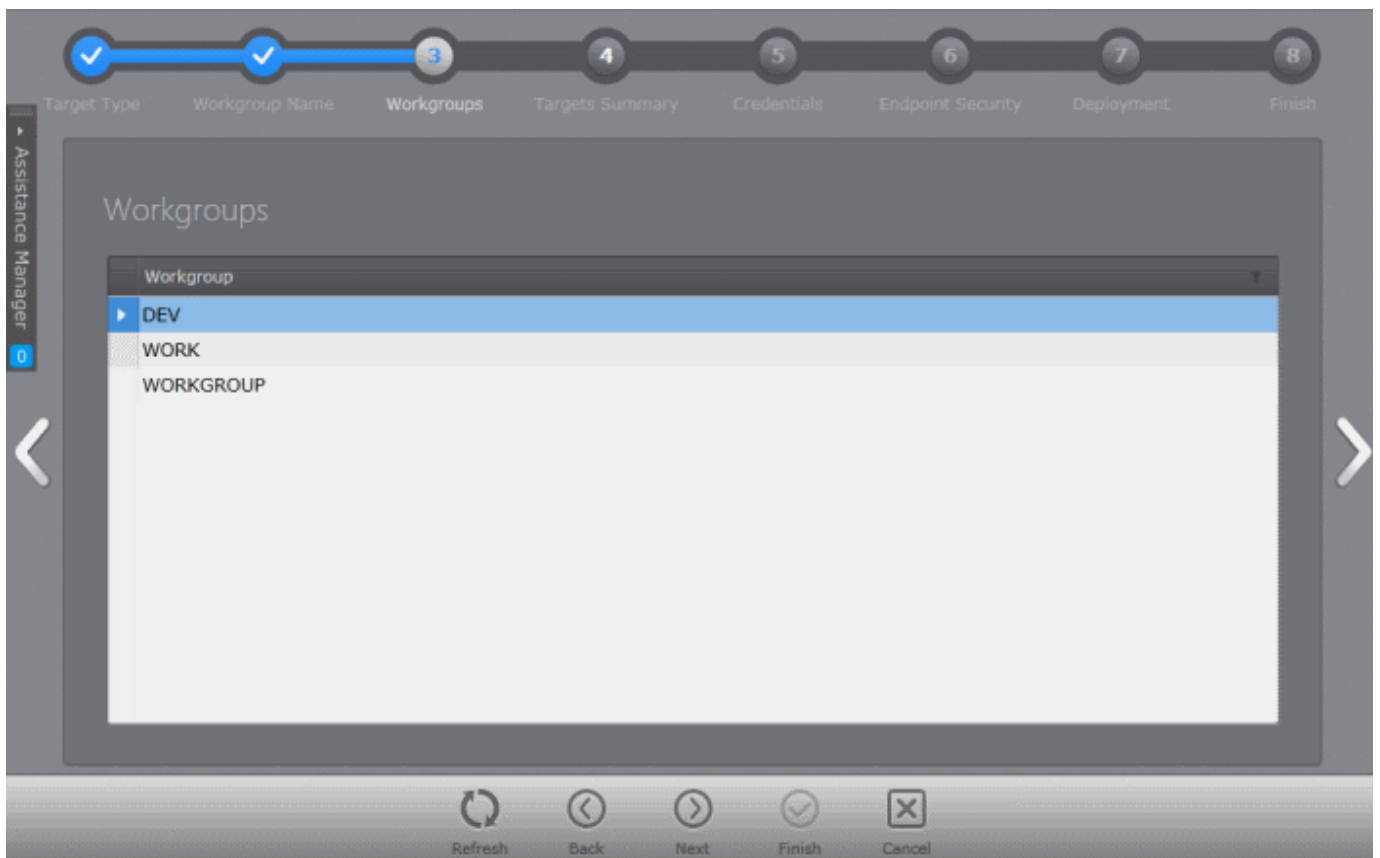- Choose 'Workgroup' and move to the next step by clicking the right arrow.

Step 2 - Workgroup Name

The next step is to select the Workgroup(s) from which the endpoints are to be imported.
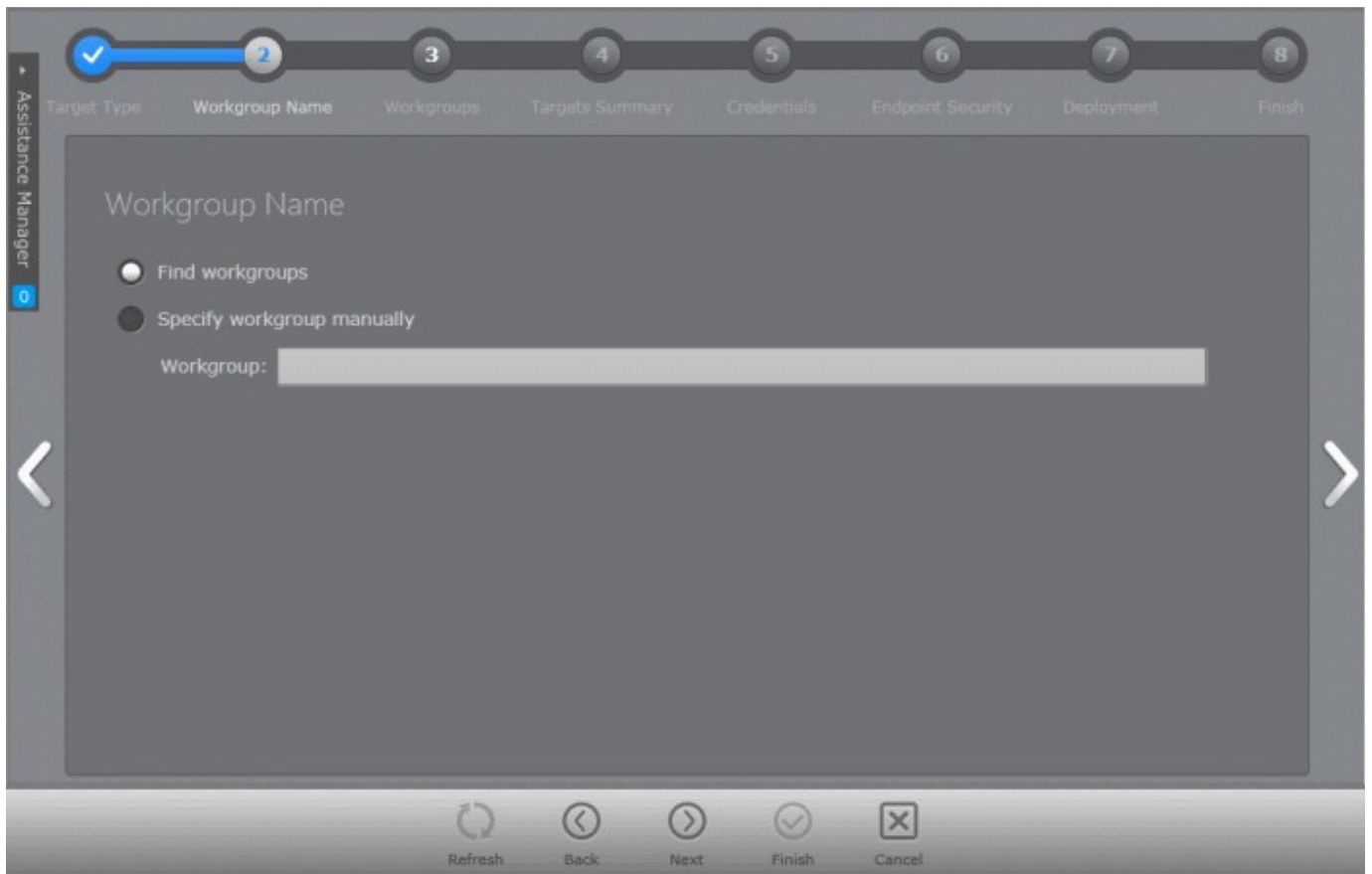

CESM enables the administrator to specify the workgroup name in two ways:

- **Find Workgroups** - Makes CESM to search for the workgroups associated with the network and enables. administrator to select the workgroup(s) from which the endpoints are to be imported in the next step.

- Select the workgroup(s) and click the right arrow to move to **step 3** to select the endpoints.
- **Specify Workgroup manually** - allows the administrator to enter the name of the Workgroup from which the endpoints are to be imported in the 'Workgroup:' text box.

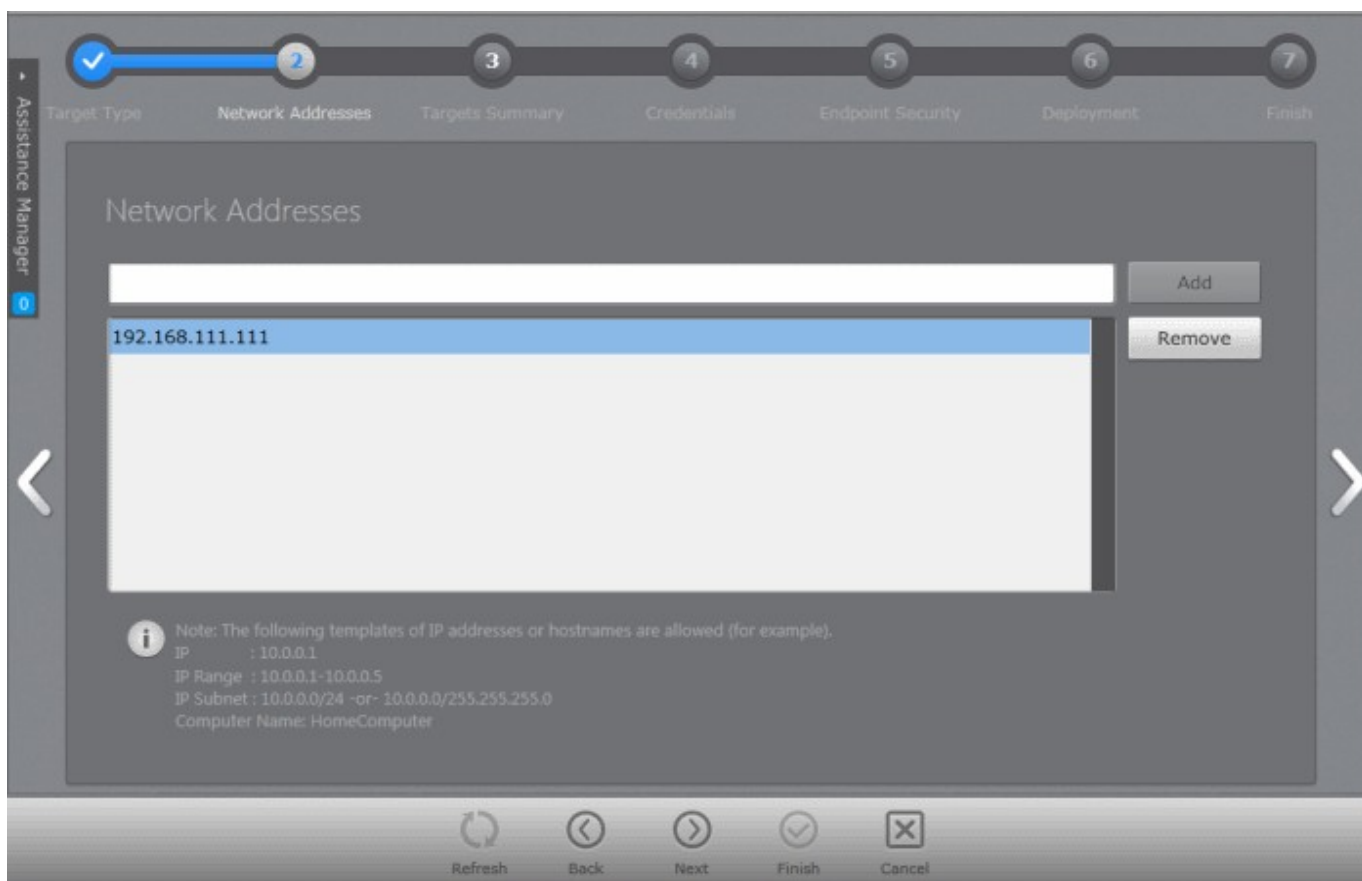**Note**: The Workgroup is discovered from the local area network attached to the CESM service computer.
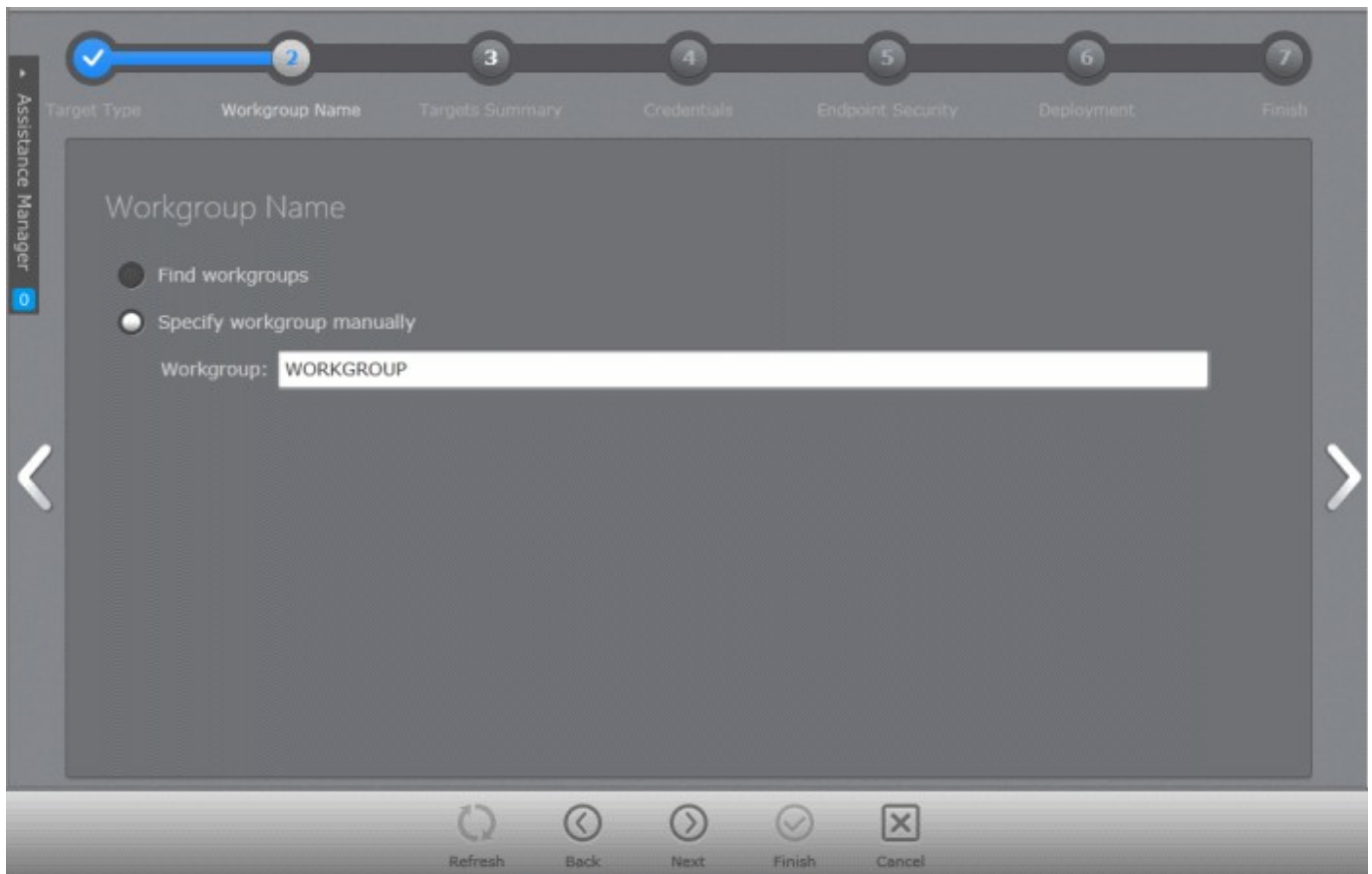
- Enter the name of a network Workgroup and click the right arrow to move to **step 3** to select the endpoints.

Importing Computers by Network or IP Addresses

- Choose 'Network Addresses' and move to the next step by clicking the right arrow.

Step 2 - Adding Network Addresses

The next step is to add the target computers by specifying their IP address(es).

Computers can be added in four ways:

- **Import individual computers by specifying their IP addresses one-by-one** - Enter the IP address of the computer and click the 'Add' button. The IP address will be added and displayed below the text box. To add more computers, repeat the process.

- **Import individual computers by specifying their names one-by-one** - Enter the name of the target computer as identified in the network and click the 'Add' button. The computer name will be added and displayed below the text box. To add more computers, repeat the process.

- **Import a group of computers by specifying their IP Address range** - Enter the IP Address range of the target computers with the Start address and End address separated by a hyphen (e.g. 192.168.111.111-192.168.111.150) and click the 'Add' button. The entered IP address range will be added and displayed below the text box. To add more IP address ranges, repeat the process.

- **Import a group of computers by specifying IP Addresses and Subnet mask** - Enter the IP Address and Subnet mask (e.g. 192.168.111.111/24 or 192.168.111.111/255.255.255.0) in the text field and click the 'Add' button. The entered IP address/subnet mask will be added and displayed below the text box. To add more IP address/subnet mask, repeat the process.

    - To remove a computer/computer group added by mistake, select the item and click the 'Remove' button.
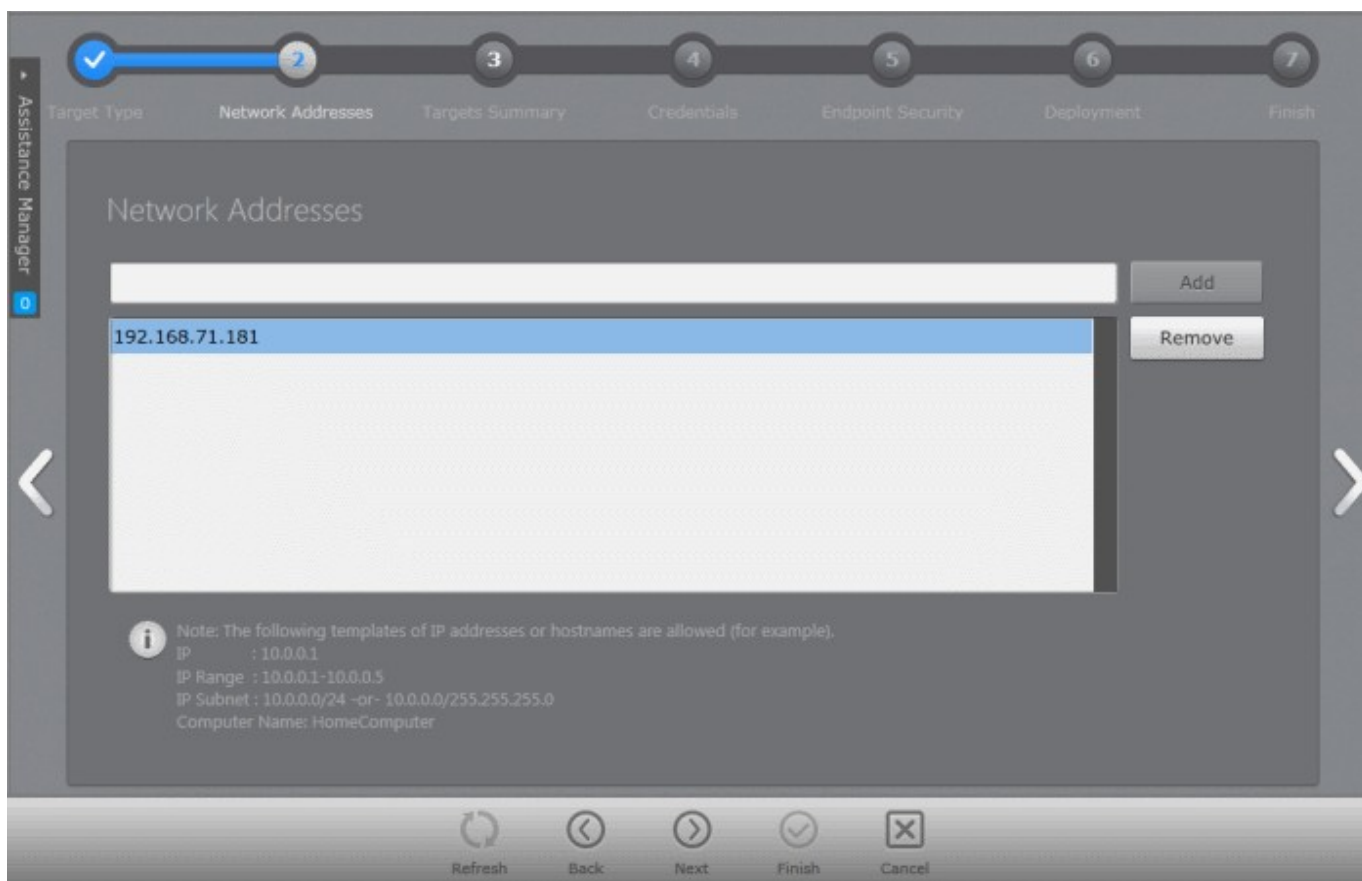   - Click the right arrow to move to the next step.

Note: IP addresses are specified relative to the CESM service computer.

Importing Linux and Mac OS based Computers

- Choose 'Deploy to Linux/Mac OS X endpoint(s)', specify the Secure Shell (SSH) port number (default = 22) of the computers for CESM to connect to them and move to the next step by clicking the right arrow.

Step 2 - Adding Network Addresses

The next step is to add the target computers by specifying their IP address(es).

Computers can be added in four ways:

- **Import individual computers by specifying their IP addresses one-by-one** - Enter the IP address of the computer and click the 'Add' button. The IP address will be added and displayed below the text box. To add more computers, repeat the process.

- **Import individual computers by specifying their names one-by-one** - Enter the name of the target computer as identified in the network and click the 'Add' button. The computer name will be added and displayed below the text box. To add more computers, repeat the process.

- **Import a group of computers by specifying their IP Address range** - Enter the IP Address range of the target computers with the Start address and End address separated by a hyphen (e.g. 192.168.111.111-192.168.111.150) and click the 'Add' button. The entered IP address range will be added and displayed below the text box. To add more IP address ranges, repeat the process.

- **Import a group of computers by specifying IP Addresses and Subnet mask** - Enter the IP Address and Subnet mask (e.g. 192.168.111.111/24 or 192.168.111.111/255.255.255.0) in the text field and click the 'Add' button. The entered IP address/subnet mask will be added and displayed below the text box. To add more IP address/subnet mask, repeat the process.

  - To remove a computer/computer group added by mistake, select the item and click the 'Remove' button.
  - Click the right arrow to move to the next step.

Note: IP addresses are specified relative to the CESM service computer.
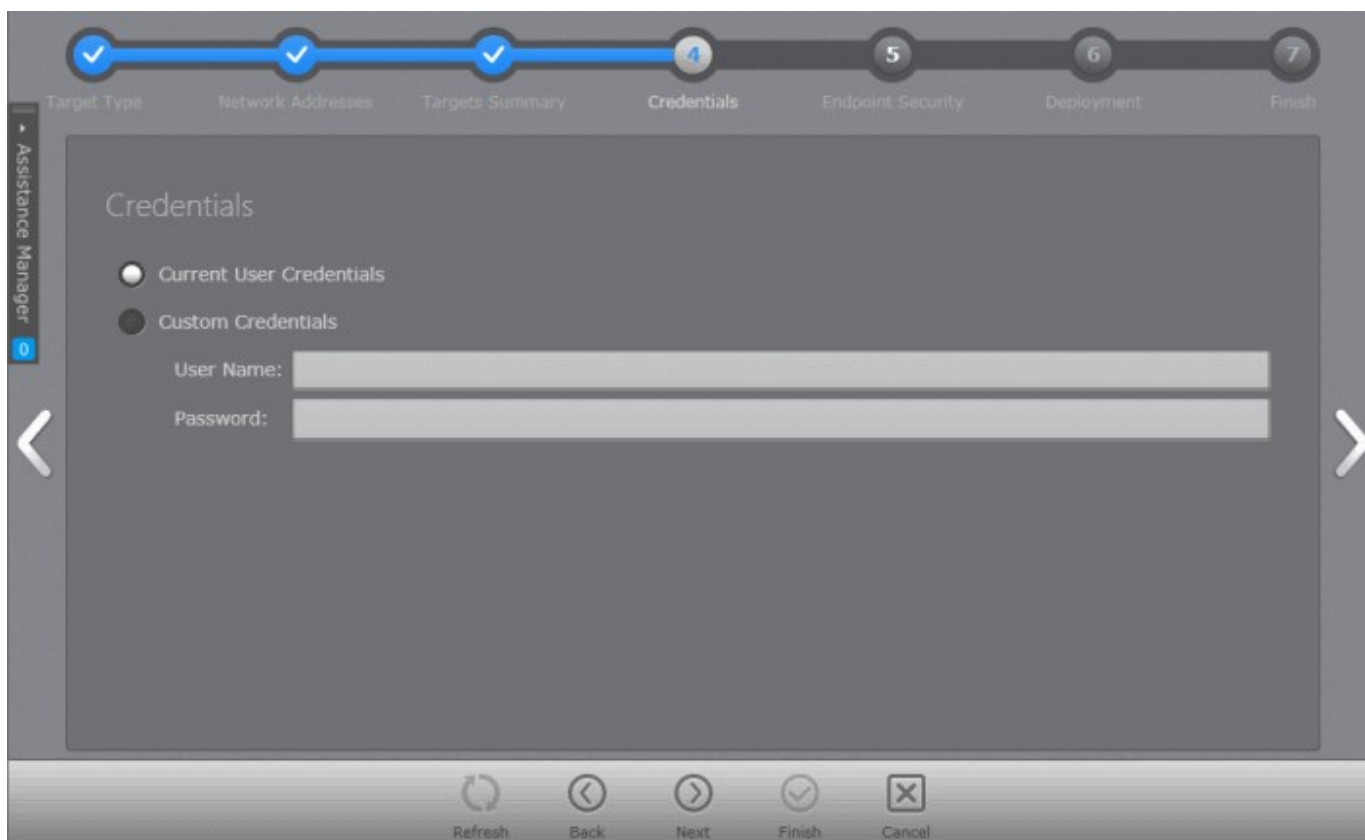
Step 3 - Targets Summary

In this step, all the endpoints included in the previous Step 2 will be displayed.
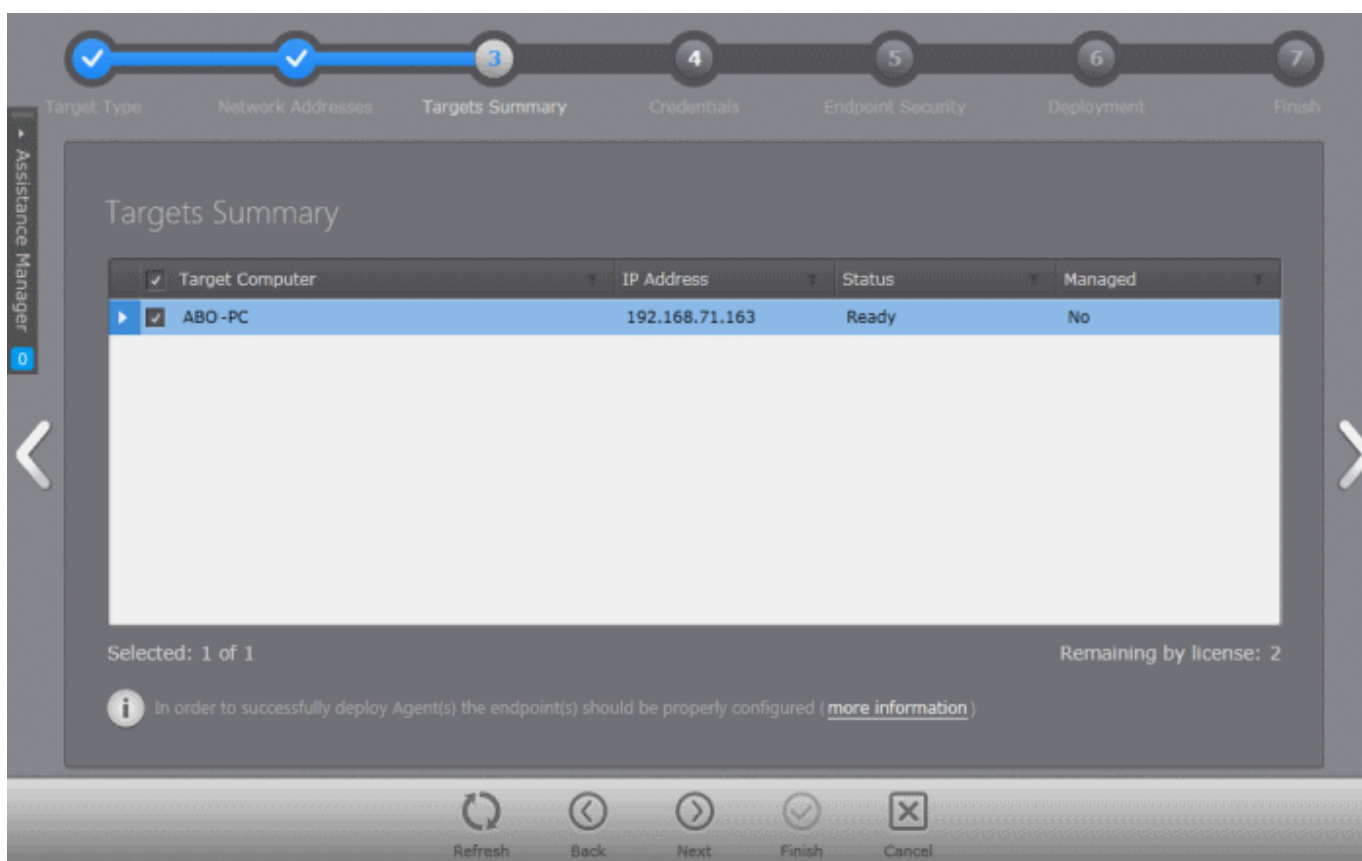
- Select the endpoint(s) that you want to deploy the agent and CES to. You can use the filter option to select the endpoints from the list displayed.

  - Click the filter icon ▼ in the 'Target Computer' column header to search for a particular endpoint and click 'Apply'.
  - Click the filter icon in the 'IP' column header to search for endpoints with particular IP(s) and click 'Apply'.
  - Click the filter icon in the 'Status' column header to search for endpoints that are 'Ready' or 'Unavailable' and click 'Apply'.
  - Click the filter icon in the 'Managed' column header to search for endpoints that are 'Managed' or 'No' and click 'Apply'.
  - Click the right arrow or swipe left to move to the next step.

Step 4 - Credentials

The next step is to select the administrative account (login) credentials that will be used to remotely upload the installation package using the administrative share on all target computer(s).

| Credentials - Table of Parameters	
Current User Credentials (Selected by default)	Selecting this option will install the agent using the credentials of the currently logged -in CESM administrator account in each endpoint.
Custom Credentials	Selecting this option allows the administrator to specify an administrative account for installation of the agent.
User Name:	Enter the user-name of the dedicated network administrator.
Password:	Enter the password of the dedicated network administrator.

• Click the right arrow after entering the credentials to move to the next step.

Step 5 - Endpoint Security

The next step is to choose installation options for Comodo Endpoint Security (CES). The following sections contain guidance on the choosing the installation options for:

• **Windows based endpoints**
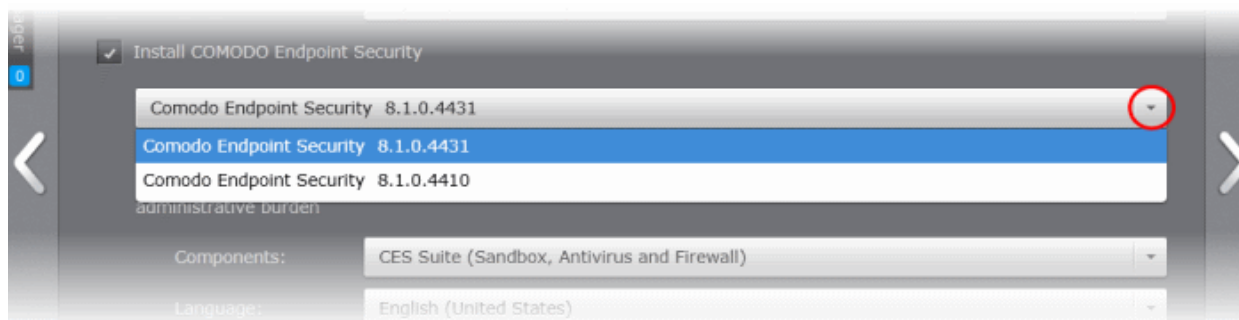• **Mac OS based endpoints**

For Windows based Endpoints
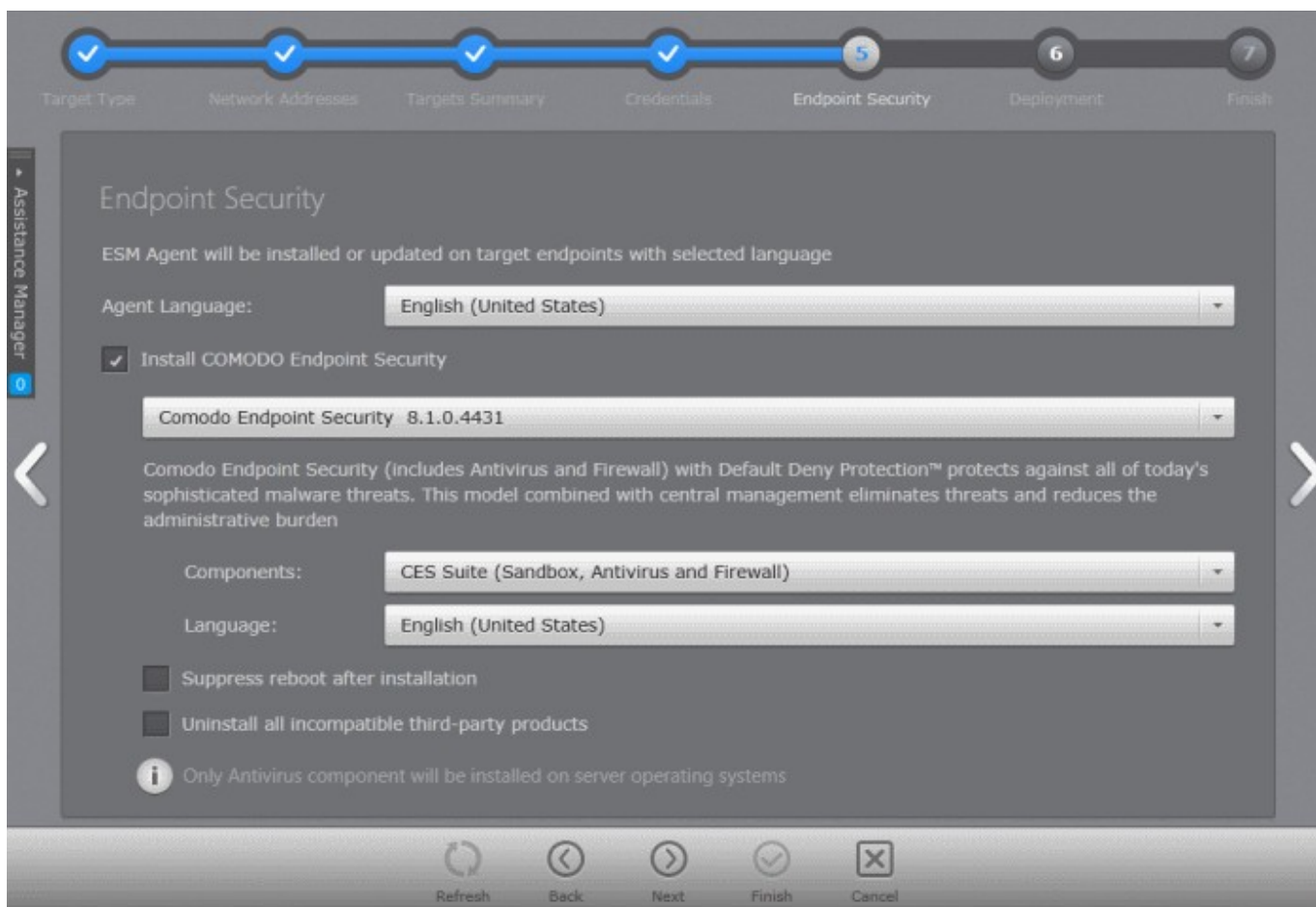
- Select the language in which the agent is to be installed from the 'Agent Language' drop-down.
- Select 'Install Comodo Endpoint Security' check box if you wish CES/CAS to be installed along with the agent.

Note: If the option to install CES is not selectable:

- Your license for Comodo Endpoint Security Manager did not include CES/CAS software. Refer to the section **Upgrading your License** for more information.

- If the CES/CAS installation packages are not downloaded to CESM console. Refer to the section **Preferences** > **Downloading ESM Packages** for more details on downloading the installation packages.

- Select the version of CES you wish to install on the selected endpoints from the drop-down. The base package is same for both CES and CAS. CESM will automatically install CES or CAS depending on whether the endpoint is a Windows Client computer or a Windows Server. **Note** - the drop-down will be empty the first time CESM is run. You must first click 'Check For Updates' then 'Update' to populate the drop-down as explained in the previous Step 5 - Checking for Updated Software.

- Select the components that you want to include from the Components drop-down:

    - CES Suite, which contains all the components (Sandbox, Antivirus and Firewall)

- CES Sandbox and Antivirus
- CES Sandbox and Firewall
- CES Sandbox only

- Select the language in which the CES is to be installed from the Language drop-down.
- **Suppress reboot after installation** - CES installation will restart of the endpoints for the installation to take effect. If you do not want the endpoints to be restarted on completion of installation, select this check box. CES installation will complete but will take effect only on the next restart of the endpoint.
- **Uninstall all incompatible third-party products** - Selecting this option uninstalls select third party antivirus, firewall and other desktop security software from the endpoints, prior to the installation of CES. Performing this step will remove potentially incompatible products and thus enable CES to operate correctly. Some incompatible products can be detected, but not automatically uninstalled and must be removed manually. If your product is detected but not uninstalled, please consult your vendor's documentation for precise uninstallation guidelines.

However the following steps will help most Windows users:

- Click the Start button to open the Windows Start menu.
- Select Control Panel > Programs and Features (Win 7, Vista); Control Panel > Add or Remove Programs. (XP).
- Select your current antivirus or firewall program(s) from the list.
- Click Remove/Uninstall button.
- Repeat process until all required programs have been removed.

Click Here to see the full list of incompatible products.

- Click the right arrow to move to the next step.

Tip: You can also install CES manually onto endpoint computers. The CES/CAS installation package can be downloaded as an executable file from **Preferences** > **Packages** interface, by clicking 'Download offline package' beside the required package. The package contains both the agent and the CES/CAS software and can be transferred onto media such as DVD, CD, USB memory for manual deployment onto target machines.

For Mac OS based Endpoints
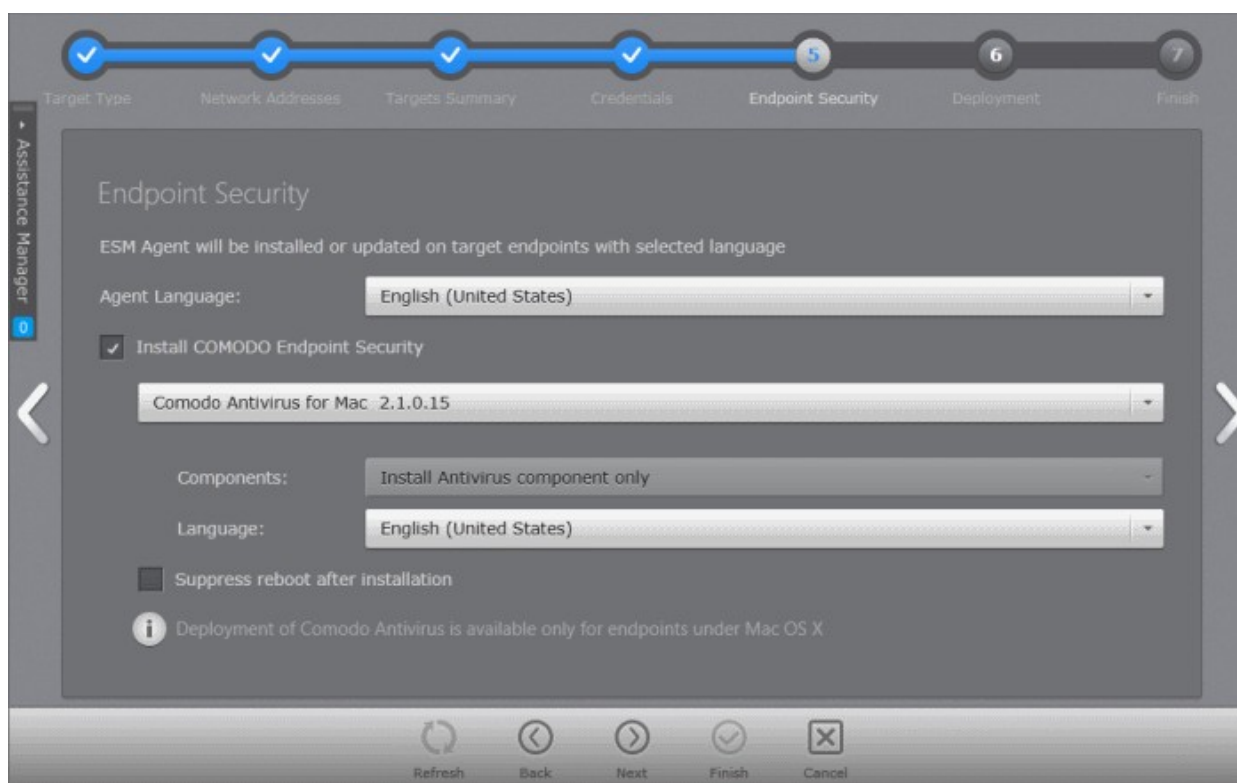
- Select the language in which the agent is to be installed from the 'Agent Language' drop-down.
- Select 'Install Comodo Endpoint Security' check box if you wish Comodo Antivirus for Mac to be installed along with the agent.

> **Note:** If the option to install CES is not selectable:
>
> - Your license for Comodo Endpoint Security Manager did not include CES/CAS/CAV for Mac software. Refer to the section **Upgrading your License** for more information.
>
> - If the CES/CAS/CAV for Mac installation packages are not downloaded to CESM console. Refer to the section **Preferences** > **Downloading ESM Packages** for more details on downloading the installation packages.

- Select the version of CAV for Mac you wish to install on the selected endpoints from the drop-down. **Note** - the drop-down will be empty the first time CESM is run. You must first click 'Check For Updates' then 'Update' to populate the drop-down as explained in the previous Step 5 - Checking for Updated Software.
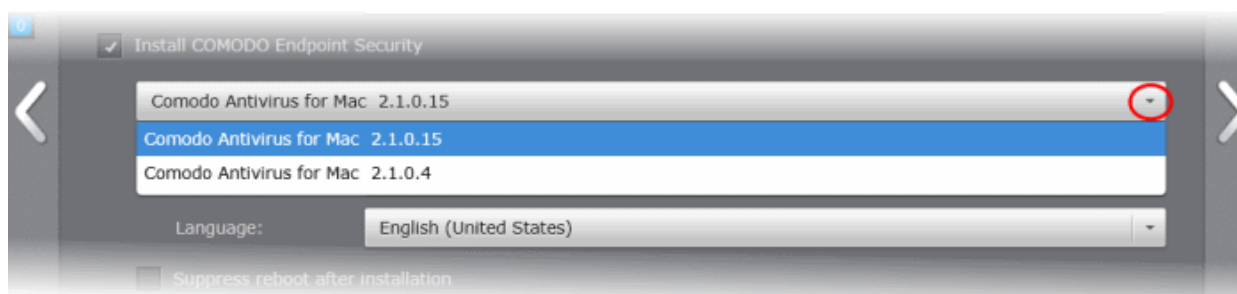

- **Suppress reboot after installation** - CAV for Mac installation will reboot of the endpoints for the installation to take effect. If you do not want the endpoints to be rebooted on completion of installation, select this check box. CAV installation will complete but will take effect only on the next restart of the endpoint.

- Click the right arrow to move to the next step.

Step 6 - Deployment Progress

- Click 'Start Deployment'.
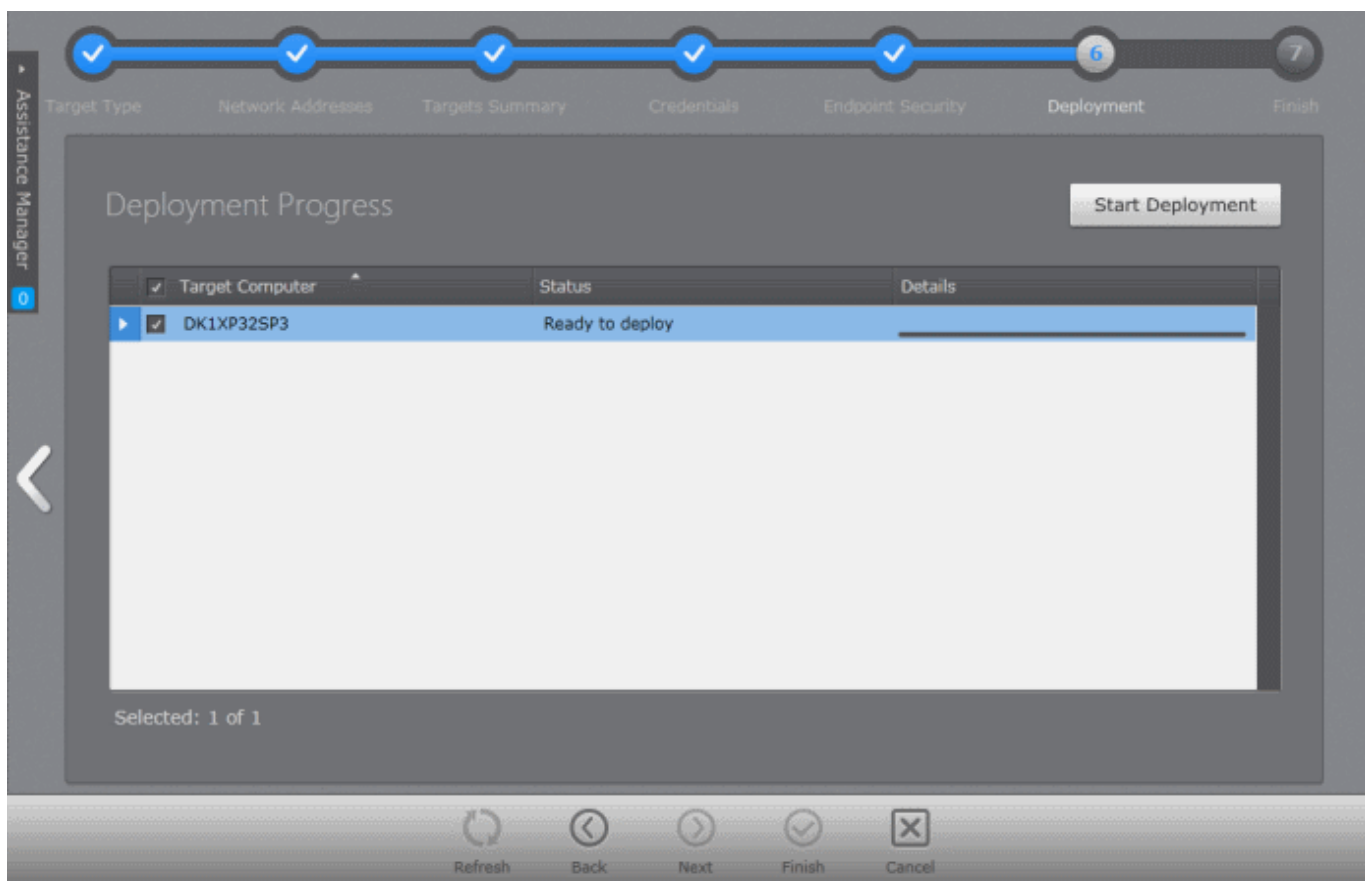
CESM will start installing the agent/CES/CAS/CAV for Mac on to the selected endpoints and the progress per endpoint will be displayed.
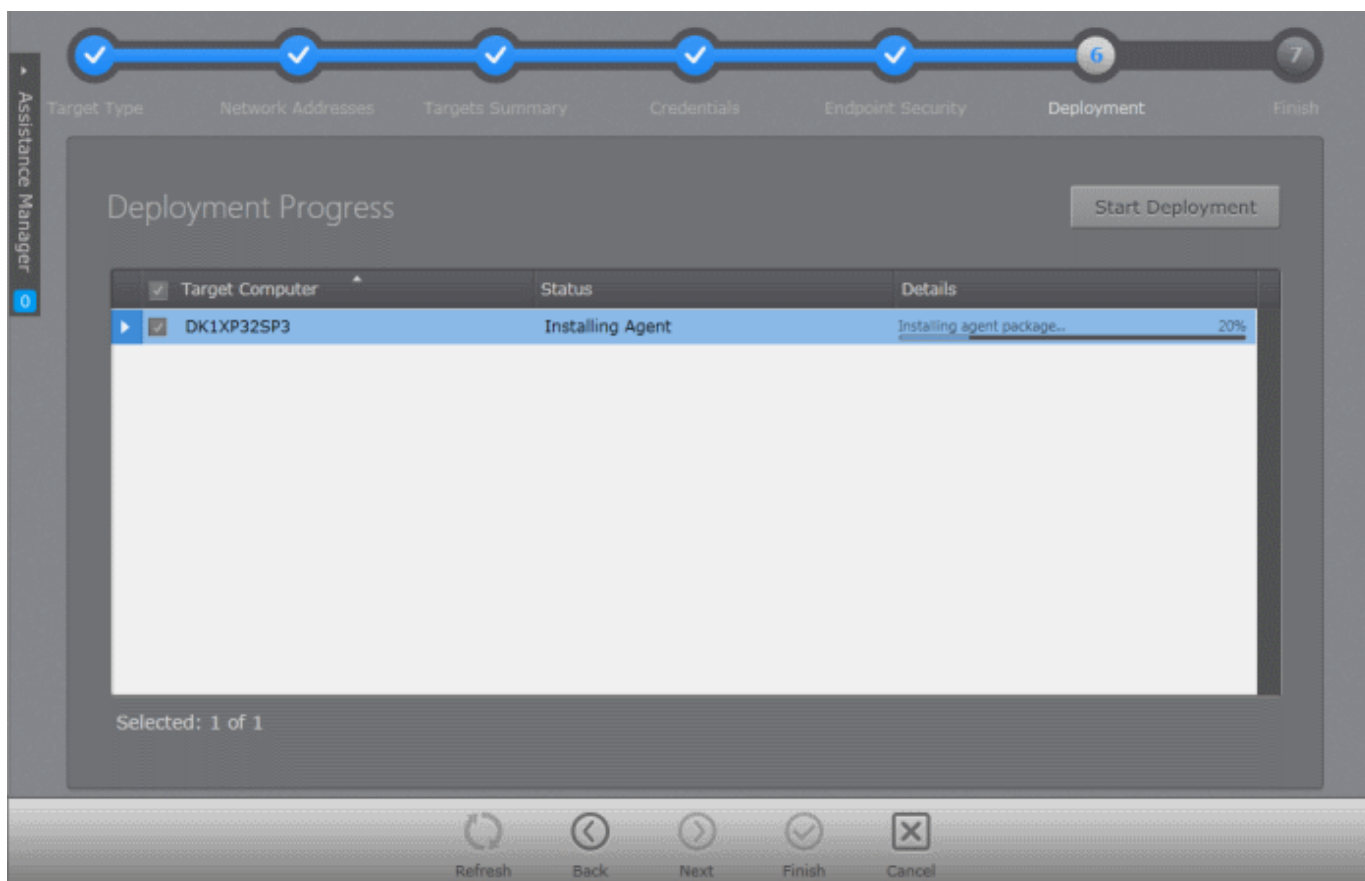
If any of the selected endpoints have older versions of CES than the one selected in the previous Step 6, they will be automatically uninstalled and the selected version will be installed.

Step 7 - Deployment Complete
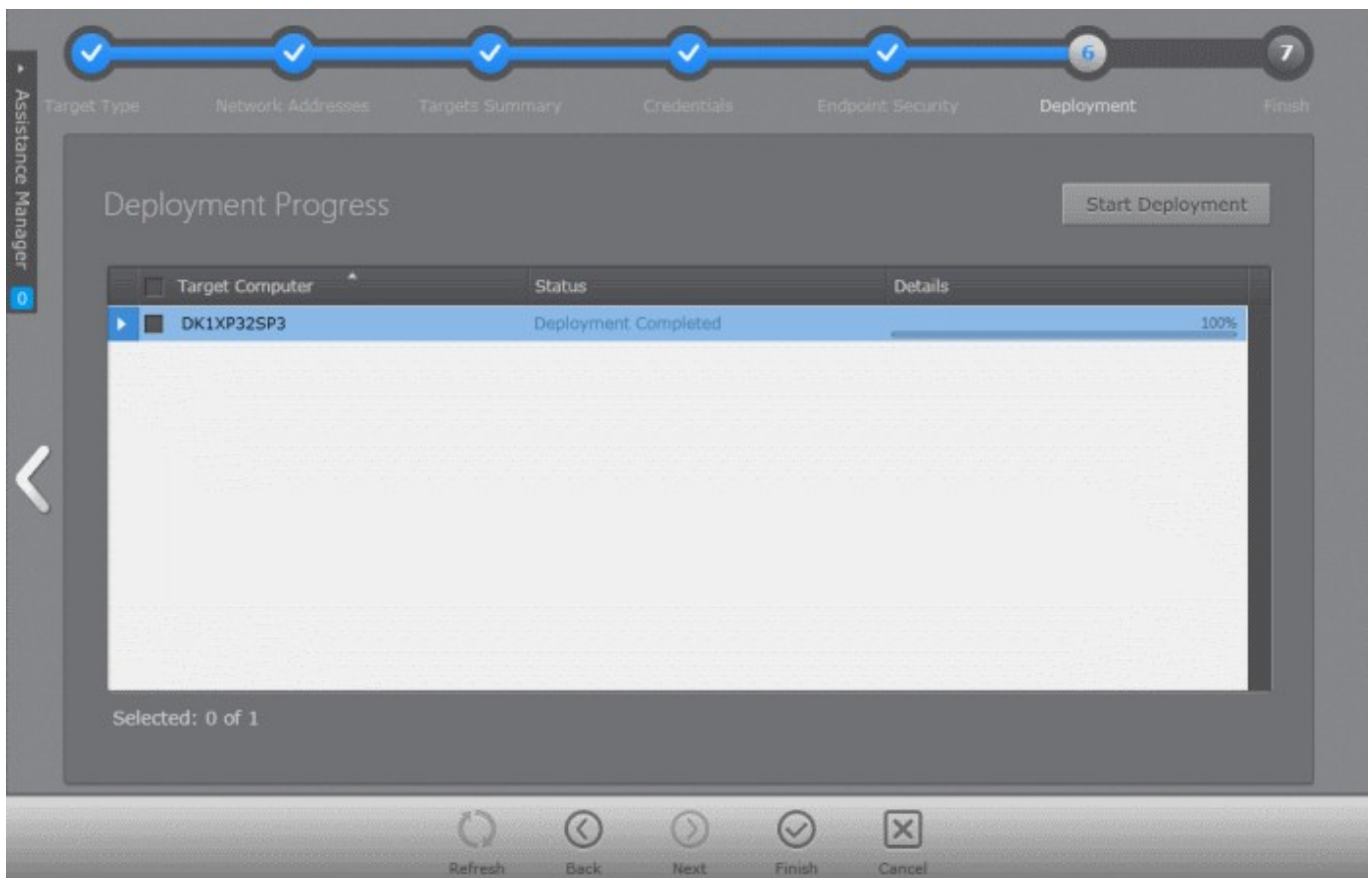
On completion of installation, the results screen will appear.

- If deployment fails, click on the words 'Deployment Failed' to discover the reason. The info box also contains advice that may remediate the issue.
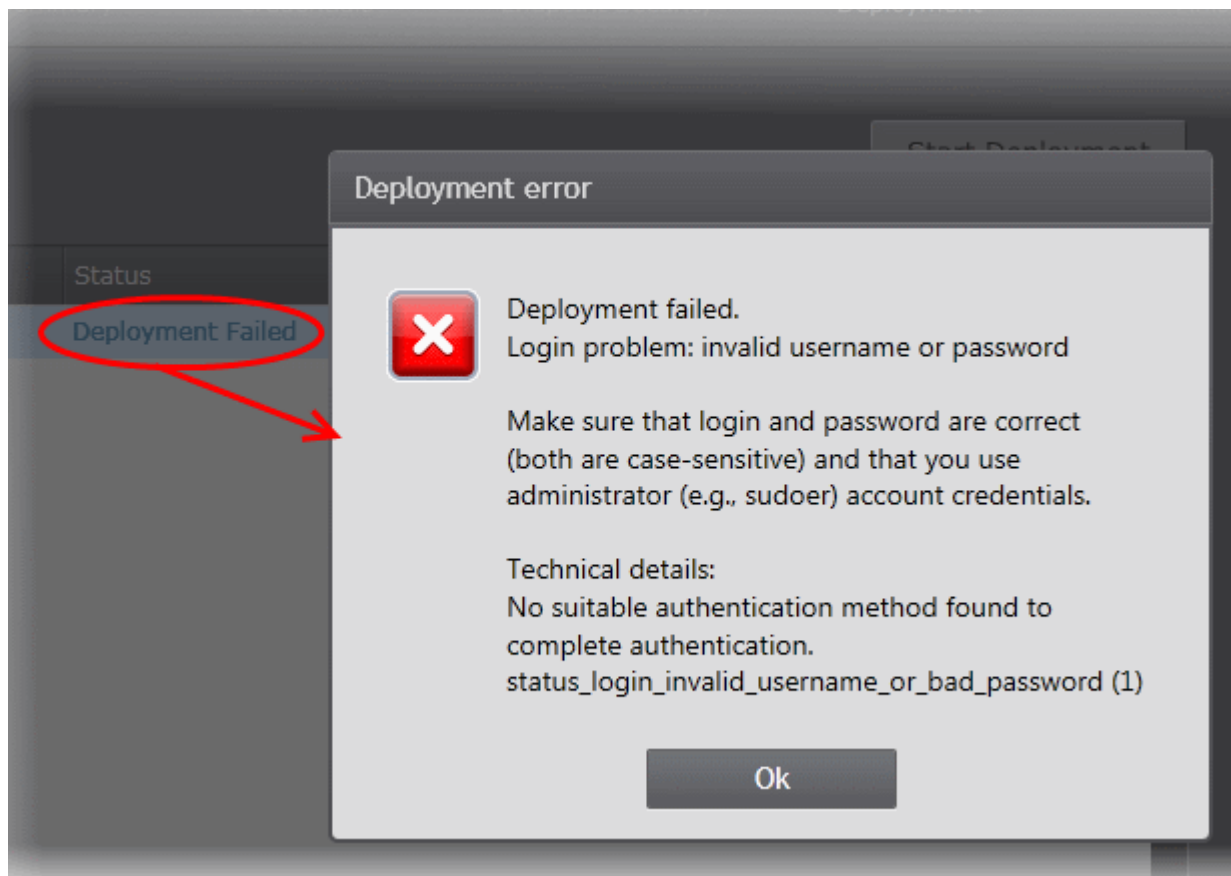
- Click the 'Finish' or swipe the screen to the left to exit the wizard.

The endpoints selected in **Step 3** are now added to CESM and are ready for management through CESM. Refer to the section '**The Computers Area**' for more details on how to view the list of imported endpoints.

The newly added computers will be added to the default group 'Unassigned'. If this group has been changed to use a specific policy, that policy will be applied after the agent installation is completed. The administrator can create and name new groups according to the structure of the organization and move the added computers into them from 'Unassigned' group. Once created, admins can run tasks on entire groups of computers (such as applying security policy to CES, running AV scans, updating AV databases and more). Refer to '**The Groups Area**' for more details.

3.2.2. Adding Computers by Manual Installation of Agent

Installing the CESM agent locally is an alternative way of establishing connectivity between an endpoint and the CESM Central Service server. This is useful for scripting installation, or should the endpoint not be reachable from the CESM server's network.

The CESM Agent setup file can be downloaded as an executable from the admin console. The file can be transferred onto media such as DVD, CD, USB memory so that the agent can be installed manually onto target machines rather than via the CESM interface. A single copy of the installation files can be used to install the agent on any number of target machines.

Upon successful installation, the agent automatically establishes connection to the CESM Central Service Server and the endpoint can be controlled by the Administrator in the same way as it would if it were imported via the **Add Computers wizard**.

The endpoint security software, Comodo Endpoint Security (CES) can be remotely installed on the endpoint and managed by CESM once installation of the Agent is completed. If the Agent is installed first (with the endpoint having no CES), the **deployment wizard** can be used to install CES via the installed Agent.

The newly added computer will be included to the default group 'Unassigned'. The administrator can then import the computer into the required group or sub group to which the computer is allotted.

Downloading the Offline Agent Installer

Agent installation files for Windows, Linux and Mac OS are available from the administrative console of CESM. The administrator can choose to download agent installation file(s) according to the Operating System of the endpoints to be added to CESM.

To download the installer

- Open the 'Packages' screen by choosing 'Preferences' > 'Packages' from the drop-down at the top-left

You can download a package in two ways:

- Under the 'Checked In Packages' tab, click on the link in the package file column to directly download the package

- Right click on the link and choose 'Copy link address' to copy download URL to clipboard for downloading the package using a different browser or your favorite download manager

Important Note: Web browsers run on server OS may not allow downloading files through it by default, due to policy restrictions. For this reason, in order to download the agent setup file through the CESM admin console accessed through a web browser like Internet Explorer installed on a server, the local computer policy of the server has to be configured to disable the file download restrictions.

Installing the Agent onto the Endpoint

The agent setup file can be copied to the target endpoint computer from DVD, CD, USB memory or by any other means and saved in a desired location. The agent can also be deployed using a third-party software distribution package.

The installation process can be started in the following ways:

For Linux Computers

- First use the change mode command "chmod +x DebianAgentSetup.run" to make the downloaded agent setup file as an executable.
- Then use sudo command to execute the installer with administrative privileges "sudo ./debianagentsetup.run [IP] [port]".

For Mac OS Computers

- Drag and drop the MacAgentSetup.dmg file into your "Applications" directory.

For Windows Computers

- By double clicking the setup file to start the installation wizard.
- From the Windows CMD line. Command line options are as follows:

The command should be entered in the following format:

        `<file path in which agent setup file is stored>/ AgentSetup.exe /Options`

The options are explained in the following table. Some Options have multiple notations. These are separated by ' | ' in the following table.

Option	Description
/s | /server <Server Host>	Pointing the endpoint to the ESM server by specifying its host name or address.
/p | /port <port number>	To specify the port number of the ESM Server. Default port numbers are: • 57194 for connecting using HTTPS port. • 57193 for connecting using HTTP port.
/l | /log <logfile.log>	To specify the path and file name to store the log file.
/q | /quiet	To agent the agent in silent mode. The agent installation will not require any user interaction.
/help	Display the help information on installing the agent.

        Example: C:\Setup Files\AgentSetup.exe /server 10.0.0.1 /port 9901 /l c:\agentlog.log /q

Step 1 - Select the Language

Select the language that you want to use for the agent setup.
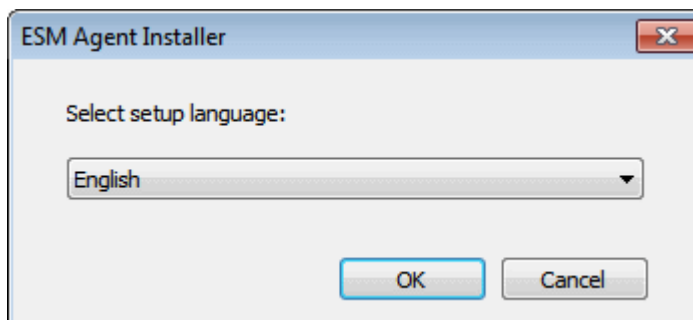
**Step 2 - Welcome Screen**

The welcome screen of the agent installation wizard will be displayed.

Click 'Next' to continue.

Step 3 - Specifying Server Address and Port

In the next step you must enter the host or IP address of the server in which CESM is installed and the port number the endpoint should be connected. By default, these fields will be populated with the details of the server from which the agent is downloaded.
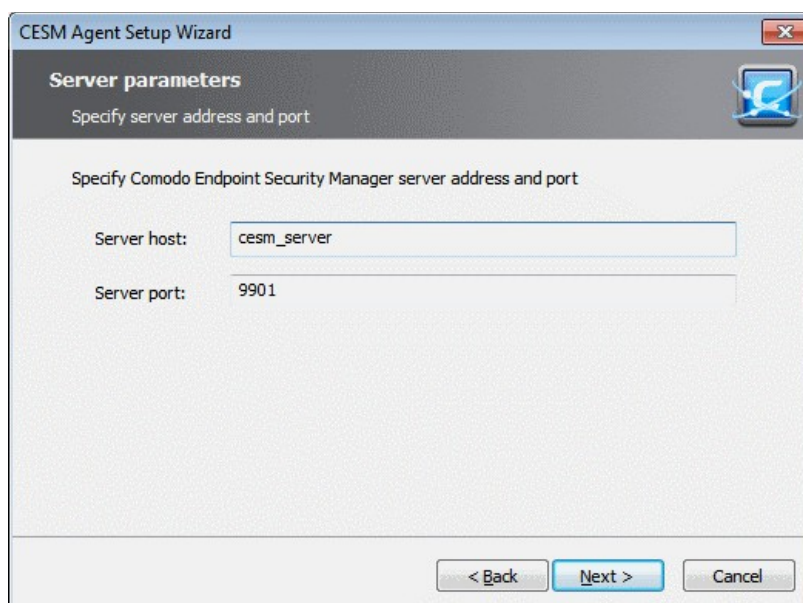
If you want to connect the endpoint to another CESM server, enter that server host or IP address and the port number and click 'Next'.

Step 4 - Selecting Products to be Installed

The next stage is to select the products to be installed. The installer will first check whether any of these items are already installed. You must first uninstall any older versions of CES or the Agent that are detected.
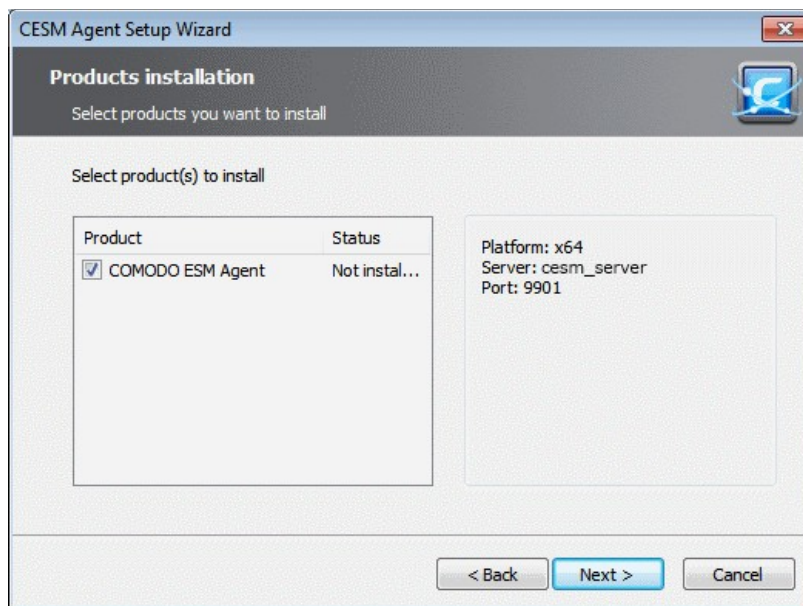
Ensure that the required products are selected in then click 'Next'.
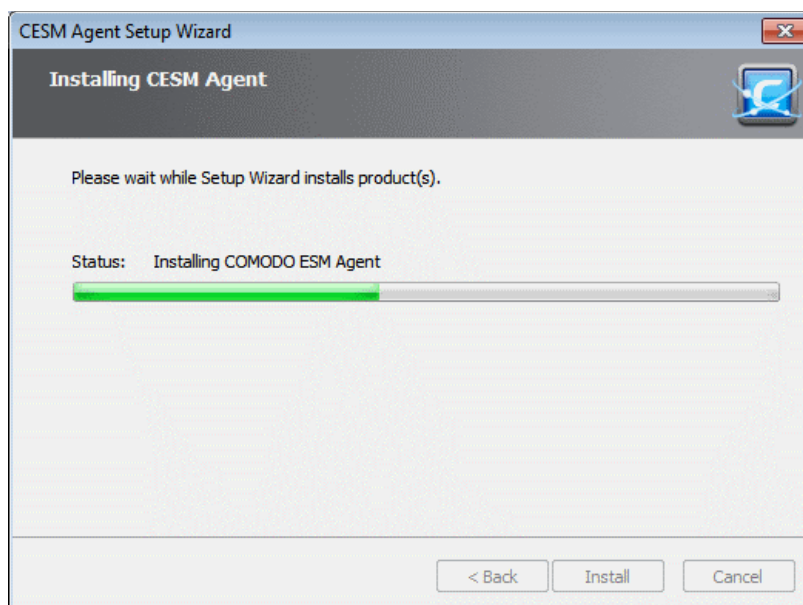
Step 5 - Ready to Install

The next step allows you to confirm the choices made in the previous step. Click 'Back' if you want to review and change the choices made.
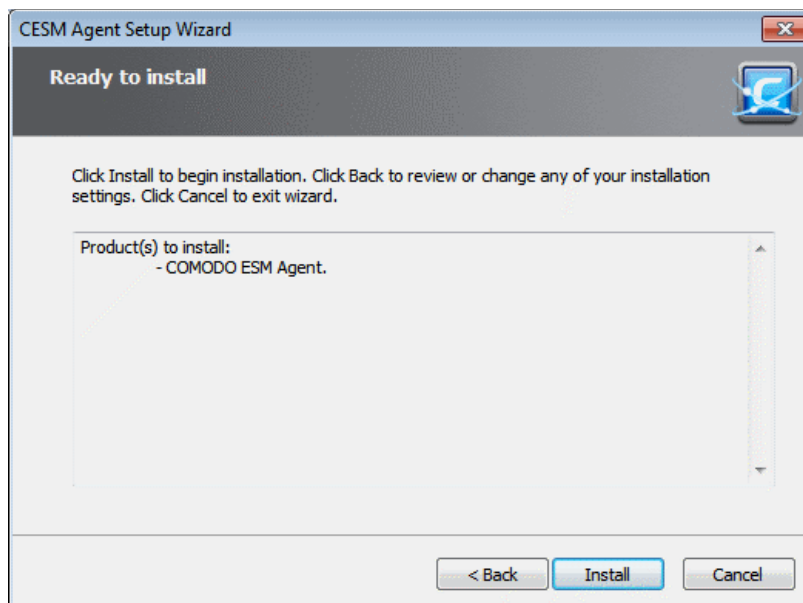
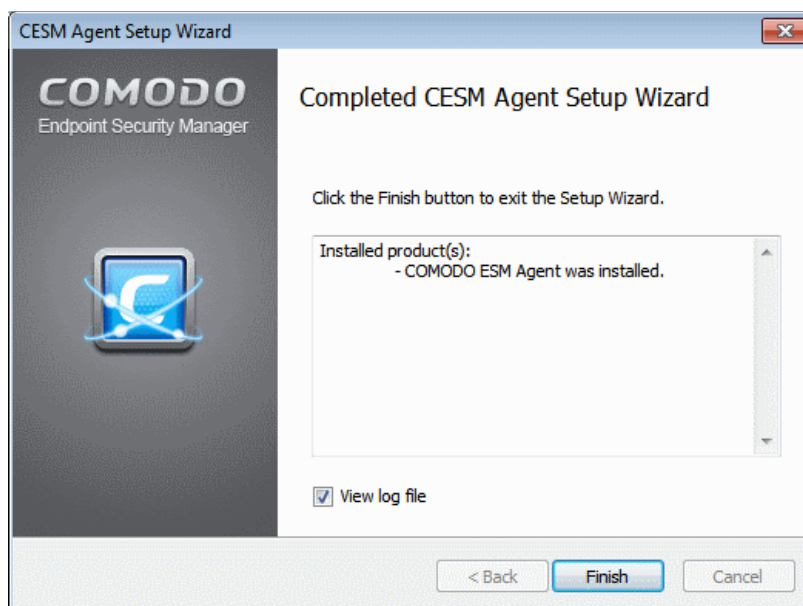To commence the installation, click 'Install'.

Step 6 - Installation Progress

The installation progress will be displayed.

Step 7 - Installation Complete

Upon setup completion, the 'Finish' dialog will be displayed.

- If you want to view the installation log file after completion of installation, leave View log file check box selected, else de-select it.

- Click 'Finish' to exit the wizard.

The agent will now automatically establish the connection to your CESM Service Server. Once the endpoint is connected, the administrator can start managing it and install CES on to it. Refer to **Updating Comodo Software on Managed Computers** for more details.

## 3.2.3. Updating Comodo Software on Managed Computers

Once an endpoint is managed, CESM allows the administrator to update the CESM agent as well as install/update CES/ CAS through the 'Add Computer' wizard.

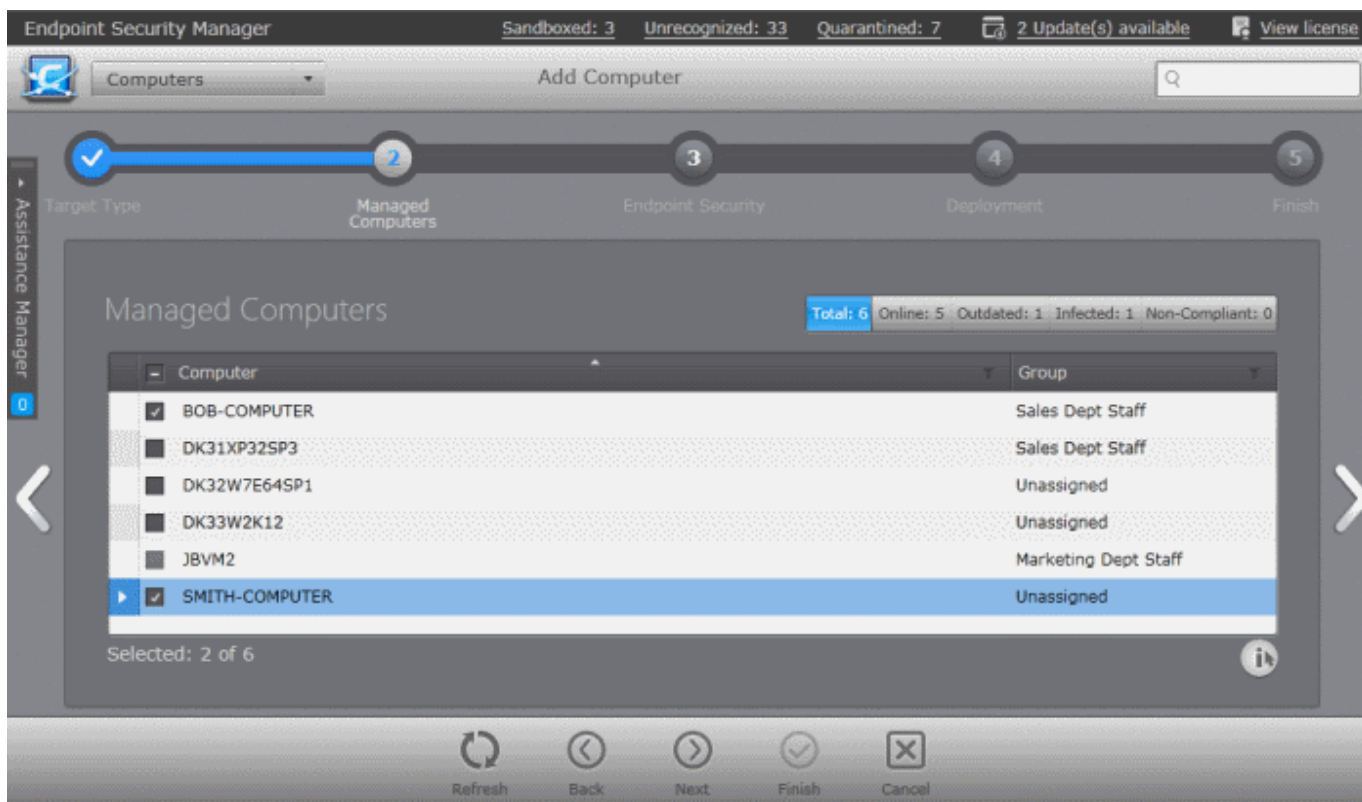**To update software on managed computers**

- Click 'Add' from the 'Computers' area to start the 'Add Computers' wizard.
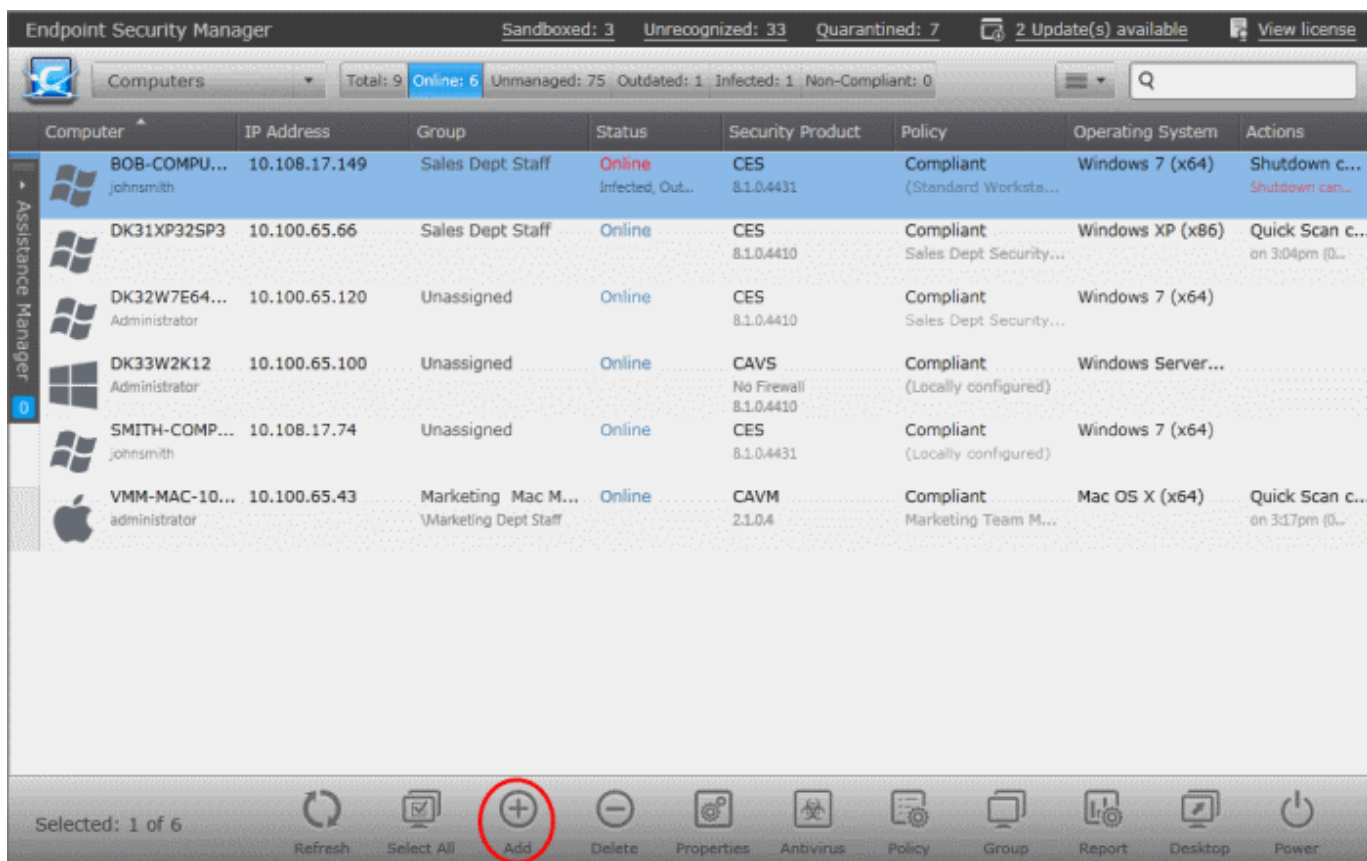
- Select 'Managed Computers' and click the right arrow or swipe left to proceed to the next step.
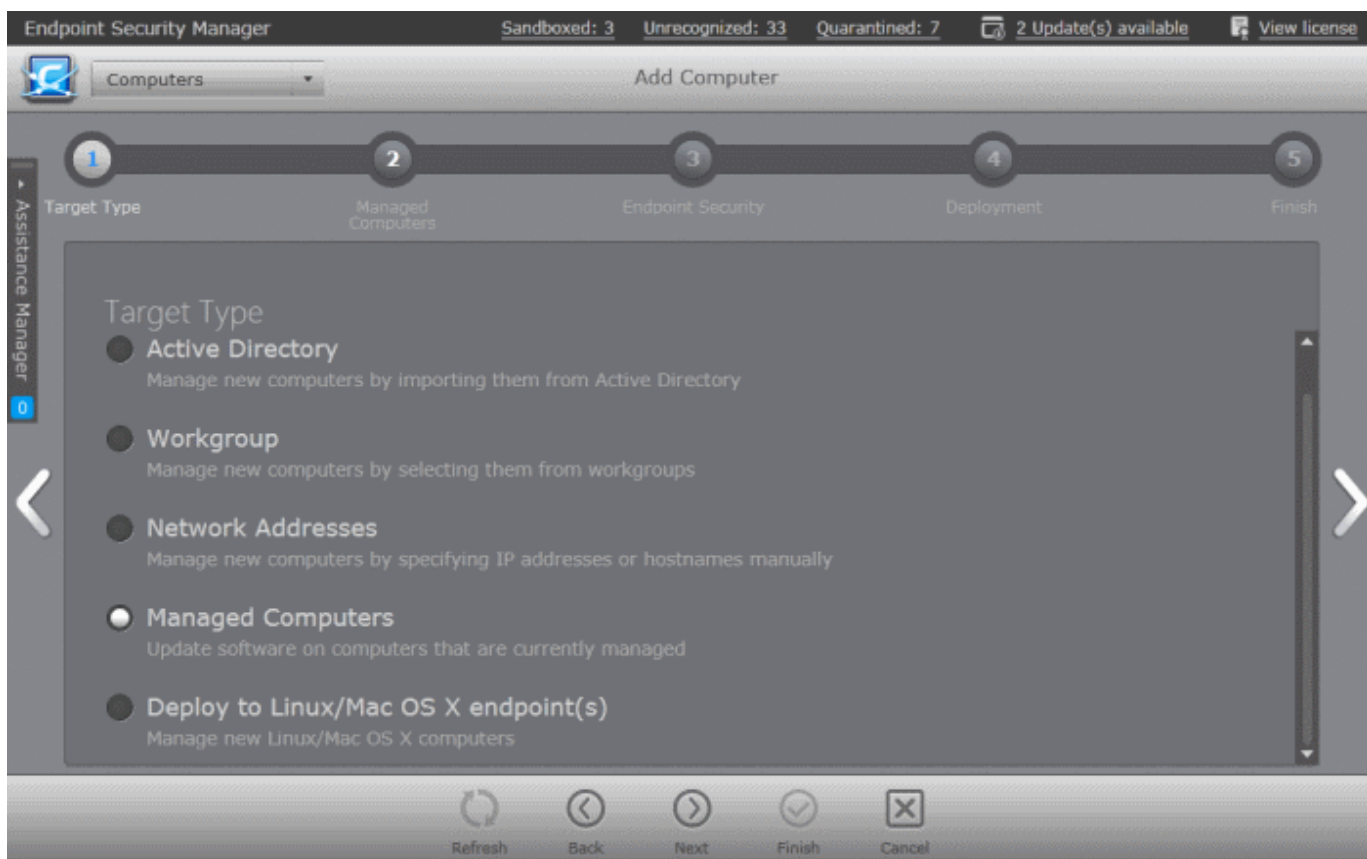
All the managed computers will be listed.

- Select the Windows based endpoints that you want to check and update CESM Agent and CES/CAS from the list.

- Click the funnel icon   in the 'Computer' column header to search for a particular endpoint, enter the endpoint name and click 'Apply'.

- After selecting the endpoints, click the right arrow or swipe left to proceed to the next step.

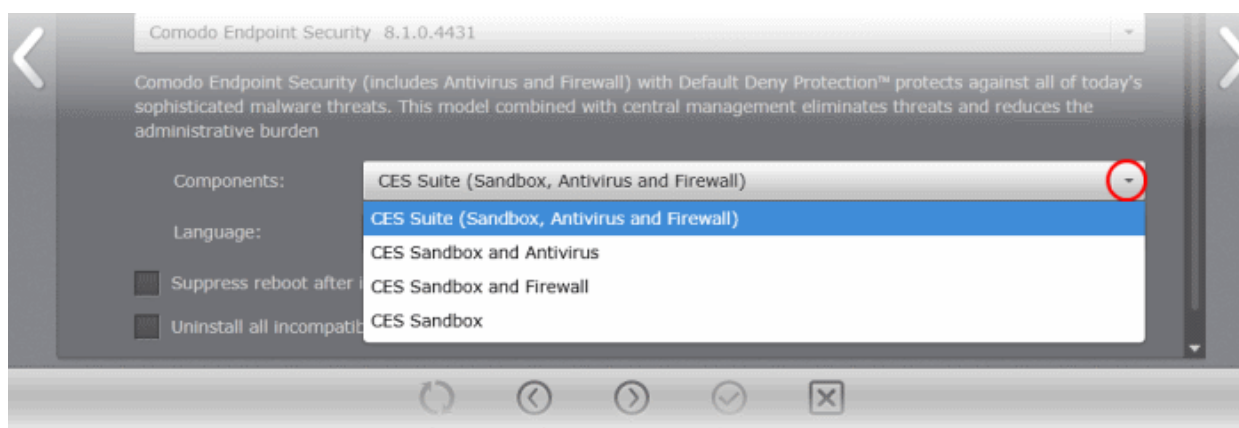- Click the right arrow or swipe left to move to the next step.
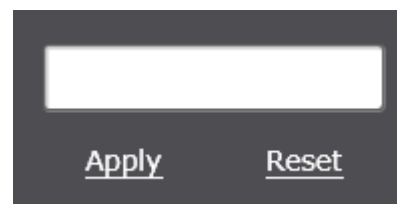
The next step is to choose installation options for Comodo Endpoint Security (CES).
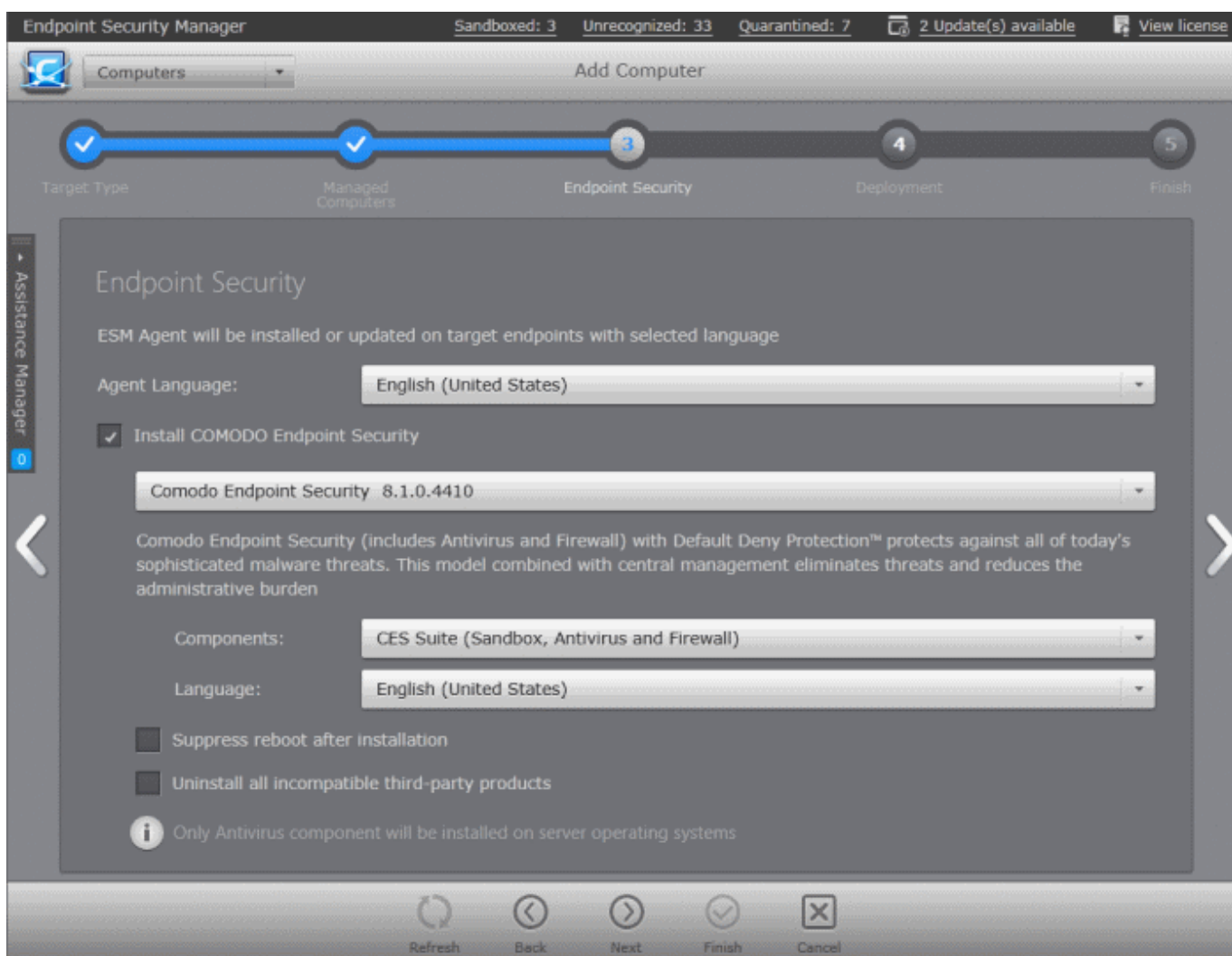
- Select 'Install Comodo Endpoint Security' check box if you wish CES/CAS to be installed along with the agent.

- Select the version of CES you wish to install on the selected endpoints from the drop-down. The base package is same for both CES and CAS. CESM will automatically install CES or CAS depending on whether the endpoint is a Windows Client computer or a Windows Server.
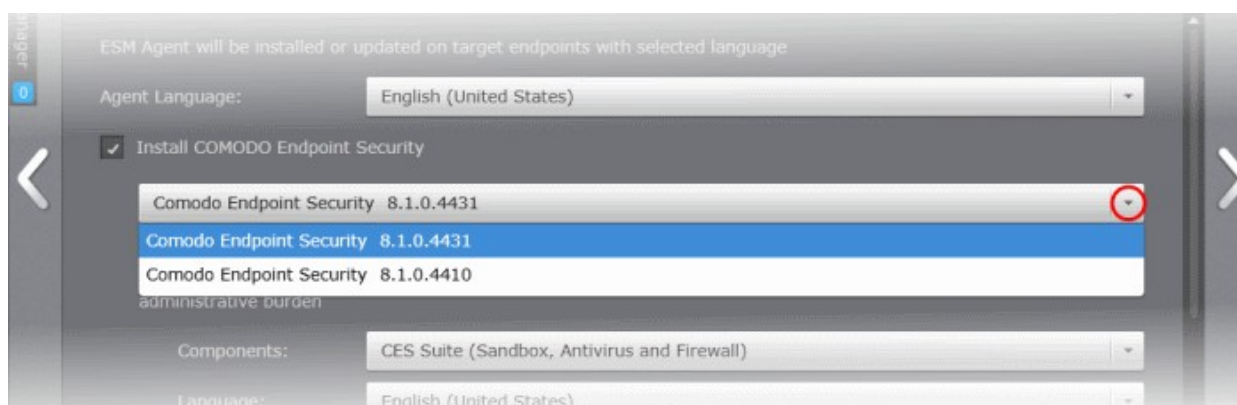
- Select the components that you want to include from the Components drop-down:

- CES Suite, which contains all the components (Sandbox, Antivirus and Firewall)
- CES Sandbox and Antivirus
- CES Sandbox and Firewall
- CES Sandbox only

- Select the language in which the CES is to be installed from the Language drop-down.
- **Suppress reboot after installation** - CES/CAS deployment requires a system restart in order for the managed security software to function properly. If you do not want the endpoints to be restarted on completion of installation, select this check box.
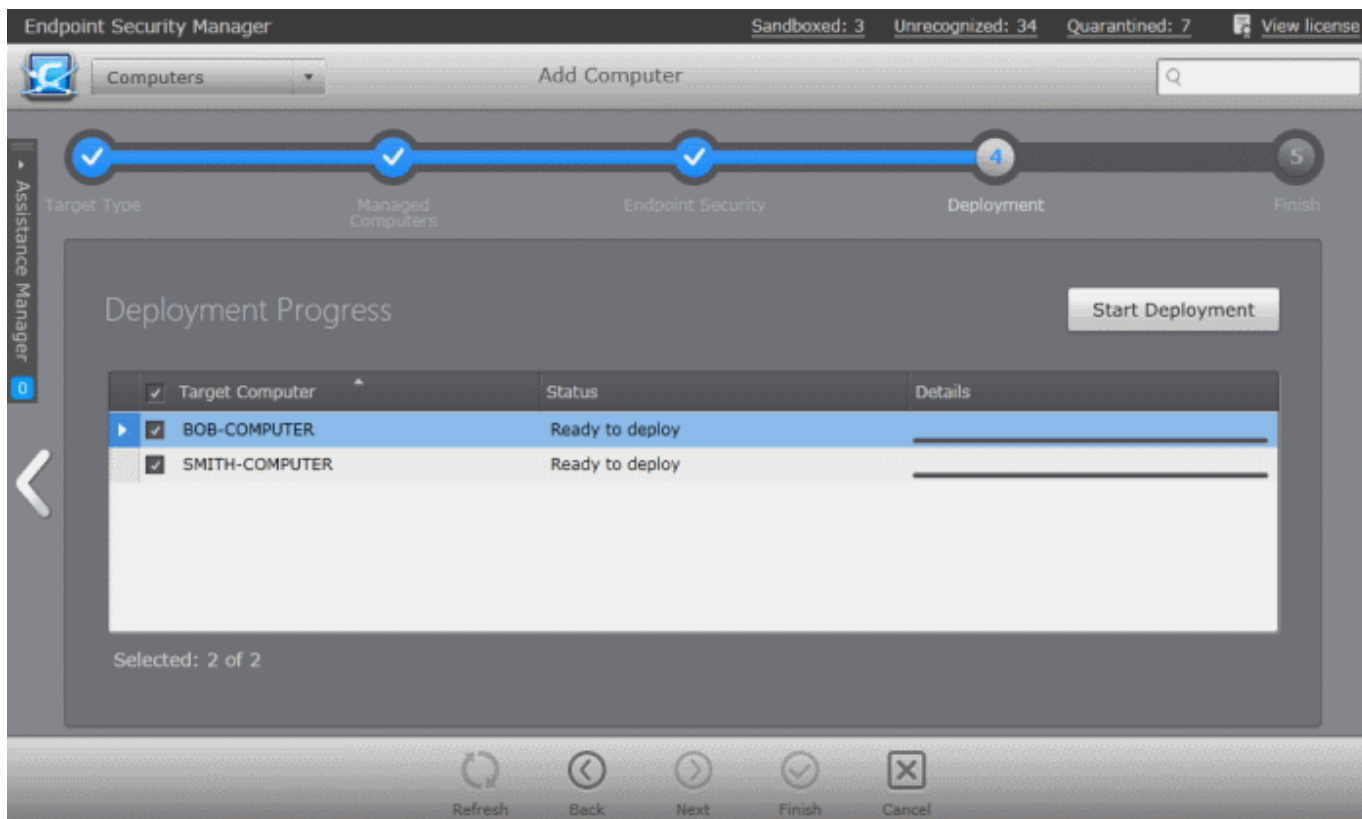
   CES/CAS installation will complete but will take effect only on the next restart of the endpoint. The endpoint(s) that are not restarted after CES/CAS installation will be indicated by 'Reboot pending' status. The administrator can restart the endpoints at a later time from the Computers area.

- **Uninstall all incompatible third-party products -** Selecting this option uninstalls select third party antivirus, firewall and other desktop security software from the endpoints, prior to the installation of CES. Performing this step will remove potentially incompatible products and thus enable CES to operate correctly. Some incompatible products can be detected, but not automatically uninstalled and must be removed manually. If your product is detected but not uninstalled, please consult your vendor's documentation for precise uninstallation guidelines.

   Click here to see the full list of incompatible products.
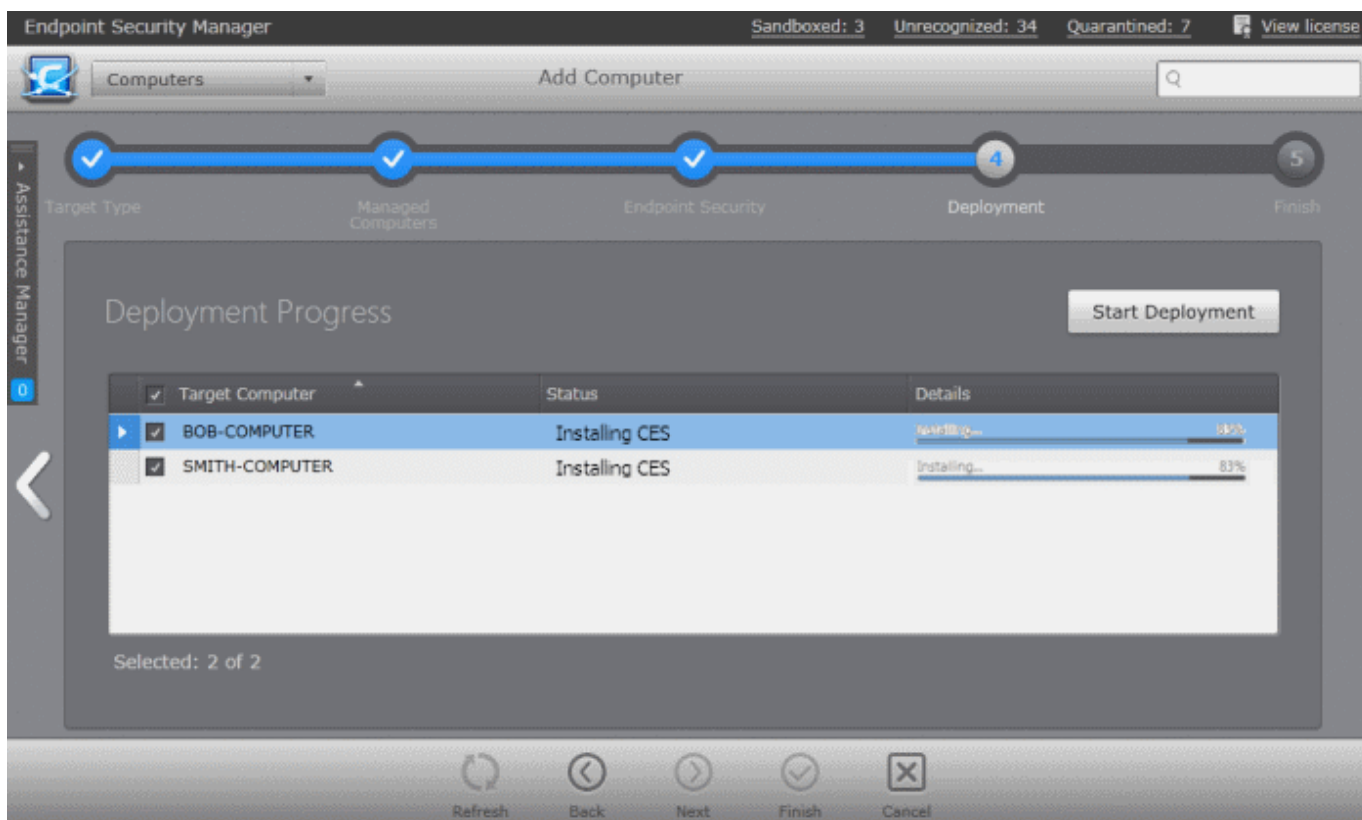
- Click the right arrow to move to the next step.

The next step is the deployment process.

- Click 'Start Deployment'.

The deployment progress will be displayed.

On completion of installation, the results screen will appear.

- Click the 'Finish' icon or swipe the screen to the left to exit the wizard.

If the 'Suppress reboot after installation' checkbox, is not selected in the **Endpoint Security step**, the endpoints will be restarted on completion for the installation to take effect.

- If no end user has logged-on to the endpoint, the endpoint will be restarted automatically

- If an end user has logged-in to the endpoint, a 'Restart your computer' dialog with a count down timer will be displayed at the endpoint as shown below:
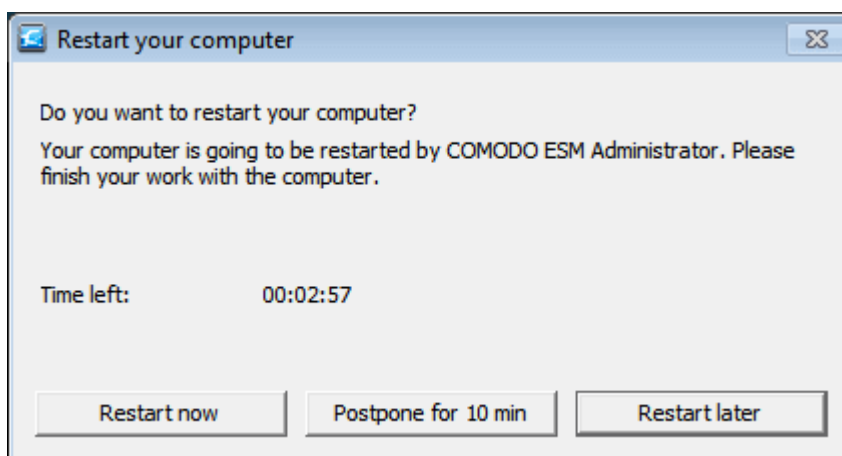

The user can choose to restart the computer immediately or postpone the restart. If no action is taken, the endpoint will restart automatically upon lapse of the countdown timer.

If the 'Suppress reboot after installation' checkbox, is selected in the **Endpoint Security step**, the endpoints will not be restarted on completion and will be indicated with 'Reboot pending' status in the 'Computers' area. The administrator can restart the endpoint at a later time by right-clicking on it and choosing 'Reboot' from the context sensitive menu or select the endpoint and click Power > Reboot from the options at the bottom of the interface.

## 3.2.4. Importing Unmanaged Endpoints from Network

CESM is capable of automatically discovering computers that are left unmanaged in the network or new computers that are added to the network and enables them to be selectively imported for remote management.

CESM checks the specified domain in the network using Active Directory (AD)/ Lightweight Directory Access Protocol (LDAP) periodically for the unmanaged computers and newly added computers. The number of computers discovered from the network is displayed on the 'Unmanaged' button at the top of the 'Computers' area and is dynamically updated.
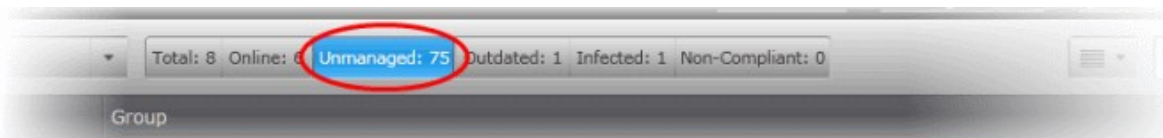
Clicking the 'Unmanaged' button displays the unmanaged computers in the 'Computers' area and enables the administrator to import them into CESM. The administrator can choose to manage selected computers by remotely installing the CASM agent on to them or to protect and manage selected computers by remotely installing the CESM agent and CES/CAS on to them.

> **Note**: CESM will discover the unmanaged computers only if Auto Discovery is enabled and the Auto Discovery Settings are configured under Preferences > Auto Discovery Settings. Please refer to **Auto Discovery Settings** for more details.
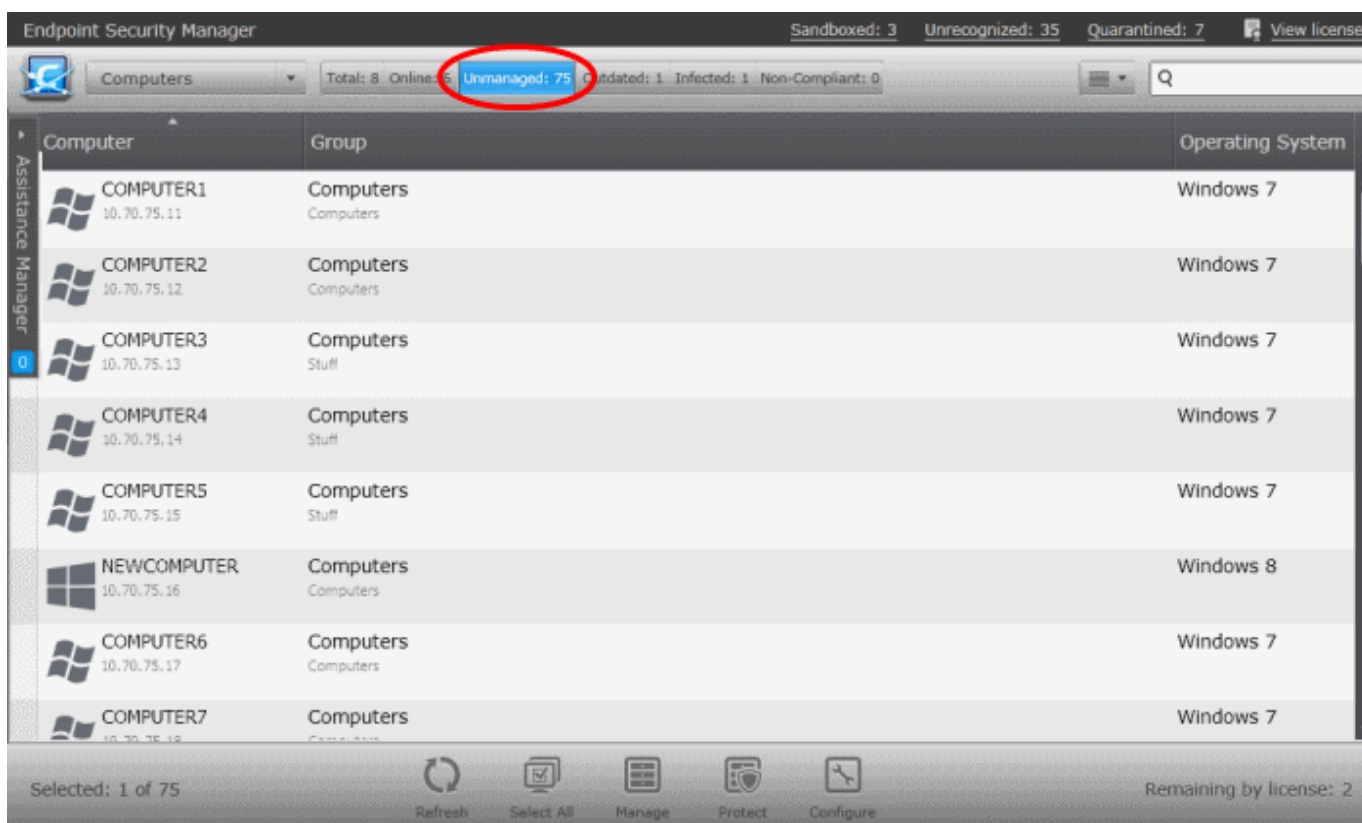
- To import Windows based computers for remote management and protection, select the computers and click 'Protect' at the bottom of the interface. Refer to the section **Importing Unmanaged Windows Computers for Centralized Management and Protection** for more details.

- To import Mac OS X based computers for remote management and protection, select the computers and click 'Protect' at the bottom of the interface. Refer to the section **Importing Unmanaged Mac OS X Computers for Centralized Management and Protection** for more details.

- To import Linux based computers for remote management, select the computers and click 'Manage' at the bottom of the interface . Refer to the section **Importing Unmanaged Linux Computers for Centralized Management** for more details.
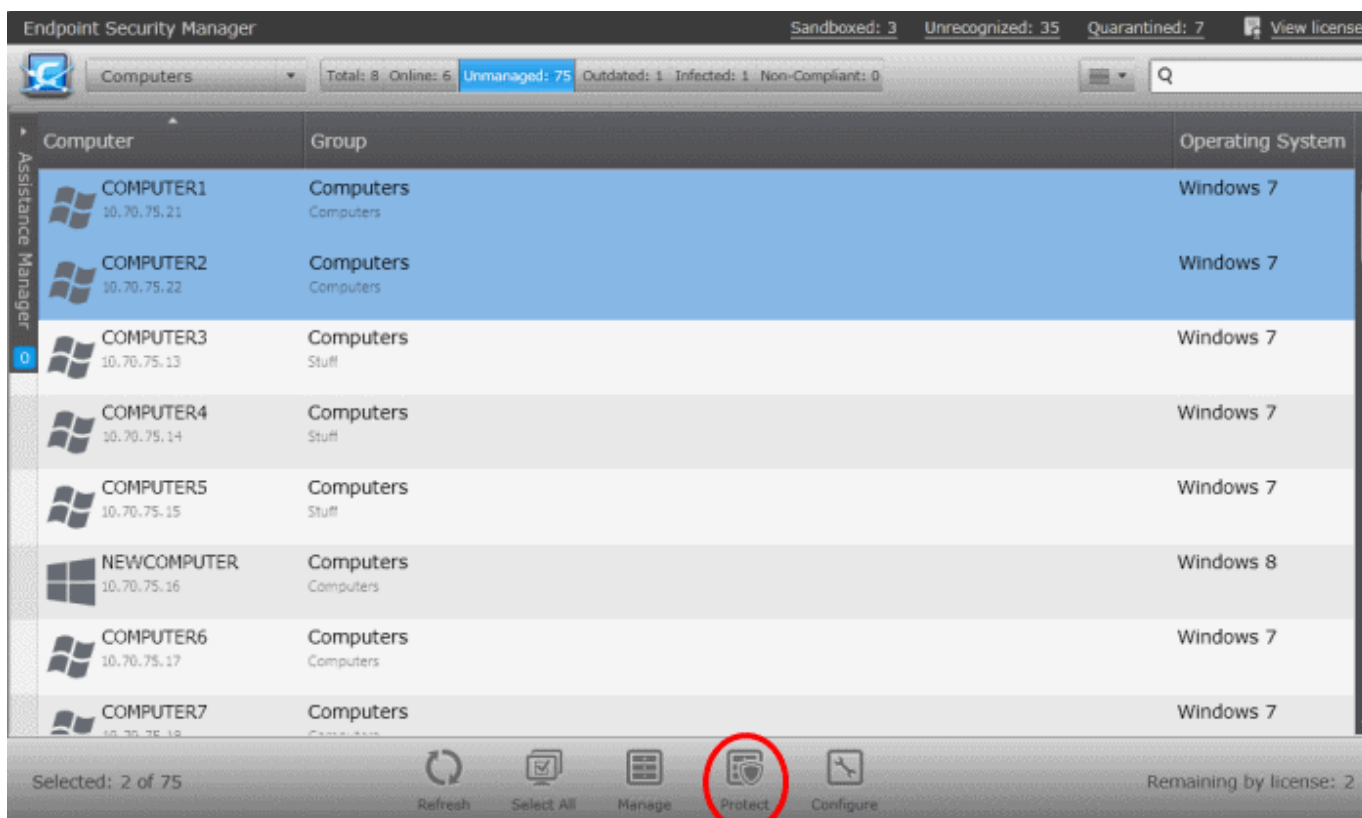
- To configure the auto discovery settings, click Configure. Refer to the section **Auto Discovery Settings** for more details.

3.2.4.1. Importing Unmanaged Windows Computers for Centralized Management and Protection

The administrator can import Windows based computers discovered as unmanaged into CESM for centralized management and protection by remotely installing the agent and the managed security software from the 'Computers' > 'Unmanaged' area.

Step 1 - Select the Target Computers

- Open the 'Computers' area by choosing 'Computers' from the drop-down at the top left and click the 'Unmanaged' button.

- Select the computers to be protected and managed and click 'Protect' from the bottom of the interface

CESM will acquire the Login Credentials from the Auto Discovery Settings and select the latest version of CES/CAS to be installed on to the endpoint with default settings and move to **Step 4 - Deployment Progress** directly, skipping **Step 2 - Credentials** and **Step 3 - Endpoint Security**. If the administrator needs to reconfigure the credentials and/or to choose installation options for Comodo Endpoint Security (CES), they can click the left arrow from **Step 4 - Deployment Progress** to move to the previous steps.

Step 2 - Credentials

The next step is to select the administrative account (login) credentials that will be used to remotely upload the installation package using the administrative share on all target computer(s).

Credentials - Table of Parameters	
Current User Credentials (Selected by default)	Selecting this option will install the agent using the credentials of the currently logged -in CESM administrator account in each endpoint.
Custom Credentials	Selecting this option allows the administrator to specify an administrative account for installation of the agent.
User Name:	Enter the user-name of the dedicated network administrator.
Password:	Enter the password of the dedicated network administrator.

- Click the right arrow after entering the credentials to move to the next step.
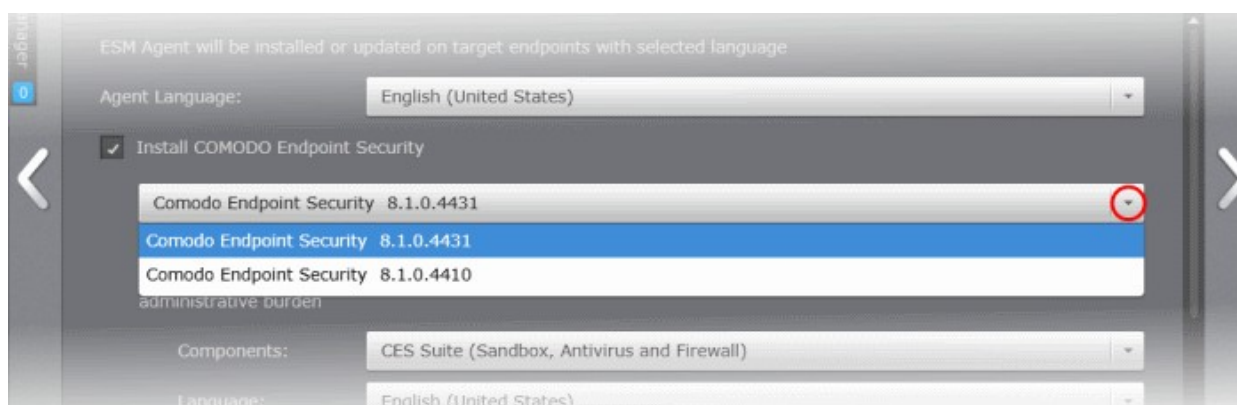
Step 3 - Endpoint Security

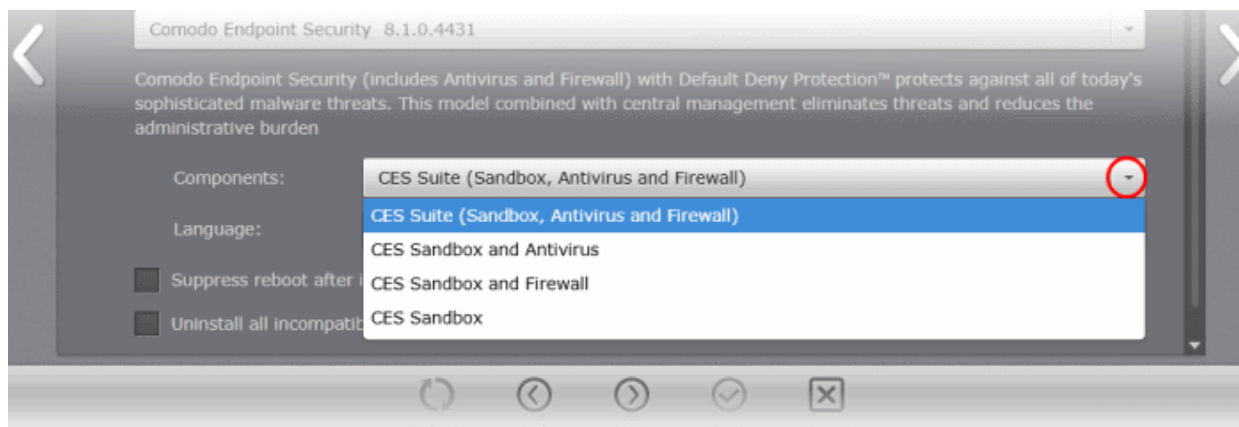The next step is to choose installation options for Comodo Endpoint Security (CES):

- Select 'Install Comodo Endpoint Security' check box if you wish CES to be installed along with the agent.

Note: If the option to install CES is not selectable, your license for Comodo Endpoint Security Manager did not include CES software.

- Select the version of CES/CAS you wish to install on the selected endpoints from the drop-down. The base package is same for both CES and CAS. CESM will automatically install CES or CAS depending on whether the endpoint is a Windows Client computer or a Windows Server.

- Select the components that you want to include from the Components drop-down:

- CES Suite, which contains all the components (Sandbox, Antivirus and Firewall)
- CES Sandbox and Antivirus
- CES Sandbox and Firewall
- CES Sandbox only

- Select the language in which the CES is to be installed from the Language drop-down.

- **Suppress reboot after installation** - CES installation will restart of the endpoints for the installation to take effect. If you do not want the endpoints to be restarted on completion of installation, select this check box. CES installation will complete but will take effect only on the next restart of the endpoint.

- **Uninstall all incompatible third-party products** - Selecting this option uninstalls select third party antivirus, firewall and other desktop security software from the endpoints, prior to the installation of CES. Performing this step will remove potentially incompatible products and thus enable CES to operate correctly. Some incompatible products can be detected, but not automatically uninstalled and must be removed manually. If your product is detected but not uninstalled, please consult your vendor's documentation for precise uninstallation guidelines.
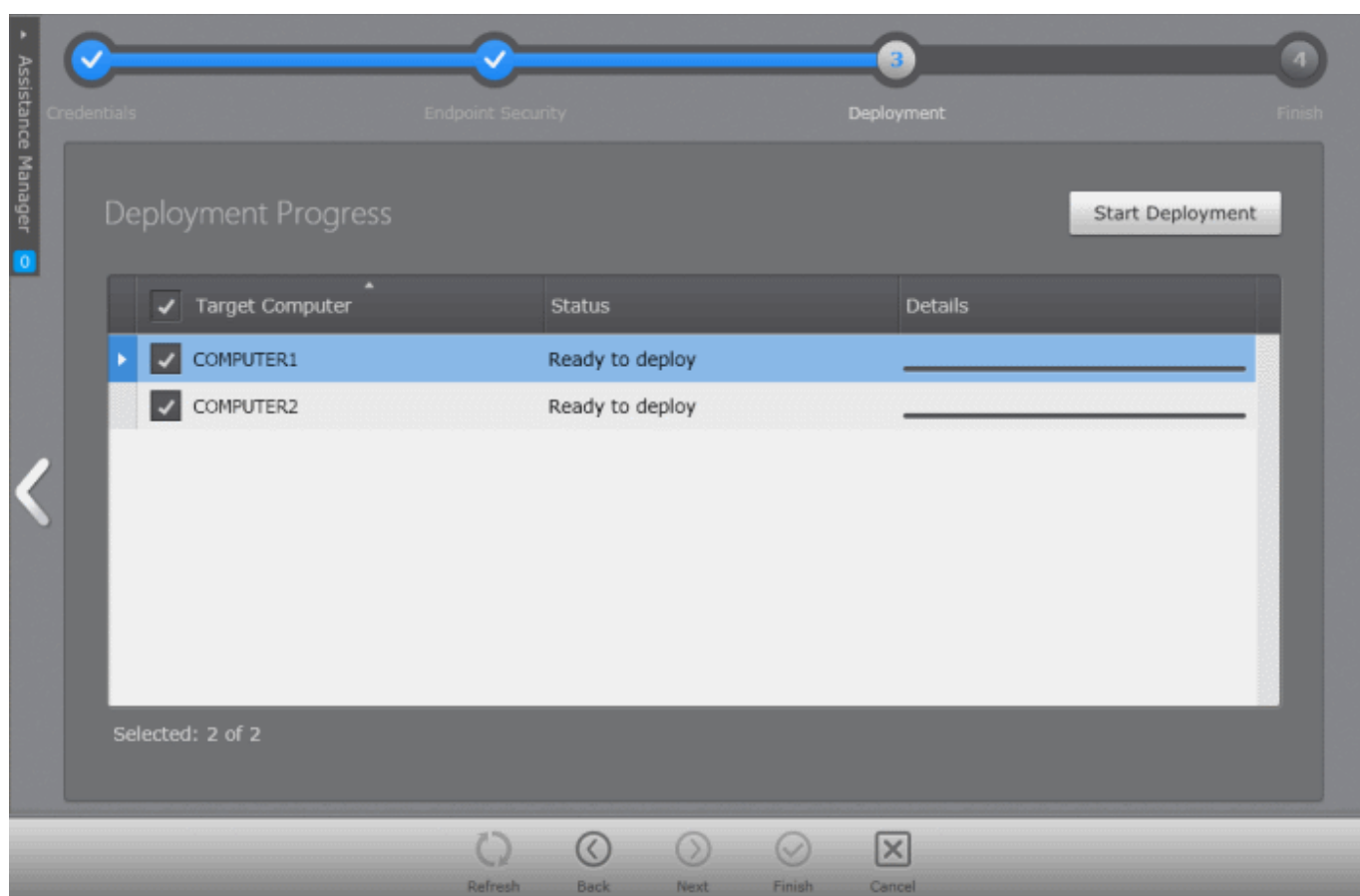
However the following steps will help most Windows users:

  - Click the Start button to open the Windows Start menu.
  - Select Control Panel > Programs and Features (Win 7, Vista); Control Panel > Add or Remove Programs. (XP).
  - Select your current antivirus or firewall program(s) from the list.
  - Click Remove/Uninstall button.
  - Repeat process until all required programs have been removed.

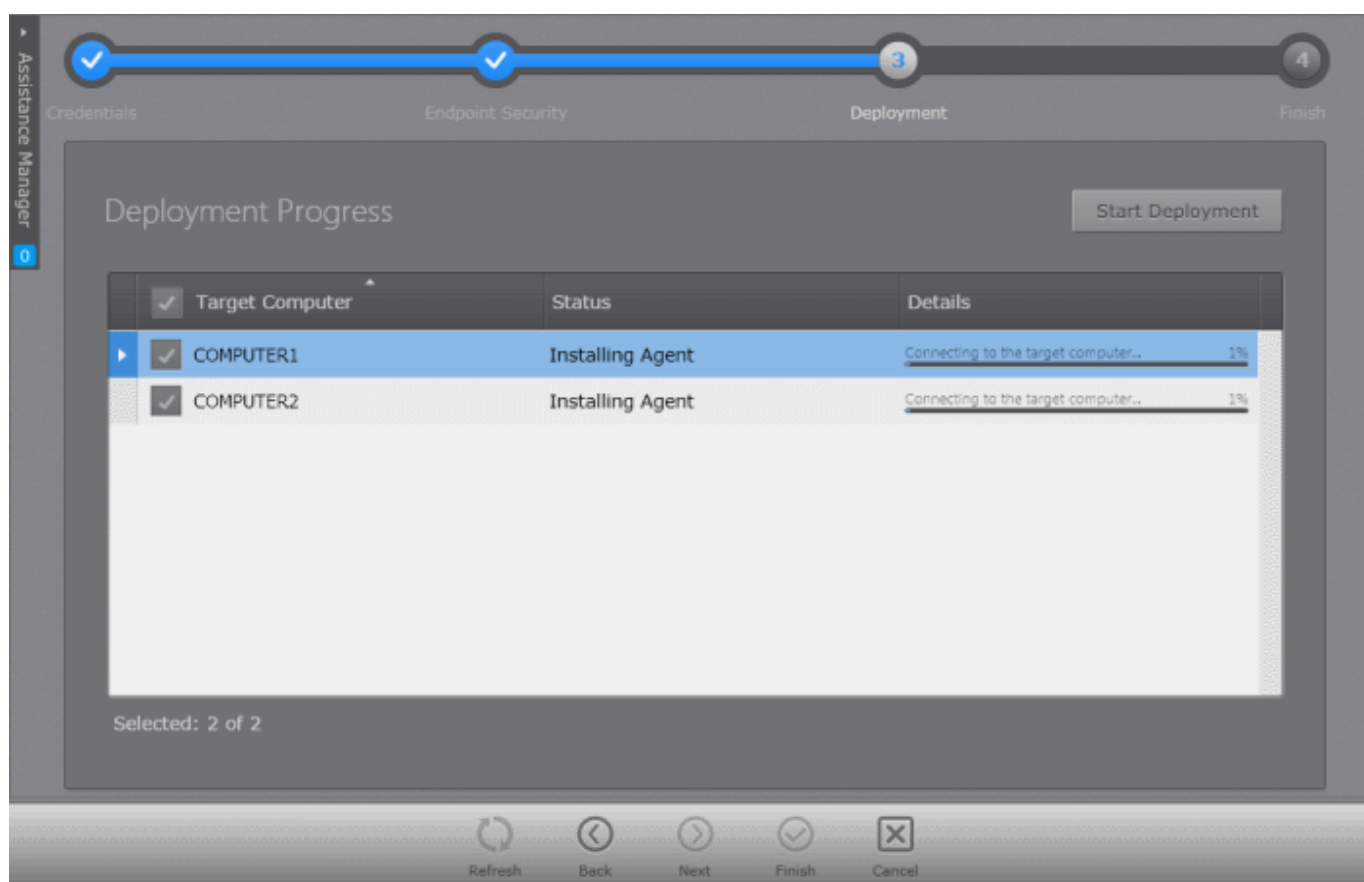 **Click Here** to see the full list of incompatible products.

- Click the right arrow to move to the next step.

Step 4 - Deployment Progress
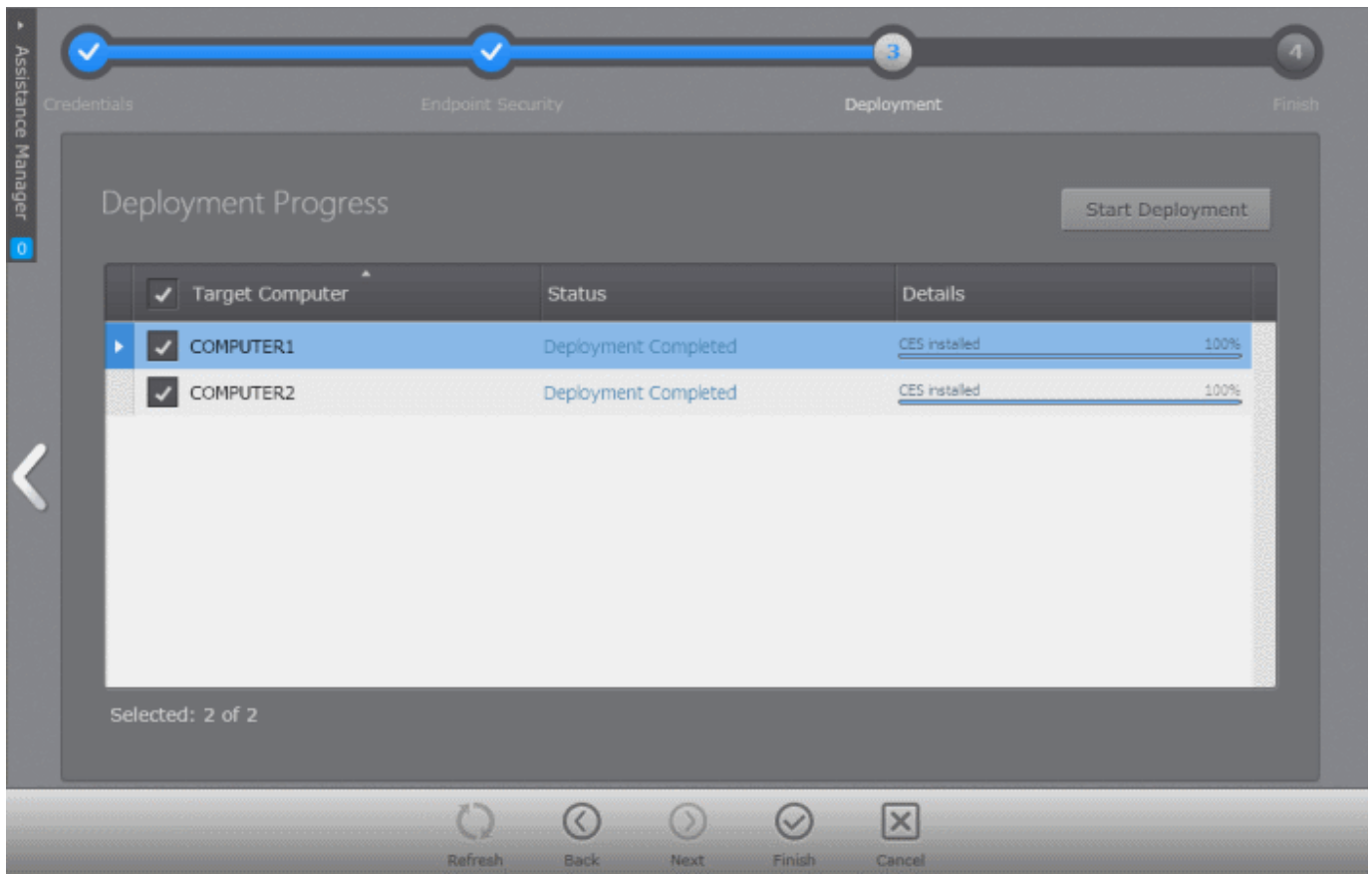
- Click 'Start Deployment'.

CESM will start installing the agent/CES/CAS on to the selected computers and the progress per computer will be displayed.
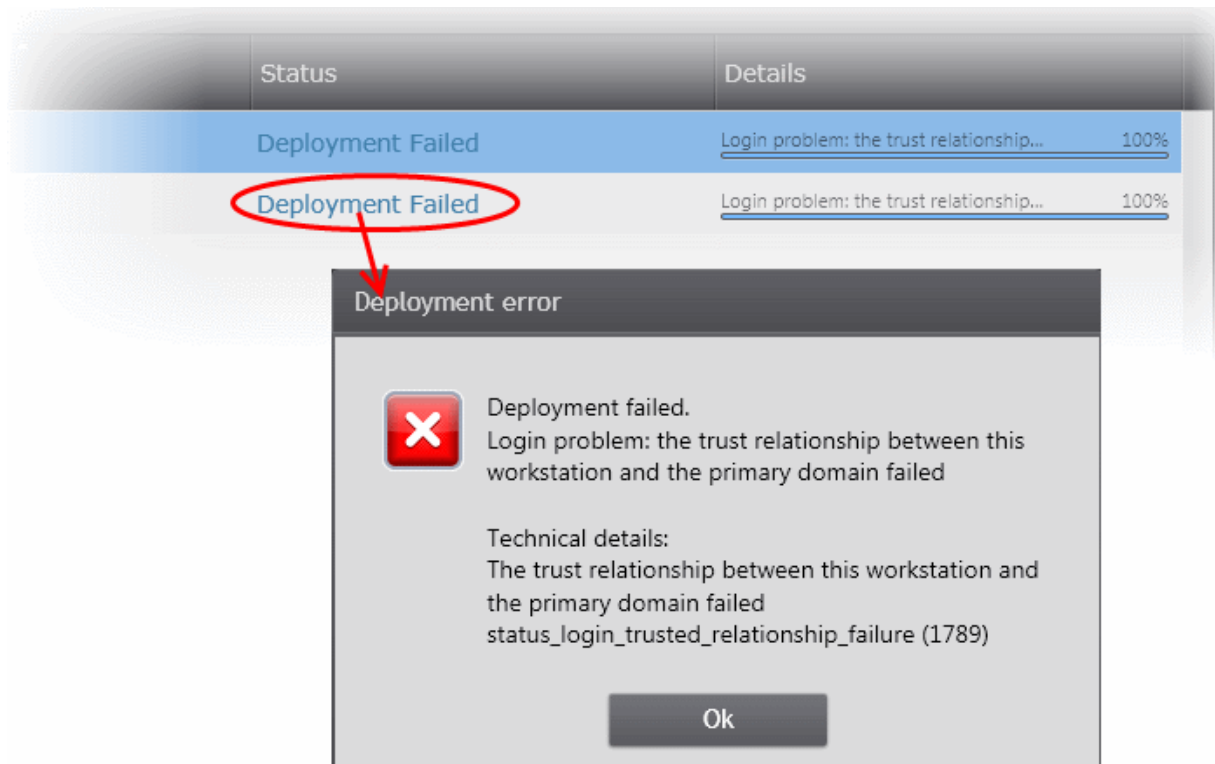
If any of the selected endpoints have older versions of CES, they will be automatically uninstalled and the selected version will be installed.

Step 5 - Deployment Complete

On completion of installation, the results screen will appear.

- If deployment fails, click on the words 'Deployment Failed' to discover the reason. The info box also contains advice that may remediate the issue.

- Click the 'Finish' or swipe the screen to the left to exit the wizard.

The endpoints selected in **Step 1** are now added to CESM and are ready for management through CESM. Refer to the section

'**The Computers Area**' for more details on how to view the list of imported endpoints.
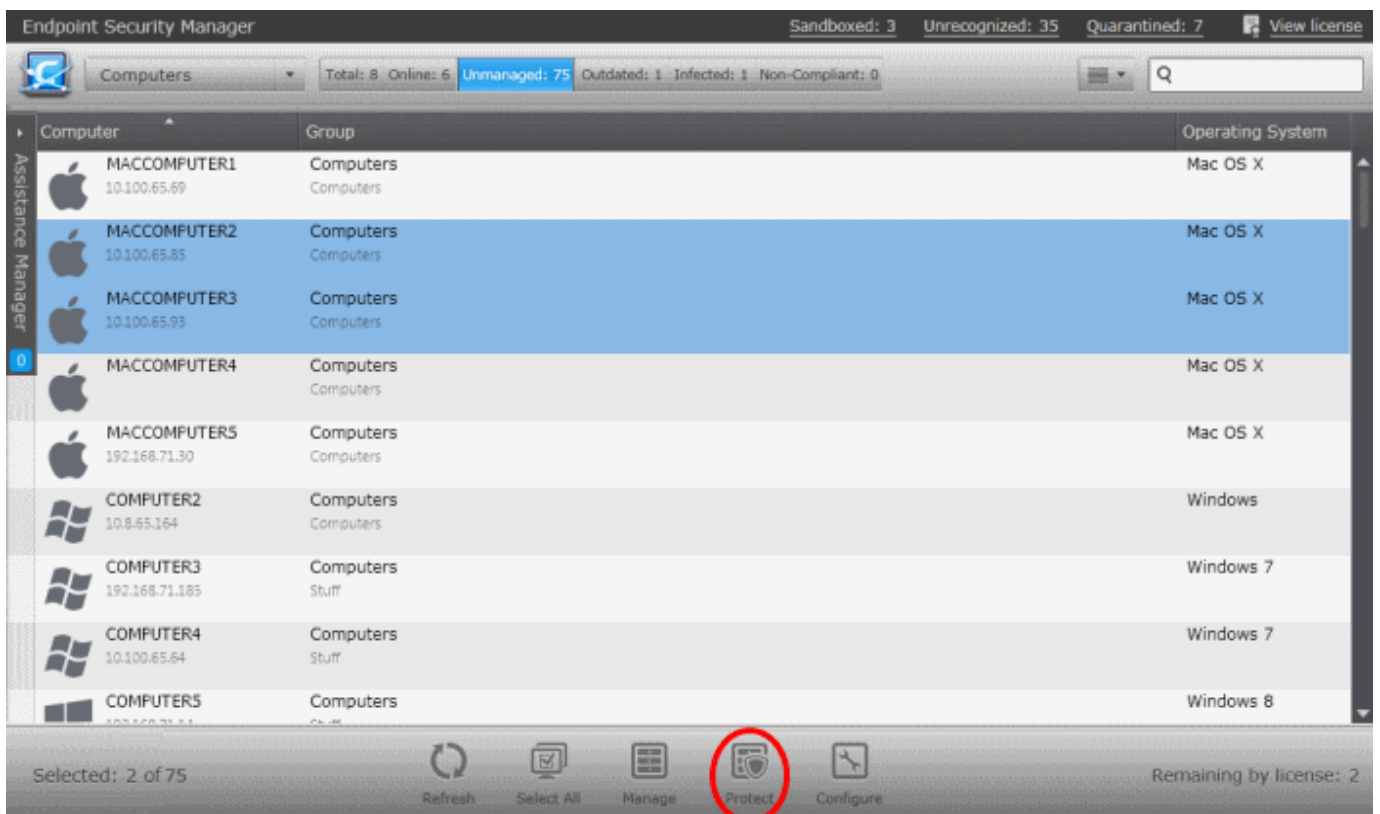
The newly added computers will be added to the default group 'Unassigned'. If this group has been changed to use a specific policy, that policy will be applied after the agent installation is completed. The administrator can create and name new groups according to the structure of the organization and move the added computers into them from 'Unassigned' group. Once created, admins can run tasks on entire groups of computers (such as applying security policy to CES, running AV scans, deploying agents, updating AV databases and more). Refer to '**The Groups Area**' for more details.

3.2.4.2. Importing Unmanaged Mac OS X Computers for Centralized Management and Protection

The administrator can import Mac OS X based computers discovered as unmanaged into CESM for centralized management and protection by remotely installing the agent and the managed security software from the 'Computers' > 'Unmanaged' area.
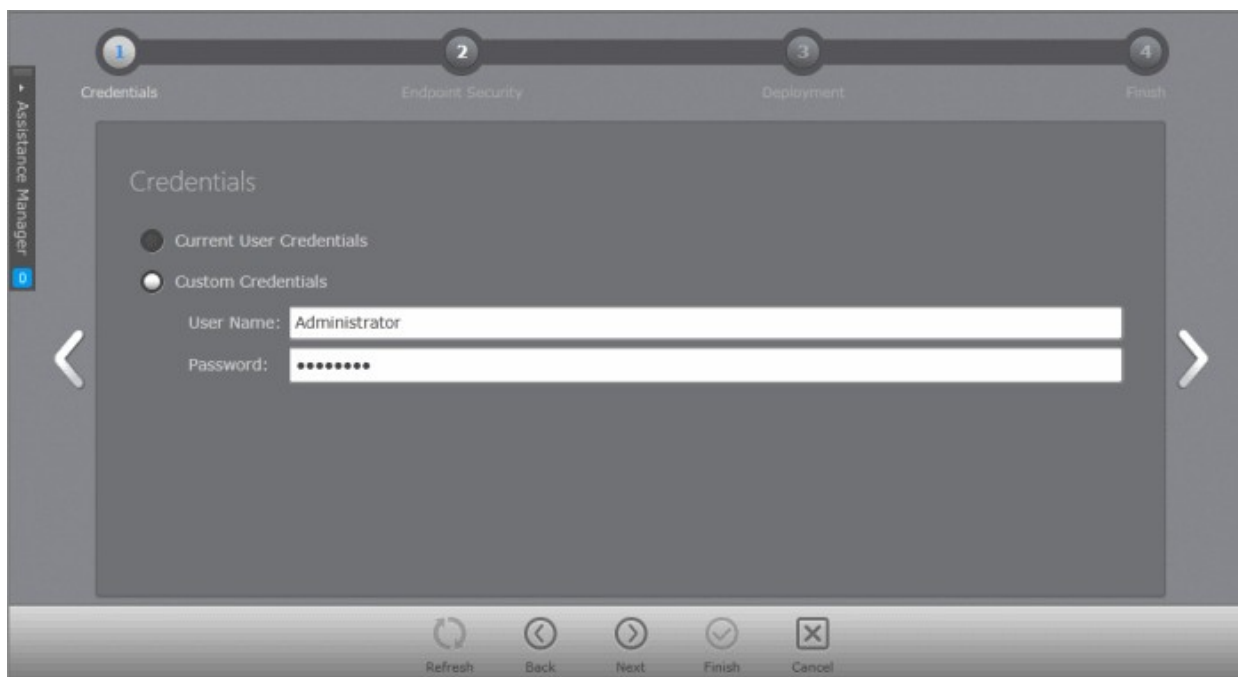
Step 1 - Select the Target Computers

- Open the 'Computers' area by choosing 'Computers' from the drop-down at the top left and click the 'Unmanaged' button.

- Select the computers to be protected and managed and click 'Protect' from the bottom of the interface

CESM will acquire the Login Credentials from the Auto Discovery Settings and select the latest version of CAV for Mac to be installed on to the endpoint with default settings and move to **Step 4 - Deployment Progress** directly, skipping **Step 2 - Credentials** and **Step 3 - Endpoint Security**. If the administrator needs to reconfigure the credentials and/or to choose installation options for Comodo Endpoint Security (CES), they can click the left arrow from **Step 4 - Deployment Progress** to move to the previous steps.

Step 2 - Credentials

The first step is to select the administrative account (login) credentials that will be used to remotely upload the installation package using the administrative share on all target computer(s).
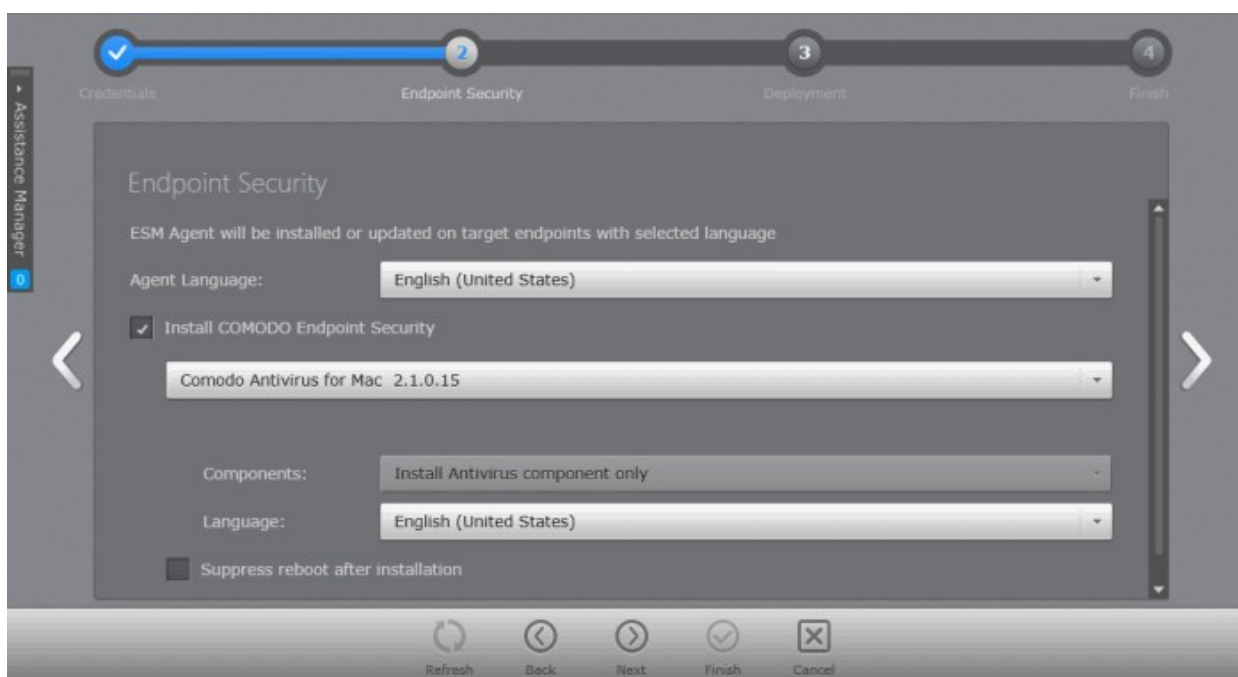
Credentials - Table of Parameters	
Current User Credentials (Selected by default)	Selecting this option will install the agent using the credentials of the currently logged -in CESM administrator account in each endpoint.
Custom Credentials	Selecting this option allows the administrator to specify an administrative account for installation of the agent.
User Name:	Enter the user-name of the dedicated network administrator.
Password:	Enter the password of the dedicated network administrator.

- Click the right arrow after entering the credentials to move to the next step.

Step 3 - Endpoint Security

The next step is to choose installation options for Comodo Endpoint Security (CES):

- Select 'Install Comodo Endpoint Security' check box if you wish CAV for Mac to be installed along with the agent.

Note: If the option to install CAV is not selectable, your license for Comodo Endpoint Security Manager did not include CAV software.

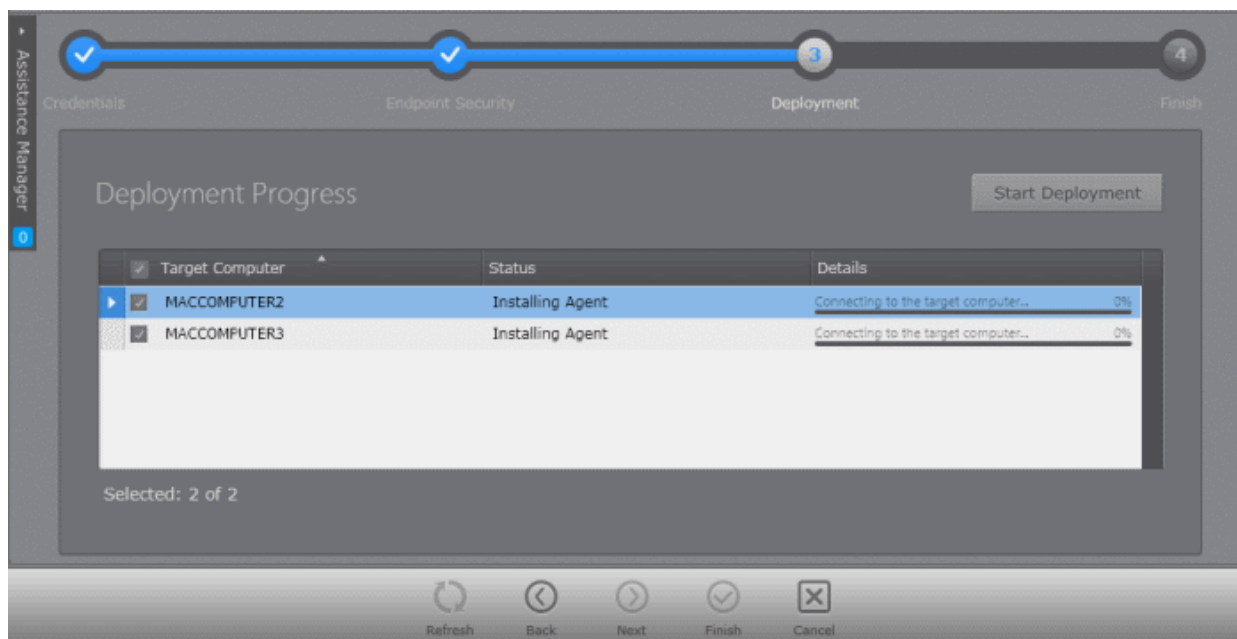- Select the version of CAV you wish to install on the selected endpoints from the drop-down.
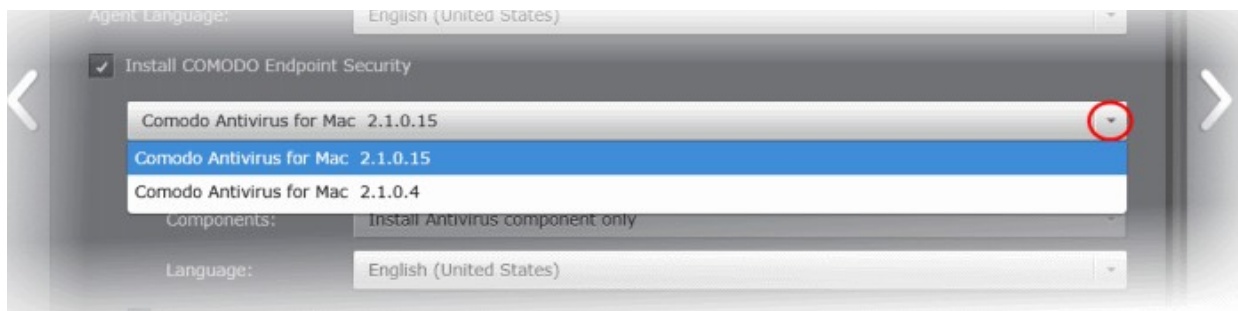
- **Suppress reboot after installation** - CAV installation will restart of the endpoints for the installation to take effect. If you do not want the endpoints to be restarted on completion of installation, select this check box. CAV installation will complete but will take effect only on the next restart of the endpoint.

- Click the right arrow to move to the next step.

Step 4 - Deployment Progress
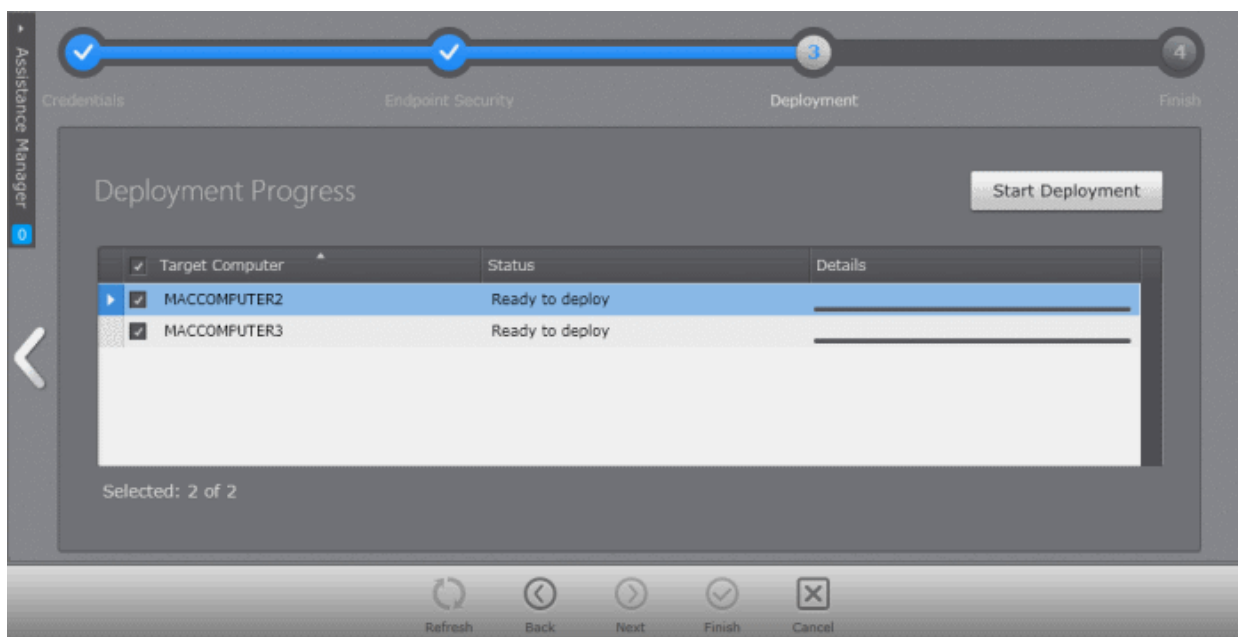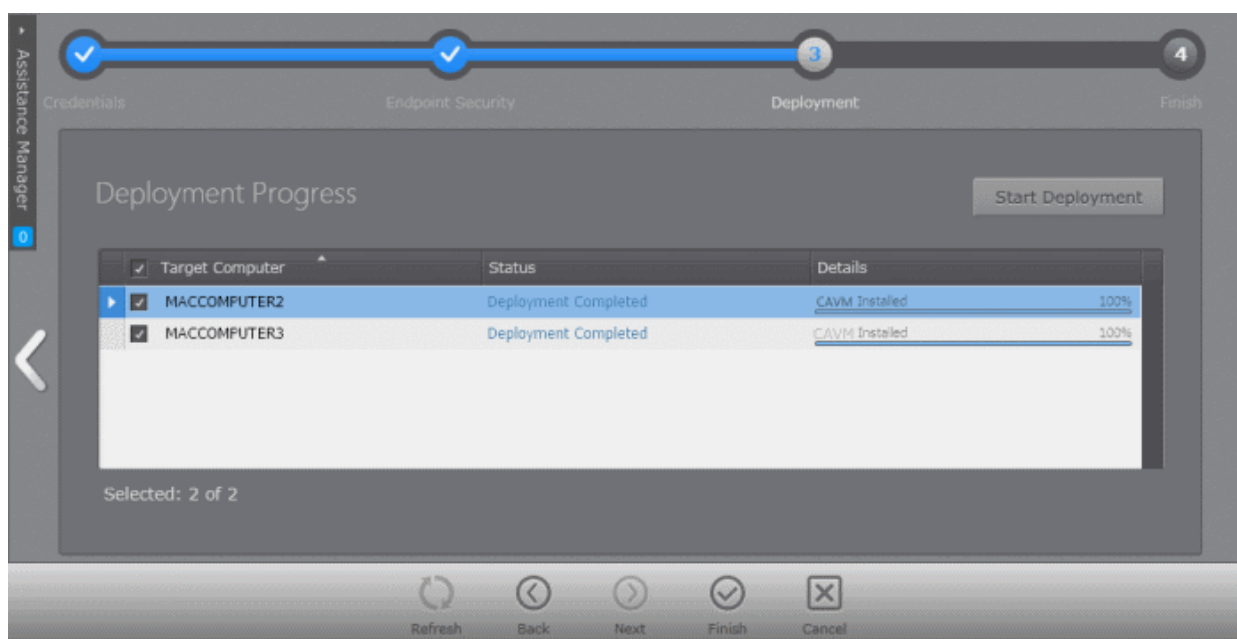

- Click 'Start Deployment'.

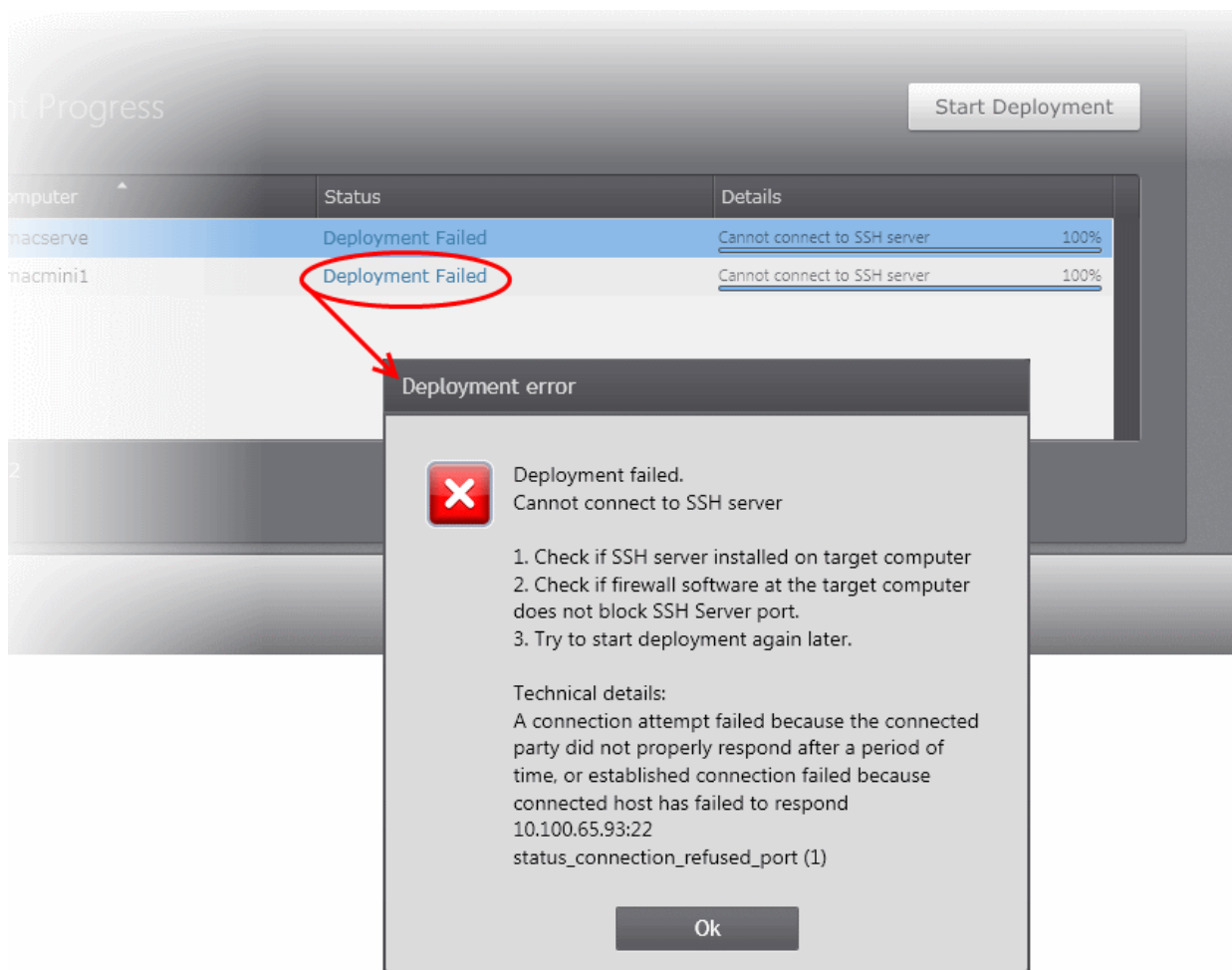CESM will start installing the agent/CAV on to the selected computers and the progress per computer will be displayed.

If any of the selected endpoints have older versions of CES, they will be automatically uninstalled and the selected version will be installed.

Step 5 - Deployment Complete

On completion of installation, the results screen will appear.

- If deployment fails, click on the words 'Deployment Failed' to discover the reason. The info box also contains advice that may remediate the issue.

- Click the 'Finish' or swipe the screen to the left to exit the wizard.

The endpoints selected in **Step 1** are now added to CESM and are ready for management through CESM. Refer to the section '**The Computers Area**' for more details on how to view the list of imported endpoints.

The newly added computers will be added to the default group 'Unassigned'. If this group has been changed to use a specific policy, that policy will be applied after the agent installation is completed. The administrator can create and name new groups according to the structure of the organization and move the added computers into them from 'Unassigned' group. Once created, admins can run tasks on entire groups of computers (such as applying security policy, running AV scans, deploying agents, updating AV databases and more). Refer to '**The Groups Area**' for more details

3.2.4.3. Importing Unmanaged Linux based Endpoints for Centralized Management

The administrator can import Linux based computers discovered as unmanaged into CESM for centralized management by remotely installing the agent from the 'Computers' > 'Unmanaged' area.
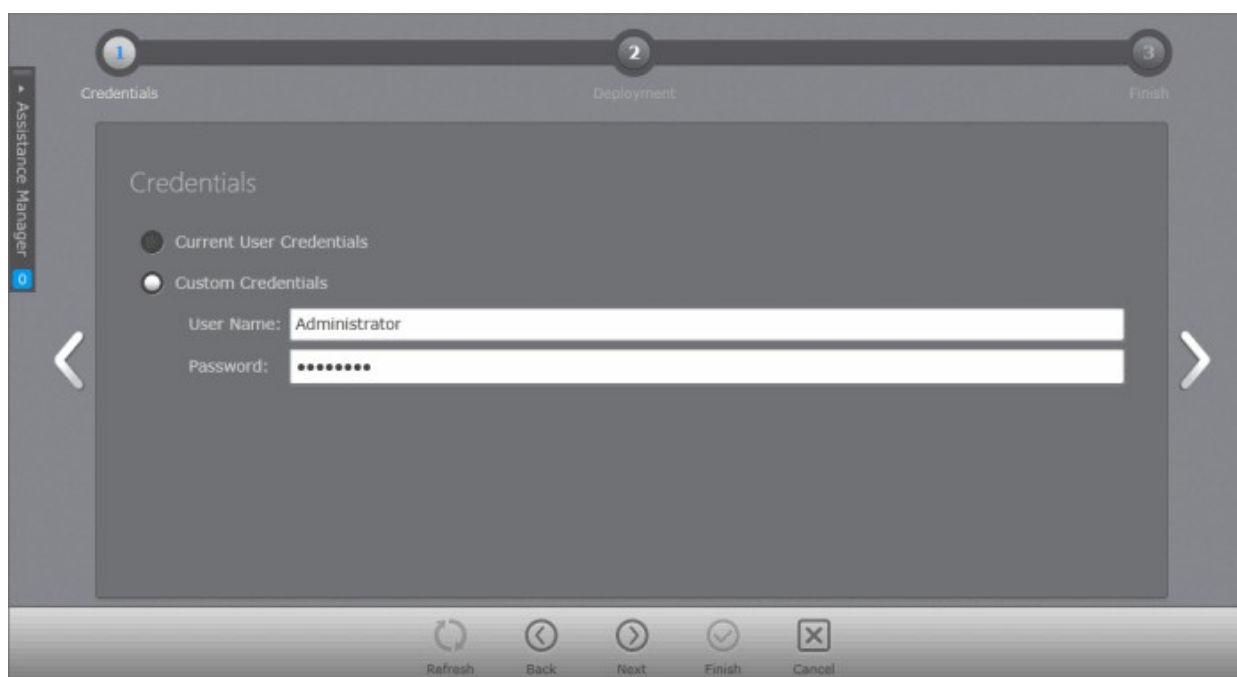
Step 1 - Select the Target Computers

- Open the 'Computers' area by choosing 'Computers' from the drop-down at the top left and click the 'Unmanaged' button.

- Select the Linux based computers to be managed and click 'Manage' from the bottom of the interface
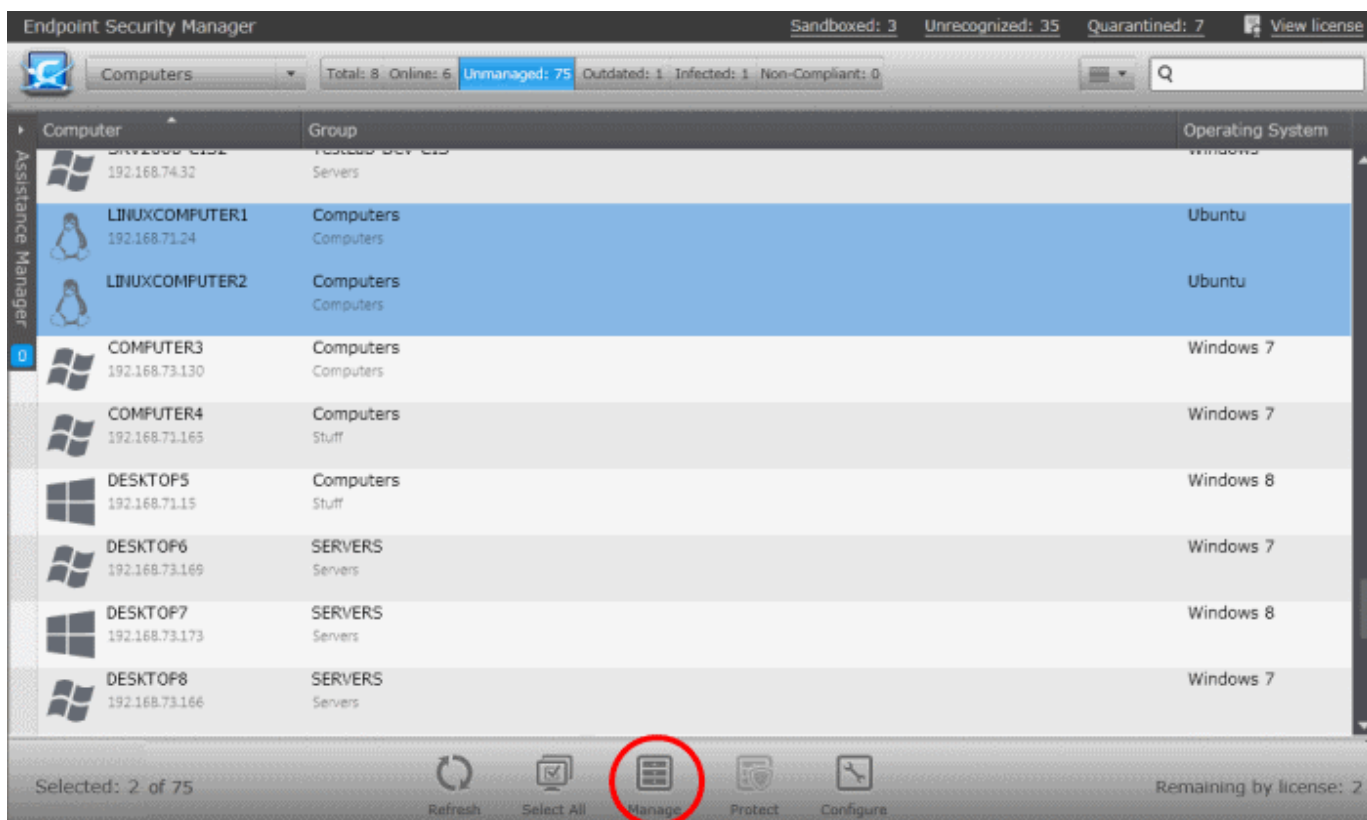
CESM will acquire the Login Credentials from the Auto Discovery Settings and move to **Step 2 - Deployment Progress** directly, skipping **Step 1 - Credentials**. If the administrator needs to reconfigure the credentials, they can click the left arrow from **Step 2 - Deployment Progress** to move to the previous step.

Step 1 - Credentials

The next step is to select the administrative account (login) credentials that will be used to remotely upload the installation package using the administrative share on all target computer(s).

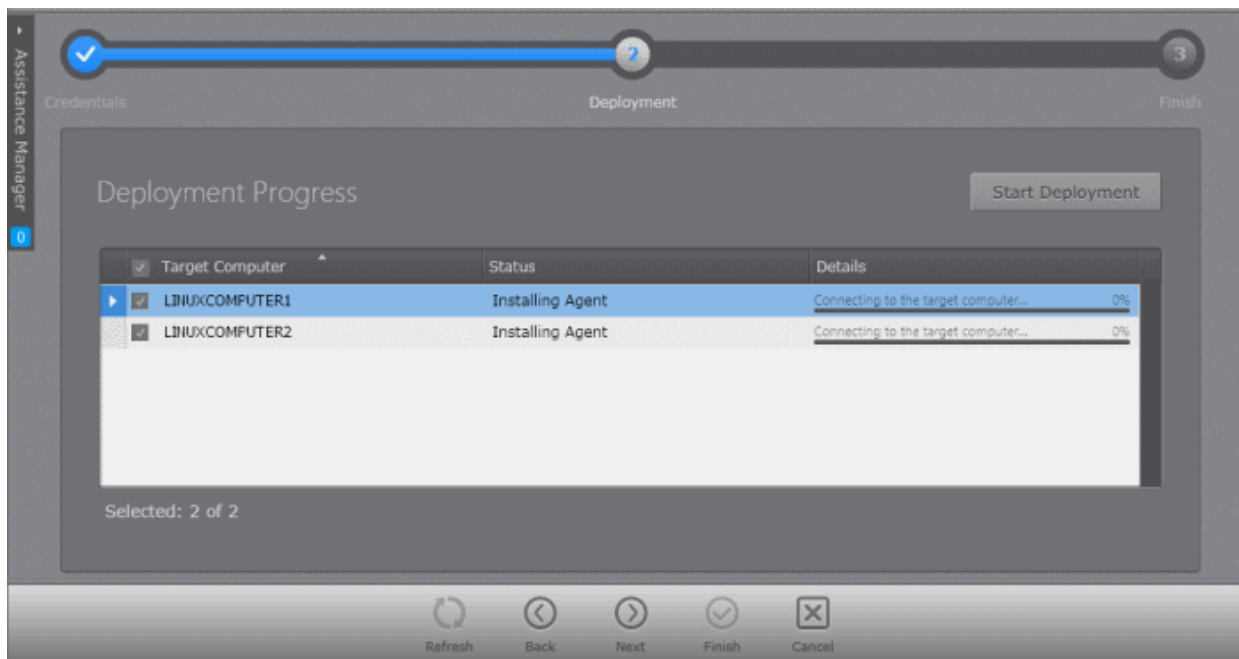| Credentials - Table of Parameters	
Current User Credentials (Selected by default)	Selecting this option will install the agent using the credentials of the currently logged -in CESM administrator account in each endpoint.
Custom Credentials	Selecting this option allows the administrator to specify an administrative account for installation of the agent.
User Name:	Enter the user-name of the dedicated network administrator.
Password:	Enter the password of the dedicated network administrator.

- Click the right arrow after entering the credentials to move to the next step.

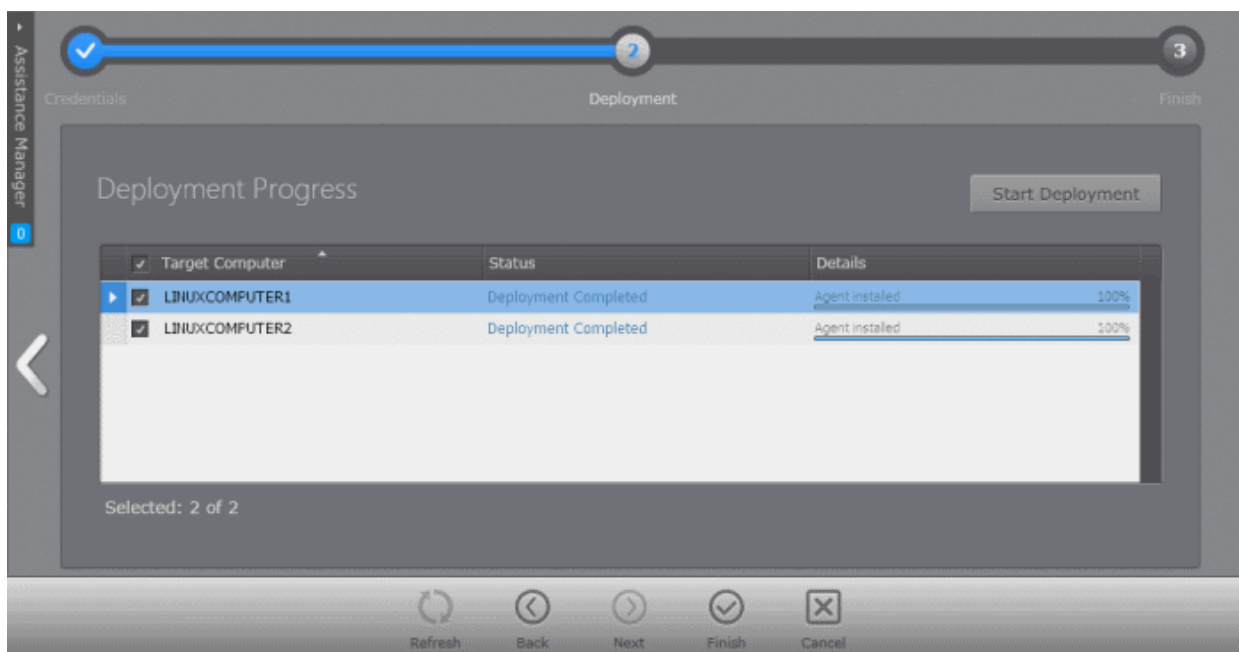**Step 2 - Deployment Progress**
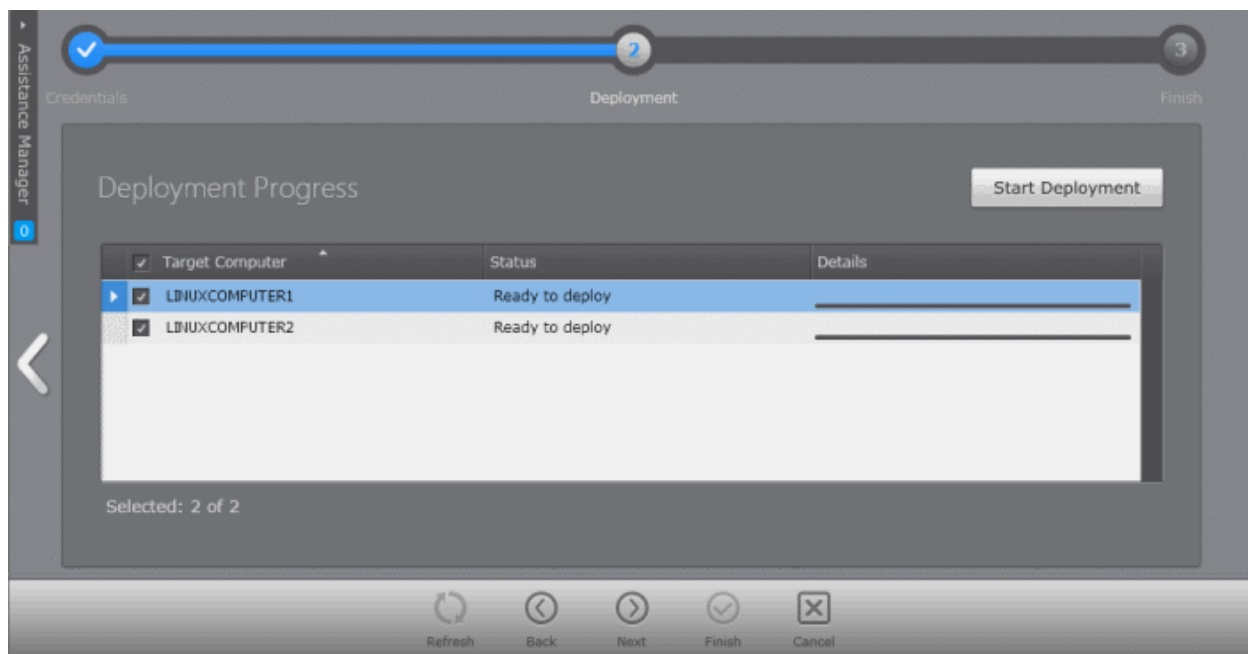
- Click 'Start Deployment'.

CESM will start installing the agent on to the selected computer(s) endpoints and the progress per computer will be displayed.
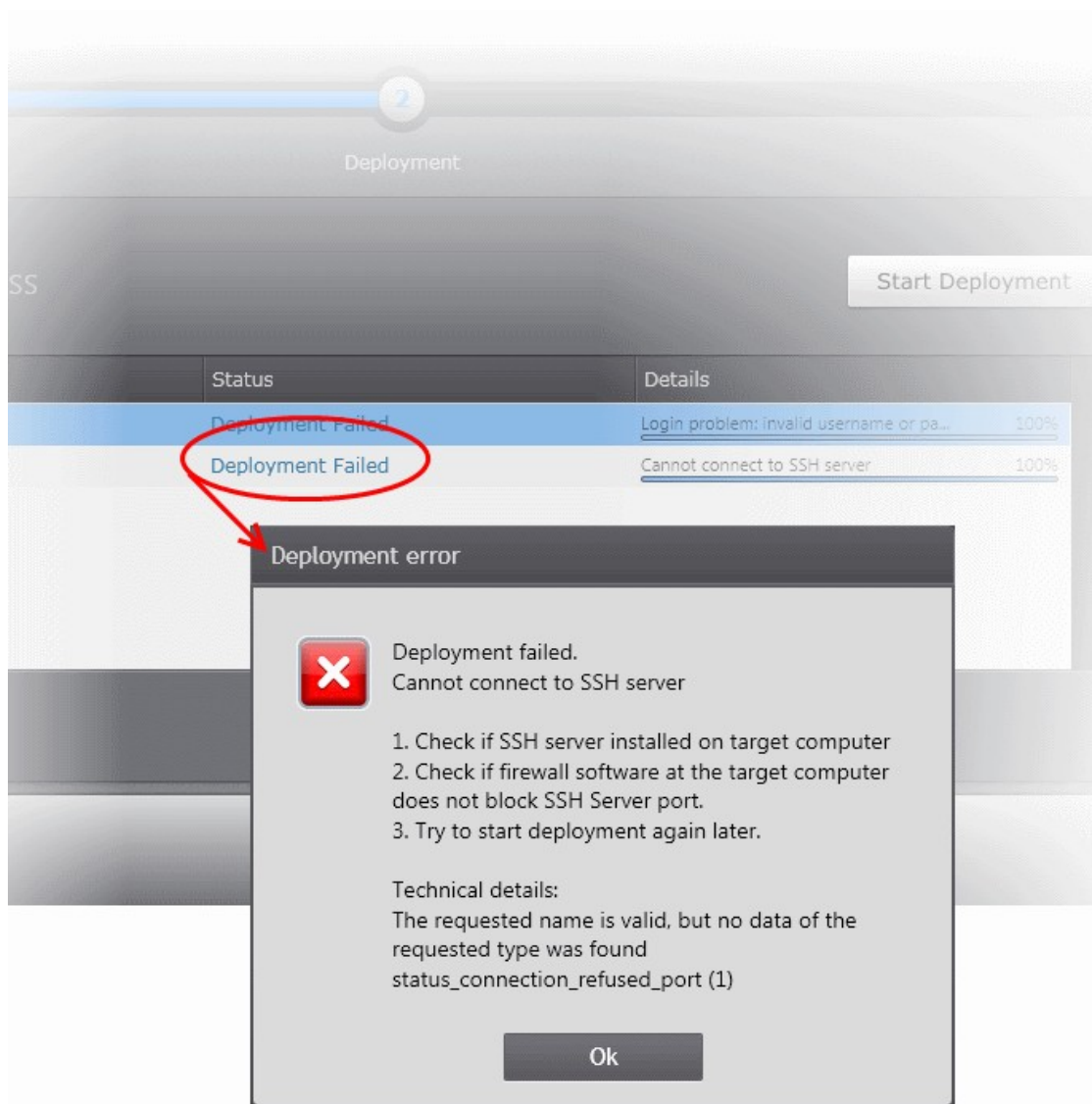
Step 3 - Deployment Complete

On completion of installation, the results screen will appear.

- If deployment fails, click on the words 'Deployment Failed' to discover the reason. The info box also contains advice that may remediate the issue.

- Click the 'Finish' or swipe the screen to the left to exit the wizard.

The endpoints selected in **Step 1** are now added to CESM and are ready for management through CESM. Refer to the section '**The Computers Area**' for more details on how to view the list of imported endpoints.

The newly added computers will be added to the default group 'Unassigned'. If this group has been changed to use a specific policy, that policy will be applied after the agent installation is completed. The administrator can create and name new groups according to the structure of the organization and move the added computers into them from 'Unassigned' group. Refer to '**The Groups Area**' for more details.

3.3.Running On-Demand Scan on Selected Endpoints

The 'Computers' area allows the administrators run instant scan on selected endpoints, irrespective of the groups they belong to. The administrator can choose to run a full scan or selected areas of the endpoint, by choosing a scan profile.

> **Tip**: The administrators can also run a scan on a selected single endpoint from the **Computer Properties > Endpoint Security interface**. Refer to the section **Viewing and Managing Endpoint Security Software** for more details.
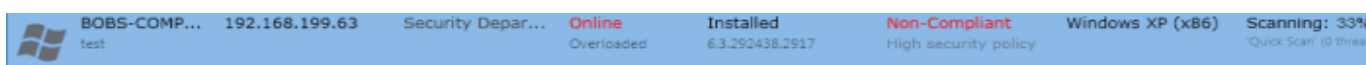
To run a full scan on selected endpoints

1. Select 'Computers' from the area selection drop-down menu to open the 'Computers' interface.

2. Choose the endpoints to be scanned. You can select multiple endpoints at once by pressing and holding the Ctrl or Shift key, from list, tile or 3D Panoramic view.

> **Note**: You can select only the endpoints on to which CES is installed and AV is enabled.

3. Click 'Antivirus' > 'Scan' from the options at the bottom.
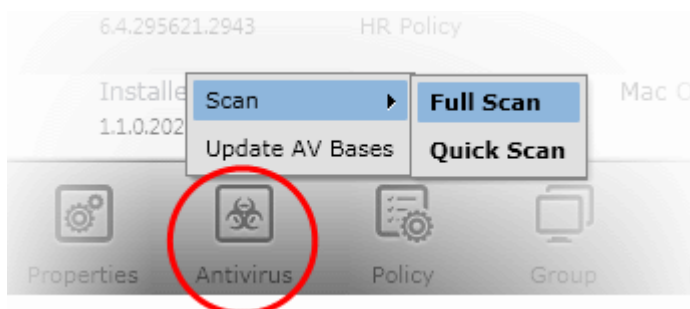
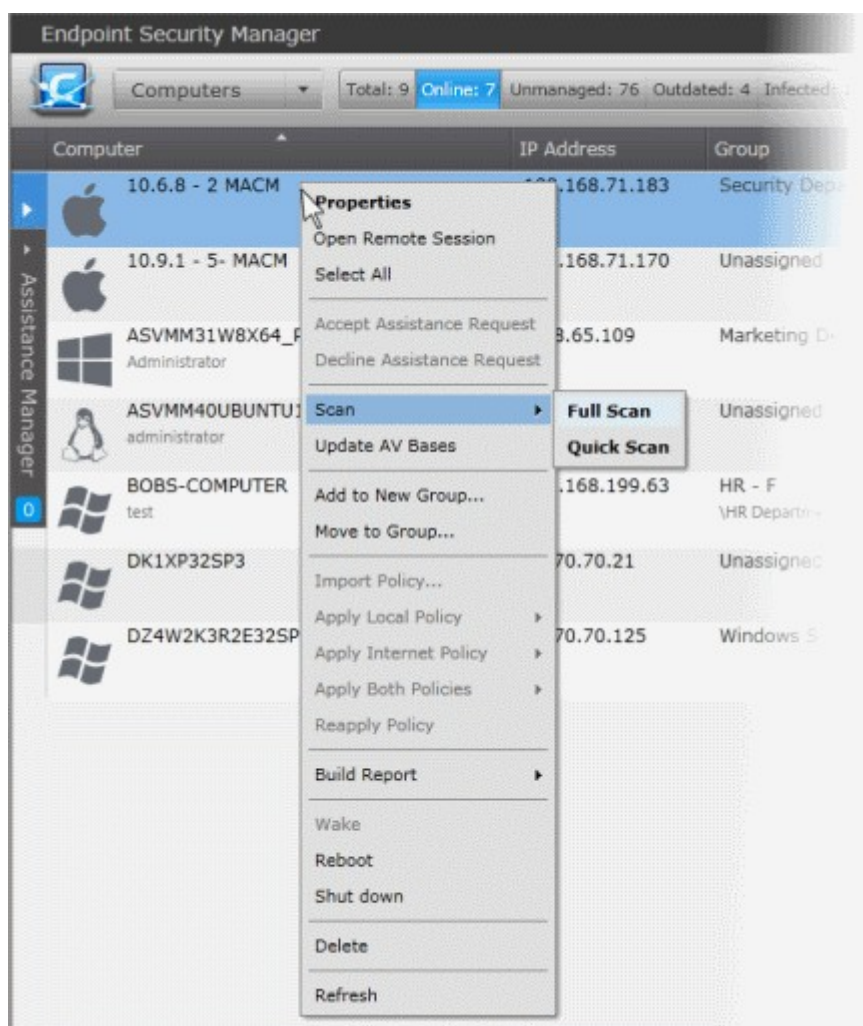Select a type of a scan of the endpoint. It will be commenced and the progress will be displayed.

You can also run the scans from the right click options with choices to select the areas to be scanned in the endpoints.

To run scan on selected areas of endpoints

1. Select 'Computers' from the area selection drop-down menu to open the 'Computers' interface.

2. Choose the endpoints to be scanned. You can select multiple endpoints at once by pressing and holding the Ctrl or Shift key, from list, tile or 3D Panoramic view.

> **Note**: You can select only the endpoints on to which CES is installed and AV is enabled.

3. Right click and select 'Scan' from the context sensitive menu.

4. Select the Scan Profile from the drop-down, depending on the areas to be scanned on the endpoints. The default scan profiles are:

    -   **Full Scan** - This profile covers every local drive, folder and file on the endpoint.

    -   **Quick Scan** - Covers critical areas in the endpoint which are highly prone to infection from viruses, rootkits and other malware. This includes system memory, auto-run entries, hidden services, boot sectors, important registry keys and system files. These areas are responsible for the stability of the computer and keeping them clean is essential.

    -   More scan profiles can be defined in the following ways:

        -   Creating custom scan profiles while creating/editing a security policy and applying it to the endpoints. For more details, refer to the section **Creating a Custom Scan Profile**.

        -   Creating a custom scan profile at an endpoint, importing its CES/CAS settings while creating a security profile and applying it to selected endpoints. For more details on creating scan profiles, please refer to CES online help guide at **http://help.comodo.com/topic-84-1-499-5558-Scan-Profiles.html**.

The on-demand scan will be started on the selected endpoints and the progress will be displayed.

On completion of scanning:

-   If malware is discovered during the scan that is not handled successfully (deleted, disinfected or quarantined) then the endpoint will be indicated as Infected in the 'Computers' area.

-   The results of the scan can be viewed as an Infection report from the Reports area - click 'Reports' then the 'Computer Infections'. The report can also be exported as a pdf file or a spreadsheet file for printing purposes. Refer to **Reports > Computer Infections** for more details.

3.4. Updating Virus Database on Individual Endpoints

The 'Computers' area allows the administrators to update the virus signature database on selected endpoints, identified as outdated computers, irrespective of the groups they belong to.

To update selected computers

1. Select 'Computers' from the area selection drop-down menu to open the 'Computers' interface.

2. Select the endpoints to be updated. You can select multiple endpoints at once by pressing and holding the Ctrl or Shift key, from list, tile or 3D Panoramic view.
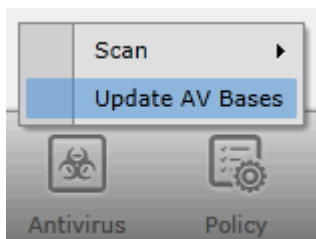
> **Note**: You can select both Windows based endpoints on to which CES/CAS is installed and AV is enabled and Mac OS X based endpoints with CAV for Mac installed and enabled.

3. Click 'Antivirus'> 'Update AV Bases' from the bottom or right click on a selected endpoint and choose Update AV Bases from the context sensitive menu.

The Progress will be displayed.

… and on completion, the virus signature database at the endpoints will be made up-to-date.
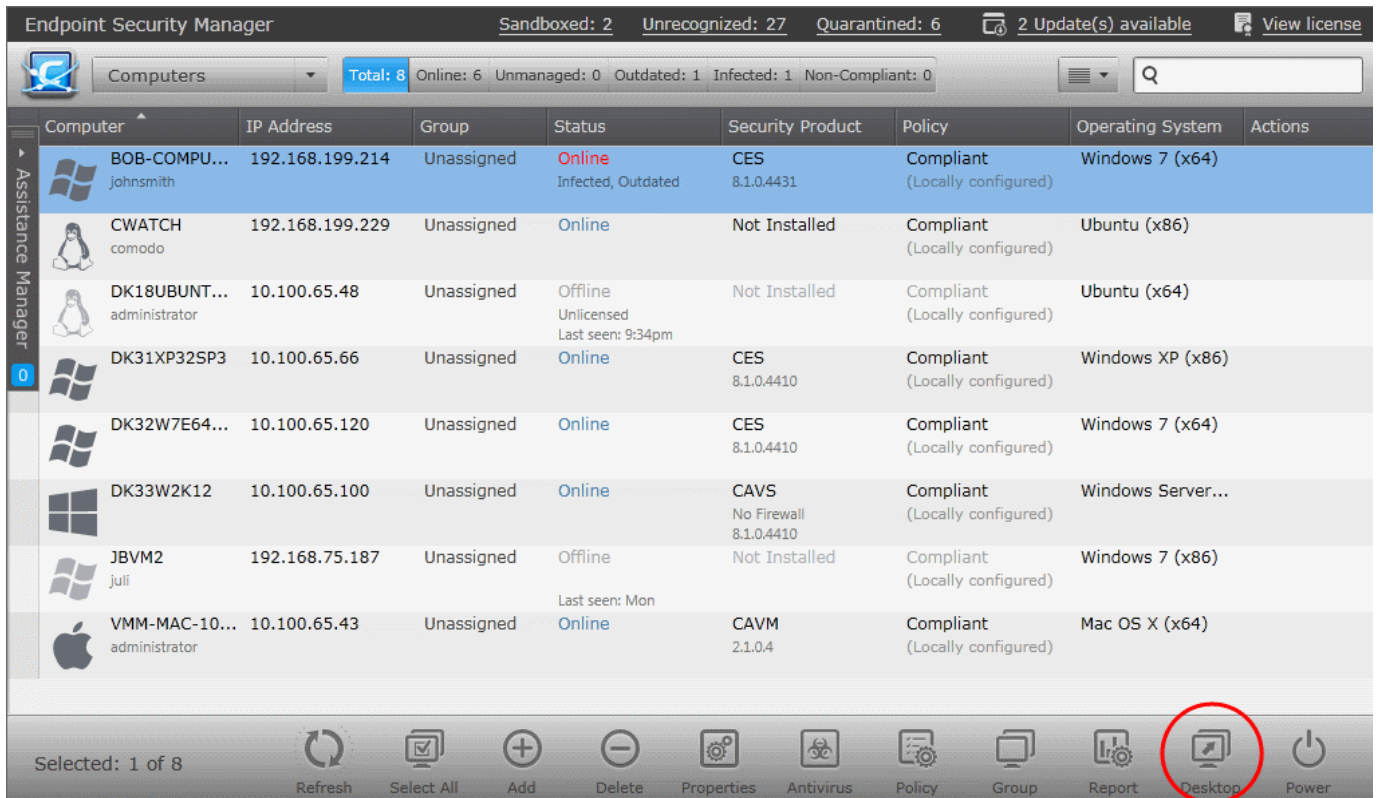
3.5. Accessing Endpoints through Remote Desktop Sharing Session

CESM allows administrators to conduct desktop sharing sessions with endpoints to solve issues, install third party software or for other system maintenance.

To start a remote sharing session

1. Select 'Computers' from the area selection drop-down menu to open the 'Computers' interface.

2. Select the endpoint to be controlled.

3. Click 'Desktop' from the bottom or right-click the endpoint and select 'Open Remote Session' from the context sensitive menu.

CESM will initiate a remote desktop session with the selected endpoint. A message will be shown on the endpoint asking the user to accept the request:

- If no user is logged-on at the endpoint, the remote desktop access connection will be established automatically upon lapse of the timer.

- If an end user is logged-in at the endpoint, the end user can accept or deny the connection request. If no action is taken till the lapse of the timer, the connection will be automatically established.

On successful establishment of the connection, a new browser window will open or a new tab will open in the current browser window, displaying the desktop of the remote computer, depending on the browser you are using.
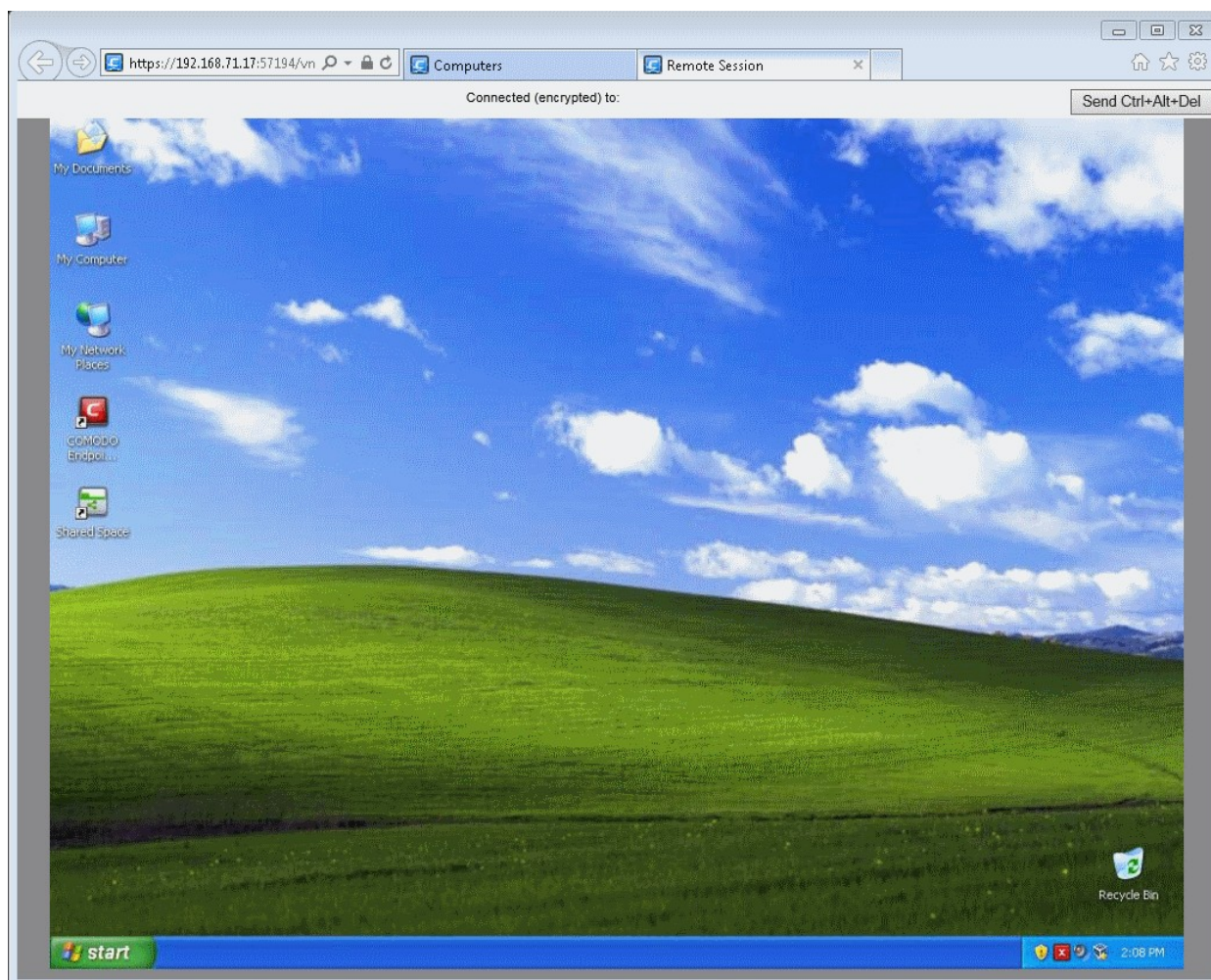
The administrator can take control of the remote computer, through the desktop sharing session.

3.6.Managing Power Options on Endpoints

CESM allows administrators to wake, reboot or shut down selected endpoints direct from the 'Computers' screen.

To manage power on an endpoint

1.   Select 'Computers' from the area selection drop-down menu to open the 'Computers' interface.

2. Select the target endpoint. Hold CTRL + click to select multiple endpoints or click 'Select All' to select all the endpoints.

3. Click 'Power' from the bottom or right-click the endpoint and select the power option, Wake, Reboot or Shutdown, from the context sensitive menu.
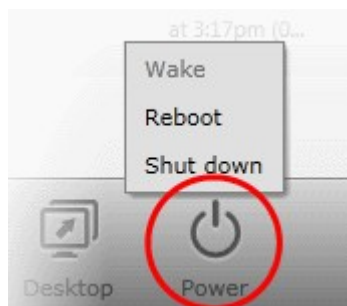
4. If 'Wake' option is chosen, the endpoint will wake from sleep mode. If the endpoint is either turned off or not properly configured, the message 'Waking up failed' will be displayed under Actions column in the respective endpoint row.

• To restart the endpoint, click 'Reboot'. An alert will be displayed that the endpoint will be rebooted immediately if there is no user is logged in.
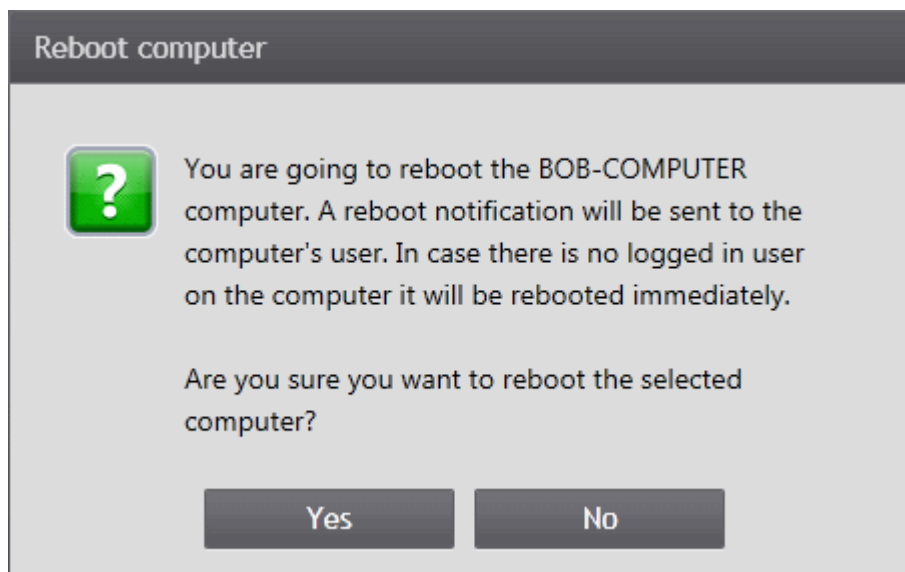
Any user that is logged in will be shown the following message:
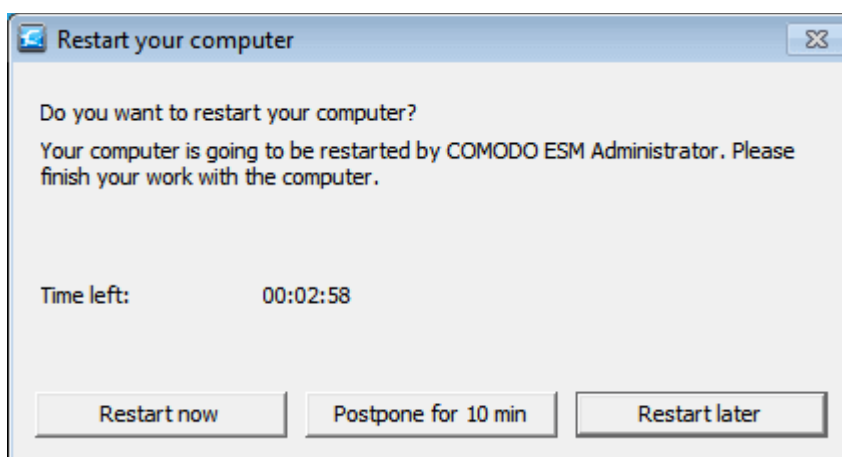
- The machine will automatically restart when the countdown finishes unless the user selects one of the options shown above.
- To shutdown the endpoint, click 'Shutdown'. If no user is logged in then the endpoint will be shut down immediately.
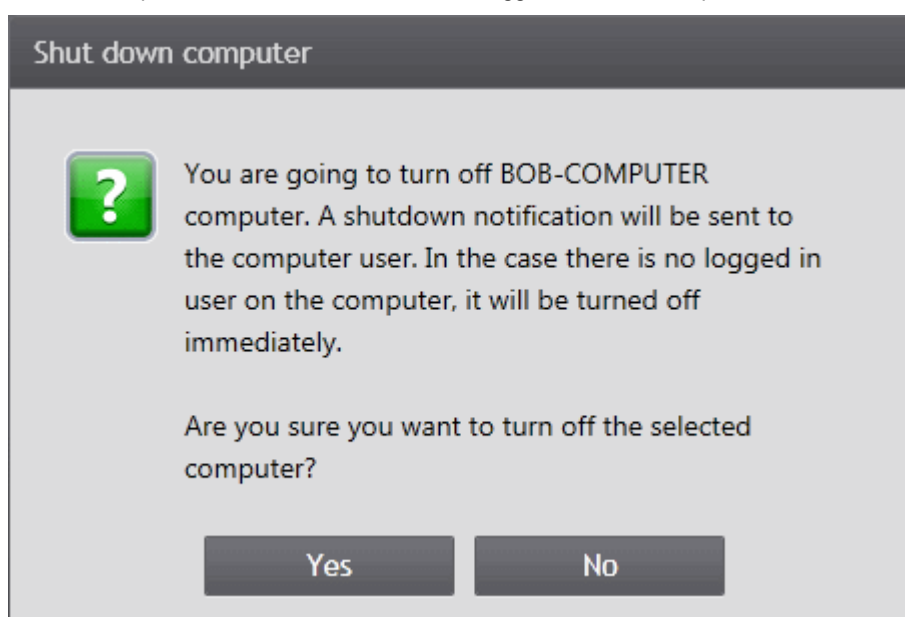
Any user that is logged in will be shown the following message:
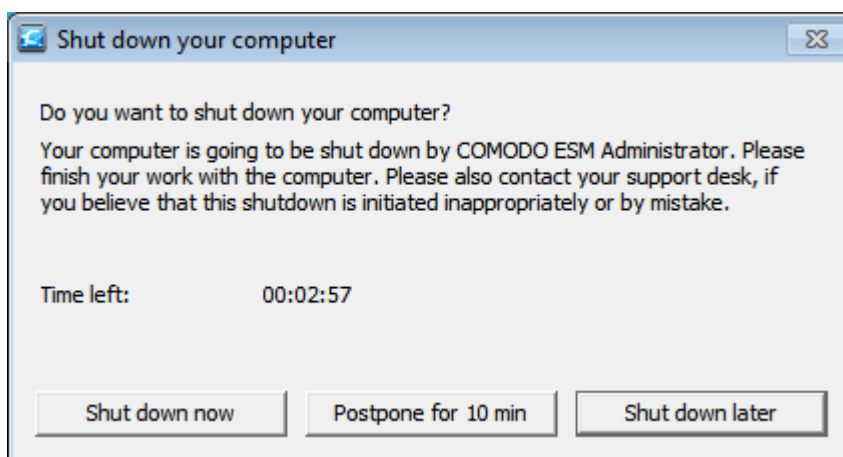
- • The machine will automatically shut down when the countdown finishes unless the user selects one of the options shown above.

4. The Groups Area

Creating groups of computers allows an administrator to split large networks up into convenient and/or logical groupings. For example, an administrator may create groups of computers called 'Sales Department', 'Accounts Department' , 'Vista Workstations', 'XP Workstations', 'Domain Controllers', '64 bit Machines' or 'All Managed Computers'. Subgroups can also be created for even greater granularity. For example, the group 'Windows 7 Workstations' may have two subgroups, '32 bit' and '64 bit'. Once created, an administrator can manage and execute tasks on all machines belonging to that group. For example:

- • Security policies can be applied to all endpoints in a group or subgroup.

- • Antivirus scans can be run on all endpoints in a group or subgroup.

- • Antivirus signatures can be updated for all endpoints in a group or subgroup.

- • Reports can be generated for all endpoints in a group or subgroup.

CESM ships with a default group called 'Unassigned'. Newly imported computers which are yet to be assigned to a specific group will be added to the 'Unassigned' group.

To open the Groups area, choose 'Groups' from the drop-down at the top left of the administrative console.

Column Heading	Description
Group	Displays the name of the group and the subgroup.
Computers Count	Displays the number of endpoints in the group and the subgroup.
Local Policy	Indicates the security policy applied to the endpoints connected to CESM through the local network.
Internet Policy	Indicates the security policy applied to the endpoints connected to CESM through the Internet. For further reading on 'Policies', please see '**The Policies Area**'.

The 'Groups' area enables the administrator to:

- **Define groups and to add previously imported endpoint computers into them as desired**
- **Edit existing groups to add or remove endpoints and to change security policies applied**
- **Reorganize group(s) and sub group(s)**
- **Run on-demand scans on all endpoints in a selected group**
- **Update virus signature database on all the endpoints**
- **Generate reports on endpoints belonging to a group**

4.1. Creating New Groups and Importing Existing Endpoints

Administrators can create endpoint groups and subgroups as required, import computers into it and apply security policies in the Create Group wizard.

To create a new group / subgroup

1. Open 'Groups' area by selecting 'Groups' from the drop-down at the top left.

The existing Groups and the security policies applied to them will be displayed.
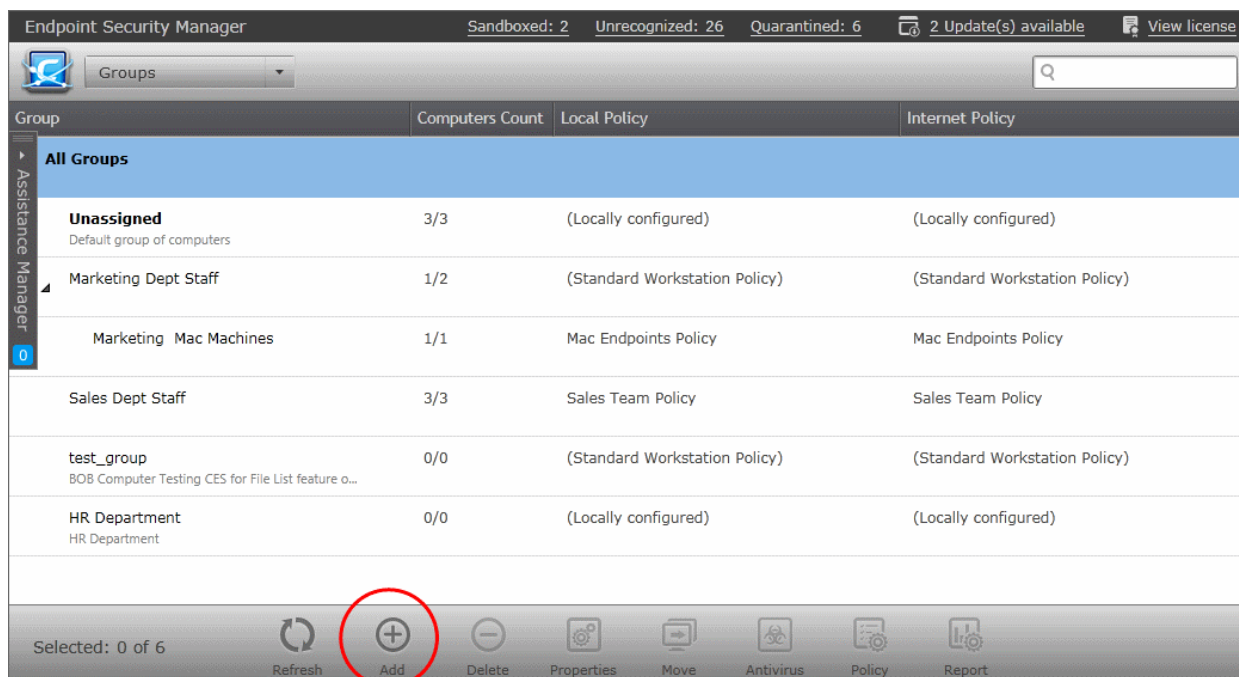
2. To add a new top level group, click 'All Groups' and 'Add' from the bottom of the screen.

3. To add a new subgroup, click on the parent group under which you want to add a subgroup and click 'Add' from the bottom of the screen.
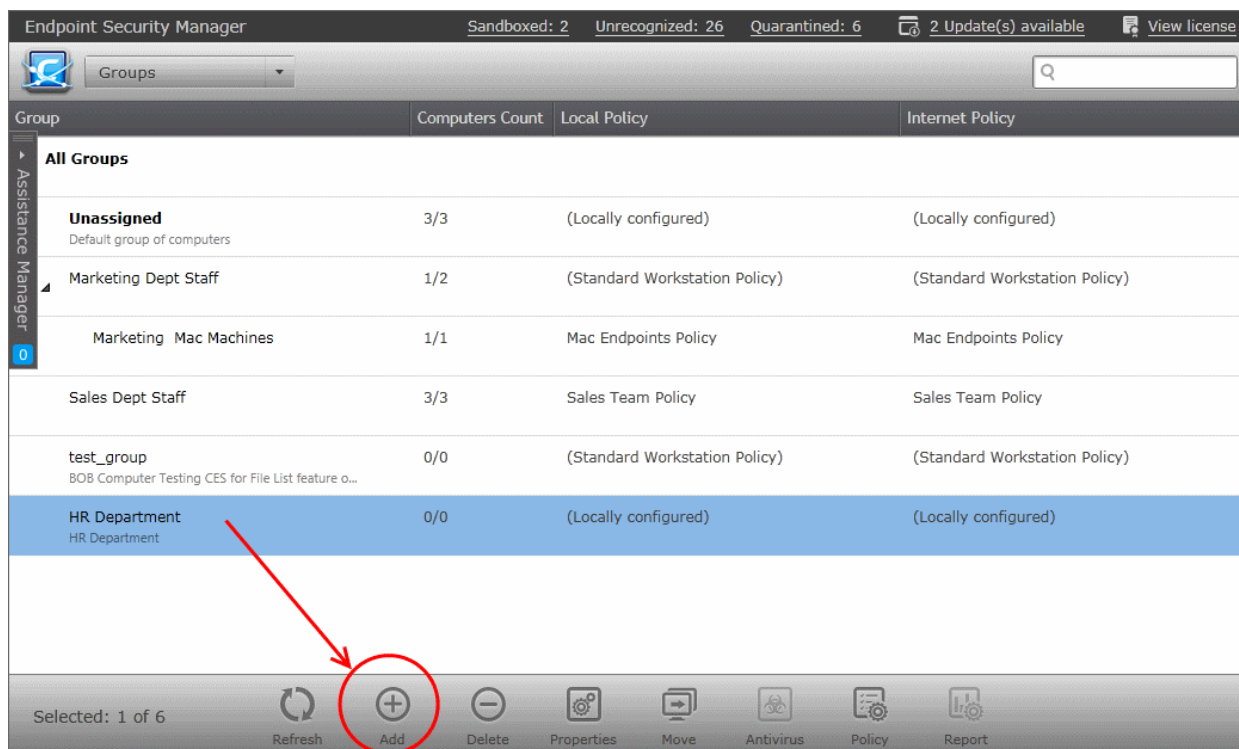
Step 1 - Naming the group and Defining Security Policies

The dialog for creating a new group will be displayed.

- Enter a name as the group has to identified by CESM in the 'Name' text field.

- Enter a short description for the created group in the 'Description' text field. This description will appear in the 'Groups' area Interface.

Next step is to specify the Local and Internet connection security policies for the member endpoints of the group.

The specifics of each policy are set in the Comodo Endpoint Security software in one endpoint and can be imported and applied to other endpoints. The 'Policy Options' allows the administrator to assign a local security policy and Internet security policy for the CES installations in the endpoints of the group from the policies that are previously imported into CESM. Refer to **Creating a New Security Policy** for more details on importing policies into CESM from the configurations made in the individual endpoints.

- Select a local security policy and Internet security policy from the respective drop-downs.

- Click 'Create Group' after selecting the security policies for the group.

The newly created group / subgroup will be displayed in the 'Groups' area.

Step 2 - Selecting Computers

The next step is to add endpoints to the newly created group / subgroup.

- Select the group and click on 'Properties' at the bottom of the screen.
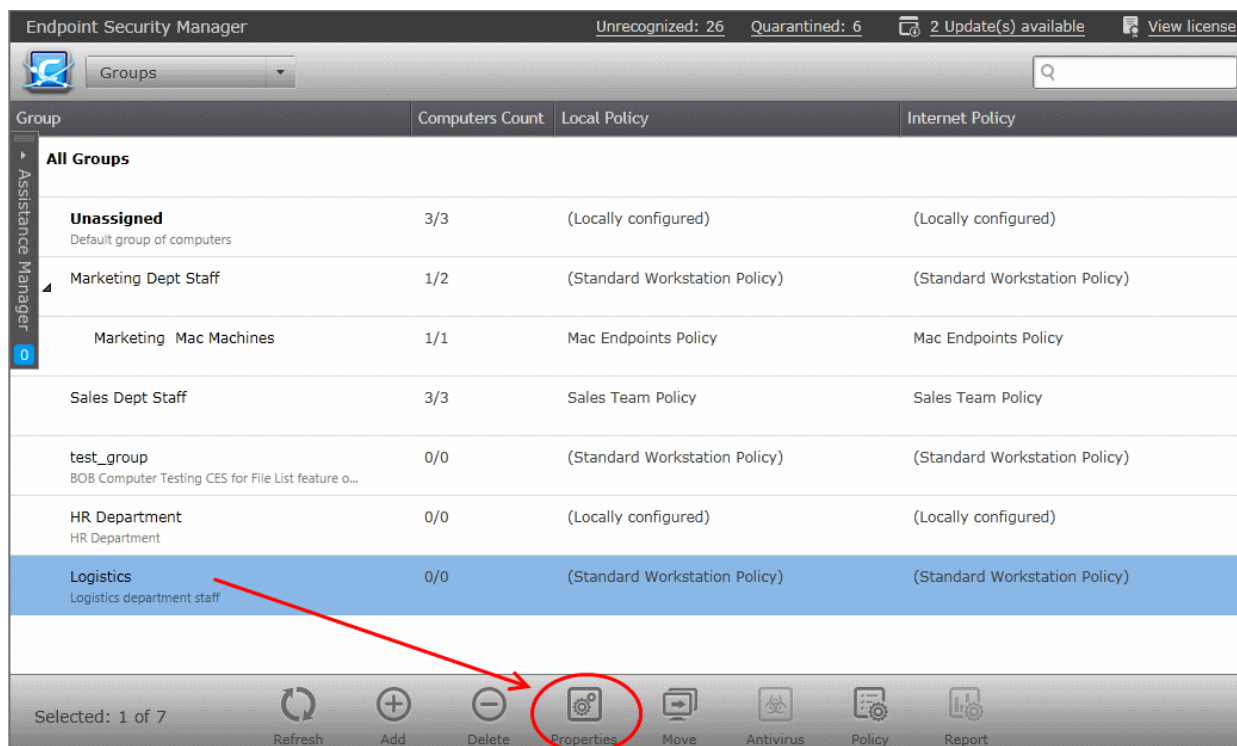
- In the Properties area of the selected group, click on Computers.

All the computers managed by CESM will be displayed as a list with their IP address and existing group details.
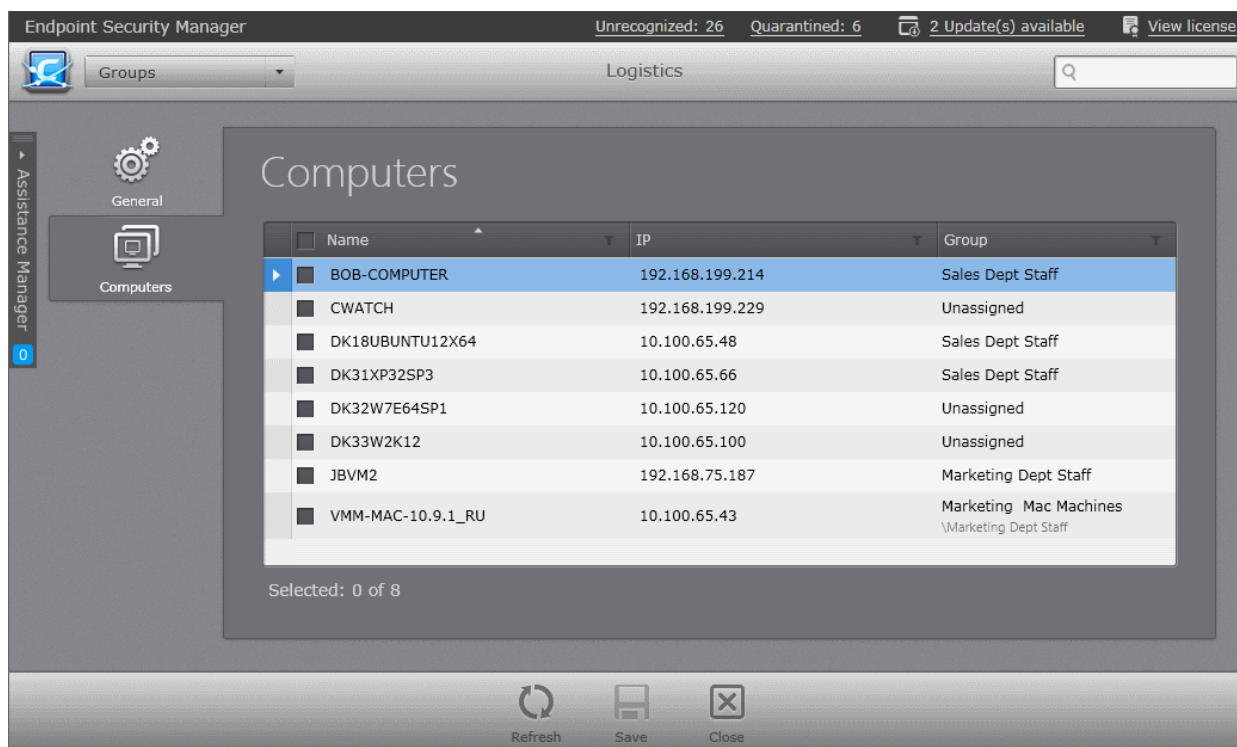
- Click the filter icon ▼ in the 'Name' column header to search for a particular endpoint and click 'Apply'.

- Click the filter icon ▼ in the 'IP' column header to search for endpoints with particular IP(s) and click 'Apply'.
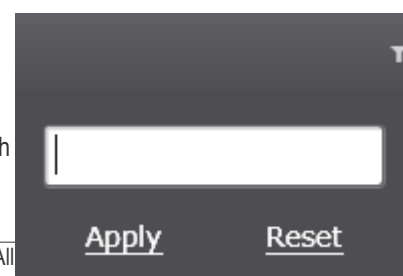
- • Click the filter icon ⊤ in the 'Group' column header to search for endpoints belonging to a specific group and click 'Apply'.
- • Select the endpoint computers to be added to the new top level group or subgroup and click on the 'Save' button at the bottom of the screen.

The selected endpoints will be assigned to the new group and will be applied with the security policy as chosen in step 2.

> **Note**: The endpoints and policies for the groups or subgroups can be changed any time from the properties screen. Refer to the section '**Viewing and Managing Groups**' for more details.

4.2. Viewing and Managing Groups

The Group Properties interface provides the system administrators with the ability to view and manage groups/sub groups and their member computers. The interface displays all defined groups and the managed endpoints within each group.

From this interface the administrator can:

- • View a summary on details such as security policy applied and the member endpoints of the selected group or sub group.
- • Drive the CES installations of endpoints in local administration mode to remote administration mode.
- • Edit a 'Group' or 'Sub Group' to rename, add or remove member endpoints and to change default security policies assigned to the endpoints.
- • Generate reports for the endpoints belonging to a group or sub group as a single file.

To access the 'Group Properties' interface

1. Open 'Groups' area by selecting 'Groups' from the drop-down at the top left.

The existing Groups and the security policies applied to them will be displayed.

2. Click the down arrow beside a group to open the tree structure of its sub groups.

3. Open the Group Properties interface for a selected group or sub group by:

- • Selecting the Group and clicking 'Properties' from the options at the bottom; or
- • Right clicking on the Group and selecting 'Properties' from the context sensitive menu.
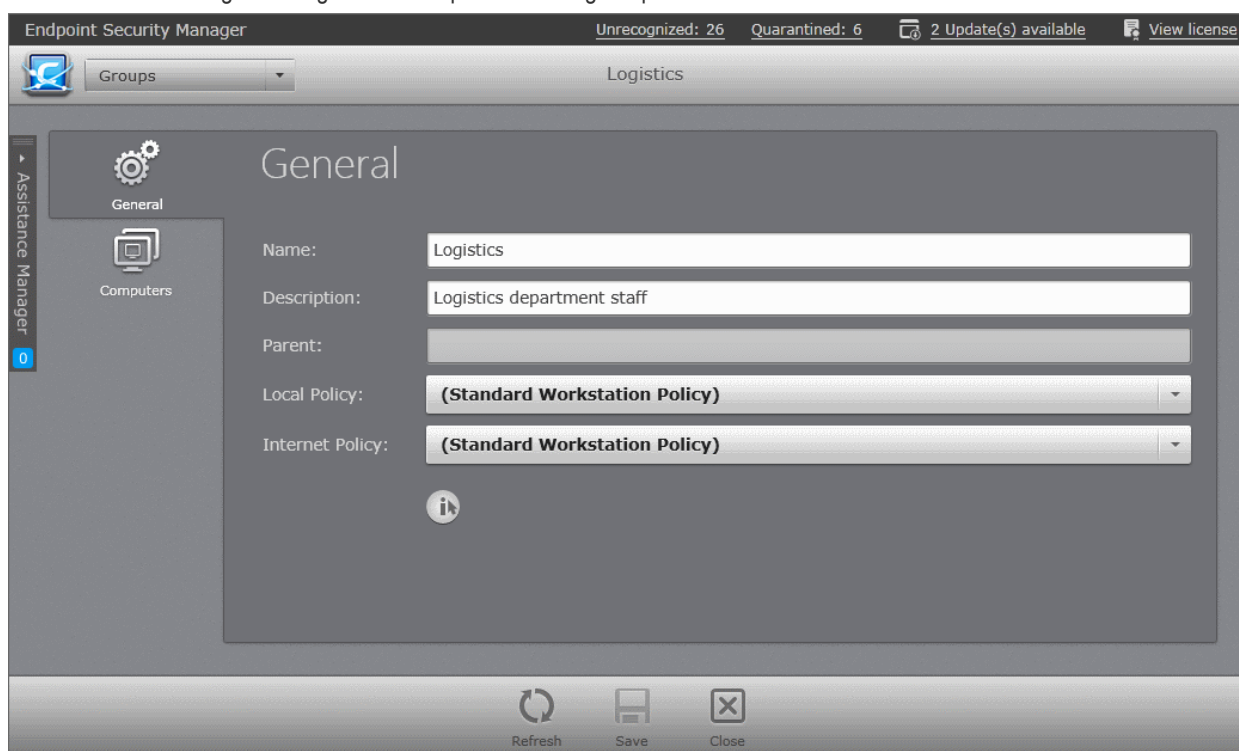
The 'Group Properties' screen contains two tabs:

- **General Screen** - Displays the name, description and default policies assigned to the group and enables the administrator to edit those details.

- **Computers Screen** - Displays the list of all endpoint computers added to CESM, with the members of the group preselected, allowing administrator to add more computers to the group and remove existing members. Computers that are removed from a specific group but are not re-assigned to another named group, will be automatically added to the 'Unassigned' group.

Viewing General Properties of a Group or Sub group

The General Properties screen displayed by clicking the 'General' tab from the left hand side navigation, shows the name and description of the group or the sub group and allows the administrator to rename the group if required. If it is a sub group, the screen displays the parent to which the sub group belongs. Also, it displays the default local connection mode and internet connection mode security policies applied to the member endpoints of the selected group and allows the administrator to change them.
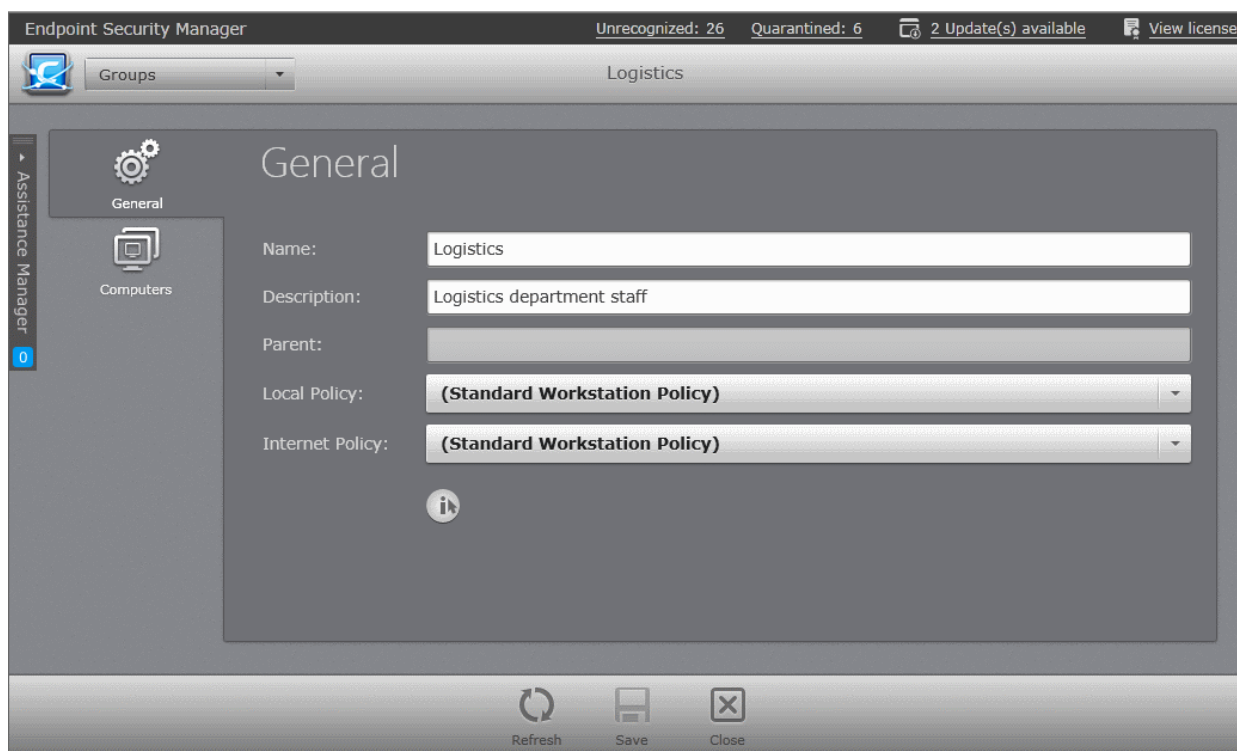
- To change the name of the group, directly edit the 'Name:' text field.

- To change the description of the group, directly edit the 'Description:' text field.

- To change the default security policy applied to the member endpoints in local connection mode, select the mode from the 'Local Policy' drop-down.

- To change the default security policy applied to the member endpoints in Internet connection mode, select the mode from the 'Internet Policy' drop-down.

Alternatively, you can change the default security policy of a group or a sub group directly by right clicking on it and selecting 'Apply Local Policy' or 'Apply Internet Policy' from the context sensitive menu and choosing the required policy from the sub menu or select the Group or sub group, click Policy > 'Apply Local Policy', 'Apply Internet Policy', apply 'Both Policies' and choosing the required policy or 'Reapply Policy'.
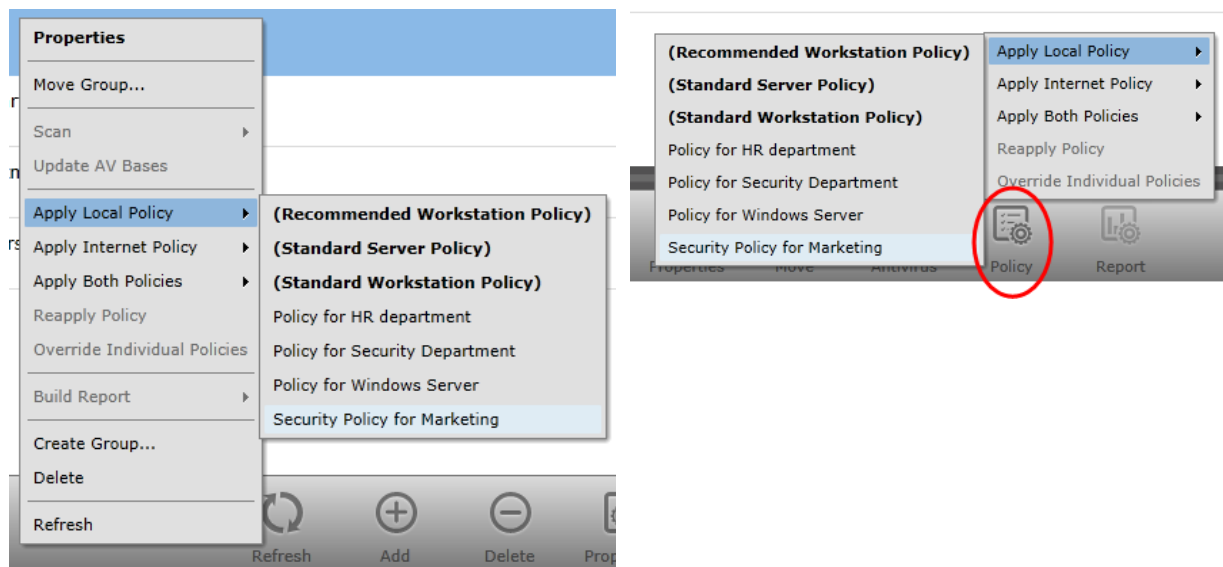
- Click 'Save' for your changes to take effect.

Adding or Removing Endpoints from a Group or Sub group

The Computers screen, displayed by clicking the Computers tab from the left hand side navigation, shows a list of all the computers added to CESM along with details of the group or sub group they belong to, IP address. Endpoints that are member of the selected group are preselected.
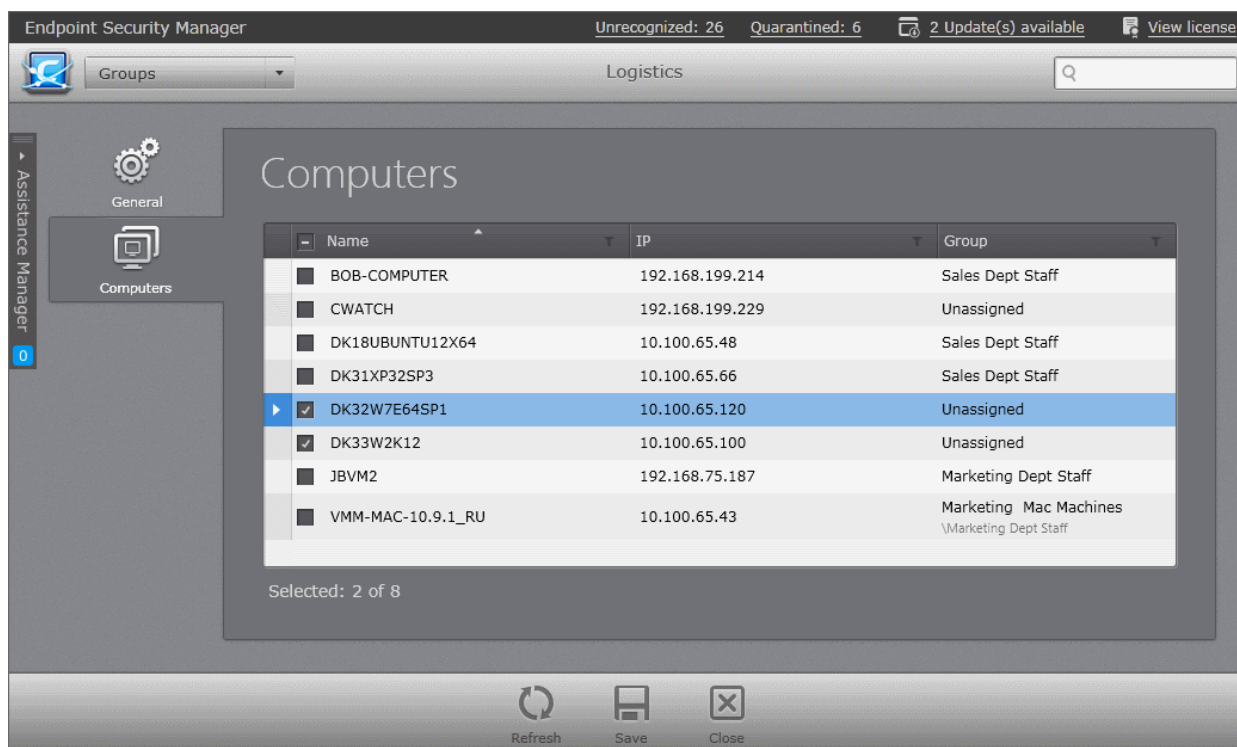
- To add new member endpoint from a different group or 'Unassigned' group, select the endpoint.
- To remove an endpoint from the group de-select the endpoint.
- Click 'Save' for your changes to take effect.

Tip: You can move individual endpoints from one group to another from the Computers area. Refer to the section **Viewing and Managing Group and Security Policy Details** for more details.

4.3. Reorganizing Groups and Sub Groups

The administrator can change the hierarchy of endpoint groups and sub groups at any time, according to the changes in the Organization. The Groups interface allows the administrator to move sub group(s) belonging to one group to other or to even to move a group as a sub group to other group as per the desired hierarchy. If a top level group is moved as a sub group to another group, its sub groups will also move with the top level group.

To move a group or sub group

1. Open 'Groups' area by selecting 'Groups' from the drop-down at the top left.

The existing Groups and the security policies applied to them will be displayed.

2. Click the down arrow beside a group to open the tree structure of its sub groups.

3. Select the group(s) or sub group(s) to be moved. Press and hold the Shift or Ctrl key from the keyboard, to select multiple items.

4. Click the 'Move' from the options at the bottom.

Alternatively, right click on the group/sub group and choose 'Move Group' from the context sensitive menu.
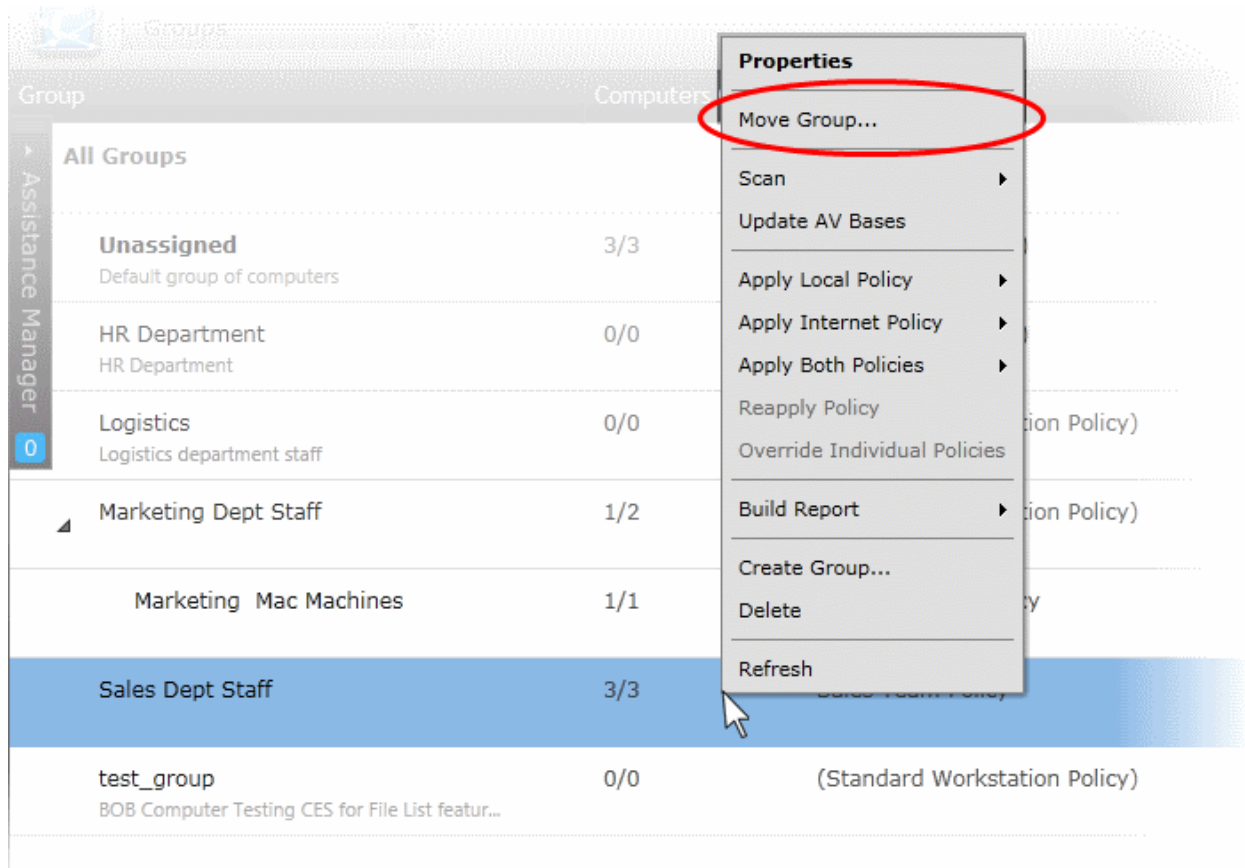
The 'Move Groups' interface will open.
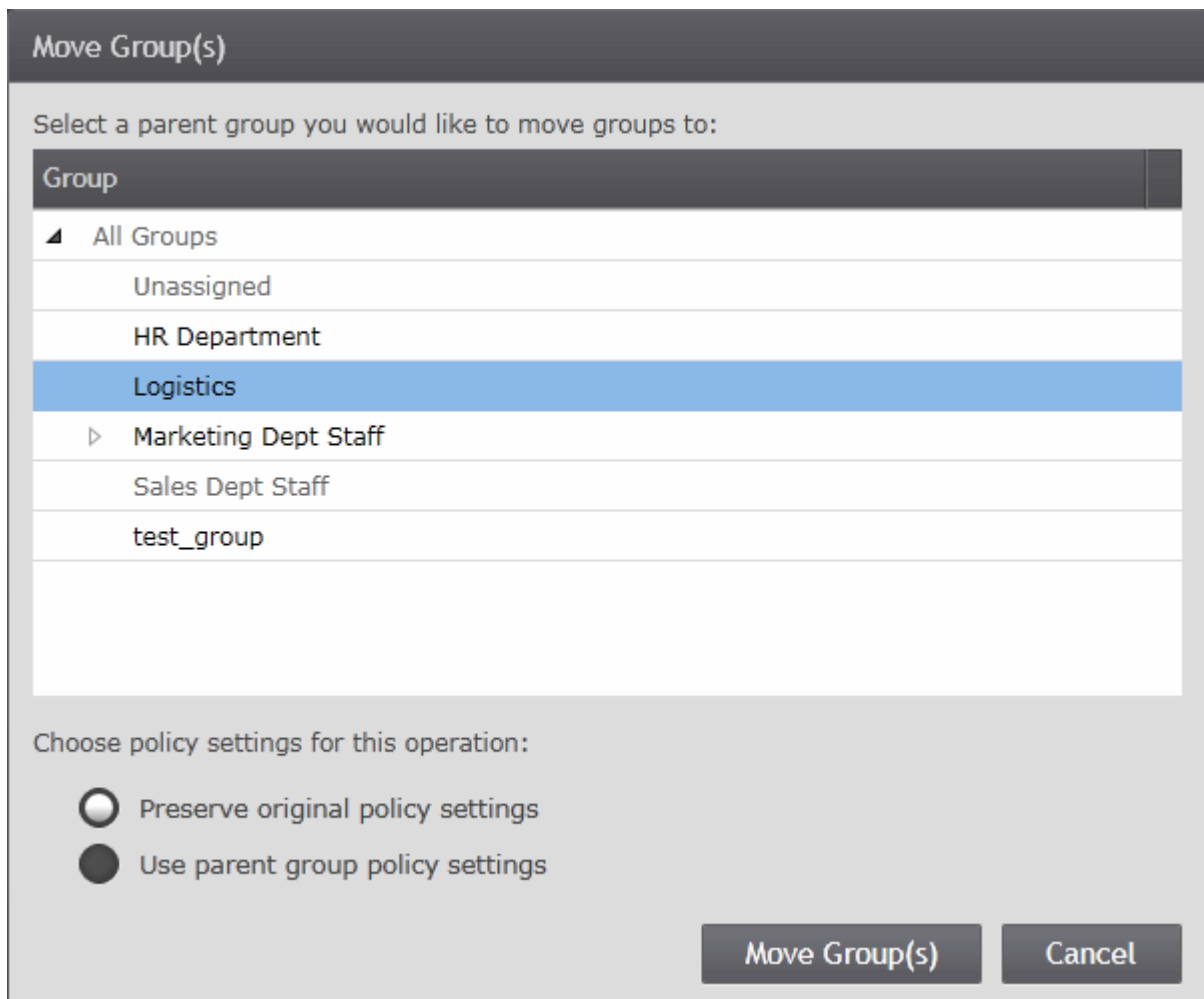
- Choose the group or sub group, to which the group(s)/sub group(s) selected in the previous step is/are to be moved as sub group(s)

- Choose the Policy Settings for the moved group(s)/sub group(s)

    - **Preserve original policy settings** - The member endpoints of the moved groups/sub groups will continue to be applied with the policy settings of the respective groups/sub groups to which they are the member of.

    - **Use parent group policy settings** - The member endpoints of the moved groups/sub groups will be applied with the policy settings of the new parent group immediately.

- Click 'Move Groups'

The selected group(s)/sub group(s) will be immediately moved to the new parent.

4.4. Running On-Demand Scan on Endpoint Groups

The 'Groups' area allows the administrator to run on-demand Antivirus (AV) scans on all the endpoints in selected group(s) or sub group(s) simultaneously. The administrator can choose to run a full scan or selected areas of the endpoints, by choosing a scan profile.

To run a full scan on the endpoints

1. Open the 'Groups' area by choosing Groups from the drop-down at the top left. To open the tree structure view of the sub groups, click the down arrow beside a group.

2. Select the group(s)/sub group(s) whose endpoints are to be scanned. You can select multiple groups at once by pressing and holding the Ctrl or Shift key.

Note: You can select only the Groups with endpoints having CES/CAS installed and AV enabled and Mac OS X based endpoints with CAV for Mac installed and enabled.

3. Click 'Antivirus' > 'Scan' > Full Scan/Quick Scan from the options at the bottom.

A Full Scan or Quick Scan of the endpoints will be commenced immediately. You can view the progress at the '**Computers**' area.

The administrator can also run the scans from the right click options with choices to select the areas to be scanned in the endpoints.

To run scan on selected areas of endpoints in a group

1. Open the 'Groups' area by choosing Groups from the drop-down at top left. To open the tree structure view of the sub groups, click the down arrow beside a group.

2. Select the group(s)/sub group(s) whose endpoints are to be scanned. You can select multiple groups at once by pressing and holding the Ctrl or Shift key.

Note: You can select only the Groups/Sub group(s) with endpoints having CES/CAS installed and AV enabled and Mac OS X based endpoints with CAV for Mac installed and enabled.

3. Right click and select 'Antivirus Scan' > 'Scan' from the bottom or right- click on the selected endpoint.
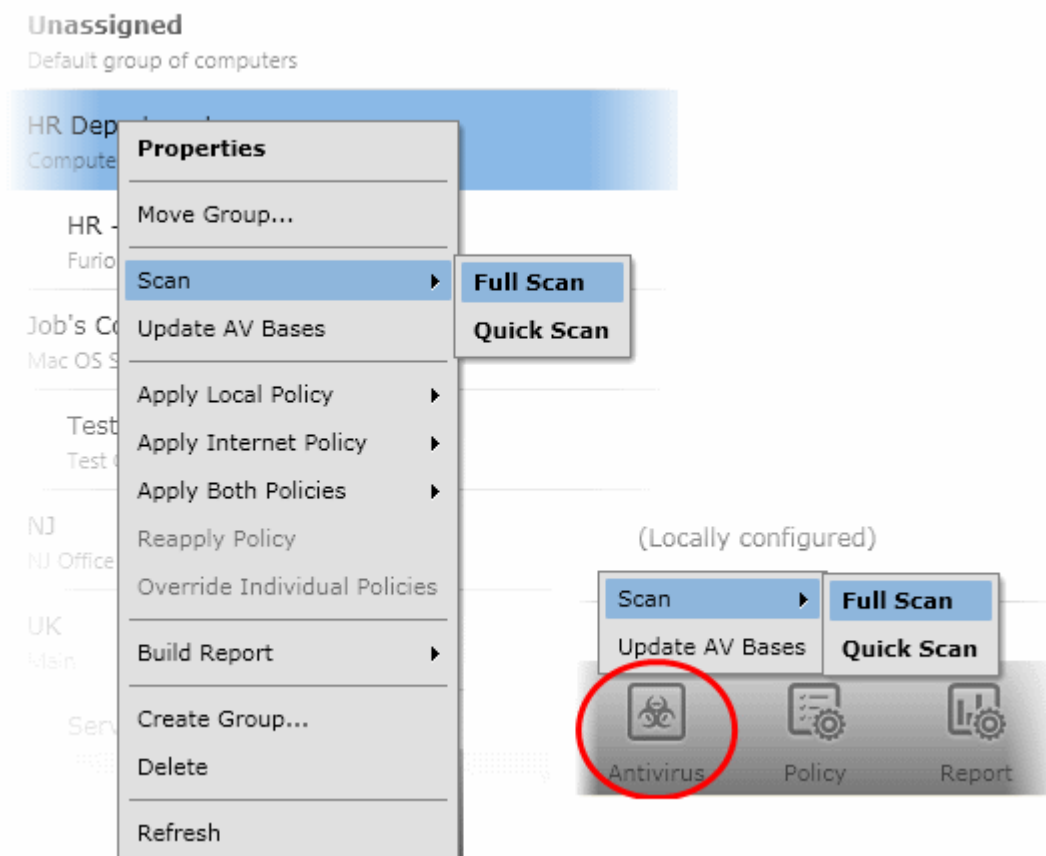
4. Select the Scan Profile from the drop-down, depending on the areas to be scanned on the endpoints. The default scan profiles are:

    •   **Full Scan** - This profile covers every local drive, folder and file on the endpoints.

    •   **Quick Scan** - Covers critical areas in the endpoints which are highly prone to infection from viruses, rootkits and other malware. This includes system memory, auto-run entries, hidden services, boot sectors, important registry keys and system files. These areas are responsible for the stability of the computer and keeping them clean is essential.

    •   More scan profiles can be defined in the following ways:

        •   Creating custom scan profiles while creating/editing a security policy and applying it to the groups. For more details, refer to the section **Creating a Custom Scan Profile**.

        •   Creating a custom scan profile at an endpoint, importing its CES/CAS settings while creating a security profile and applying it to selected groups. For more details on creating scan profiles, please refer to CES online help guide at **http://help.comodo.com/topic-84-1-499-5558-Scan-Profiles.html**.

The on-demand scan will be started on the selected endpoints and the progress will be displayed in the 'Computers' area.

On completion of scanning:

    •   If malware is discovered during the scan that is not handled successfully (deleted, disinfected or quarantined) then the endpoint will be indicated as Infected in the 'Computers' area.

The results of the scan can be viewed as an Infection report from the Reports area - click 'Reports' then the 'Computer Infections'. The report can also be exported as a pdf file or a spreadsheet file for printing purposes. Refer to **Reports > Computer Infections** for more details.

4.5. Updating Virus Signature Database on Endpoint Groups

The 'Groups' area allows the administrators to update the virus signature database on all the endpoints in selected group(s) or

sub group(s), identified as outdated computers.

To update endpoints in a group

1. Open the 'Groups' area by choosing Groups from the drop-down at the top left. To open the tree structure view of the sub groups, click the down arrow beside a group.

2. Select the group(s)/sub group(s) whose endpoints are to be updated. You can select multiple groups at once by pressing and holding the Ctrl or Shift key.

Note: You can select both the Groups/Sub group(s) with Windows based endpoints having CES/CAS installed and AV enabled and Mac OS X based endpoints with CAV for Mac installed.

3. Click Antivirus> 'Update AV Bases' from the bottom or right click on a selected group and choose 'Update AV Bases' from the context sensitive menu.

The Progress will be displayed in the **Computers** area...

… and on completion, the virus signature database at the endpoints will be made up-to-date.

4.6. Generating Reports for Selected Group

The Groups area allows the administrators to generate various reports on all the endpoints in a group or a sub group as a single file. The generated report can be accessed from the **Reports** area.

To generate reports on the endpoints in a group

1. Open the 'Groups' area by choosing Groups from the drop-down at the top left. To open the tree structure view of the sub groups, click the down arrow beside a group.

2. Select the group(s)/sub group(s) for which you wish to generate report. You can select multiple groups at once by pressing and holding the Ctrl or Shift key.

3. Click 'Report' and select the type of report to be generated. Alternatively, select the group(s)/sub group(s), right click, choose 'Build Report' from the context sensitive menu and select the report to be generated.

The report generation will be started and the progress will be displayed in the Reports area.
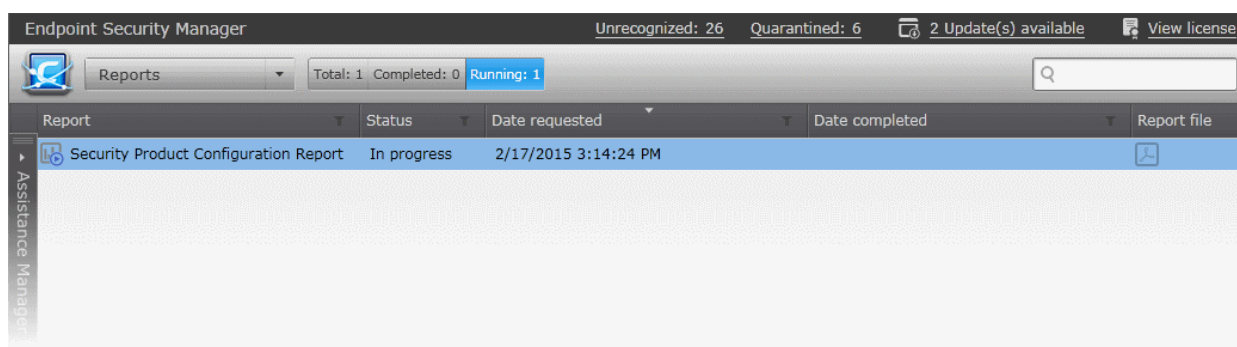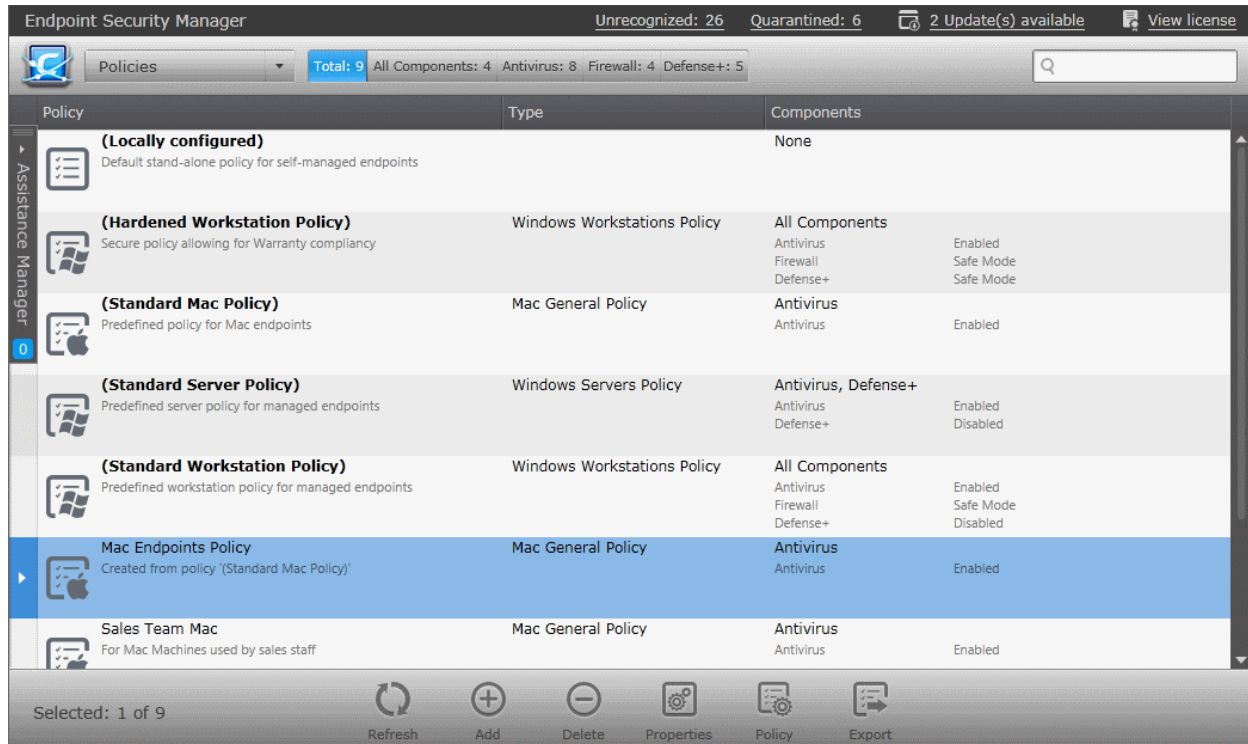
On completion, the administrator can download the report from the Reports area. Refer to the section **The Reports area** for more details.

5.The Policies Area

A policy is a security configuration of endpoint security software, Comodo Endpoint Security (CES),

Comodo Antivirus for Servers (CAS) or Comodo Antivirus for Mac OS (CAVM) which can be deployed on an endpoint or a group of endpoints. Each policy determines the antivirus settings, Internet access rights, firewall traffic filtering rules, Defense+ application control and system settings for an endpoint.

The 'Policies' area allows administrators to view and edit all available policies, to create and apply custom policies and to import/export policies.

CESM ships with five pre-defined policies which can be applied to groups or endpoints and servers as required. 'Locally Configured' is the default policy which is applied when endpoints are first imported.

- *Locally Configured (default)*. 'Locally Configured' means that CES/CAS/CAVM settings can be managed by the local user and policy compliance will not be enforced by CESM. Machines or groups with this policy will always report a compliance status of 'OK'. Changes made to the security product settings on to the machine with 'Locally Configured' policy are dynamically stored in the policy. If a machine is switched to 'Locally Configured' from a different policy, then the last settings stored in the 'Locally Configured' policy will be restored.

- *Hardened Workstation Policy*. Highly secure policy for managed workstations running Comodo Endpoint Security installed on Windows based workstations. This policy must be implemented if your organization wishes to take advantage of the warranty.

- *Standard Mac Policy*. The standard workstation policy contains settings which are optimized for Comodo Antivirus for Mac OS (CAVM) installed on Apple Mac OS based Workstations. The policy is not applied to any group or endpoint by default.

- *Standard Server Policy*. The standard server policy contains settings which are optimized for Comodo Antivirus for Servers (CAS) installed on Windows Servers. The policy is not applied to any group or endpoint by default.

- *Standard Workstation Policy*. The standard workstation policy contains settings which are optimized for Comodo Endpoint Security (CES) installed on windows Workstations. The policy is not applied to any group or endpoint by default.

The following sections are intended to provide details explanations on:

- **Creating a new policy** - A step-by-step wizard that takes admins through the policy import, specification and deployment process.

- **Viewing and managing security policies** - Guidance to administrators on viewing, reconfiguring and exporting ESM polices.

Before proceeding with creating a policy, read the 'Key Concepts' section below to gain a baseline understanding first.

Policies - Key concepts

- Policies are security settings for the installed components of CES/CAS/CAVM configured and tested on a local machine via the standard CES/CAS/CAVM interface. Policies can be applied to individual endpoints and groups of endpoints. If you add an endpoint to a group, then the endpoint will adopt the group policy.

- Policies can be imported from an endpoint into the ESM console then applied to target computers or groups of computers. The machine chosen for this purpose can be considered a template of sorts for other equivalently configured machines in the organization (i.e. having the same hardware/software - a computer used to image other endpoints in the organization is ideal for this purpose). This allows admins to create a 'model' configuration on one machine that can be rolled out to other computers.

- Policies can also be created by:
    - Importing CES/CAS configuration from a previously saved .xml file or image.
    - Importing an existing policy to use as the starting point for a new policy.

- Policies can be named according to criteria deemed suitable by the administrator. For example, policies based on security levels could be named 'Highly Secure', 'Medium Security' and 'Low Security'.

- At the administrator's discretion, a policy can cover settings for all or only some of the three CES components that may be installed on an endpoint:- Antivirus, Firewall, and Defense + settings and system settings:- Power and Device settings management. A policy which excludes settings for one of the CES/CAS/CAVM components installed on the endpoint receiving policy is considered as locally configured (see below) for the settings of that component.

- The ESM agent installed at each endpoint is responsible for connecting the target machine to the respective ESM server and the remote management of the CES/CAS/CAVM installation. Only the agent applies the security policy settings to different components of the application and checks whether the application is compliant to policy.

- Each endpoint has two types of policy assigned to it - 'Local Policy' and 'Internet Policy':
    - A 'local policy' is the CES/CAS/CAVM security settings that will apply when the endpoint is within the local network.
    - An 'Internet policy' is automatically applied when the endpoint connects to ESM from an IP address outside the local network.

- Policy, as mentioned earlier, refers to the actual security configuration of CES/CAS/CAVM. An endpoint can have any chosen policy and can be in either 'Remote' or 'Local' mode.

5.1. Creating a New Security Policy

The 'Create Policy' wizard enables administrators to create new security policies and to apply them to groups of target computers. Policies can be created by:

- Creating a completely new policy. Administrators have the option to import local security settings as a basis for the new policy.

- Using another, pre-existing, policy as a base.

- Importing policies from a .xml file.

Policies can be created according to the security requirements of different groups of computers which are in turn, created according to the requirements of the organization. So it is recommended to first create groups and then to create policies, so that the policies can be applied to the groups as required.

It is also recommended to retain the group 'Unassigned' with the 'Locally Configured' policy until all the computers have been imported into ESM, so that ESM will not overwrite the policy on new discovered computers once the agent is installed in it.

The following sections explain in detail on:

- **Creating a New Security Policy for Windows based endpoints**

- **Creating a New Security Policy for MacOS based endpoints**

5.1.1. Creating a New Security Policy for Windows Based Endpoints

There are eight steps involved in creation of a security policy for Windows based workstations. The steps are displayed below the title bar with the current step highlighted in bold. To move backwards or forwards between steps, use the arrows on either side of the main interface (or left click and drag to swipe the screens left or right) or click a step with a click-able active link below the title bar.

To start the 'Create Policy' wizard

- Select 'Policies' from the drop-down at the top left.

- Click 'Add' from the 'Policies' area.

The wizard will start with Step 1- Creation Method.

Step 1 - Choose the creation method

The new policies can be created from three types of sources:

- **Computers** - Imports the security settings configured locally from a selected source computer to create a new policy.

- **Another Policy** - Enables to choose an existing policy and use it as the starting point to create a new policy.

- **A saved Policy XML file** - Imports the policy from the policy xml file from the computer running the administration console.

Explanations on importing from different source types can be found in the following sections: **Importing from Computers, Importing from Another Policy** and **Importing from XML File**.

- Select the source type and click the right arrow to move to step 2.

> **Tip:** You might create a policy from another policy if you want to exclude a CES/CAS component from policy but use the settings in other components, or change the agent-specific settings of the policy (such as to have a different compliance polling interval, or to disallow local mode access) for a particular endpoint or group).

Importing from Computers

- Choose 'Create New' if you wish to import the security settings from a target endpoint as the new policy and click the right arrow to move to Step 2 - Import Settings from another Computer.

Step 2 - Import Settings from another Computer

All endpoint computers added to ESM will be displayed.

You can search for a specific endpoint using sorting, filtering and searching options:

- To switch the sorting of endpoint names in the 'Computer' column between ascending and descending orders, click the down arrow at the right of the 'Computer' column header.
- To search for a particular endpoint, click the funnel icon in the 'Computer' column header, enter the name of the endpoint in full or part and click 'Apply'.
- To search for an endpoint based on the group name, click the funnel icon in the 'Group' column header, enter the group name in full or part and click 'Apply'.
- To search for an endpoint with online or offline status, click the funnel icon in the 'Status' column header, select the status and click 'Apply'.
- To search for endpoint with based on installation state of the security product, click the funnel icon in the 'Security Product' column header, choose from 'Installed', 'Unsupported' or 'Not Installed' options and click 'Apply'.
- To remove a filter, click the funnel icon in the respective column header and click 'Reset'.

- Choose the computer from which you wish to import the settings. The computer should have CES/CAS installed and be in local mode, configured as per requirements, and should be online to enable ESM to import the settings.
- Click the right arrow to move to **Step 3 - Settings**.

Importing from Another Policy

- Choose 'Create from Another Policy' if you wish to import the security settings from an existing Policy and click the right arrow to move to Step 2 - Selecting Source Policy.

Step 2 - Selecting Source Policy

A list of all the existing policies with their descriptions and the configuration states of the security product components are displayed.

You can search for a specific policy using the filtering and searching options:

- To search for a particular policy, click the funnel icon in the 'Policy' column header, enter the name of the Policy in full or part and click 'Apply'.

- To search for a policy based on the enabled states of the components, click the funnel icon in the 'Components' column header, select the components and click 'Apply'.

- To remove a filter, click the funnel icon in the respective column header and click 'Reset'.

- Select the source policy from which you wish to create a new policy and click the right arrow to move to **Step 3 - Settings**.

Importing from a saved XML File

- Choose 'Create from XML file' if you wish to import the security settings from a previously saved policy xml file in the computer running the administration console. Click the right arrow to move to Step 2 - Selecting Source File.

Step 2 - Selecting Source File

- Click 'Browse' and navigate to the required policy XML file and click 'Open'.

- Click the right arrow to move to **Step 3 - Settings**.

Step 3 - Settings

The next step is to select the components of CES/CAS for which the security settings are to be imported into the policy.
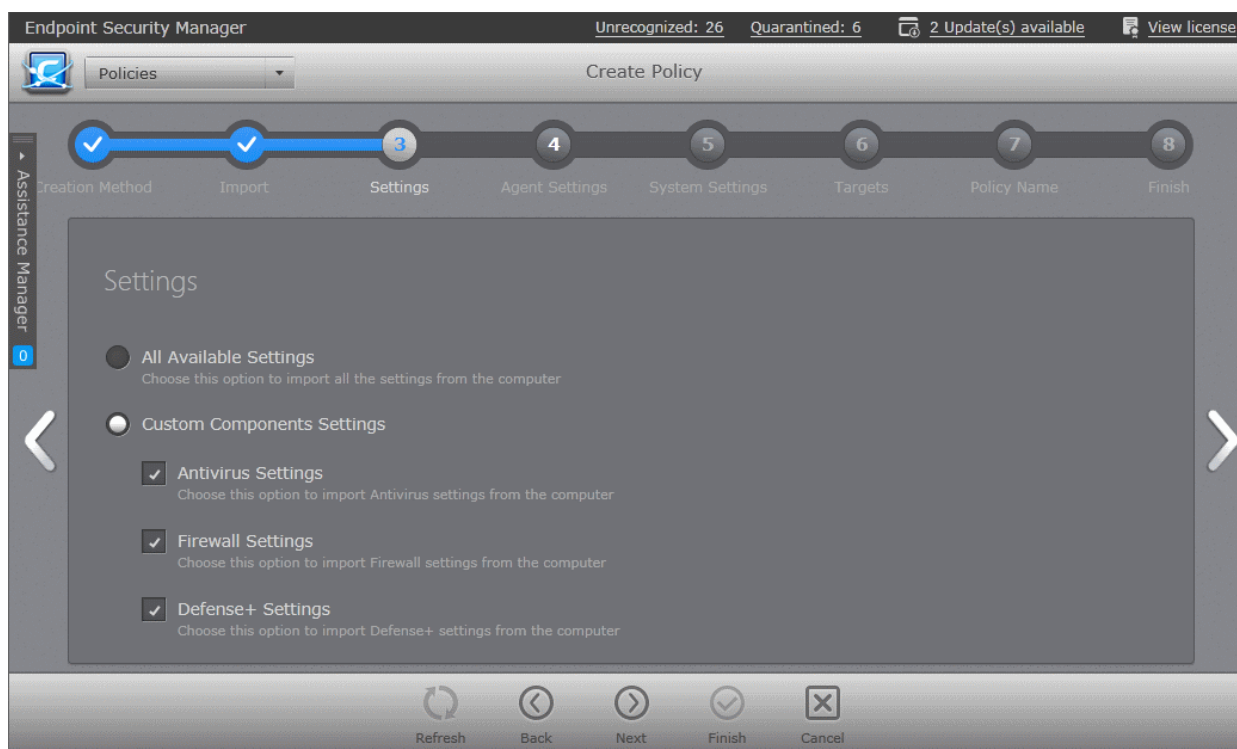
- **All Available Settings** - Imports all the settings from the source selected in the chosen step 2, above.
- **Custom components settings** - Enables the administrator to select the components of CES/CAS so that only those settings corresponding to the selected components are imported into the policy from the source selected in step 2.

- **Antivirus Settings** - Imports the settings relevant to the Antivirus component.
- **Firewall Settings** - Imports the settings relevant to the Firewall component.
- **Defense+ Settings** - Imports the settings relevant to the Defense+ component.
- Make your selections and click the right arrow to move to step 4 - Agent Settings.

Step 4 - Agent Settings

The next step allows the administrator to configure the ESM agent installed at the target computers, for which the policy has to be applied.
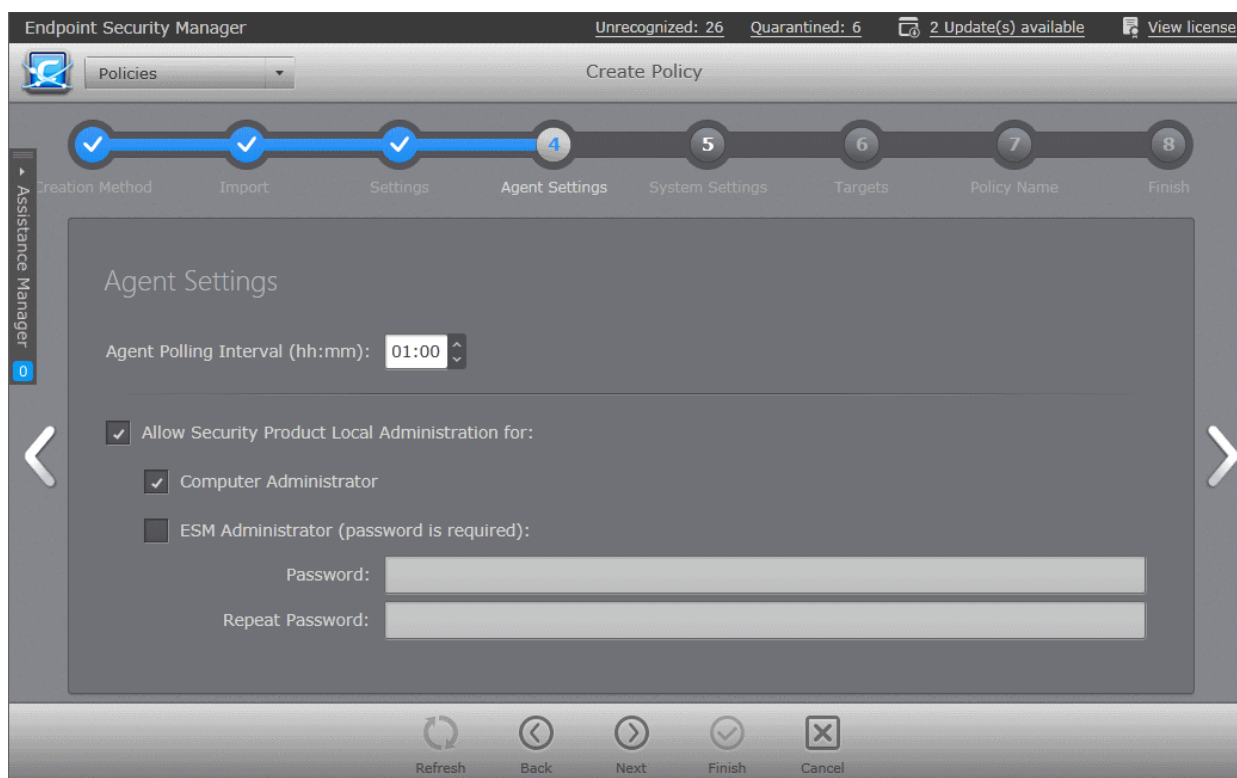
- **Agent polling interval** - The administrator can set the time interval (in hours and minutes) for the agent to periodically check whether the CES/CAS at the target computer is compliant with the applied security policy. The result will be dynamically displayed in the Policy Status tile and System Status - Compliancy status tile on the dashboard. (Default = 1 hour, up to but not including 24 hours).
- **Allow Security Product Local Administration for** - Configures the agent to allow the security product installation at the target machine to be switched to local administration mode should the user desire to change the security settings. The administrator may choose to not allow the user to alter the security settings in his/her computer, so as to not lead to a security hole in the network. On selecting the 'Allow Local Administration' check box, the administrator should specify how the access to local administration has to be restricted by selecting an option from the following check boxes:
    - **Computer administrator** - Selecting this option will require the computer user to either have administrative credentials or enter credentials while switching CES/CAS at the target machine to local administration mode.
    - **ESM Administrator (password is required)** - Allows the administrator to specify a password in the text box below this option. This password should be entered for switching the CES/CAS to local administration mode.
- Click the right arrow to move to the step 5 - System Settings.

Step 5 - System Settings

The next step allows the administrator to configure the system settings like power management, connectible devices management and resource monitoring settings to be deployed on to the target computers, for which the policy has to be applied.

- **Enable power options management** - Allows the administrator to configure power settings. On selecting the 'Enable power options management' check box, the administrator can specify the power settings from the options below:
    - **Turn off the display** - Allows the administrator to select the period after which the display will be switched off if the system is continuously idle. (Default = Never)
    - **Turn off hard disk** - Allows the administrator to select the period after which the hard disk will be turned off if the system is continuously idle. (Default = Never)
    - **System standby** - Allows the administrator to select the period after which the system will go into standby mode if the system is continuously idle. (Default = Never)
    - **System hibernates** - Allows the administrator to select the period after which the system will go into hibernation mode if the system is continuously idle. (Default = Never)
- **Enable device settings management** - The administrator can configure connectible device settings by the selecting this check box and from the options below:
    - **Disable USB mass storage devices(s)** - Selecting this option will disable connecting USB mass storage devices at the target computers. (Default = Not Selected)
    - **Disable optical device(s)** - Selecting this option will disable using optical disks like CD, DVD and Blu-ray disks at the target computers. (Default = Not Selected)
    - **Disable floppy device(s)** - Selecting this option will disable using floppy devices at the target computers.

(Default = Not Selected)

- **Enable System Monitoring** - Selecting this option makes CESM to generate alerts if the system resource usage crosses the thresholds configured in the options below. If the system resource usage exceeds the limits specified, the endpoint will be indicated as 'Overloaded'. The administrator can view the alerts generated, from the 'Computer Properties' > 'Monitoring Alerts' pane. Refer to the section **Viewing System Monitoring Alerts** for more details.

  - **Alert when CPU exceeds NN% usage for TT seconds** - Generates alert when the CPU usage at the target computer is continuously larger than the percentage specified in the slider for the time (in seconds) specified in the time drop-down combo box. The administrator can specify the maximum CPU usage allowance in the slider and the period in the drop-down combo box. (Default = 70% for 30 seconds)

  - **Alert when RAM exceeds NN% usage for TT seconds** - Generates alert when the system memory usage at the target computer is continuously larger than the percentage specified in the slider for the time (in seconds) specified in the time drop-down combo box. The administrator can specify the maximum system memory usage allowance in the slider and the period in the drop-down combo box. (Default = 70% for 30 seconds)

  - **Alert when network usage exceeds NN% usage for TT seconds** - Generates alert when the data traffic from/to the endpoint is continuously larger than the network utilization percentage specified in the slider, for the time (in seconds) specified in the time drop-down combo box. The administrator can specify the network usage limit in the slider and the period in the drop-down combo box. (Default = 70% for 30 seconds)

  - **Alert when there is less than NN% free space left on system drive** - Generates alert when the remaining space in the hard disk drive partition on which the Operating System is installed, reduces below the percentage of total partition size, specified in the slider. The administrator can specify the minimum amount of free space to be maintained in the system drive through the slider. (Default = 5%)

- Click the right arrow to move to the step 6 - Selecting Targets.

Step 6 - Selecting Targets

The administrator can select the target computer group(s) and/or sub group(s) onto which the created policy has to be applied. To open the tree structure view of the sub groups, click the down arrow beside a group.

- Check 'Assign policy to groups after finish' if you want to apply the newly created policy after it is imported to an existing group. You can also assign this policy at a later stage to groups if you do not want to do so now. See **Editing a Security Policy** section for more details.

- For the group(s)/sub group(s) of computers connected through the local network you wish to apply the new policy, select 'For Local Policy' check box.

- For the group(s)/sub group(s) of computers connected through the Internet you wish to apply the new policy, select 'For Internet Policy' check box.

- **Options**:

  - **Override individual computers policy after finish** - Selecting this option will apply the new policy onto computers that are currently in 'Non Compliant' status within the selected groups, upon completion of policy creation, even if 'Apply policy after finish' is not selected. For the other endpoints in the selected group, the new policy will be applied on the next polling time. (Default = Not Selected)

  - **Apply policy after finish** - Selecting this option will apply newly created policy to all it's targets, irrespective of their compliancy status, right after policy creation is finished. If this option is not selected, the new policy will be applied during the next polling time. (Default = Selected)

- Make your selections and click the right arrow to move to step 7 - Importing the Settings and Creating the Policy.

Step 7 - Importing the Settings and Creating the Policy

The next step requires the administrator to specify a name and provide a description for the policy created.
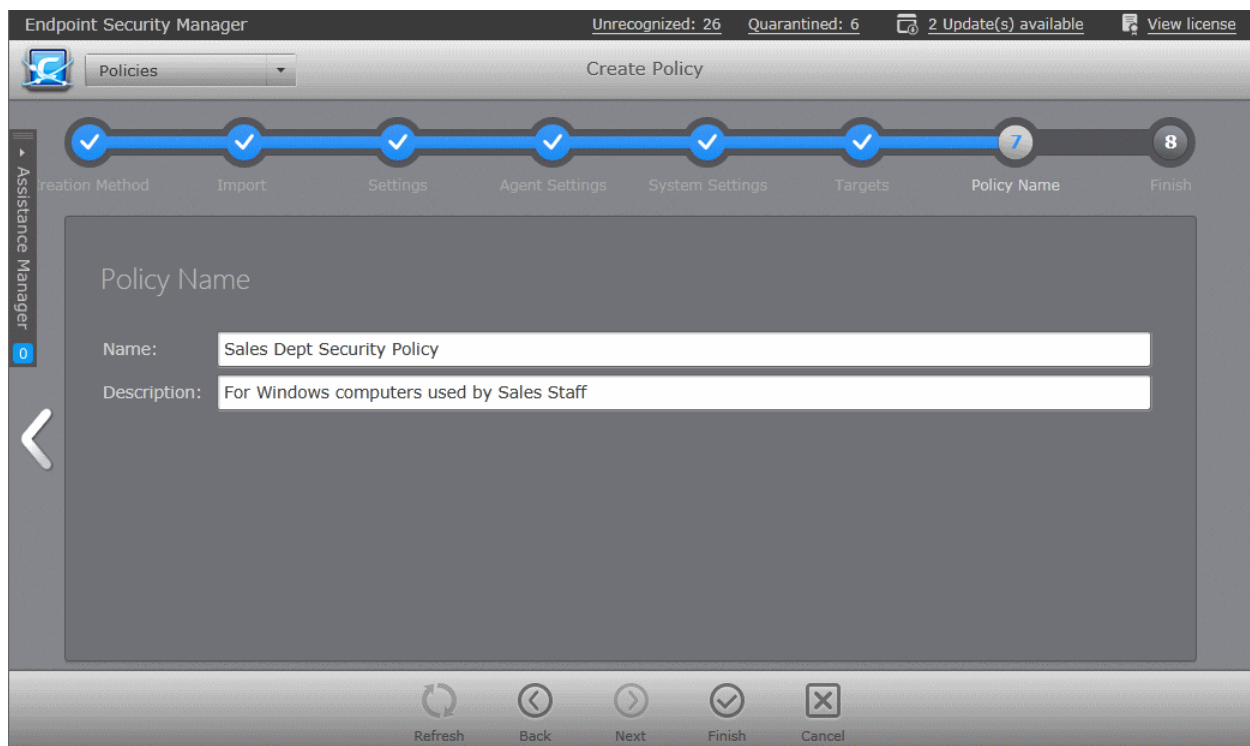
- **Name** - Enter a name according to criteria deemed suitable to the security settings.

- **Description** - Enter short text that best describes the policy.

- Click the 'Finish' icon ![icon], click step 8 from the navigation below the title bar or swipe the screen to left to complete the policy creation process. On completion:

  - The 'Policy' interface will open with the new policy added.

The new policy will be applied to the target computers selected in **step 6** as per the options selected in the same.
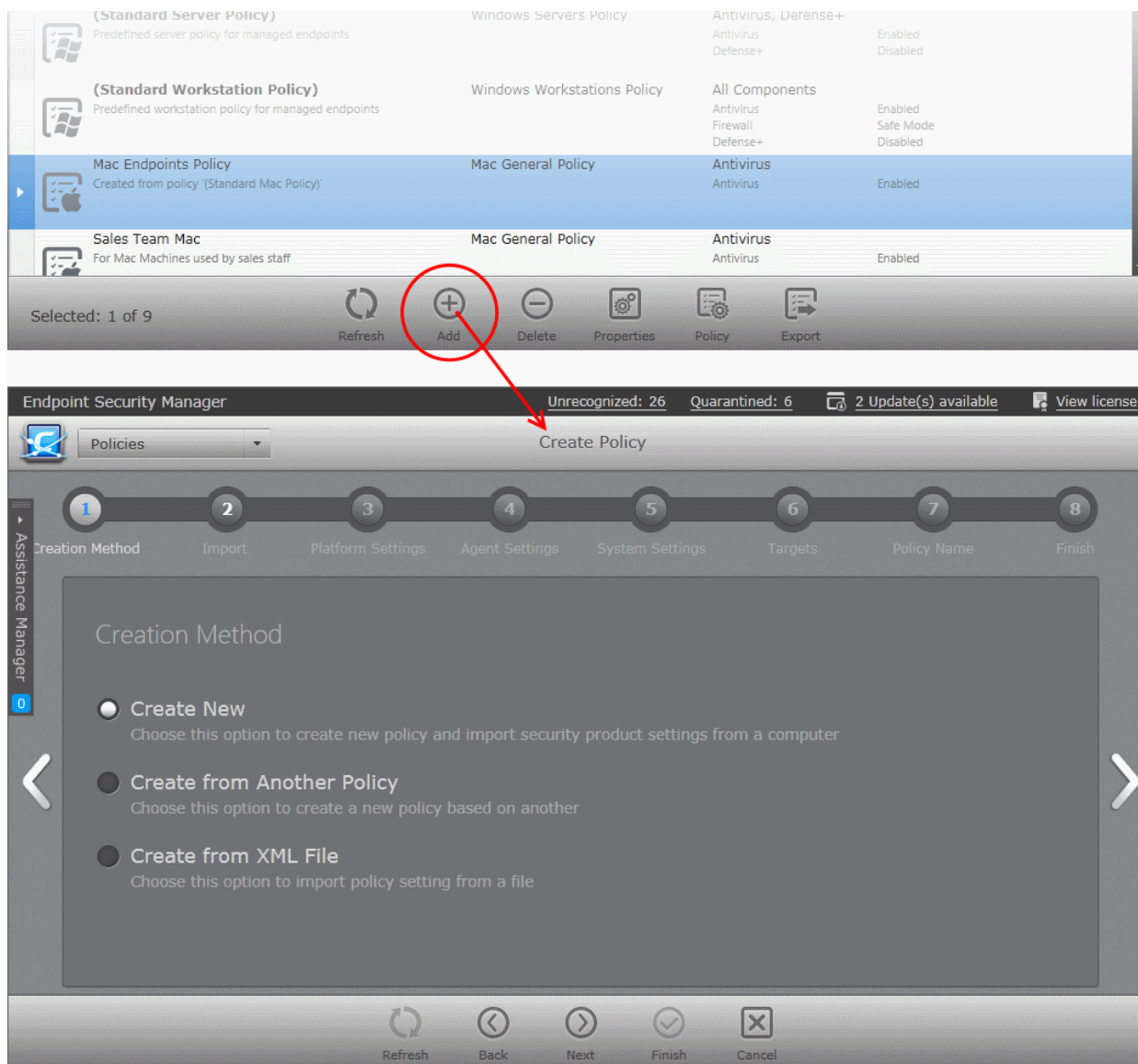
5.1.2. Creating a New Security Policy for Mac OS Based Endpoints

There are seven steps involved in creation of a security policy for Mac OS based workstations. The steps are displayed below

the title bar with the current step highlighted in bold. To move backwards or forwards between steps, use the arrows on either side of the main interface (or left click and drag to swipe the screens left or right) or click a step with a click-able active link below the title bar.

To start the 'Create Policy' wizard

- Select 'Policies' from the drop-down at the top left.

- Click 'Add' from the 'Policies' area.

The wizard will start with Step 1- Creation Method.

Step 1 - Choose the creation method

The new policies can be created from three types of sources:

- **Computers** - Imports the security settings configured locally for the CAVM, from a selected source computer to create a new policy.

- **Another Policy** - Enables to choose an existing policy and use it as the starting point to create a new policy.

- **A saved Policy XML file** - Imports the policy from the policy xml file from the computer running the administration console.

Tip: You might create a policy from another policy if you want to retain the CAVM settings from policy but change the system monitoring settings/agent-specific settings or vice versa.

Explanations on importing from different source types can be found in the following sections: **Importing from Computers, Importing from Another Policy** and **Importing from XML File**.

- Select the source type and click the right arrow to move to step 2.

Importing from Computers

- Choose 'Create New' if you wish to import the security settings from a target endpoint as the new policy and click the right arrow to move to Step 2 - Import Settings from another Computer.

Step 2 - Import Settings from another Computer

All endpoint computers added to ESM will be displayed.

You can search for a specific endpoint using sorting, filtering and searching options:

- To switch the sorting of endpoint names in the 'Computer' column between ascending and descending orders, click the down arrow at the right of the 'Computer' column header.
- To search for a particular endpoint, click the funnel icon in the 'Computer' column header, enter the name of the endpoint in full or part and click 'Apply'.
- To search for an endpoint based on the group name, click the funnel icon in the 'Group' column header, enter the group name in full or part and click 'Apply'.
- To search for an endpoint with online or offline status, click the funnel icon in the 'Status' column header, select the status and click 'Apply'.
- To search for endpoint with based on installation state of the security product, click the funnel icon in the 'Security Product' column header, choose from 'Installed', 'Unsupported' or 'Not Installed' options and click 'Apply'.
- To remove a filter, click the funnel icon in the respective column header and click 'Reset'.

- Choose the Mac computer from which you wish to import the settings. The computer should have CAVM installed and be in local mode, configured as per the requirements, and should be online to enable ESM to import the settings.
- Click the right arrow to move to **Step 3 - Agent Settings**.

Importing from Another Policy

- Choose 'Create from Another Policy' if you wish to import the security settings from an existing Policy and click the right arrow to move to Step 2 - Selecting Source Policy.

Step 2 - Selecting Source Policy

A list of all the existing policies with their descriptions and the configuration states of the security product components are displayed.

You can search for a specific policy using the filtering and searching options:

- To search for a particular policy, click the funnel icon in the 'Policy' column header, enter the name of the Policy in full or part and click 'Apply'.
- To search for a policy based on the enabled states of the components, click the funnel icon in the 'Components' column header, select the components and click 'Apply'.
- To remove a filter, click the funnel icon in the respective column header and click 'Reset'.
- Select the source policy from which you wish to create a new policy and click the right arrow to move to **Step 3 - Agent Settings**.

Importing from a saved XML File

- Choose 'Create from XML file' if you wish to import the security settings from a previously saved policy xml file in the computer running the administration console. Click the right arrow to move to Step 2 - Selecting Source File.

Step 2 - Selecting Source File

- Click 'Browse' and navigate to the required policy XML file and click 'Open'.

- Click the right arrow to move to **Step 3 - Agent Settings**.

Step 3 - Agent Settings

The next step allows the administrator to configure the ESM agent installed at the target computers, for which the policy has to be applied.
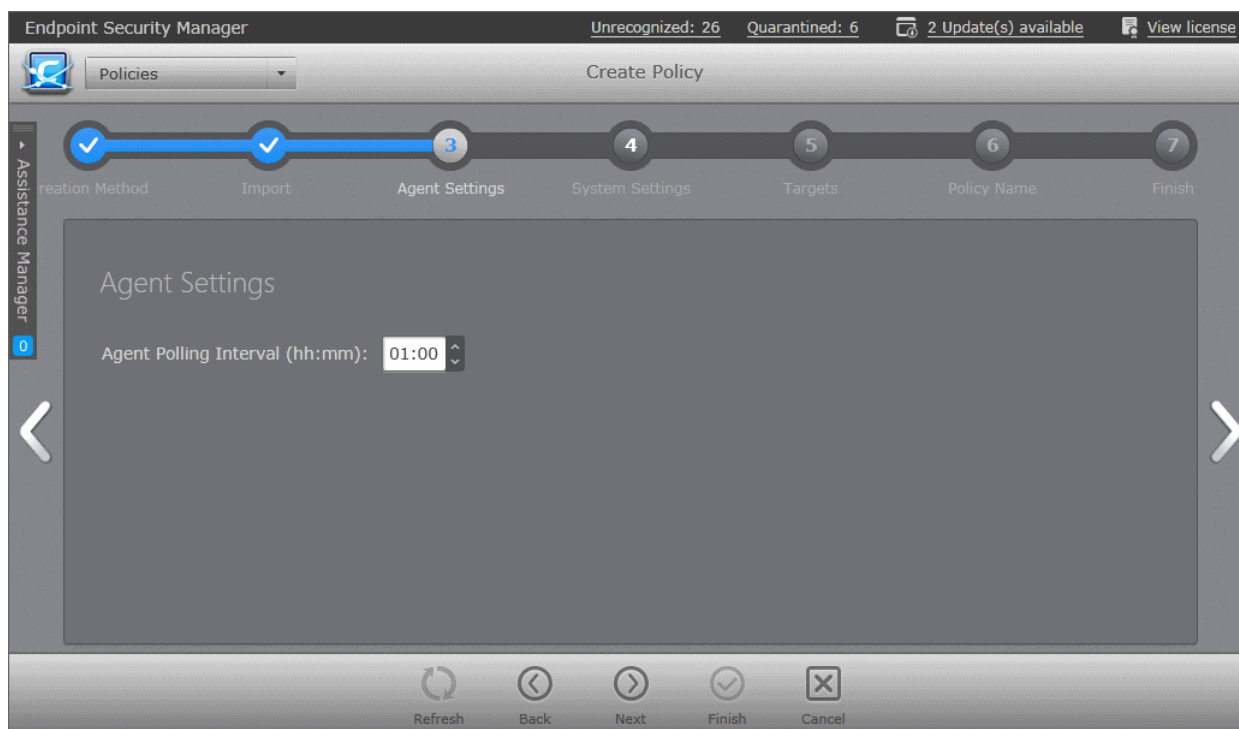
- **Agent polling interval** - The administrator can set the time interval (in hours and minutes) for the agent to periodically check whether the CAVM at the target computer is compliant with the applied security policy. The result will be dynamically displayed in the Policy Status tile and System Status - Compliancy status tile on the

dashboard. (Default = 1 hour, up to but not including 24 hours).

• Click the right arrow to move to the step 4 - System Settings.

Step 4 - System Settings

The next step allows the administrator to configure the system settings like power management, connectible devices management and resource monitoring settings to be deployed on to the target computers, for which the policy has to be applied.

• **Enable power options management** - Allows the administrator to configure power settings. On selecting the 'Enable power options management' check box, the administrator can specify the power settings from the options below:

  • **Turn off the display** - Allows the administrator to select the period after which the display will be switched off if the system is continuously idle. (Default = Never)

  • **Turn off hard disk** - Allows the administrator to select the period after which the hard disk will be turned off if the system is continuously idle. (Default = Never)

  • **System standby** - Allows the administrator to select the period after which the system will go into standby mode if the system is continuously idle. (Default = Never)

  • **System hibernates** - Allows the administrator to select the period after which the system will go into hibernation mode if the system is continuously idle. (Default = Never)

• **Enable System Monitoring** - Selecting this option makes CESM to generate alerts if the system resource usage crosses the thresholds configured in the options below. If the system resource usage exceeds the limits specified, the endpoint will be indicated as 'Overloaded'. The administrator can view the alerts generated, from the 'Computer Properties' > 'Monitoring Alerts' pane. Refer to the section **Viewing System Monitoring Alerts** for more details.

  • **Alert when CPU exceeds NN% usage for TT seconds** - Generates alert when the CPU usage at the target computer is continuously larger than the percentage specified in the slider for the time (in seconds)

specified in the time drop-down combo box. The administrator can specify the maximum CPU usage allowance in the slider and the period in the drop-down combo box. (Default = 70% for 30 seconds)

- **Alert when RAM exceeds NN% usage for TT seconds** - Generates alert when the system memory usage at the target computer is continuously larger than the percentage specified in the slider for the time (in seconds) specified in the time drop-down combo box. The administrator can specify the maximum system memory usage allowance in the slider and the period in the drop-down combo box. (Default = 70% for 30 seconds)

- **Alert when network usage exceeds NN% usage for TT seconds** - Generates alert when the data traffic from/to the endpoint is continuously larger than the network utilization percentage specified in the slider, for the time (in seconds) specified in the time drop-down combo box. The administrator can specify the network usage limit in the slider and the period in the drop-down combo box. (Default = 70% for 30 seconds)

- **Alert when there is less than NN% free space left on system drive** - Generates alert when the remaining space in the hard disk drive partition on which the Operating System is installed, reduces below the percentage of total partition size, specified in the slider. The administrator can specify the minimum amount of free space to be maintained in the system drive through the slider. (Default = 5%)

- Click the right arrow to move to the step 5 - Selecting Targets.

Step 5 - Selecting Targets

The administrator can select the target computer group(s) and/or sub group(s) onto which the created policy has to be applied. To open the tree structure view of the sub groups, click the down arrow beside a group.

- Check 'Assign policy to groups after finish' if you want to apply the newly created policy after it is imported to an existing group. You can also assign this policy at a later stage to groups if you do not want to do so now. See **Editing a Security Policy** section for more details.

- For the group(s)/sub group(s) of computers connected through the local network you wish to apply the new policy, select 'For Local Policy' check box.

- For the group(s)/sub group(s) of computers connected through the Internet you wish to apply the new policy, select 'For Internet Policy' check box.

- **Options**:

    - **Override individual computers policy after finish** - Selecting this option will apply the new policy onto computers that are currently in 'Non Compliant' status within the selected groups, upon completion of policy creation, even if 'Apply policy after finish' is not selected. For the other endpoints in the selected group, the new policy will be applied on the next polling time. (Default = Not Selected)

    - **Apply policy after finish** - Selecting this option will apply newly created policy to all it's targets, irrespective of their compliancy status, right after policy creation is finished. If this option is not selected, the new policy will be applied during the next polling time. (Default = Selected)

- Make your selections and click the right arrow to move to step 6 - Importing the Settings and Creating the Policy.

Step 6 - Importing the Settings and Creating the Policy

The next step requires the administrator to specify a name and provide a description for the policy created.
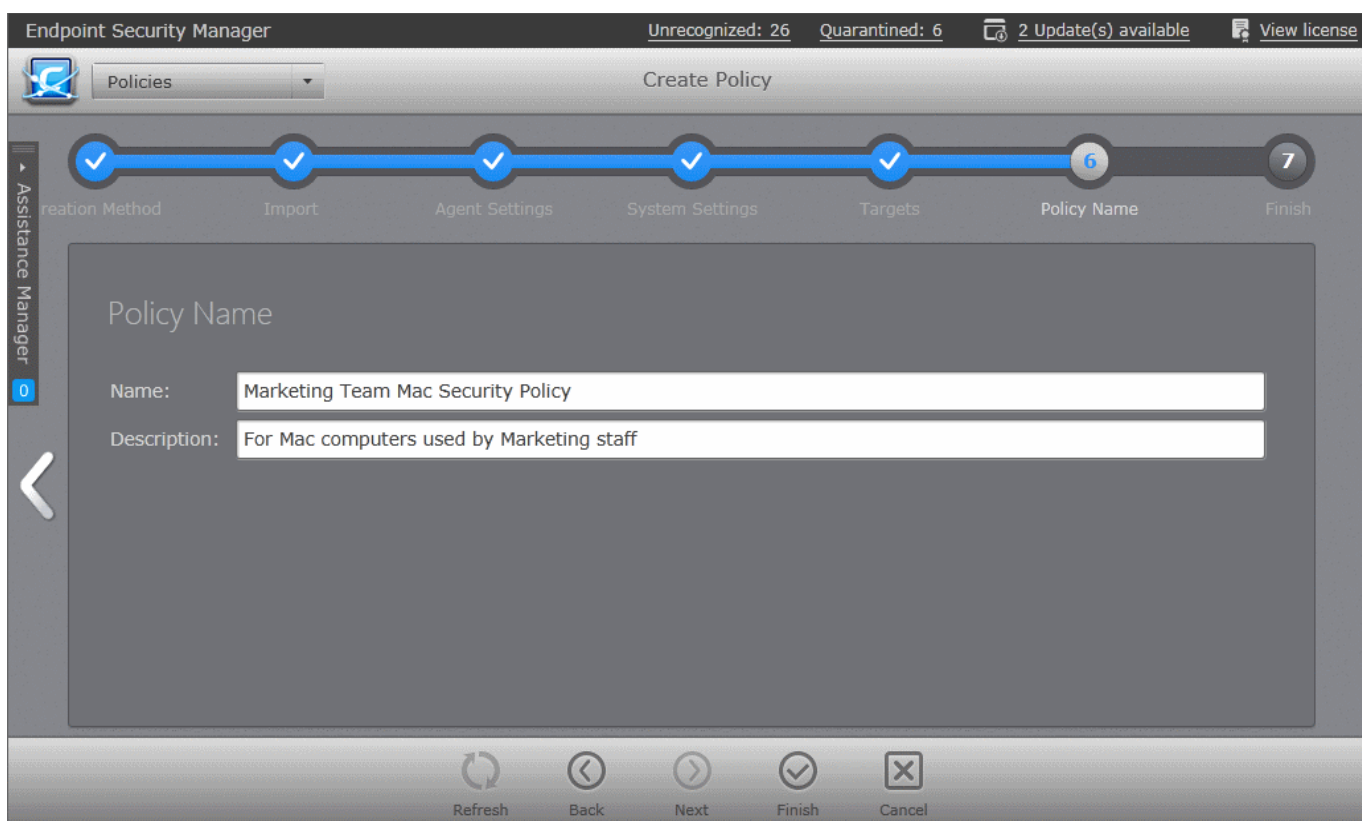
- **Name** - Enter a name according to criteria deemed suitable to the security settings.

- **Description** - Enter short text that best describes the policy.

- Click the 'Finish' icon , click step 7 from the navigation below the title bar or swipe the screen to left to complete the policy creation process. On completion:

    - The 'Policy' interface will open with the new policy added.

The new policy will be applied to the target computers selected in **step 5** as per the options selected in the same.

5.2. Editing a Security Policy

The 'Policies' interface enables the administrator to:

- View a list of all policies along with their descriptions and the security component covered by the policy.

- View and modify the details of any policy - including name, description, CES/CAS/CAVM components, target computers and whether the policy should allow local configuration.

- Configure various settings such as Antivirus settings, Firewall settings, Defense+ settings, General CES/CAS/CAVM settings, Agent settings and System Monitoring settings of any policy.

- Add or remove policies as per requirements.

- Export any policy to .xml file.

- Assign or reassign policies to endpoint groups.

To open the interface, select 'Policies' from the drop-down at the top left. The 'Policies' interface will open with the default view being a list of all policies:
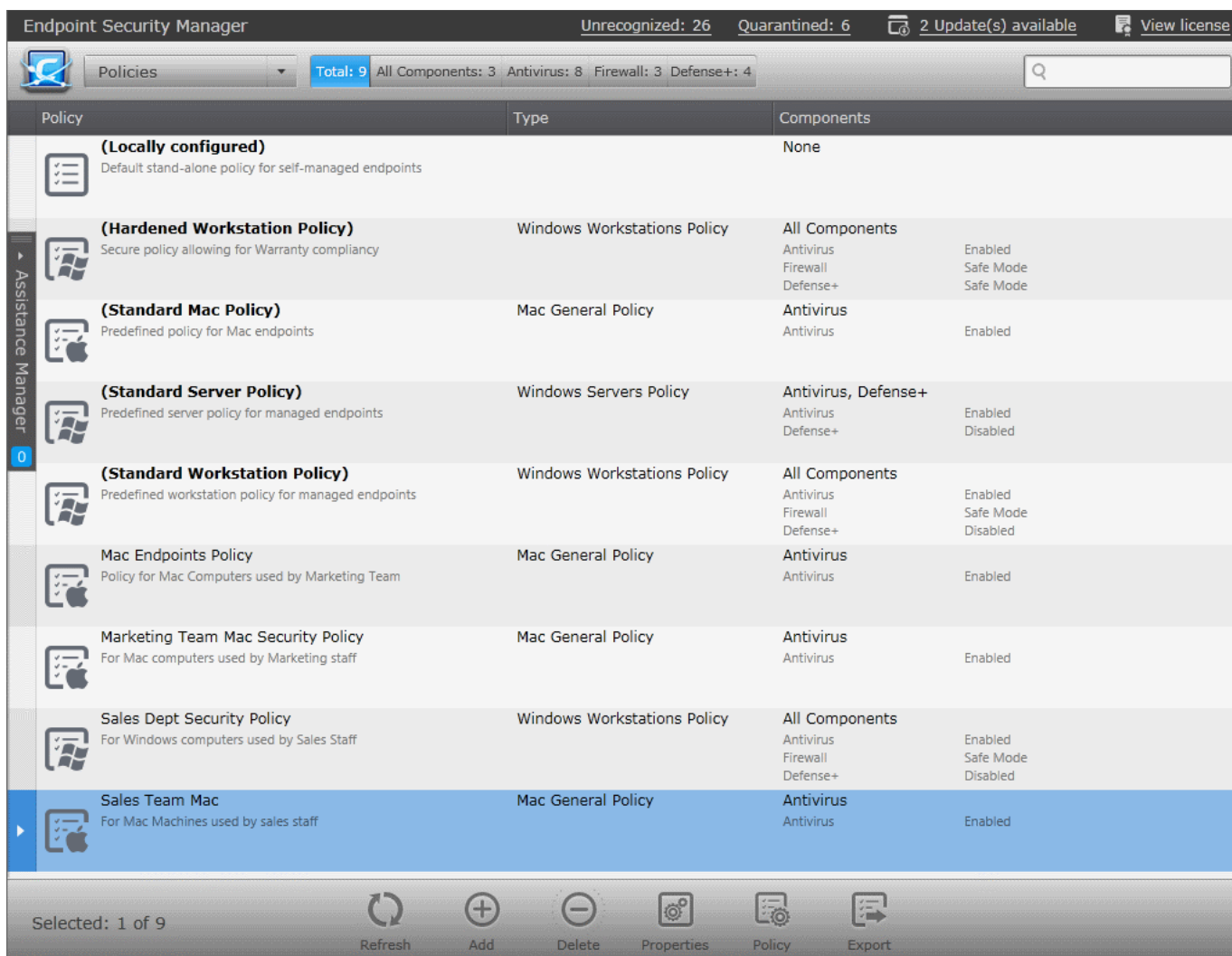
View All Policies Interface - Table of Column Descriptions

Column Heading	Description
Policy	Displays the name of the Policy.
Type	Indicates the type of endpoint to which the policy can be applied
Components	Indicates the components of CES/CAS for which the policy applies the configuration settings.

Filter Options

The filter options in the gray stripe, gives at-a-glance statistics of total number of policies and the numbers of policies in which the Antivirus, Firewall and Defense+ components of CES/CAS/CAVM are enabled. Using the buttons, the administrator can filter the policies with required component CES/CAS/CAVM component is enabled.
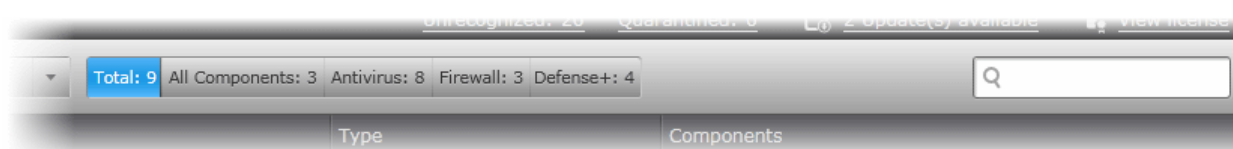
The search field in the right allows the administrator to search for a specific policy entering its name partially or fully.

The 'Policies' interface also allows the administrator to:

- **Create a new policy**
- **Export a policy into an xml file for importing to ESM at a later time**
- **Remove policies**
- **View details, reconfigure and apply policies to groups**

Creating a Policy

- Click the Add Policy icon from the bottom of the interface. The 'Create Policy' Wizard will be started. Refer to the section **Creating a New Policy** for a detailed description on the wizard.

Exporting a Policy

Any policy added to ESM can be saved as a .xml file to the computer running the administration console. The .xml file can be imported into ESM and a new policy can be created from it at a later time.

To export an existing policy

- Select the policy by clicking or touching the desired policy from 'Policies' interface to highlight it. Click the Export icon . Alternatively, right click on the selected policy and select 'Export...' from the context sensitive menu. The Windows 'Save As' dialog will appear.

- Select the destination in the computer from which you are accessing ESM, provide a file name and click 'Save'.

The policy will be saved as an xml file. The file can be imported into ESM at any time.

Removing Policies

The administrator can remove one or more unwanted policies by simply selecting them by clicking or touching the desired policy to highlight it and clicking the Delete icon . Alternatively, right click on the selected policy and select 'Delete' from the context sensitive menu.

A confirmation dialog will be displayed.
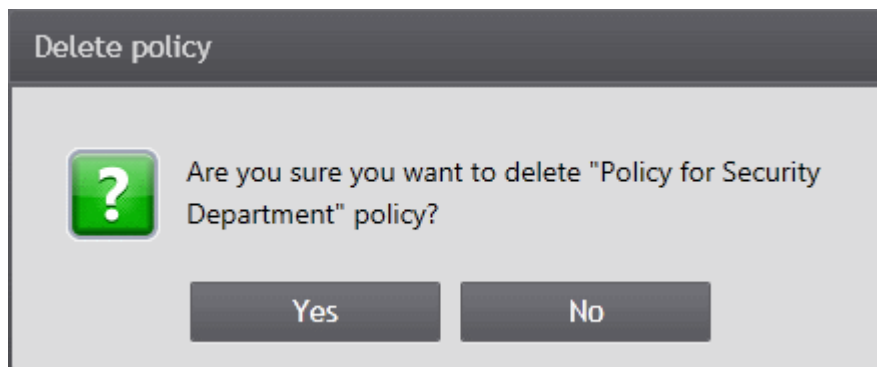
- Click 'Yes' to remove the selected item(s).

Note: Policies which are currently applied and used by groups or endpoints cannot be deleted. Before removing an unwanted policy, the administrator has to apply a different policy to the groups/endpoints to which this policy is currently applied.

The pre-defined policies Servers Policy and Workstations Policy cannot be removed.

Tip: Hold Shift or CTRL to select multiple items.

Viewing Details and Reconfiguring a Policy

Selecting a policy and clicking the 'Properties' icon [icon] from the Policy screen opens the policy details interface with its name displayed at the top. The interface can also be opened by right clicking on the policy and selecting 'Properties' from the context sensitive menu. The interface allows administrators to configure Antivirus settings, Firewall settings, Defense+ settings, General CES/CAS settings, File Rating, Agent settings and System monitoring settings for the selected policy. The policy can also be assigned to other groups from this interface.
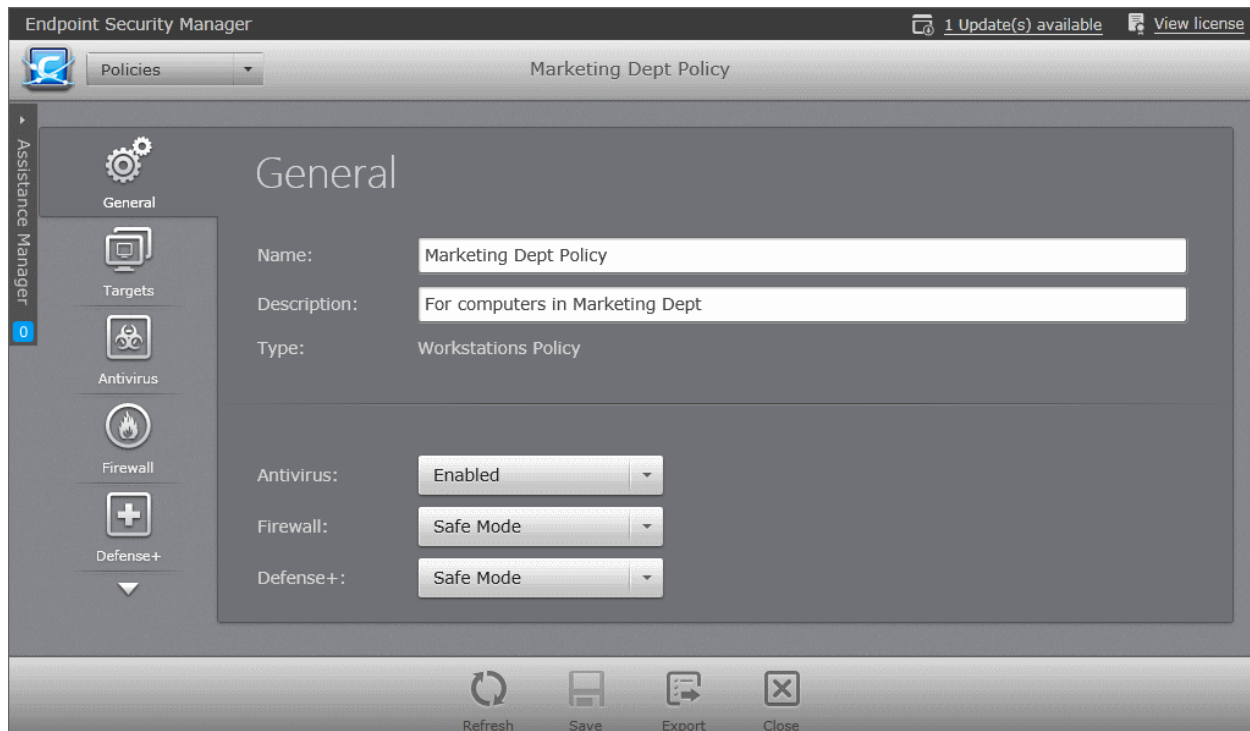
The 'Policy Properties' interface contains a maximum of 10 tabs in the left hand side navigation pane to open the respective configuration pane at the right.

- **General Properties** - Displays the general details like name and description of the policy. The administrator can edit these details directly.

- **Policy Targets** - Enables the administrator to select target group(s) on which the selected policy has to be applied.

- **Antivirus Settings** - Enables the administrator to configure predefined and scan profiles, schedule scans for the policy and define exclusions for Antivirus scans run as per the policy.

- **Firewall Settings** - Enables the administrator to set Firewall protection level and firewall alert settings for the policy.

- **Web Filtering Settings** - Enables the administrator to configure websites to be allowed and blocked to the users by managing philatelists, blacklists and custom categories of websites, for the policy.

- **Defense+ Settings** - Enables the administrator to configure HIPS settings, Auto-Sandbox rules and Viruscope settings for the policy.

- **File Rating** - Enables the administrator to configure File Rating settings, view and manage Trusted Files list, Trusted Vendors list and create and manage 'File Groups' and 'Registry Groups' for the policy. The 'File Groups' and 'Registry Groups' can be used for adding Exclusions for Antivirus scans, creating Auto-Sandbox rules and so on.

- **General Security Product Settings** - Enables the administrator to configure General settings like User Interface, update options, proxy and host settings and log settings for the CES/CAS/CAVM installations in the endpoints applied with the policy.

- **Agent Settings** - Enables the administrator to configure the ESM agent deployed onto the endpoints for the policy.

- **System Settings** - Enables the administrator to configure System Monitoring Settings, Power and Device

---

management settings for the policy.

The administrator can scroll through the tabs by using the up or down arrow located at the top and bottom in the left pane.

Depending on the type of the policy chosen, the 'Policy Properties' allows the administrator to view and manage the following configurations. The following table shows the configurations that are available for each policy type.

Windows Workstations Policy - For Windows based endpoints with CES installed	Windows Servers Policy - For Windows Servers with CAS installed	Mac General Policy - For Mac OS based endpoints with CAVM installed
General Properties	General Properties	General Properties
Policy Targets	Policy Targets	Policy Targets
Antivirus Settings	Antivirus Settings	Antivirus Settings
Firewall Settings	Defense+ Settings	General Security Product Settings
Web Filtering Settings	File Rating	Agent Settings
Defense+ Settings	General Security Product Settings	System Settings
File Rating	Agent Settings	
General Security Product Settings	System Settings	
Agent Settings		
System Settings		

5.2.1. General Properties

The General screen shows the name and description of the policy as well as the CES/CAS components for that policy. To open the interface, click on the 'General' icon [ ] in the left pane. The General properties of the selected policy will be displayed.

General Properties - Table of Parameters

Parameter	Description
General Details	
Name	Displays the name of the Policy. The administrator can change the name by directly editing the text box.
Description	Displays the short description of the policy. The administrator can change the description by directly editing the text box.
Platform	Indicates the operating system of the endpoints to which the policy can be applied
Type	Indicates whether the policy can be applied to workstations or servers
CES/CAS/CAVM Components summary	
Antivirus	Indicates the current configuration state of Antivirus as per the policy and enables the administrator to enable or disable it from the drop-down. The Antivirus Settings screen allows more granular configuration of the Antivirus component. Refer to **Configuring Antivirus Settings** for more details.
Firewall (*Available only for Windows Workstations policy type and not for Windows*	Indicates the currently configured security level of Firewall as per the policy and enables the administrator to change the security level from the drop-down. For details explanations on options available, refer to the section **Configuring Firewall Settings > General Settings.**

Servers and Mac General policy types.)	The Firewall Settings screen allows more granular configuration of the Firewall component. Refer to **Configuring Firewall Settings** for more details.
HIPS (*Available only for Windows Workstations and Windows Servers policy types and not available for Mac General policy type*)	Indicates the currently configured security level of Host Intrusion Prevention System (HIPS) component of Defense+ as per the policy and enables the administrator to change the security level from the drop-down. For details explanations on options available, refer to the section **Configuring Defense+ Settings > HIPS Behavior Settings** The Defense+ Settings screen allows more granular configuration of the Defense+ component. Refer to **Configuring Defense+ Settings** for more details.
Auto-Sandbox (*Available only for Windows Workstations policy type and not for Windows Servers and Mac General policy types*.)	Indicates whether the Auto-Sandbox feature of Defense+ is enabled or not, as per the policy and enables the administrator to enable or disable it from the drop-down. The Auto Sandbox can be enabled or disabled and rules can be created for automatically running unrecognized files inside sandbox from the Defense+ > Sandbox interface. Refer to the section **Configuring Defense+ Settings > Sandbox** for more details.

- Click 'Save' at the bottom of the interface for your changes to take effect for the policy. The policy with the new settings will be applied to the respective endpoints during the next polling cycle of the respective CESM agents.

Note: The 'General Properties' interface allows the administrator to view and edit the details of the custom profiles, and view the details of the predefined profiles. The predefined profiles cannot be edited.

5.2.2. Selecting Target Groups

The 'Policy Targets' screen displays the computer groups to which the policy is applied for local network connection and Internet connection. It also enables the administrator to:

- Apply the policy to other groups or sub groups.
- Remove the policy from already applied groups.

To open the interface, click on the 'Targets' icon in the left pane. All the groups and sub groups configured in CESM will be displayed as a tree structure.

- For the group(s)/sub group(s) of computers connected through the local network you wish to apply the new policy, select 'For Local Policy' check box.

- For the group(s)/sub group(s) of computers connected through the Internet you wish to apply the new policy, select 'For Internet Policy' check box.

- **Options**:

    - **Override individual computers policy after finish** - Selecting this option will apply the edited policy onto computers that are currently in 'Non Compliant' status within the selected groups, upon completion of the editing process. For the other endpoints in the selected group, the edited policy will be applied on the next polling time. (Default = Not Selected)

- Click the 'Save' icon for any changes to the settings to take effect.

A policy can also be applied to groups by right-clicking on a policy or by clicking on the Policy icon at the bottom of the Policies main screen.
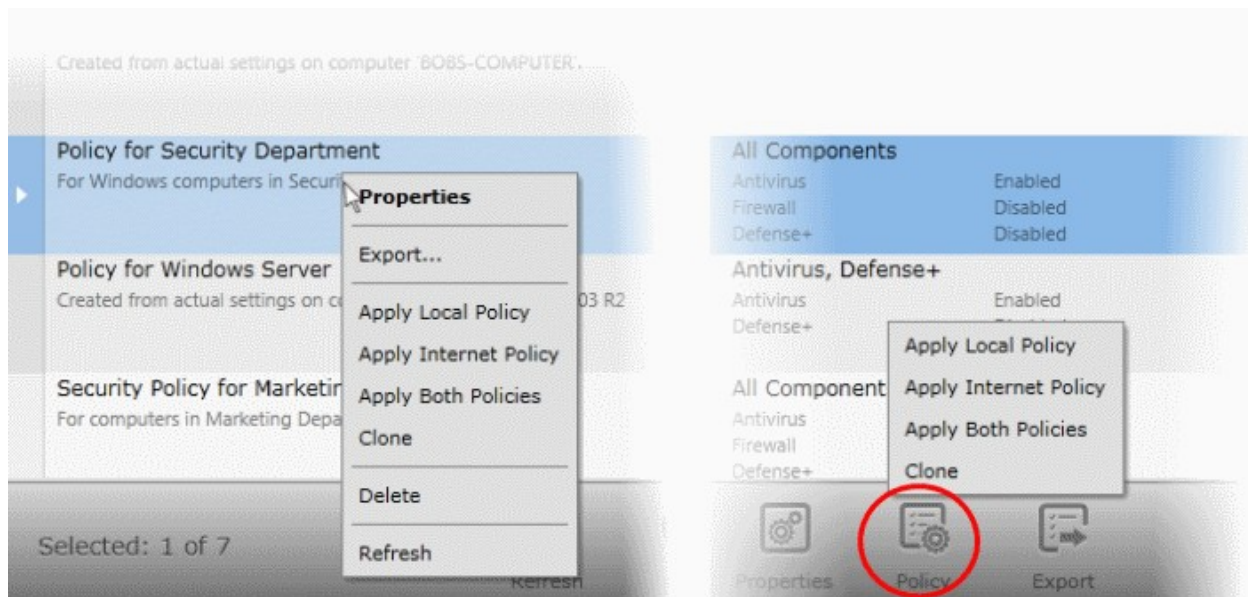
- Select 'Apply Local Policy', 'Apply Internet Policy' or 'Apply Both Policies.

The list of groups will be displayed:
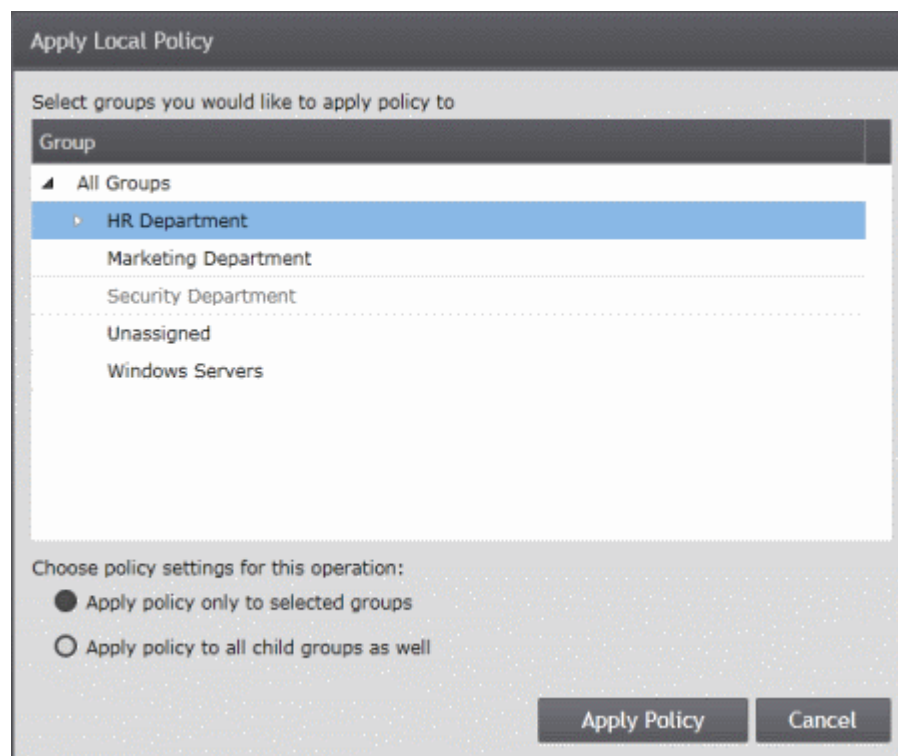
- **Apply policy only to selected groups** - Policy will be applied to parent group only.

- **Apply policy to all child groups as well** - Policy will be applied to parent as well as to all child groups under it.

Select the group from the list, choose policy setting options and click 'Apply Policy'.
Alternatively, a policy can also be applied to selected groups from **the Groups area**.
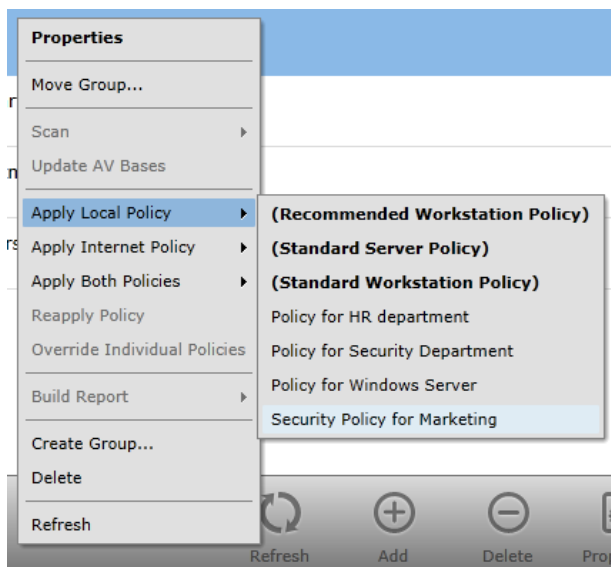
- By right-clicking on selected group(s) and choosing the policy from the Apply Local Policy, Apply Internet Policy or Apply Both Policies options.

- By selecting the group, clicking the Policy icon at the bottom of the interface and choosing the policy from the Apply Local Policy, Apply Internet Policy or Apply Both Policies options.
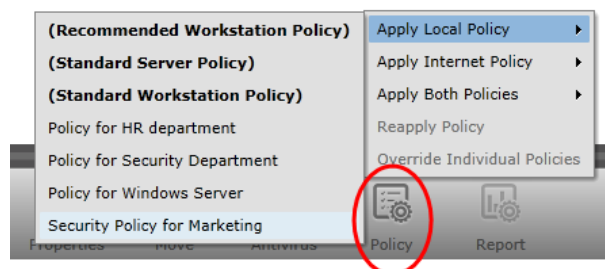
5.2.3. Configuring Antivirus Settings

The Antivirus Settings configuration screen allows an administrator to customize various options related to Real Time Scanning (On-Access Scanning), time-table scheduled scans and add trustworthy files to Exclusions list (a list of the files you consider safe), so that they would be skipped during real time, on demand and scheduled antivirus scans .

To open the interface, click on the 'Antivirus' icon in the left pane. The Antivirus Settings screen will be displayed.
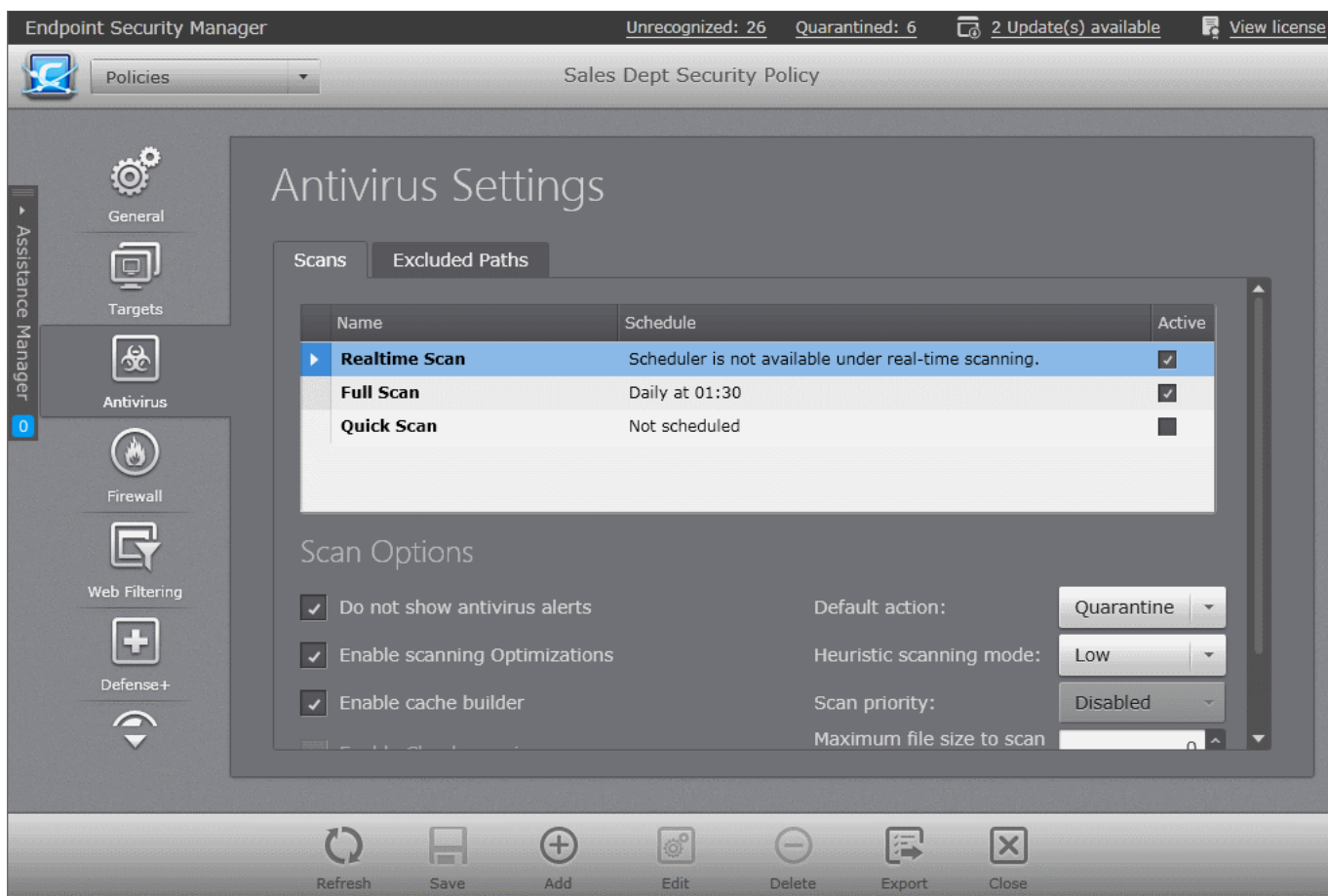
The options that can be configured in the Antivirus settings screen are:

- **Antivirus Scans** - To schedule AV scans and to configure parameters for the scheduled and on-access scanning.

- **Excluded Paths** - To add trusted files, applications and locations for excluding from a virus scan.

5.2.3.1. Antivirus Scans

The 'Scans' area enables the administrator to configure the real time scanning and schedule full computer scans, quick scans and custom scans, to run periodically on a daily, weekly or monthly basis, on the endpoints to which the policy is applied. The administrator can specify the areas in the managed computer to be scanned and various parameters for each custom scan profile.

Note: The 'Scans' interface allows administrators to view and configure antivirus scan parameters for custom profiles, and view the configuration of predefined profiles. Predefined profiles cannot be edited.

Following sections explain in detail on:

- **Scan Configuration for Windows Workstations and Servers with CES/CAS installed**
- **Scan Configuration for Mac based computers with CAVM installed**

Scan Configuration for Windows Workstations and Servers with CES/CAS installed

To open the Scans interface, click the 'Scans' tab in the Antivirus Settings configuration screen.

The 'Scans' interface displays a list of pre-configured and custom antivirus scan profiles and the properties and parameters of the selected scan under 'Scan Options'. The administrator can view or edit the parameters of a scan under 'Scan Options' and edit the schedule under the 'Schedule'.

Antivirus Scans - Table of Column Descriptions	
Column Header	**Description**
Name	Displays the name of the antivirus scan profile.
Schedule	Displays the day/date and time the scan is scheduled to run.
Active	Indicates whether the scan is active. The administrator can switch a scan between active and inactive states by selecting or deselecting the checkbox at any time. Only scans in active state will run as per schedule.

The Antivirus Scans area contains the following three pre-configured antivirus scan profiles.

- **Realtime Scan** - The Real time Scanning (aka 'On-Access Scanning') is always ON and checks files in real time when they are created, opened or copied. (as soon as a user interacts with a file, Comodo Antivirus checks it). This instant detection of viruses assures the user, that the system is perpetually monitored for malware and enjoys the highest level of protection.

  The Real Time Scanner also scans the system memory on start. If a program or file which creates destructive anomalies is launched, then the scanner blocks it and alerts the user immediately - giving the real time protection

against threats.

Since the 'Real time Scan' scans only the files that are created, opened or copied, the administrator can configure only selected parameters under scan options and cannot specify the areas to be scanned or schedule. It is highly recommended that Real Time Scan is maintained in Active state to ensure the endpoints remains continually free of infection.

- **Full Scan** - The 'Full Scan' scans every local drive, folder and file on each computer. Any external devices like USB drives, digital camera and so on are also scanned.

  The administrator can specify a schedule for full scan to run on daily, weekly or monthly basis, but cannot specify the areas to be scanned. Refer to **Schedule Options** for more details.

- **Quick Scan** - The 'Quick Scan' scans critical areas of the computer which are highly prone to infection from viruses, rootkits and other malware. The areas scanned include system memory, auto-run entries, hidden services, boot sectors and other significant areas like important registry keys and system files. These areas are of great importance to the health of each computer so it is essential to keep them free of infection.

  The administrator can specify a schedule for Quick Scan to run on daily, weekly or monthly basis, but cannot specify the areas to be scanned. Refer to **Schedule Options** for more details.

In addition to the pre-configured scans, the administrator can create custom scan profiles to scan specified areas of computers and schedule them to run periodically. Refer to the section **Creating a Custom Scan Profile** for a detailed explanation.

Scan Options

The administrator can view and configure the general behavior of the selected scan under the 'Scan Options'.

- **Do not show antivirus alerts** - This option allows to configure whether or not to show antivirus alerts when malware is encountered. Choosing 'Do not show antivirus alerts' will minimize disturbances but at some loss of user awareness. The option is selected by default for Full Scan, Quick Scan and custom scan profiles and the administrator cannot change it. If you choose not to show alerts then you have a choice of default responses that CES/CAS should automatically take - either 'Disinfect malware' , 'Block Threats' or 'Quarantine Threats'. Choose the option from 'Default Action' drop-down:

  - **Disinfect** - Deletes the file containing the detected malware from the computer
  - **Quarantine** - Moves the detected threat(s) to quarantine for your later assessment and action. The administrator can view and manage:
    - The consolidated list of all the items moved to quarantine by the CES/CAS installations at all the managed endpoints from the Quarantine area. Refer to the section **Viewing and Monitoring Quarantined Items** for more details.
    - The list of items moved to quarantine at a selected endpoint from the Computer Properties interface of the respective endpoint. Refer to the section **Viewing and Managing Endpoint Security Software** for more details.
  - **Block** - Stops the application or file from execution, if a threat is detected in it.

- **Enable scanning optimizations** - If this option is enabled, the antivirus will employ various optimization techniques like running the scan in the background in order to speed-up the scanning process.

- **Heuristic scanning mode** - Heuristic techniques identify previously unknown viruses and Trojans. 'Heuristics' describes the method of analyzing the code of a file to ascertain whether it contains code typical of a virus. If it is found to do so then the application deletes the file or recommends it for quarantine. Heuristics is about detecting virus-like behavior or attributes rather than looking for a precise virus signature that match a signature on the virus blacklist.

  This is a quantum leap in the battle against malicious scripts and programs as it allows the engine to 'predict' the existence of new viruses - even if it is not contained in the current virus database.

  You can select the level of Heuristic scanning from the drop-down:

  - **Off** - The Heuristic scanning is not enabled.
  - **Low** - 'Lowest' sensitivity to detecting unknown threats but will also generate the fewest false positives. This setting combines an extremely high level of security and protection with a low rate of false positives. Comodo recommends this setting for most users.
  - **Medium** - Detects unknown threats with greater sensitivity than the 'Low' setting but with a corresponding rise in the possibility of false positives.
  - **High** - Highest sensitivity to detecting unknown threats but this also raises the possibility of more false positives too.

- **Enable Cache Builder** - The CES/CAS installation at the endpoint runs the Antivirus Cache Builder whenever the

computer is idle, to boost the real-time scanning, if this option Is selected. The option is selected by default for Full Scan, Quick Scan and custom scan profiles and the administrator cannot change it.

- **Scan Priority** - Indicates the task priority for the scanning task at the endpoint computer. You can select the priority from the drop-down.:

    - High
    - Normal
    - Low
    - Background
    - Disabled

- **Enable Cloud Scanning** - This option enables the Antivirus to detect the very latest viruses more accurately because the local scan is augmented with a real-time look-up of Comodo's online signature database. With Cloud Scanning enabled CES/CAS at the endpoint is capable of detecting zero-day malware even if its local antivirus database is out-dated.

Note: CES uses Ports 4446 and 4447 of the endpoint computers for TCP and UDP connections to the cloud. Comodo advises to maintain these ports free and not assigned to other applications, if this option is enabled.

- **Maximum file size to scan** - This box allows the administrator to set a maximum size (in MB) for the individual files to be scanned during on-access scanning. Files larger than the size specified here, will not be not scanned.

- **Decompress and scan compressed files** - When this option is selected, the Antivirus scans archive files such as .ZIP and .RAR files. Supported formats include RAR, WinRAR, ZIP, WinZIP ARJ, WinARJ and CAB archives

- **Update virus database before scanning** - If this option is enabled, the CES/CAS at the managed computers will check for latest virus signature database updates from Comodo website and download the updates automatically before starting the scanning. (*Not applicable for Realtime Scan*)

- **Detect potentially unwanted applications** - When this check box is selected, Antivirus scans also scans for applications that:

    - A user may or may not be aware is installed on their computer, and/or
    - May have functionality and objectives that are not clear to the user.

        Example PUA's include adware and browser toolbars. PUA's are often installed as an additional extra when the user is installing an unrelated piece of software. Unlike malware, many PUA's are 'legitimate' pieces of software with their own EULA agreements. However, the 'true' functionality of the software might not have been made clear to the end-user at the time of installation. For example, a browser toolbar may also contain code that tracks a user's activity on the Internet.

    (*Not applicable for Realtime Scan*)

- **Turn off computer if no threats are found at the end of the scan** - Switches off computers after the completion of a scan if no threats are found. (*Not applicable for Realtime Scan*)

- **Run only when computer is not running on battery** - This option is useful if the policy is applied for laptops or any other battery driven portable computers. Selecting this option runs the scan only if the computer runs with the adopter connected to mains supply and not on battery. *(Not applicable for Realtime Scan)*

- **Run only when computer is IDLE** - The scheduled can will run only if the computer is in idle state, so that the user will not be disturbed when involved in computer related activities. (*Not applicable for Realtime Scan*)

Schedule Options

The administrator can view and configure the schedule of the selected scan under the 'Schedule'. The drop down at the left allows to select the period:
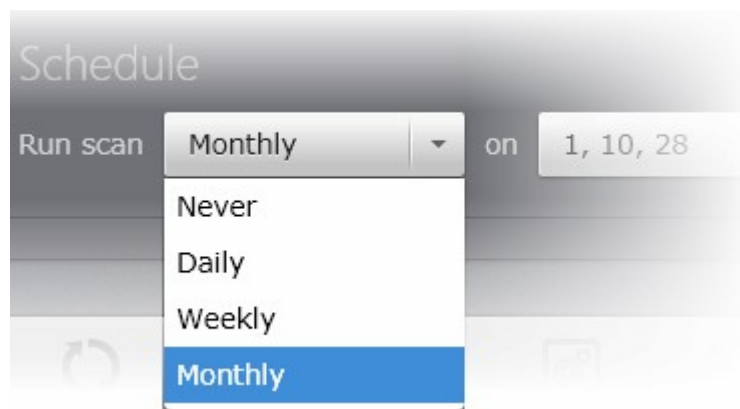
Never   -   The scan is not scheduled and will not run

Daily   -   The Scan will run daily on the specified time.

On selecting 'Daily', the administrator can edit the time at which the schedule to run daily from the drop-down combo box.

Weekly   -   The scan will run on selected day(s) of every week at the specified time.
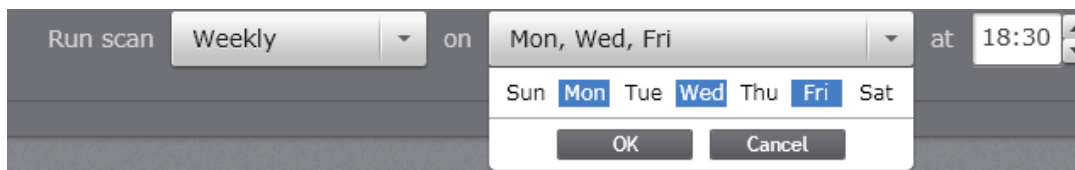
On selecting 'Weekly', the administrator can select the day(s) of the week from the Select day(s) drop-down and edit the time at which the schedule to run from the drop-down combo box.

Monthly   -   The scan will run on selected day(s) of every month at the specified time.

On selecting 'Monthly', the administrator can select the date(s) of the month from the Select day(s) drop-down and edit the time at which the schedule to run from the drop-down combo box.

Scan Configuration for Mac based computers with CAVM installed

To open the Scans interface, click the 'Scans' tab in the 'Antivirus Settings' configuration screen.

Endpoint Security Manager | Unrecognized: 26 | Quarantined: 6 | 2 Update(s) available | View license

Policies ▾ | Sales Team Mac

⚙️ General

🖥️ Targets

☣️ Antivirus

©️ Security Product

📇 Agent

📊 System

◄ Assistance Manager 0

Antivirus Settings

| Scans | Excluded Paths |

Name	Schedule
Realtime Scan	Scheduler is not available under real-time scanning.
Manual Scan	Scheduler is not available under manual scanning.
▶ **Full Scan**	Weekly on Sun at 05:30
Quick Scan	Not scheduled

☐ Enable scan

Scan Options (these options are shared among all scheduled scans)

☑ Automatically quarantine threats found during scanning

☑ Automatically update virus database

☐ Scan memory on start

☑ Decompress and scan compressed files

☑ Show scanning progress

Keep alerts on the screen for (seconds): [1]

Maximum file size to scan (MB): [20]

Schedule

Run scan [Weekly ▾] on [Sun ▾] at [05:30]

Refresh | Save | Add | Edit | Delete | Export | Close

The 'Scans' interface displays a list of pre-configured and custom antivirus scan profiles and the properties and parameters of the selected scan under 'Scan Options'. The administrator can view or edit the parameters of a scan under 'Scan Options' and edit the schedule under the 'Schedule'.

Antivirus Scans - Table of Column Descriptions	
Column Header	**Description**
Name	Displays the name of the antivirus scan profile.
Schedule	Displays the day/date and time the scan is scheduled to run.

The Antivirus Scans area contains the following three pre-configured antivirus scan profiles.

- **Realtime Scan** - The Real time Scanning (aka 'On-Access Scanning') is always ON and checks files in real time when they are created, opened or copied. (as soon as a user interacts with a file, Comodo Antivirus checks it). This instant detection of viruses assures the user, that the system is perpetually monitored for malware and enjoys the highest level of protection.

  The Real Time Scanner also scans the system memory on start. If a program or file which creates destructive anomalies is launched, then the scanner blocks it and alerts the user immediately - giving the real time protection against threats.

  Since the 'Real time Scan' scans only the files that are created, opened or copied, the administrator can configure only selected parameters under scan options and cannot specify the areas to be scanned or schedule. It is highly

recommended that Real Time Scan is maintained in 'Enabled' state to ensure the endpoints remains continually free of infection.

The Realtime Scan can be enabled or disabled using the 'Enable Scan' checkbox below the table.

- **Full Scan** - The 'Full Scan' scans every local drive, folder and file on each computer. Any external devices like USB drives, digital camera and so on are also scanned.

   The administrator can specify a schedule for full scan to run on daily, weekly or monthly basis, but cannot specify the areas to be scanned. Refer to **Schedule Options** for more details.

- **Quick Scan** - The 'Quick Scan' scans critical areas of the computer which are highly prone to infection from viruses, rootkits and other malware. The areas scanned include system memory, auto-run entries, hidden services, boot sectors and other significant areas like important registry keys and system files. These areas are of great importance to the health of each computer so it is essential to keep them free of infection.

   The administrator can specify a schedule for Quick Scan to run on daily, weekly or monthly basis, but cannot specify the areas to be scanned. Refer to **Schedule Options** for more details.

In addition to the pre-configured scans, the administrator can create custom scan profiles to scan specified areas of computers and schedule them to run periodically. Refer to the section **Creating a Custom Scan Profile** for a detailed explanation.

Scan Options

The administrator can view and configure the general behavior of the selected scan under the 'Scan Options'.

- **Automatically quarantine threats found during scanning** - Moves the files identified as malware to quarantine during the scans.

- **Update virus database before scanning** - If this option is enabled, the CES/CAS at the managed computers will check for latest virus signature database updates from Comodo website and download the updates automatically before starting the scanning. (Not applicable for Realtime Scan)

- **Scan memory on start** - If this option is selected, the system memory is scanned for virus and malware before scanning the specified areas of the endpoint at the start of each scan. (Not applicable for Realtime Scan)

- **Decompress and scan compressed files** - If this option is selected, the Antivirus scans archive files such as .ZIP and .RAR files. Supported formats include RAR, WinRAR, ZIP, WinZIP ARJ, WinARJ and CAB archives. (Not applicable for Realtime Scan)

- **Show Scanning Progress** - The AV scan progress is displayed at the endpoint if this option is selected. ((Not applicable for Realtime Scan))

- **Keep alerts on the screen for** - Allows you to set the time period (in seconds) for which the alert message displayed at the endpoint should stay on the screen. (Default = 120 seconds)

- **Maximum file size to scan** - This box allows the administrator to set a maximum size (in MB) for the individual files to be scanned during on-access scanning. Files larger than the size specified here, will not be not scanned.

Schedule Options

The Schedule Options for Scan Configuration for Mac General Policy type is are similar to those of Windows Workstation Policy type. Refer to the explanation of **Schedule Options** in the section above for details.

5.2.3.1.1. Creating a Custom Scan Profile

The administrator can create custom antivirus scans for a policy, to scan defined areas of the endpoint computers and schedule the to run on daily, weekly or monthly basis. The CES/CAS/CAVM installations at the endpoints to which the policy is applied will run the scans on the scheduled time with the parameters configured for the scan under the scan options.

To create a custom scan for a policy

- Open the 'Policies' area by choosing 'Policies' from the drop-down at the top left.

- Select the policy and open the 'Policy Properties' interface by double clicking on the policy or clicking the 'Properties' at the bottom of the interface.

- Open the 'Antivirus Settings' screen by clicking the 'Antivirus' tab from the left hand side navigation and open the 'Scans' area by clicking the 'Scans' tab.

- Click the 'Add' button at the bottom of the interface. The 'Scan Profile' Properties dialog will open.

- Enter the name for the scan profile to be created in the 'Scan name' text box.
- Add the areas to be scanned as per the scan profile:
  - For adding preset locations, select the area from the 'Add Region' drop-down.
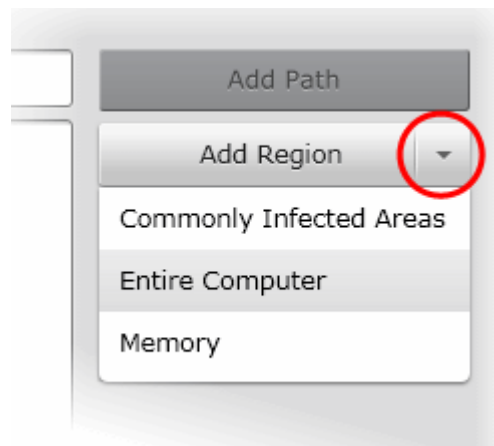
Note: The option 'Add Region' will not be available for Mac General policy Type.

  - For adding a specified location, enter the path in the 'Items to be scanned' text box and click the 'Add Path' button.

- The Item will be added to the list. Repeat the process to add more items to the profile.
- If you want to remove an item added by mistake, select the item in the list and click 'Remove'.
- Click 'OK'. The custom scan profile will be added to the 'Scans' area.

- Select the new profile from the list and configure the scan parameters from the Scan Options area. Refer to the section **Scan Options** for more details.

- Configure a schedule for the new custom scan profile from the Schedule area. Refer to the section **Schedule Options** for more details.

- Make the custom scan active by selecting the 'Active' checkbox in its row.

- Click 'Save'.

- Click 'Refresh' at the bottom of the interface, if your changes are not immediately reflected in the 'Scans' area.

The new scan profile is now created and the areas defined will be scanned as per schedule.

- To remove a custom scan profile, select it and click Delete at the bottom of the interface.

5.2.3.2. Exclusions

In the Excluded Paths area, the administrator can specify files and folders that they trust and want to exclude from all future scans of all types.
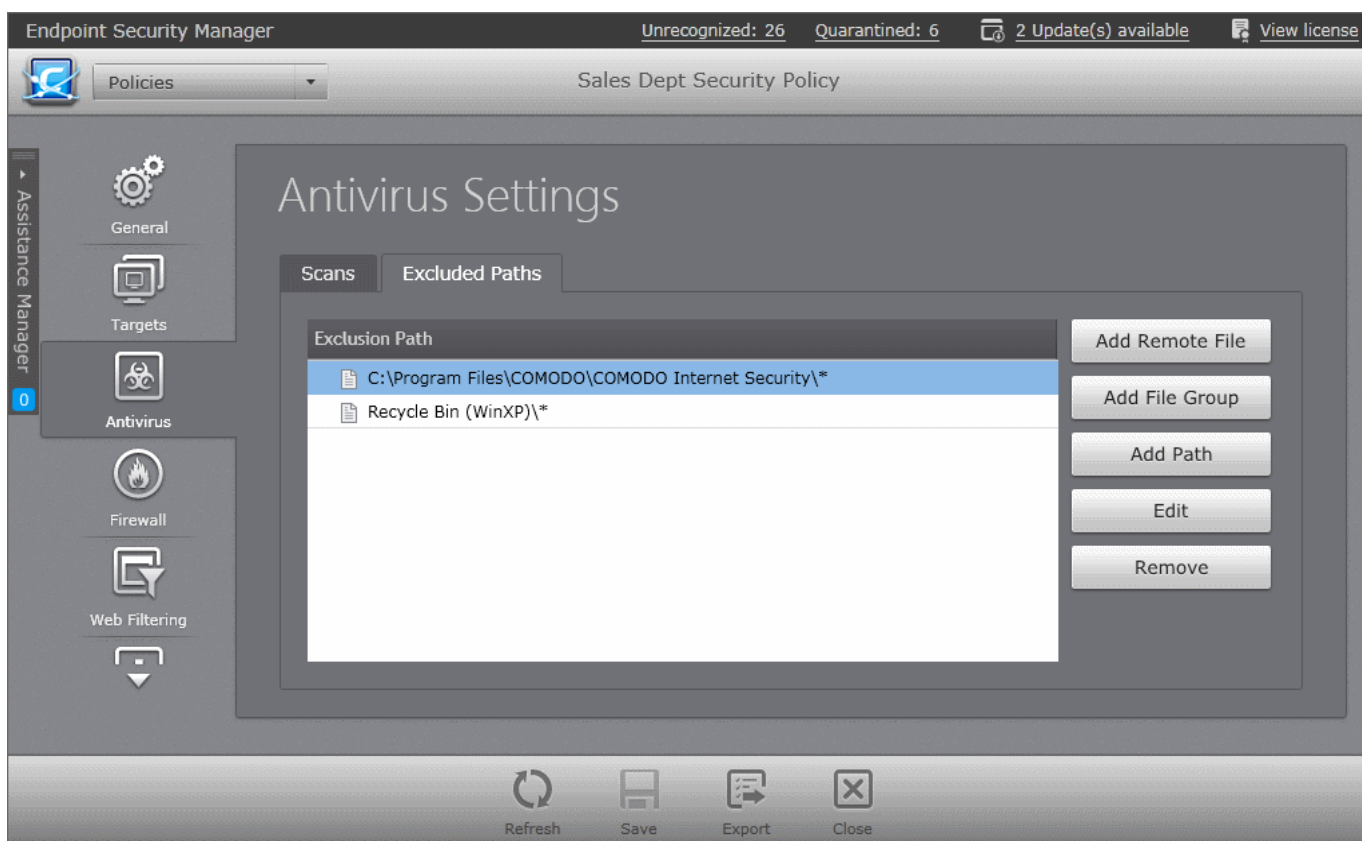
You can add files and folders to the 'Exclusions' list in the following ways:

- **Adding a specific file from a selected endpoint**
- **Adding a File Group**
- **Adding File Path**

Note: The 'Excluded Paths' interface allows the administrator to view and add/remove exclusions for the custom profiles, and only view the exclusions for the predefined profiles, 'Servers Policy' and 'Workstations Policy'. The predefined profiles cannot be edited.

The 'Add Remote File' and 'Add File Group' options are available for Windows Workstations and Windows Servers policy types.

- To change or edit an item, select the item and click 'Edit'.

- To remove an item from the exclusions list, select the item and click 'Remove'.

Adding a specific file from a selected endpoint

The administrator can add specific individual files from selected endpoints applied with the policy, so that the added files will be skipped from all future scans run on the respective endpoints based on the policy.

To add a specific file from a selected endpoint
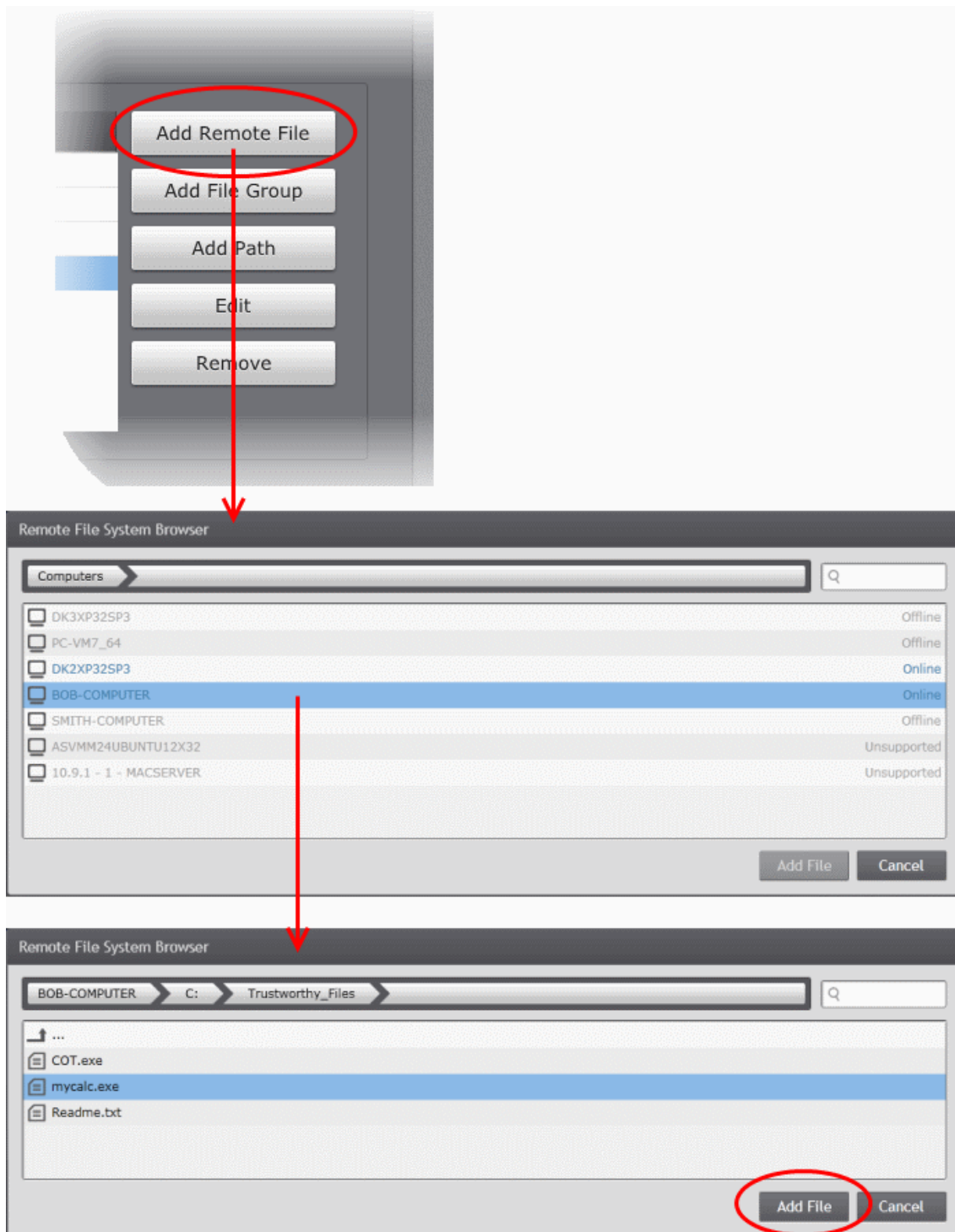
- Click 'Add Remote File'

The list of endpoints will be displayed.

- Double click on the endpoint, navigate to the file path and select the file.

> **Note**: The Endpoint needs to be online for navigation through the file path in it.

- Click 'Add File'.
- Click the 'Save' icon for the changes to take effect.

The file will be added to the to the exclusions list.

Adding a File Group

File groups are handy, predefined groupings of one or more file types. Choosing File Groups allows the administrator to exclude a category of pre-set files or folders. For example, selecting 'Executables' would exclude all files with the extensions .exe .dll .sys .ocx .bat .pif .scr .cpl . Other such predefined categories available include 'Windows System Applications' , 'Windows Updater Applications' , 'Start Up Folders' etc. CESM also enables the administrator to add custom File Groups for the policy from the File Rating Interface. Refer to the description under **Managing File Groups** in the section **Configuring File Rating Settings** for more details.

To add a file group

- Click 'Add File Group'
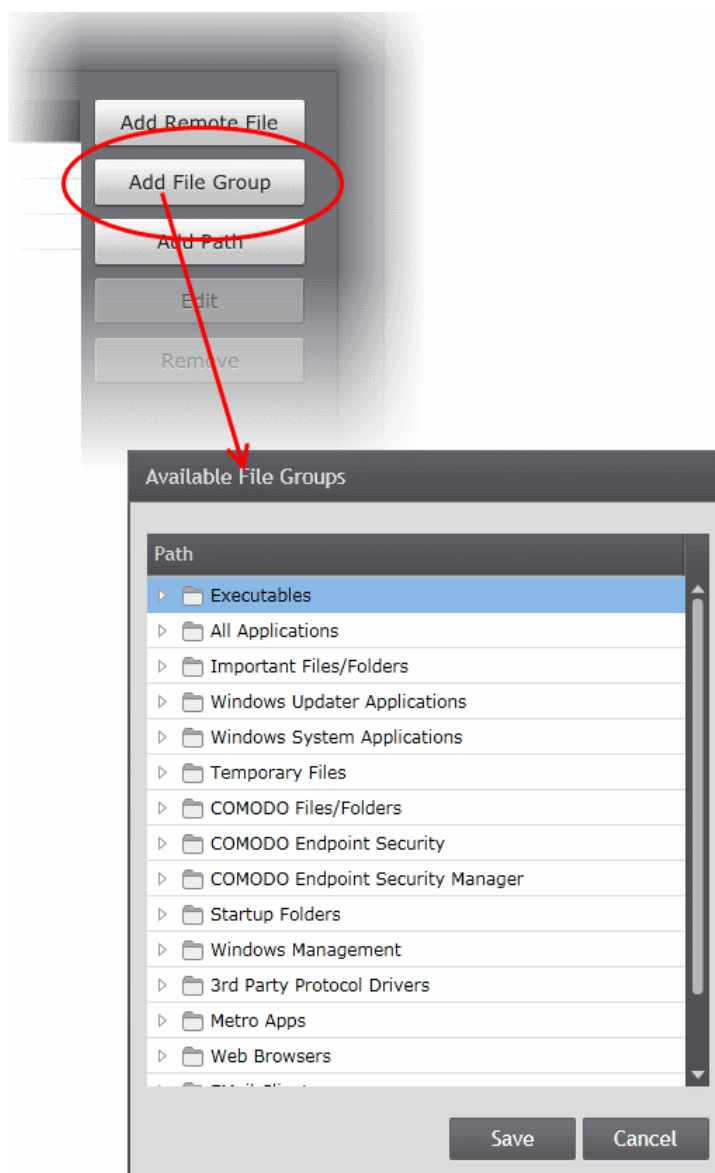
The 'Available File Groups' dialog will appear with a list of predefined and custom file groups created for the policy. The administrator can expand a group to view the member files by clicking the right arrow ▷ beside the file group name.

- Select the file group and click 'Save'.

- Repeat the process for adding more file groups.

- Click the 'Save' icon for the changes to take effect.

Adding a File Path

The administrator can add files and folders in 'Exclusions' list by selecting a standard folder and entering the path in the text field or by entering the entire path.

To add a file path

- Click 'Add Path'.
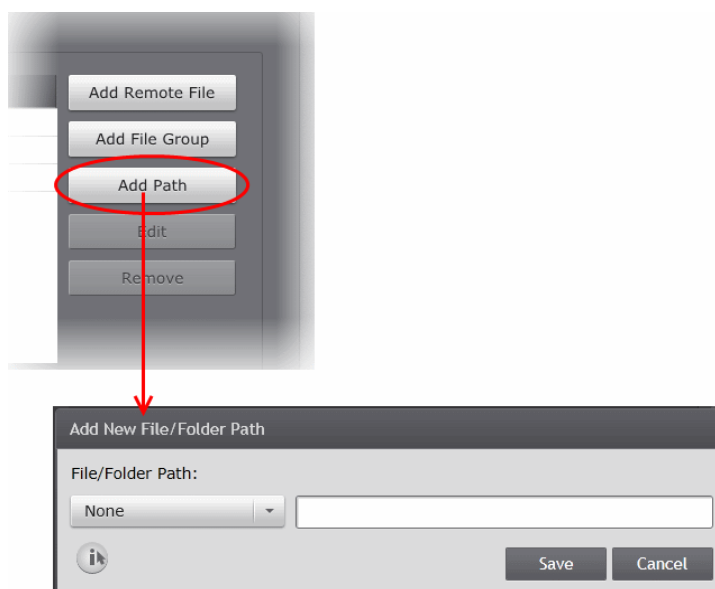
The 'Add New File/Folder Path' dialog will appear.

- Select the standard folder from the drop-down and enter the path/file name in the text box or enter the full folder/file path in the text box.
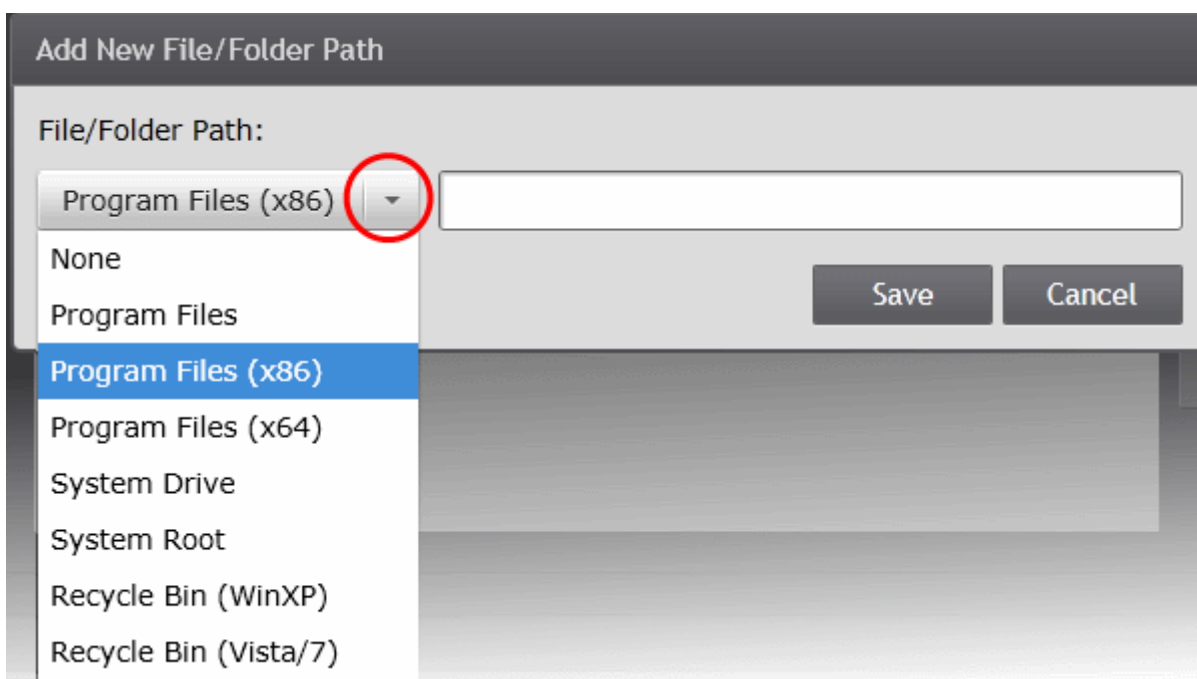
- Click Save in the 'Add New File/Folder Path' dialog

- Repeat the process for adding more folders/files groups.

- Click the 'Save' icon for the changes to take effect.

For more details on the Antivirus Settings on:

- CES - see the of CES - Antivirus Settings online help page at **https://help.comodo.com/topic-84-1-604-7469-Antivirus-Settings.html**

- CAVM - see the of CAVM - Scanner Settings online help page at **https://help.comodo.com/topic-155-1-282-2640-Scanner-Settings.html**

5.2.4. Configuring Firewall Settings

Firewall Settings screen allows an administrator to quickly configure the firewall security of an endpoint and the frequency of alerts that are generated.

Note: The 'Firewall Settings' interface allows the administrator to view and edit settings for the custom firewall profiles, and to view the configuration for the predefined profiles. The predefined profiles cannot be edited.

The Firewall Settings interface is available only for Windows Workstation Policy type.

To open the Firewall Settings interface, click on the 'Firewall' icon in the left pane. The Firewall Settings screen will be displayed.
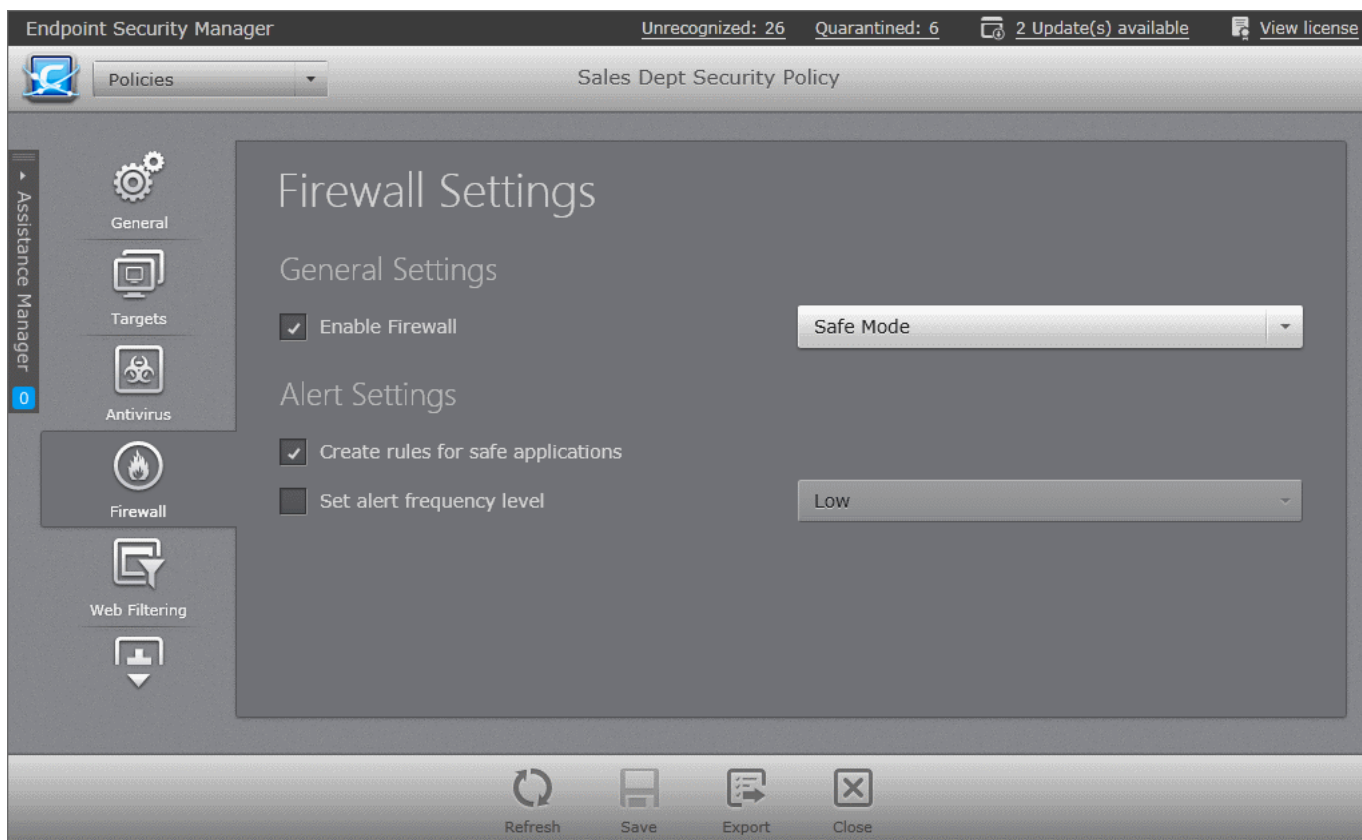
Click the links below for more details:

- **General Settings**
- **Alert Settings**

General Settings

The 'Enable Firewall' check box is disabled meaning all incoming and outgoing connections are allowed irrespective of the restrictions set by the user. Comodo strongly advise against this setting to be enabled unless you are sure that you are not currently connected to any local or wireless networks. Selecting the 'Enable Firewall' check box allows an administrator to customize firewall security from the options in the drop-down:
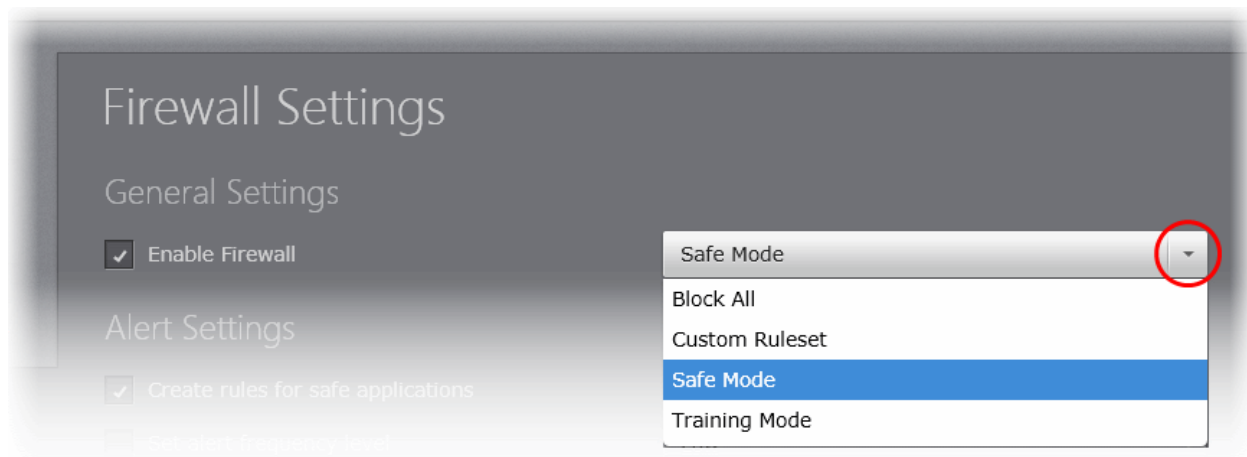
The choices available are:

- **Block All Mode**: The firewall blocks all traffic in and out of a computer regardless of any user-defined configuration and rules. The firewall does not attempt to learn the behavior of any applications and does not automatically create traffic rules for any applications. Choosing this option effectively prevents a computer from accessing any networks, including the Internet.

- **Custom Ruleset Mode**: The firewall applies ONLY the custom security configurations and network traffic policies specified by the administrator. New users may want to think of this as the 'Do Not Learn' setting because the firewall does not attempt to learn the behavior of any applications. Nor does it automatically create network traffic rules for those applications. The user will receive alerts every time there is a connection attempt by an application - even for applications on the Comodo Safe list (unless, of course, the administrator has specified rules and policies that instruct the firewall to trust the application's connection attempt).

   If any application tries to make a connection to the outside, the firewall audits all the loaded components and checks each against the list of components already allowed or blocked. If a component is found to be blocked, the entire application is denied Internet access and an alert is generated. This setting is advised for experienced firewall users that wish to maximize the visibility and control over traffic in and out of their computer.

- **Safe Mode** *(Default)*: While filtering network traffic, the firewall automatically creates rules that allow all traffic for the components of applications certified as 'Safe' by Comodo, if the checkbox Create rules for safe applications is selected. For non-certified new applications, the user will receive an alert whenever that application attempts to access the network. The administrator can choose to grant that application Internet access by selecting 'Treat this application as a Trusted Application' at the alert. This deploys the predefined firewall policy 'Trusted Application' onto the application.

   'Safe Mode' is the recommended setting for most users - combining the highest levels of security with an easy-to-manage number of connection alerts.

- **Training Mode**: The firewall monitors network traffic and create automatic allow rules for all new applications until the security level is adjusted. The user will not receive any alerts in 'Training Mode' mode. If you choose the 'Training Mode' setting, we advise that you are 100% sure that all applications installed on endpoints are assigned the correct network access rights.

> **Tip**: Use this setting temporarily while playing an online game for the first time. This suppresses all alerts while the firewall learns the components of the game that need Internet access and automatically create 'allow' rules for them. You can switch back to your previous mode later.

Alert Settings

Create rules for safe applications:

Comodo Firewall trusts the applications if:

- The application/file is included in the Trusted Files list under File Rating Settings;
- The application is from a vendor included in the Trusted Software Vendors list under File Rating Settings;
- The application is included in the extensive and constantly updated Comodo safelist.

By default, CES learns the behavior of safe applications and automatically generates the 'Allow' rules for them. These rules are listed in the Application Rules interface of CES. The Advanced users can edit/modify the rules as they wish.

• Deselect this check box if you do not want CES to create rules for safe applications automatically.

Set alert frequency level:

Administrators can configure the amount of alerts that Comodo Firewall generates, from the drop-down. It should be noted that this does not affect your security, which is determined by the rules you have configured (for example, in 'Application Rules' and 'Global Rules' in CES'). For the majority of users, the default setting of 'Low' is the perfect level - ensuring you are kept informed of connection attempts and suspicious behaviors whilst not overwhelming you with alert messages.

The Alert settings refer only to connection attempts by applications or from IP addresses that you have not (yet) decided to trust. For example, you could specify a very high alert frequency level, but not receive any alerts at all if you have chosen to trust the application that is making the connection attempt.
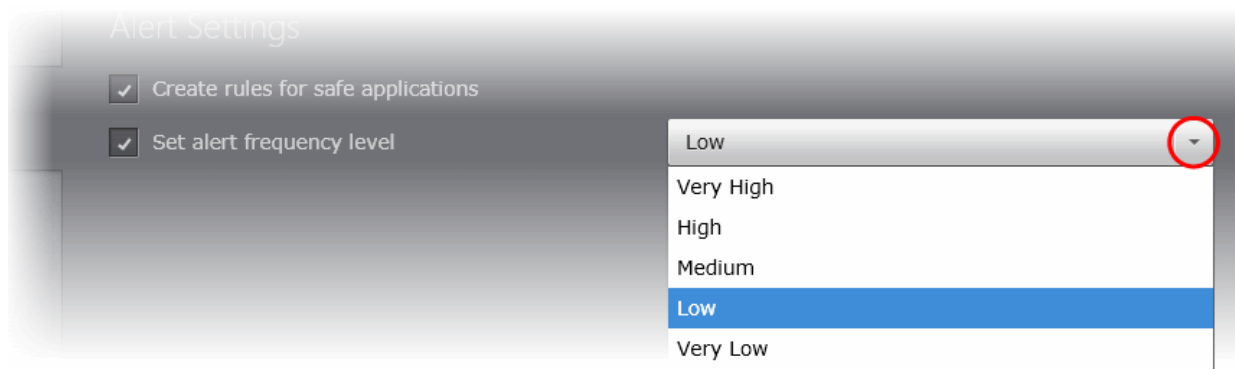
The options available are:

• **Very High**: The firewall shows separate alerts for outgoing and incoming connection requests for both TCP and UDP protocols on specific ports and for specific IP addresses, for an application. This setting provides the highest degree of visibility to inbound and outbound connection attempts but leads to a proliferation of firewall alerts. For example, using a browser to connect to your Internet home-page may generate as many as 5 separate alerts for an outgoing TCP connection alone.

• **High**: The firewall shows separate alerts for outgoing and incoming connection requests for both TCP and UDP protocols on specific ports for an application.

• **Medium**: The firewall shows alerts for outgoing and incoming connection requests for both TCP and UDP protocols for an application.

• **Low**: The firewall shows alerts for outgoing and incoming connection requests for an application. This is the setting recommended by Comodo and is suitable for the majority of users. (**Default**)

• **Very Low**: The firewall shows only one alert for an application.

Click the 'Save' icon for any changes to the settings to take effect.

For more details on the Firewall Settings, , see the of CES - Firewall Settings online help page at
http://help.comodo.com/topic-84-1-604-7471-Firewall-Settings.html

5.2.5. Configuring Website Filtering Settings

The Website filtering interface allows you to set up rules to allow or block access to specific websites from the endpoints to which the policy is applied. You can add trusted websites to whitelist, for allowing access to them and add websites to be always blocked to blacklist for preventing access to them by the endusers. You can also create and manage custom categories of websites, which can be selectively allowed or blocked. This is useful when you wish to block access to certain websites by a specific group of endpoints, while allowing them to other groups. The custom website category created for one Windows Workstation type policy will be available to all Windows Workstation type policies.

The Website Filtering panel can be accessed by clicking Security Settings > Firewall > Website Filtering tab from 'Advanced Settings' interface.

Note: The 'Website Filtering' interface allows the administrator to view and edit custom filtering profiles, and to view the

configuration for predefined profiles. Predefined profiles cannot be edited.

The 'Website Filtering' interface is available only for Windows Workstation Policy type.

To open the Website Filtering Settings interface, click on the 'Web Filtering' icon in the left pane.
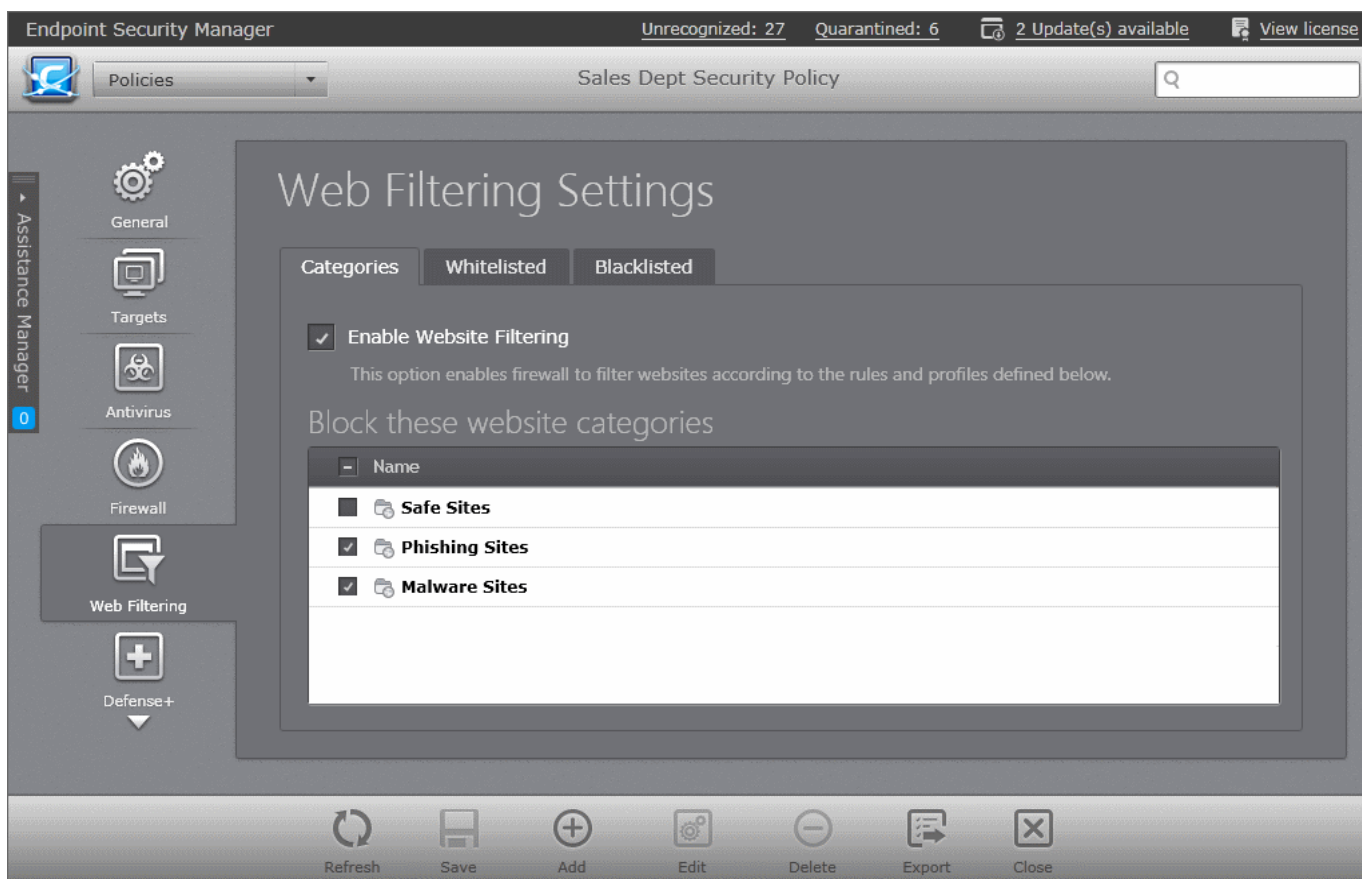
- To enable website filtering for the policy, select the 'Enable Website Filtering' checkbox.

The interface contains three tabs:

- **Categories** - Enables you to create and manage categories of websites. You can selectively allow or block access to all the websites in a category by selecting or deselecting it from the categories interface. Refer to the section '**Adding and Managing Website Categories**' for more details.

- **Whitelisted** - Enables you to add trusted websites to whitelist, to allow access to them. Refer to the section '**Adding and Managing Whitelisted Websites**' for more details.

- **Blacklisted** - Enables you to add websites to be blocked to Blacklist. Refer to the section '**Adding and Managing Blacklisted Websites**' for more details.

5.2.5.1. Adding and Managing Website Categories

CESM allows you to define website categories, each containing a set of websites. You can configure to allow or block a certain category as per a policy, meaning all the websites within the category will be allowed or blocked accordingly.

Brief Overview:

- CES constructs website filtering rules from one or more 'categories'.

- A category is a collection of one or more URL 'patterns'.

- A URL pattern can be a straight list of domain names and/or filtered terms (for example 'contains', 'starts with', 'equal to', etc.)

CESM ships with three preset categories of websites, 'Comodo Safe category', 'Comodo Phishing category' and 'Comodo

Malware category', which can be chosen to be allowed or blocked as per the policy. These categories are non-modifiable lists and are managed by Comodo. In addition to the pre-defined lists, the administrator can create custom categories with lists of websites and can selectively allow or block access to them as per the policy. A category created for one policy will be available across all policies for creating the web filtering rule.

General Advice:

It is the 'Categories' section where you specify the website(s) you wish to block or allow.

When choosing to block websites, you will be required to specify which categories should be included. You can elect to use just the pre-defined Comodo categories but, if you wish to filter specific websites, you will need to create your own category.

For example, if you wanted to block youtube.com and certain other leisure websites, you would create a category containing www.youtube.com and other leisure websites and select it under 'Block these website categories' pane.

The 'Categories' tab allows the administrator to create custom categories and manage them and select them to be blocked as per the policy.

- To open the 'Categories' interface, click the 'Categories' tab in the 'Web Filtering Settings' configuration screen.
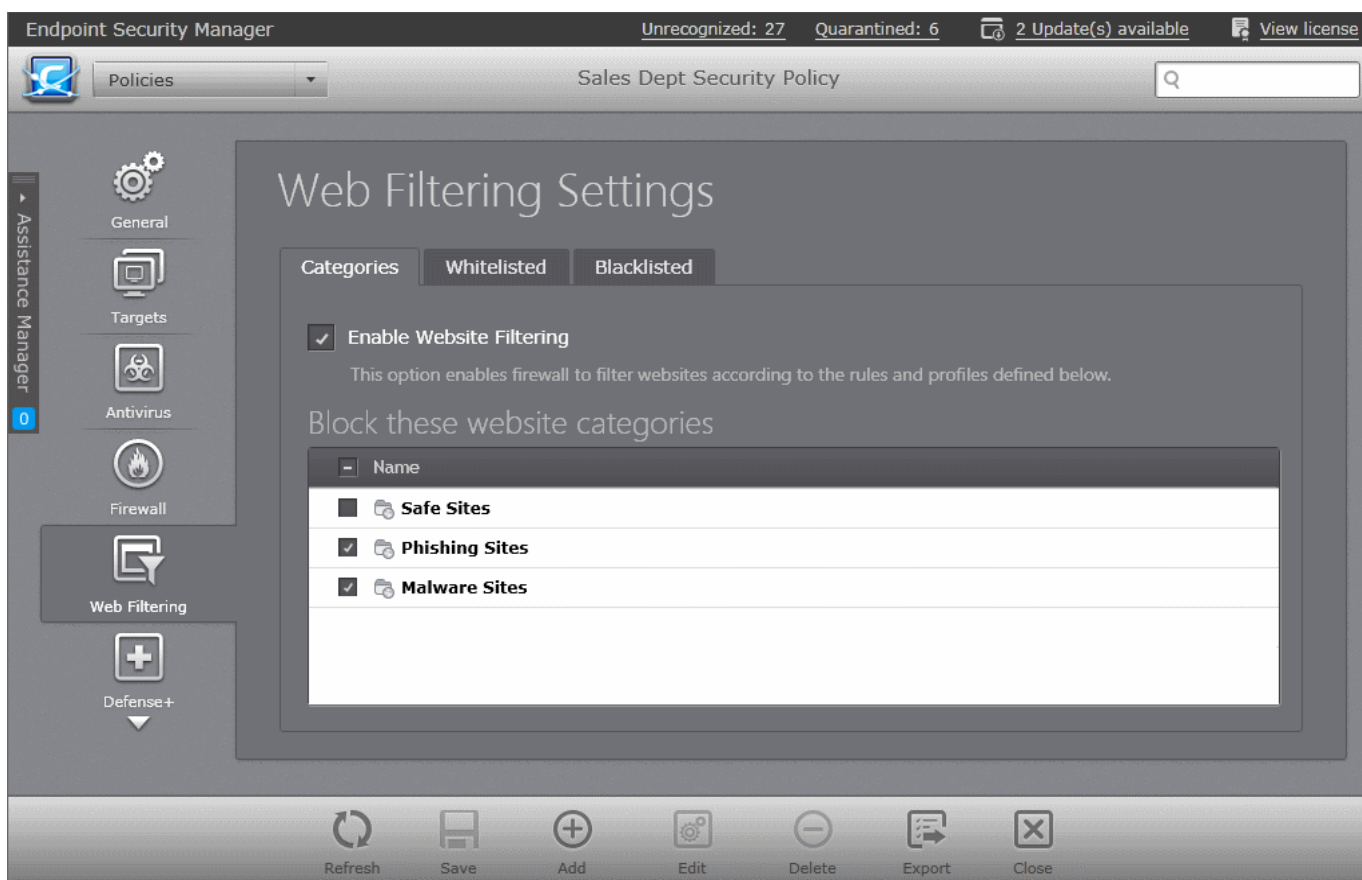
Following sections explain in detail on the tasks that can be accomplished through the 'Categories' interface:

- **Adding website categories**
- **Blocking access to selected website categories**
- **Editing a category**
- **Removing a category**

Adding Website Categories

Adding a new category involves two steps:

- **Step 1 - Create a category and define a name for the category**
- **Step 2 - Add Website to be included to the category**

Step 1 - Create a category and define a name for the category

- Open the 'Categories' pane by choosing Policies from the drop-down at the top left and clicking 'Categories' tab
- Click 'Add' from the 'Categories' pane

The 'Add New Category' dialog will appear.
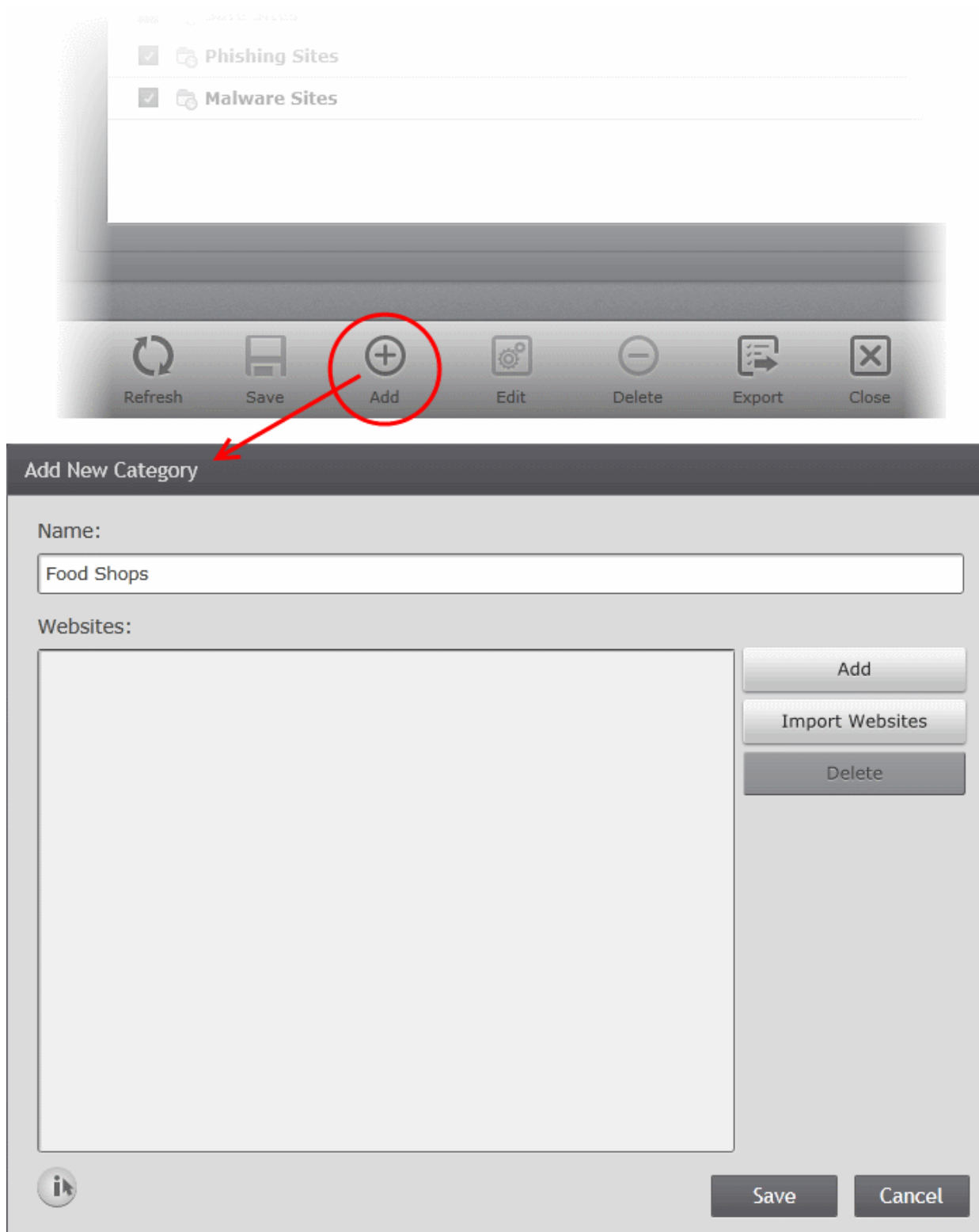
- Enter a name for the category in the 'Name' textbox.
- Enter the URLs of the websites to be added to the category.

Step 2 - Add Website to be included to the category

You can add websites to a category in two ways:

- **Manually Specify Websites one by one**

- **Upload Websites from a text file**

To manually specify URLs

- Click 'Add' from the 'Add New Category' dialog

- A text field for manually entering the URL in the right hand side pane

- Enter the full URL or a part of URL with a wildcard character '*' of the website(s) to be included in the category.

  To add a specific website/webpage, enter the full URL of the website/webpage

  - To include all sub-domains of website, add a wildcard character and a period in front of the URL. For example, *.friskywenches.com will cover friskywenches.com, login.friskywenches.com, pictures.friskywenches.com, videos.friskywenches.com and so on.
  - To include all the websites with URLs that start with a specific string, add a wildcard character after the string. For example, "pizza*" will cover 'pizzahut.com', pizzacorner.com, and so on.
  - To include all the websites with URLs that contain a specific string, add the wildcard character before and after the string. For example, "*pizza*" will cover hotpizza.com, spicypizza.com and so on.

The website will be added to the category.

- Repeat the process to add more websites.

- Click 'Save'.

The category will be added to the list in the 'Categories' pane.

To upload the list of websites from a text file

- Click 'Import Websites' from the 'Add New Category' dialog

- Navigate to the text file containing the list of URLs of the Websites to be added to the category.

Tip: The text file should contain only the list of full URLs or URLs with wildcard character (*) of the websites. The file should be of the '.txt' format.
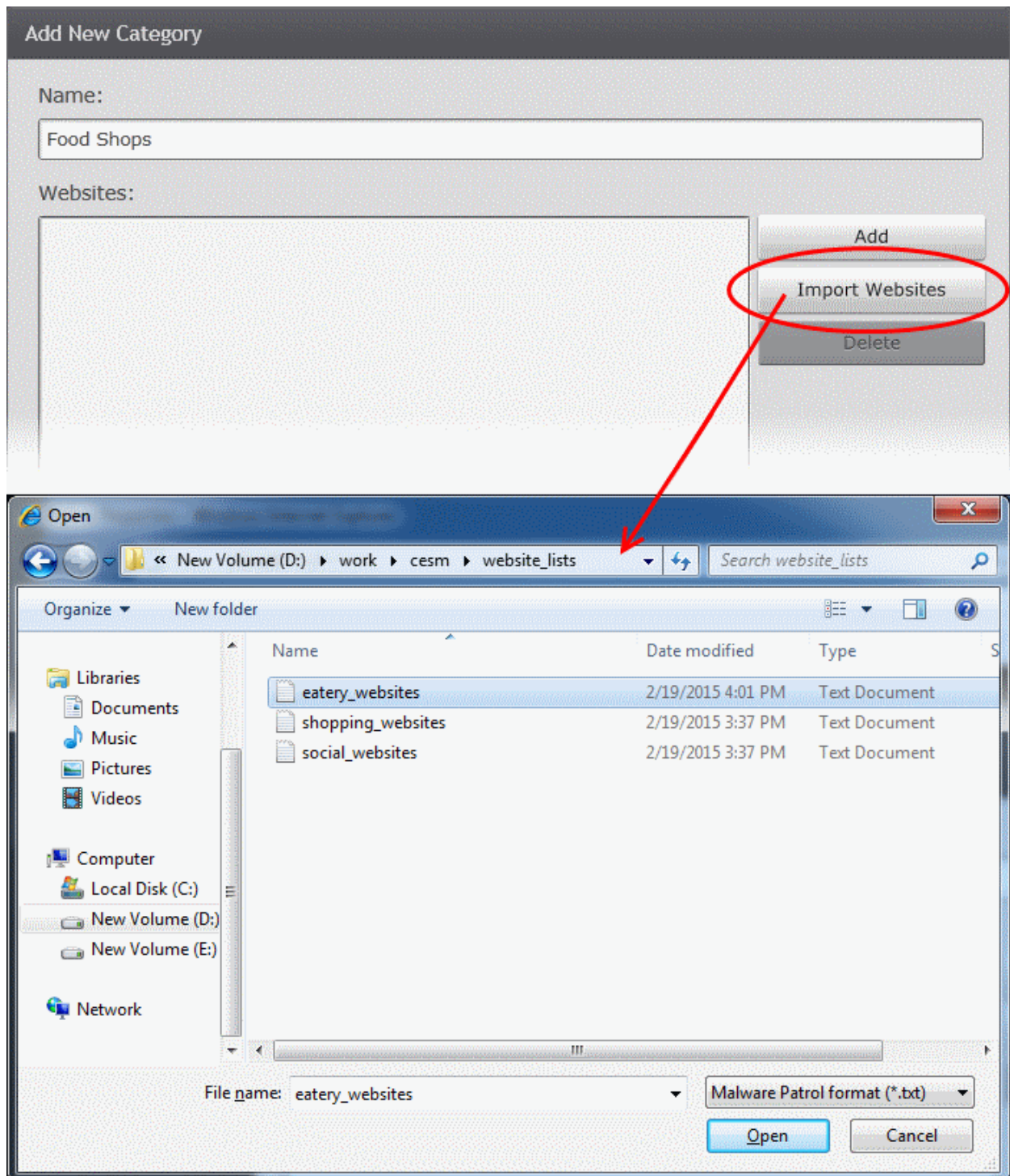
- Click 'Open'.

All the websites in the list will be automatically imported to the category.

- Click 'Save'.

The category will be added to the list in the 'Categories' pane.

Blocking Access to Selected Website Categories

You can create rules to block access to websites in selected categories from the 'Categories' interface.

To block access to selected categories

- Open the 'Categories' pane by choosing 'Policies' from the drop-down at the top left and clicking 'Categories' tab
- Ensure that the 'Enable Website Filtering' checkbox is selected

- Select the categories to be blocked from the list of categories in the 'Block these website categories' pane
- Click 'Save'.

Website Filtering rules will be created for the policy and the access to the websites included in the selected categories will be blocked from the endpoints or groups of endpoints to which the policy is applied.

Editing a Category

You can add change the name, new websites and remove websites from a category by editing it.

To edit a category

- Open the 'Categories' pane by choosing 'Policies' from the drop-down at the top left and clicking 'Categories' tab.
- Select the category to be edited from the 'Block these website categories' pane.
- Click 'Edit'. The Edit Category dialog will open
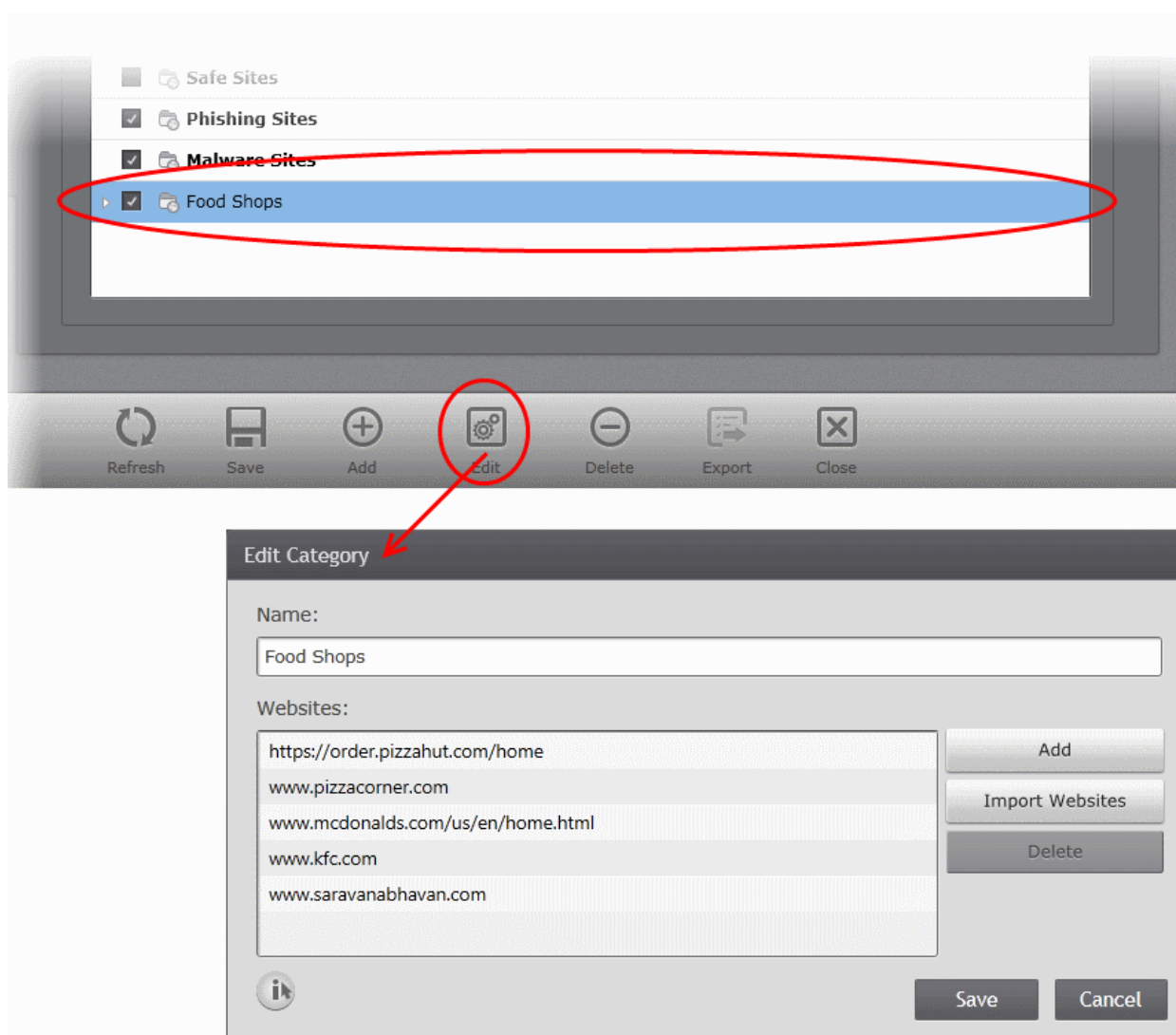
- To rename the category, directly edit the name in the 'Name' text field.
- To remove a website, select the website and click 'Delete'.
- To add new websites, click 'Add' for manually entering the websites or click import to import a list of websites from a text file. Refer to the explanation of **adding websites** in the section **Adding Website Categories** for more details.
- Click 'Save' in the 'Edit Category' dialog
- Click 'Save' in the 'Categories' interface for your changes to take effect.

Removing a Category

You can remove unwanted categories from the Categories by selecting the category and clicking 'Delete'.

5.2.5.2. Adding and Managing Whitelisted Websites

CESM policies allow you to create a whitelist of websites to which managed endpoints should always be permitted access.

The whitelist 'over-rules' any conflicting Firewall or website filtering rules created under the 'Categories' tab. Access will be allowed to whitelisted websites even if the site is also listed in a category of blocked websites. Hence it is recommended to add only trustworthy websites to the whitelist.

The 'Whitelisted' tab allows the administrator to add websites to the whitelist and manage the list.

- To open the 'Whitelisted' interface, click the 'Whitelisted' tab in the 'Web Filtering Settings' configuration screen.
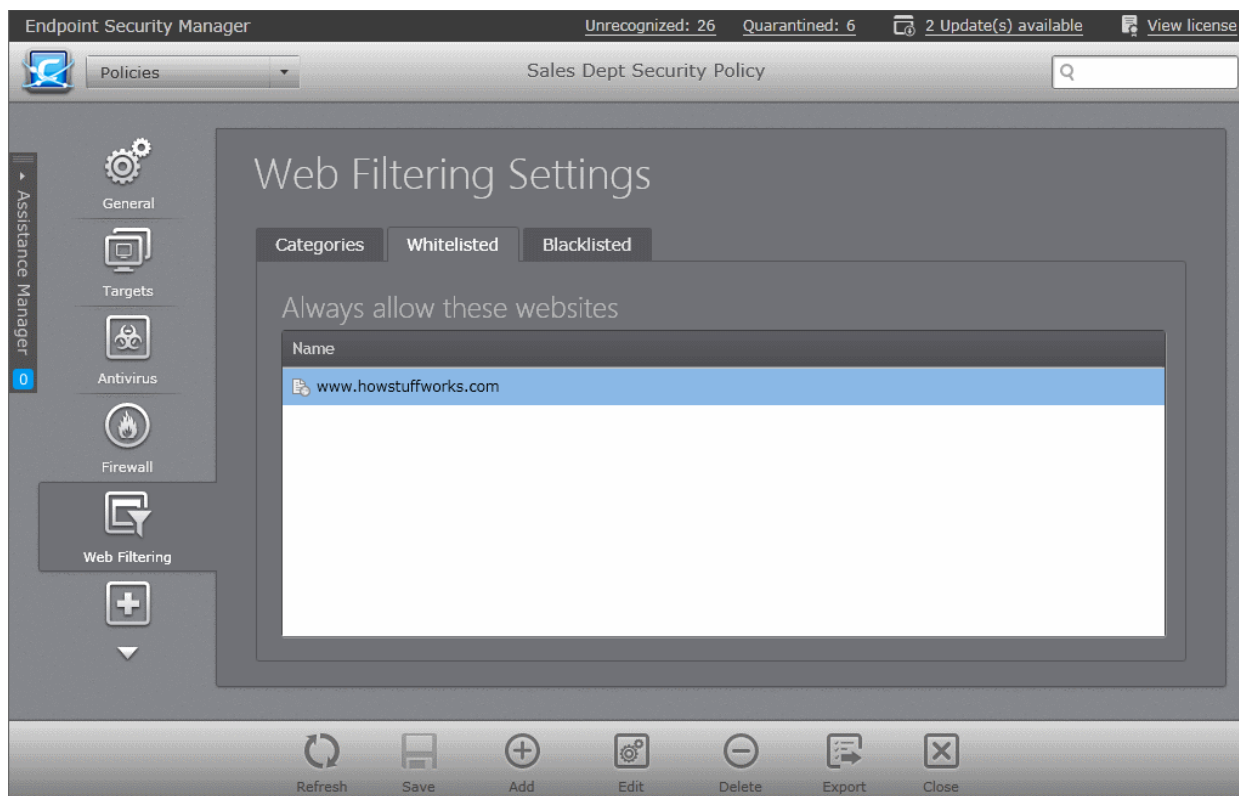
The following sections explain in detail on the tasks that can be accomplished through the 'Whitelisted' interface:

- **Adding websites to the Whitelist**

- **Editing a website address**

- **Removing a website**

Adding Websites to the Whitelist

Administrators can manually add websites by entering their URLs. Once added, the site will available to endpoint users or groups to which the policy is applied.

To add whitelisted websites

- Open the 'Whitelisted' pane by choosing 'Policies' from the drop-down at the top left and clicking 'Whitelisted' tab
- Click 'Add' from the 'Whitelisted' pane

The 'Add New Website' dialog will appear.
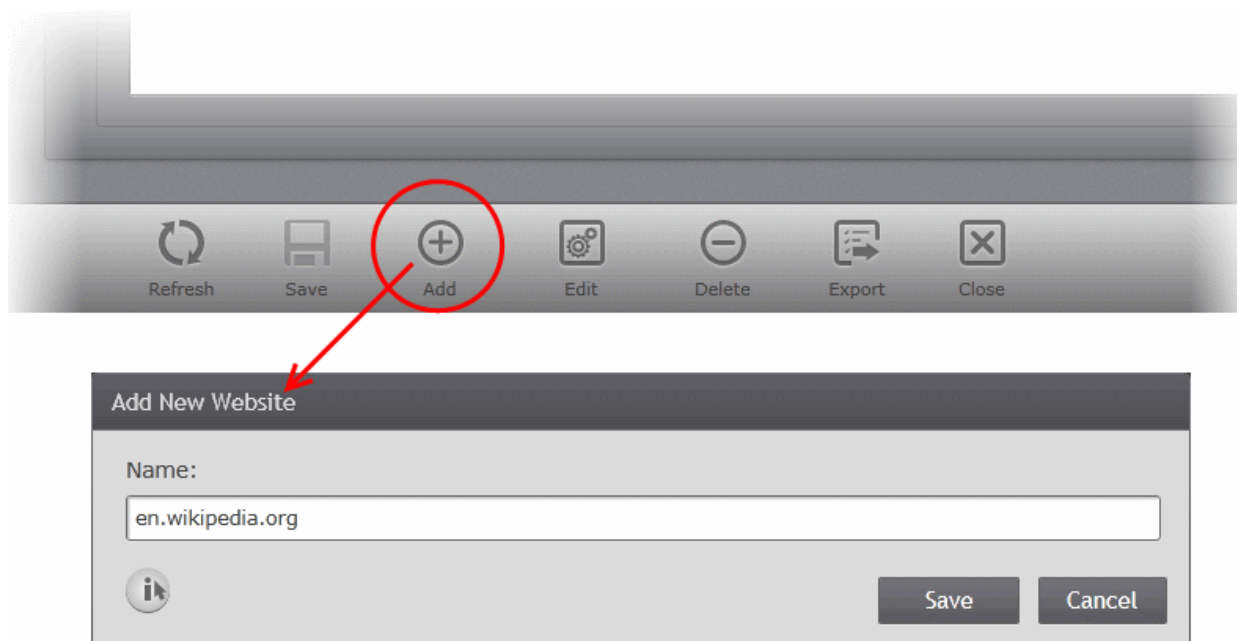
- Enter the URL of the website in the 'Name' text field and click 'Save'
- Repeat the process to add more websites one-by-one.
- Click 'Save' in the Whitelisted interface for your changes to take effect.

Editing a Website Address

The administrator can edit the URL of a website added to whitelist at anytime.

To edit a website address

- Open the 'Whitelisted' pane by choosing 'Policies' from the drop-down at the top left and clicking 'Whitelisted' tab
- Select the website address to be edited and click 'Edit' from the 'Whitelisted' interface

The 'Edit Website' dialog will appear.

- Directly edit the URL of the website in the 'Name' text field and click 'Save'.

- Click 'Save' in the Whitelisted interface for your changes to take effect.

Removing a Website

Removing a site from the whitelist will remove it's 'exemption' from other firewall or web filtering rules, so may result in users not being able to access the site.
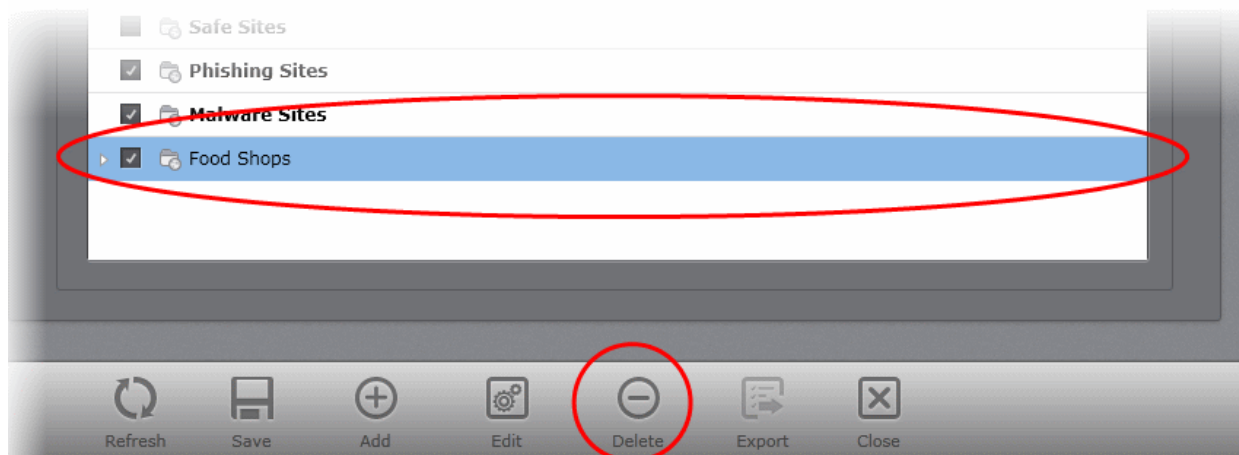
To remove a whitelisted website

- Open the 'Whitelisted' pane by choosing 'Policies' from the drop-down at the top left and clicking 'Whitelisted' tab.

- Select the website address(s) to be removed. You can select several entries to be removed at once by using Shift or Ctrl keys.

- Click 'Delete'. A confirmation dialog will be displayed.
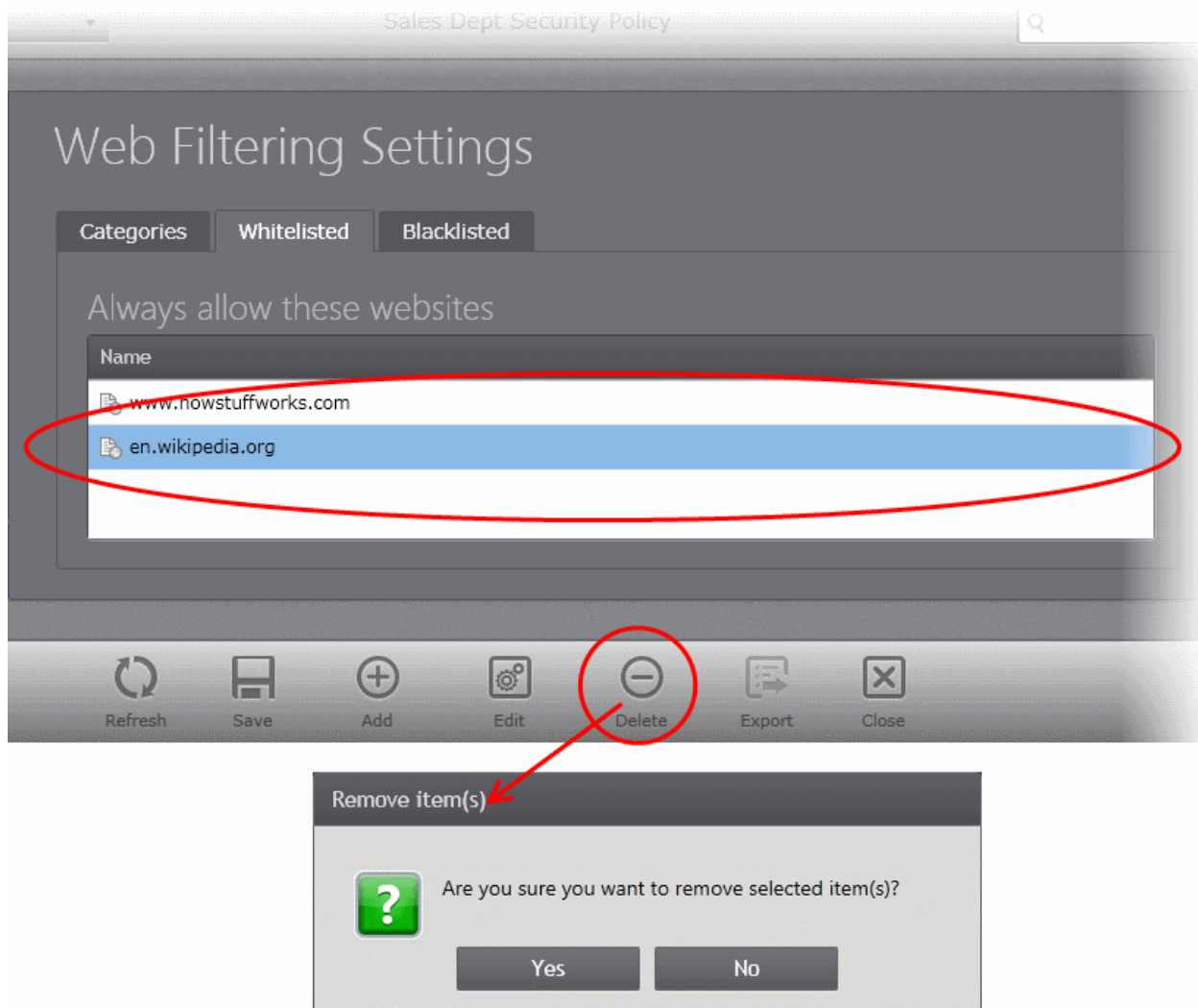
- Click 'Yes'.
- Click 'Save' in the Whitelisted interface for your changes to take effect.

5.2.5.3. Adding and Managing Blacklisted Websites

CESM policies allow you to create a list of websites which should not be accessible from managed endpoints.

The 'Blacklisted' tab allows the administrator to add websites to the blacklist and manage the list.

- To open the 'Blacklisted' interface, click the 'Blacklisted' tab in the 'Web Filtering Settings' configuration screen.
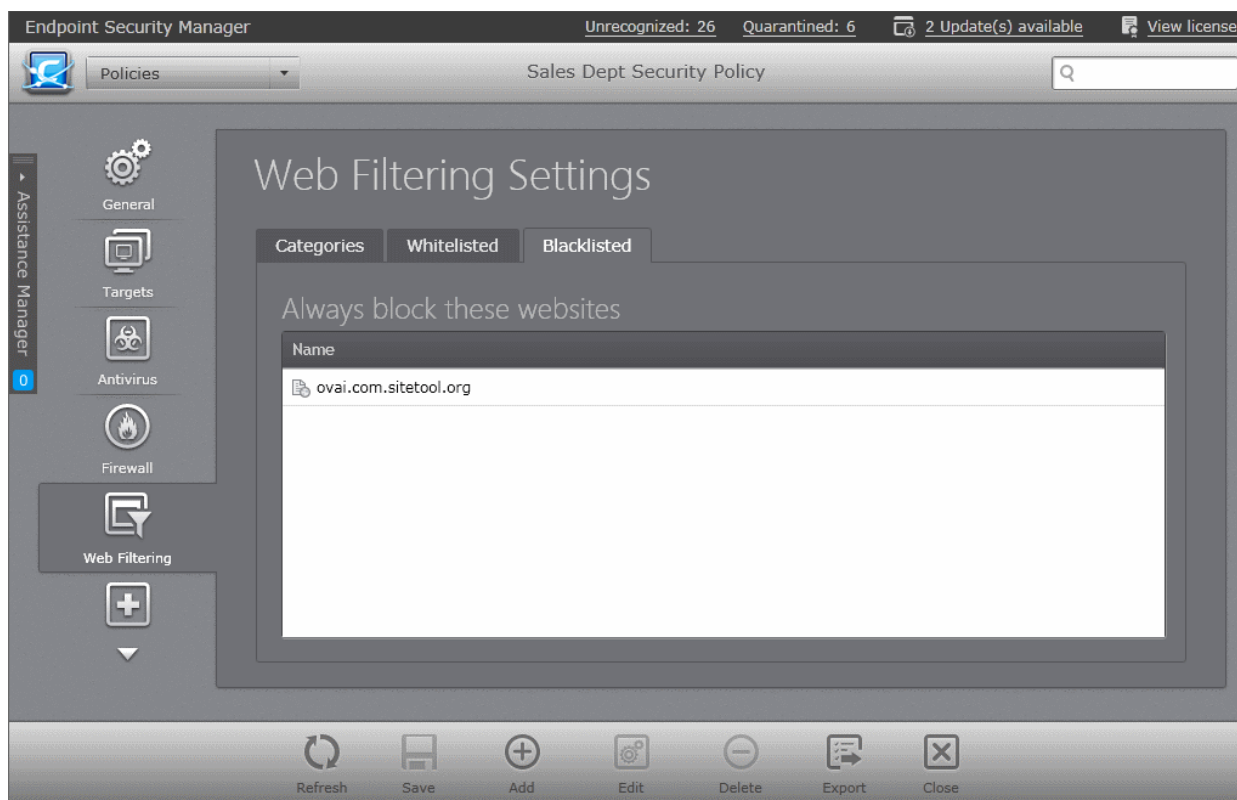
The following sections explain in detail on the tasks that can be accomplished through the 'Blacklisted' interface:

- **Adding websites to the Blacklist**
- **Editing a website address**
- **Removing a website from the blacklist**

Adding Websites to the Blacklist

Administrators can manually add sites which should be blocked to the endpoint users or groups to which the policy is applied .

To add blacklisted websites

- Open the 'Blacklisted' pane by choosing 'Policies' from the drop-down at the top left and clicking 'Blacklisted' tab.
- Click 'Add' from the 'Blacklisted' pane

The 'Add New Website' dialog will appear.
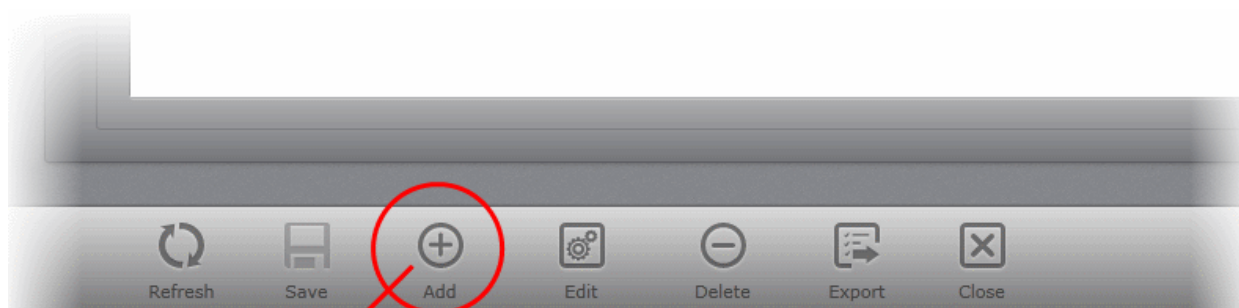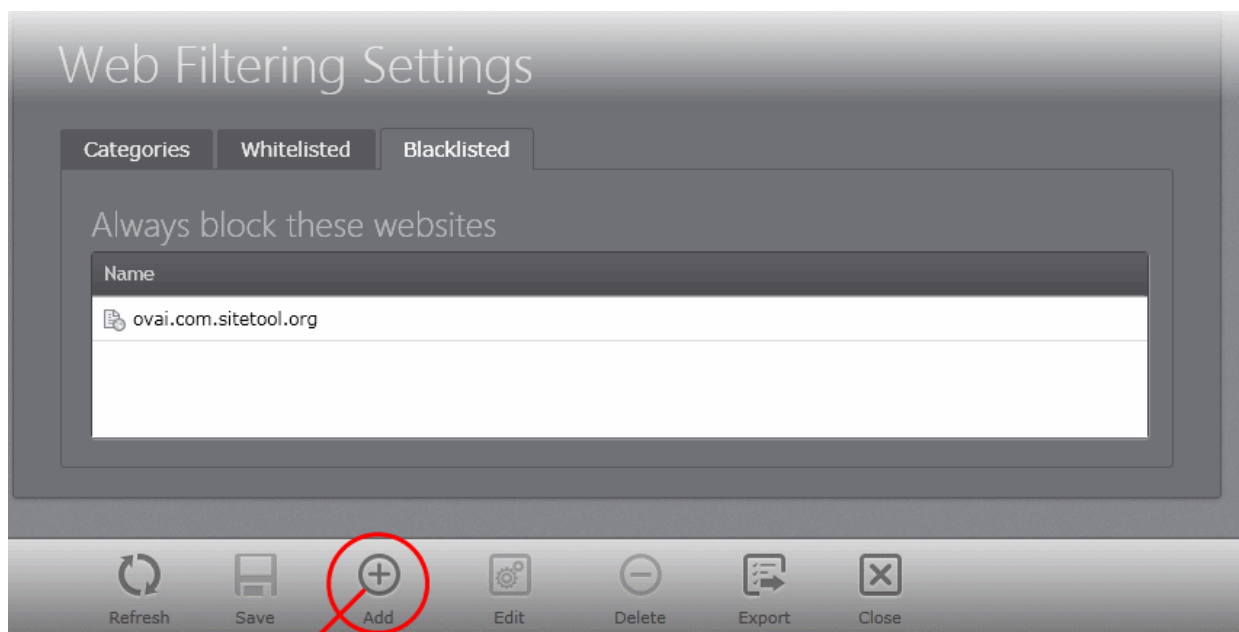
- Enter the URL of the website in the 'Name' text field and click 'Save'
- Repeat the process to add more websites one-by-one.
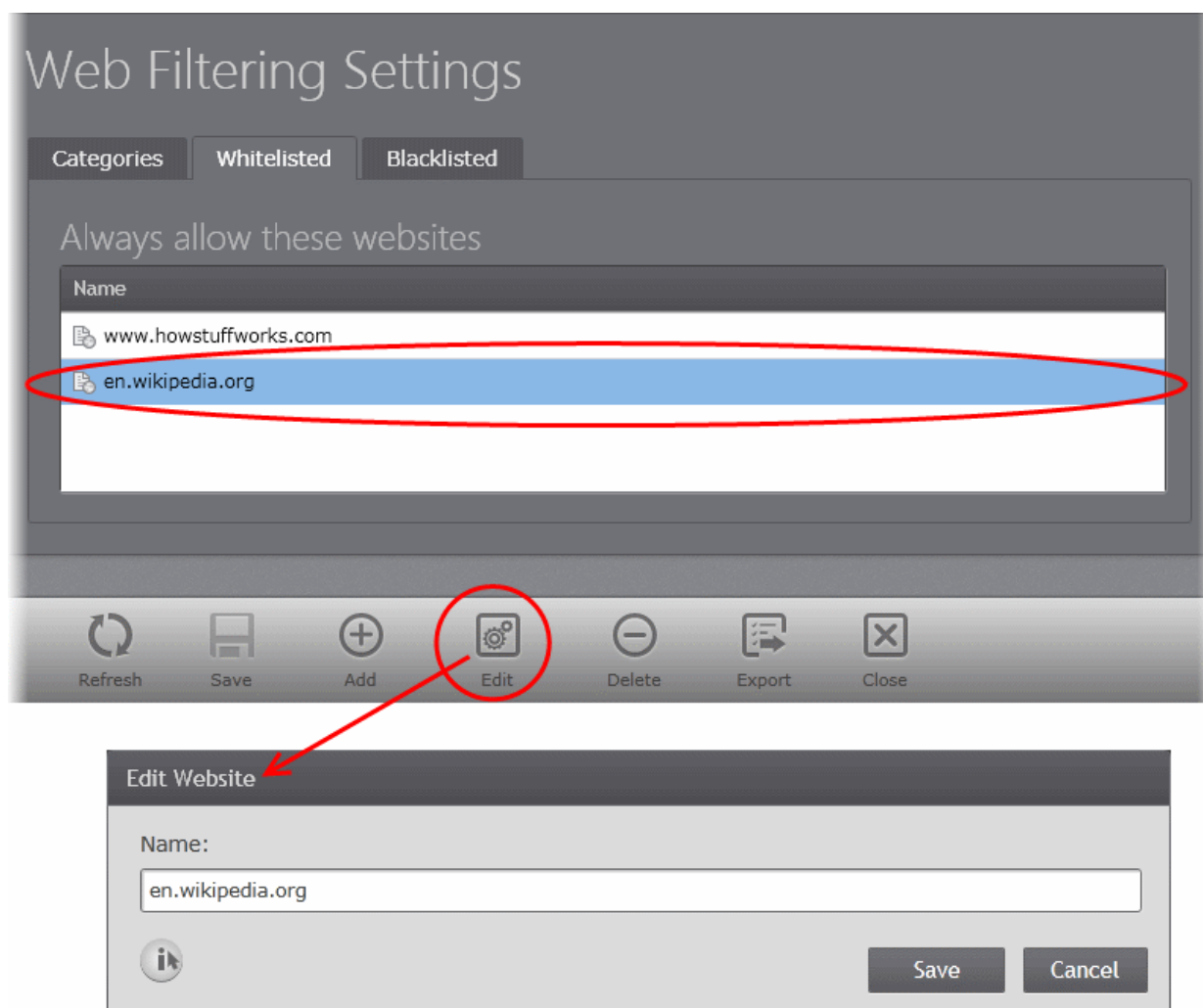- Click 'Save' in the 'Blacklisted' interface for your changes to take effect.

Editing a Website Address

The administrator can edit the URL of a website added to blacklist at anytime.

To edit a website address

- Open the 'Blacklisted' pane by choosing 'Policies' from the drop-down at the top left and clicking 'Blacklisted' tab

- Select the website address to be edited and click 'Edit' from the 'Blacklisted' interface
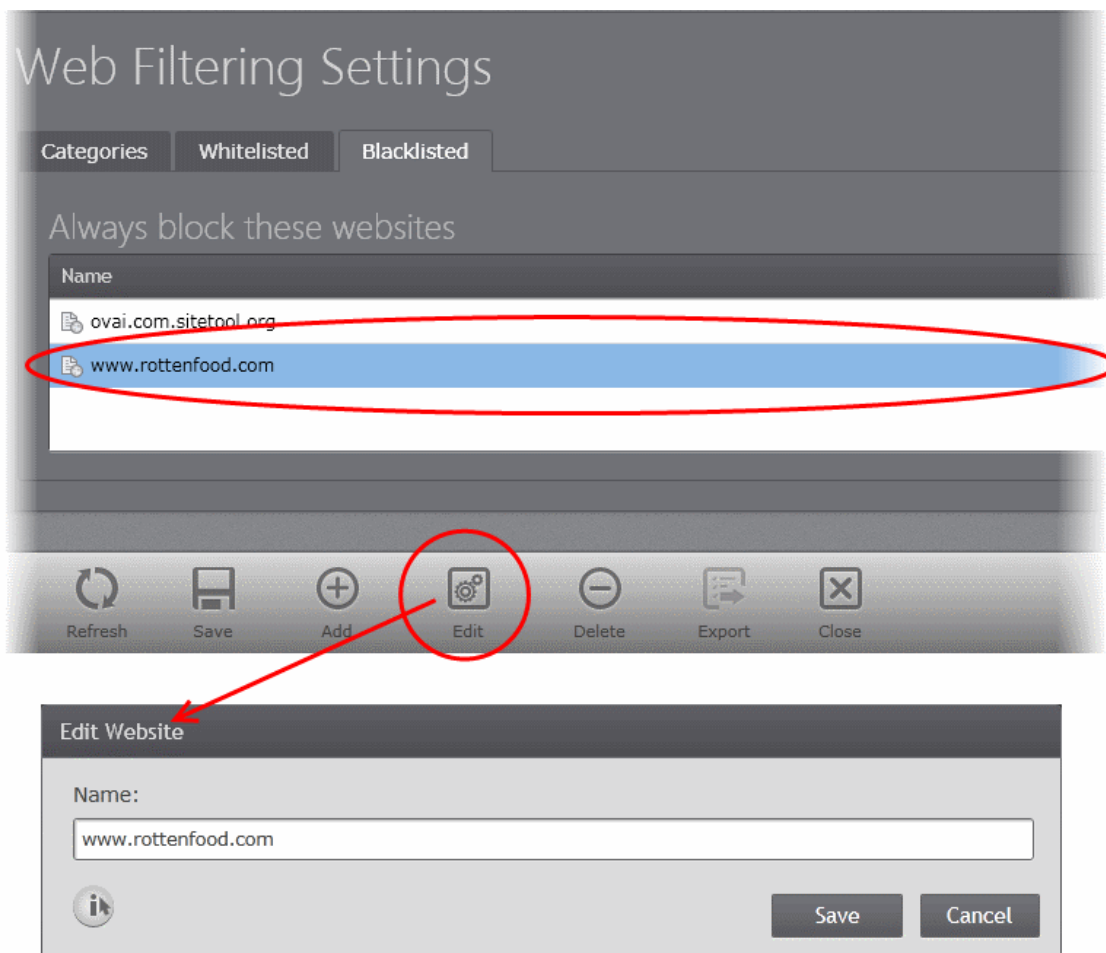
The 'Edit Website' dialog will appear.

- Directly edit the URL of the website in the 'Name' text field and click 'Save'.

- Click 'Save' in the 'Blacklisted' interface for your changes to take effect.

Removing a Website

Removing a website from the blacklist means users and groups under the policy will be able to access the site.

To remove a blacklisted website

- Open the 'Blacklisted' pane by choosing 'Policies' from the drop-down at the top left and clicking 'Blacklisted' tab.

- Select the website address(s) to be removed. You can select several entries to be removed at once by using Shift or Ctrl keys.

- Click 'Delete'. A confirmation dialog will be displayed.
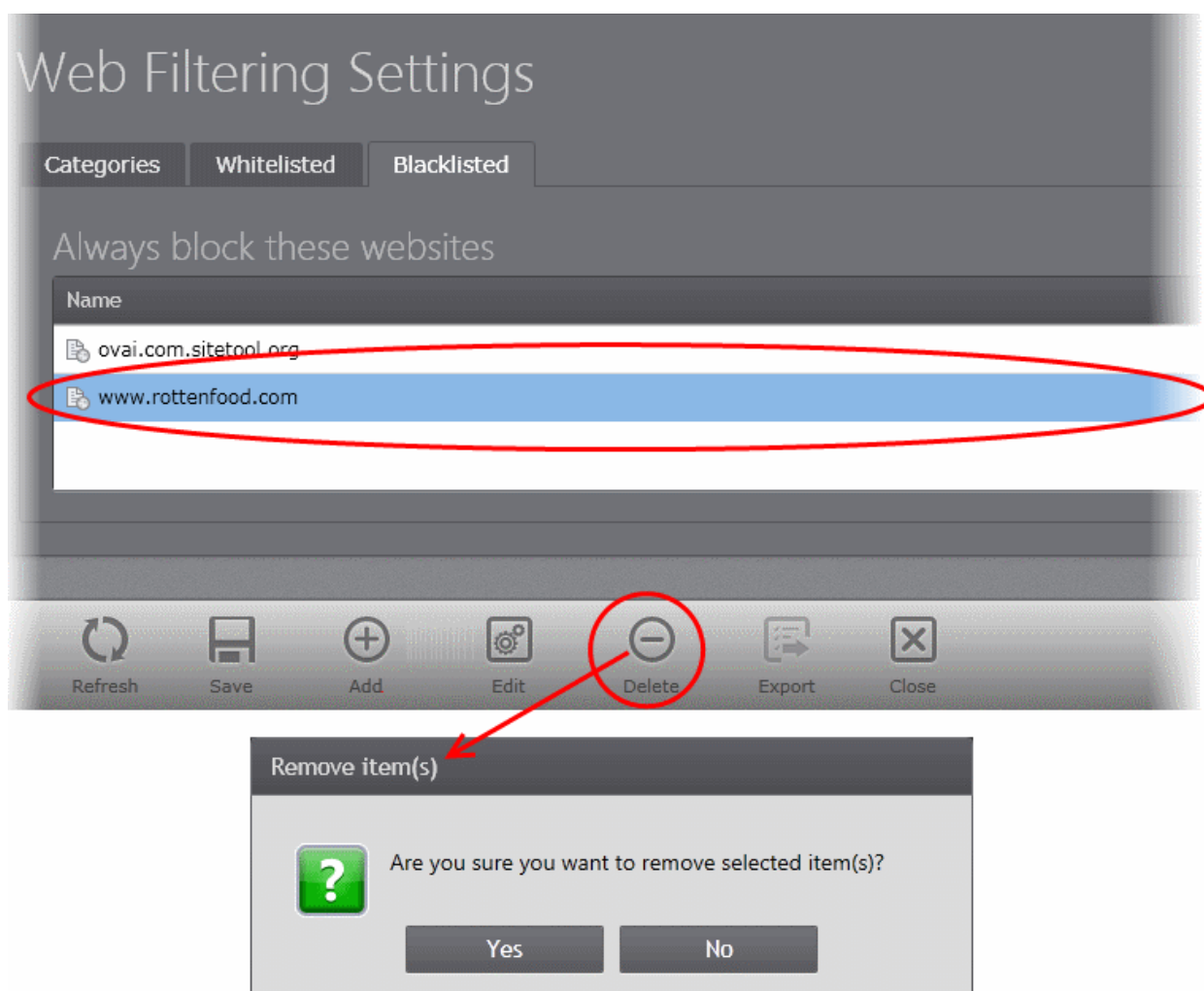
- Click 'Yes'.
- Click 'Save' in the Blacklisted interface for your changes to take effect.

5.2.6. Configuring Defense+ Settings

Defense+ is a collective term that covers the Host Intrusion Prevention (HIPS), Sandbox and Viruscope components of CES/CAS. Together, these technologies ensure all applications, processes and services on endpoints behave in a secure manner - and are prevented from taking actions that could damage endpoints or the data.

Note: The 'Defense+ Settings' interface allows the administrator to view and edit the Defense+ settings for custom policies and to view the configuration for the predefined policies. Predefined policies cannot be edited.

The 'Defense+' Settings interface is available only for 'Windows Workstation' Policy and 'Windows Servers' Policy types.

To open the Defense+ Settings interface, click on the 'Defense+' icon ![plus] in the left pane. The Defense+ Settings screen will be displayed.
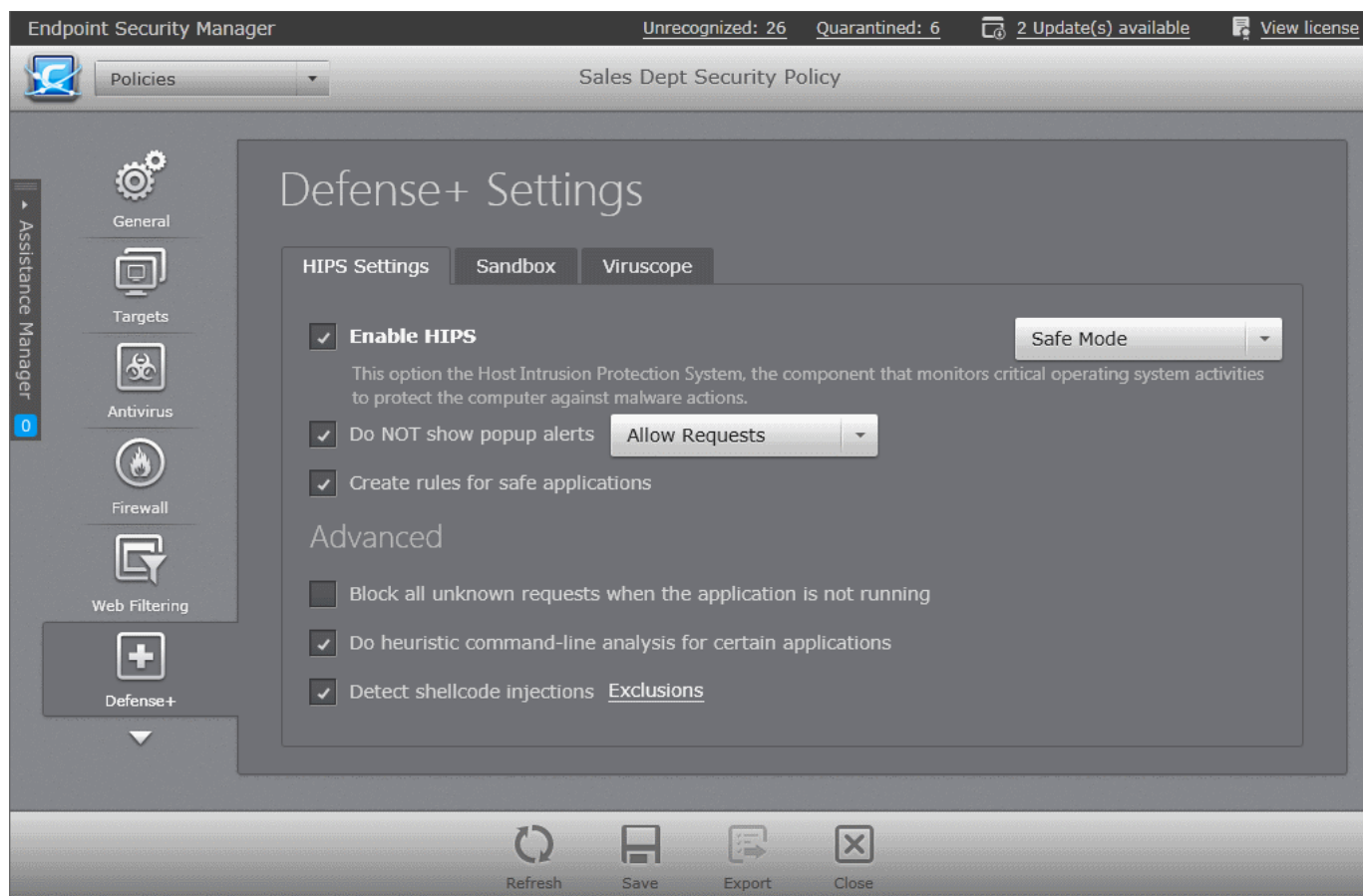
The Defense+ settings area allows an administrator to configure the following:

- **HIPS Behavior Settings**
- **Sandbox**
- **Viruscope**

> **Note**: The Sandbox and Viruscope features are available only in CES. The 'Sandbox' and 'Viruscope' tabs are visible only for 'Windows Workstation' Policy type and not for 'Windows Servers' Policy type.

HIPS Behavior Settings

HIPS constantly monitors system activity and only allows executables and processes to run if they comply with the prevailing security rules that have been enforced by the user. For the average user, CES/CAS ships with a default HIPS ruleset that works 'out of the box' - providing extremely high levels of protection without any user intervention. For example, HIPS automatically protects system-critical files, folders and registry keys to prevent unauthorized modifications by malicious programs. Advanced users looking to take a firmer grip on their security posture can quickly create custom policies and rulesets using the powerful rules interface.

> **Note for beginners**: This page often refers to 'executables' (or 'executable files'). An 'executable' is a file that can instruct your computer to perform a task or function. Every program, application and device you run on your computer requires an executable file of some kind to start it. The most recognizable type of executable file is the '.exe' file. (e.g., when you start Microsoft Word, the executable file 'winword.exe' instructs your computer to start and run the Word application). Other types of executable files include those with extensions .cpl .dll, .drv, .inf, .ocx, .pf, .scr, .sys.
>
> Unfortunately, not all executables can be trusted. Some executables, broadly categorized as malware, can instruct your computer to delete valuable data; steal your identity; corrupt system files; give control of your PC to a hacker and much more. You may also have heard these referred to as Trojans, scripts and worms.

General Settings
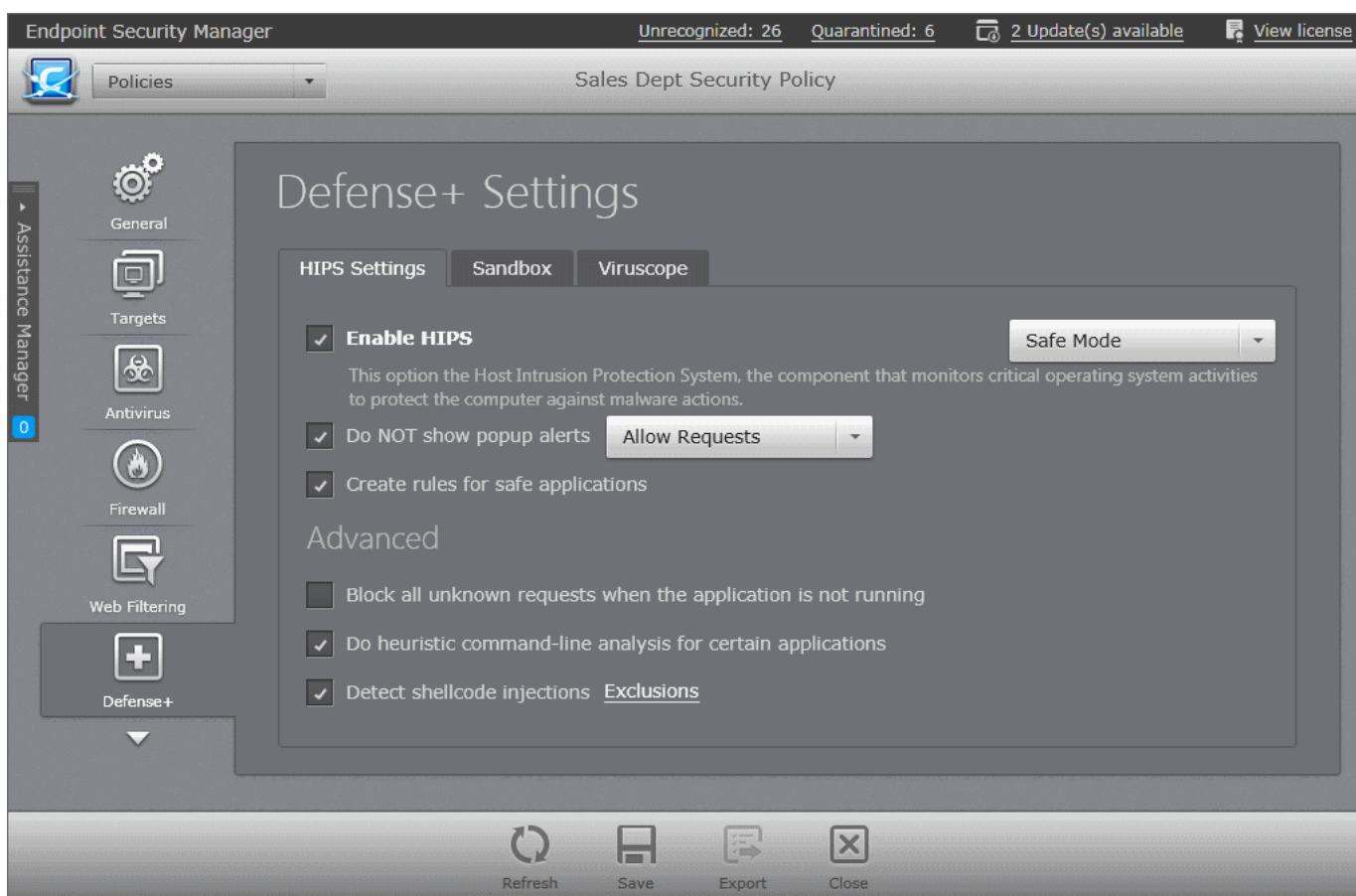
- • Enable HIPS - Allows the administrator to enable/disable the HIPS protection.*(Default=Disabled)*

If enabled, the administrator can choose the security level and configure the monitoring settings for the HIPS component. The security level can be chosen from the drop-down that becomes active only on enabling HIPS:

The choices available are:

- **Paranoid Mode:** This is the highest security level setting and means that Defense+ monitors and controls all executable files apart from those that you have deemed safe. CES/CAS does not attempt to learn the behavior of any applications - even those applications on the Comodo safe list and only uses your configuration settings to filter critical system activity. Similarly, the CES/CAS does automatically create 'Allow' rules for any executables - although you still have the option to treat an application as 'Trusted' at the Defense+ alert. Choosing this option generates the most amount of Defense+ alerts and is recommended for advanced users that require complete awareness of activity on their system.

- **Safe Mode:** While monitoring critical system activity, Defense+ automatically learns the activity of executables and applications certified as 'Safe' by Comodo. It also automatically creates 'Allow' rules these activities, if the checkbox '**Create rules for safe applications**' is selected. For non-certified, unknown, applications, you will receive an alert whenever that application attempts to run. Should you choose, you can add that new application to the safe list by choosing 'Treat this application as a Trusted Application' at the alert. This instructs the Defense+ not to generate an alert the next time it runs. If your machine is not new or known to be free of malware and other threats as in 'Clean PC Mode' then 'Safe Mode' is recommended setting for most users - combining the highest levels of security with an easy-to-manage number of Defense+ alerts.

- **Clean PC Mode:** From the time you select 'Clean PC Mode' option, Defense+ learns the activities of the applications currently installed on the computer while all new executables introduced to the system are monitored and controlled. This patent-pending mode of operation is the recommended option on a new computer or one that the user knows to be clean of malware and other threats. From this point onwards Defense+ alerts the user whenever a new, unrecognized application is being installed. In this mode, the files in 'Unrecognized Files' are excluded from being considered as clean and are monitored and controlled.

- **Training Mode:** Defense+ monitors and learn the activity of any and all executables and create automatic 'Allow' rules until the security level is adjusted. You do not receive any Defense+ alerts in 'Training Mode'. If you choose the 'Training Mode' setting, we advise that you are 100% sure that all applications and executables installed on your computer are safe to run.

- **Do NOT show popup alerts** - Configure whether or not the users are to be notified when the HIPS encounters a malware. Choosing 'Do NOT show popup alerts' will minimize disturbances but at some loss of user awareness. **(Default = Enabled)**

    - If you choose not to show alerts then you have a choice of default responses that CES should automatically take - either 'Block Requests' or 'Allow Requests'.
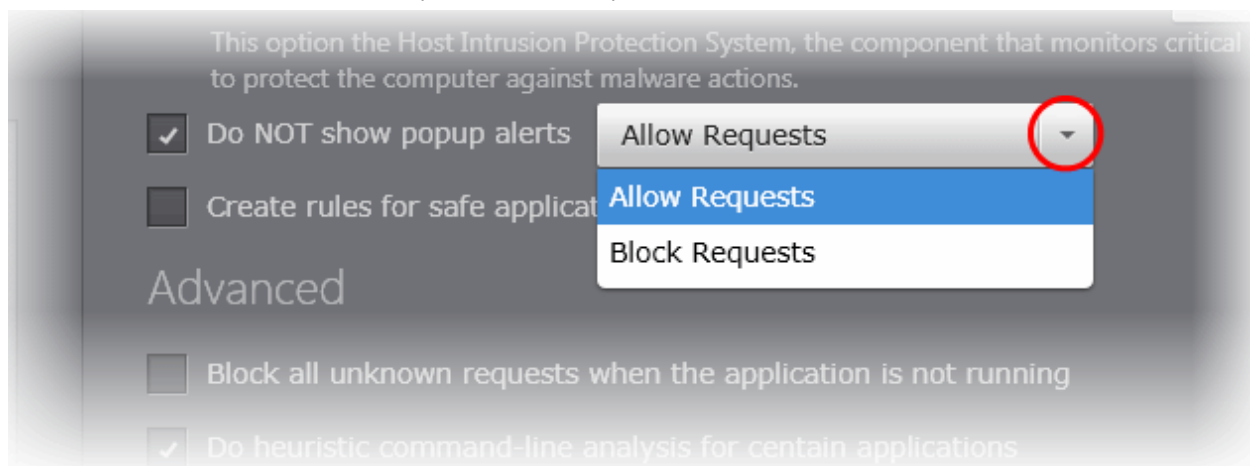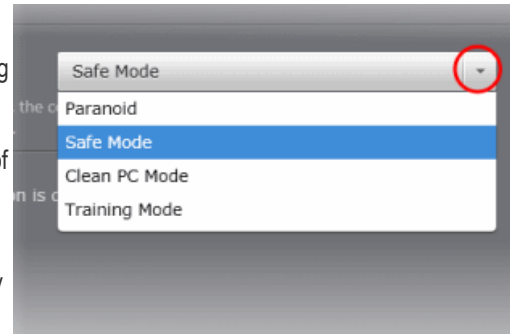
- Create rules for safe applications - Automatically creates rules for safe applications in HIPS Ruleset. **(Default = Enabled)**

Note: HIPS trusts the applications if:

- The application/file is included in the Trusted Files list.
- The application is from a vendor included in the Trusted Software Vendors list.
- The application is included in the extensive and constantly updated Comodo safelist.

By default, CES/CAS learns the behavior of safe applications and automatically generates the 'Allow' rules. These rules are listed in the HIPS Rules interface. Administrators can edit / modify the rules as they wish.

- If you do not want CES/CAS to create Allow rules for safe applications, de-select this checkbox

Advanced Settings

- **Block all unknown requests if the application is not running** - Selecting this option blocks all unknown execution requests if CES/CAS is not running/has been shut down. This is option is very strict indeed and in most cases should only be enabled on seriously infested or compromised machines while the user is working to resolve these issues. If you know your machine is already 'clean' and are looking just to enable the highest CES/CAS security settings then it is OK to leave this box unchecked. *(Default = Disabled)*

- **Do heuristic command-line analysis for certain applications** - Selecting this option instructs CES/CAS installations at the endpoints to perform heuristic analysis of programs that are capable of executing code such as visual basic scripts and java applications. Example programs that are affected by enabling this option are wscript.exe, cmd.exe, java.exe and javaw.exe. For example, the program wscript.exe can be made to execute visual basic scripts (.vbs file extension) via a command similar to 'wscript.exe c:\tests\test.vbs'. If this option is selected, CES detects c:\tests\test.vbs from the command-line and applies all security checks based on this file. If test.vbs attempts to connect to the Internet, for example, the alert will state 'test.vbs' is attempting to connect to the Internet *(Default = Enabled).*

- **Detect shellcode injections (i.e. Buffer overflow protection)** - Enabling this setting turns-on the Buffer over flow protection.

Background: A buffer overflow is an anomalous condition where a process/executable attempts to store data beyond the boundaries of a fixed-length buffer. The result is that the extra data overwrites adjacent memory locations. The overwritten data may include other buffers, variables and program flow data and may cause a process to crash or produce incorrect results. They can be triggered by inputs specifically designed to execute malicious code or to make the program operate in an unintended way. As such, buffer overflows cause many software vulnerabilities and form the basis of many exploits.

Turning-on buffer overflow protection instructs the CES/CAS to raise pop-up alerts in every event of a possible buffer overflow attack. The user can allow or deny the requested activity raised by the process under execution depending on the reliability of the software and its vendor.

Comodo recommends that this setting to be maintained selected always *(Default = Enabled).*

To exclude some of the file types from being monitored under Detect Shellcode injections

- Select the 'Detect shellcode injections' checkbox and click the Exclusions link. The 'Manage Exclusions' dialog will appear.
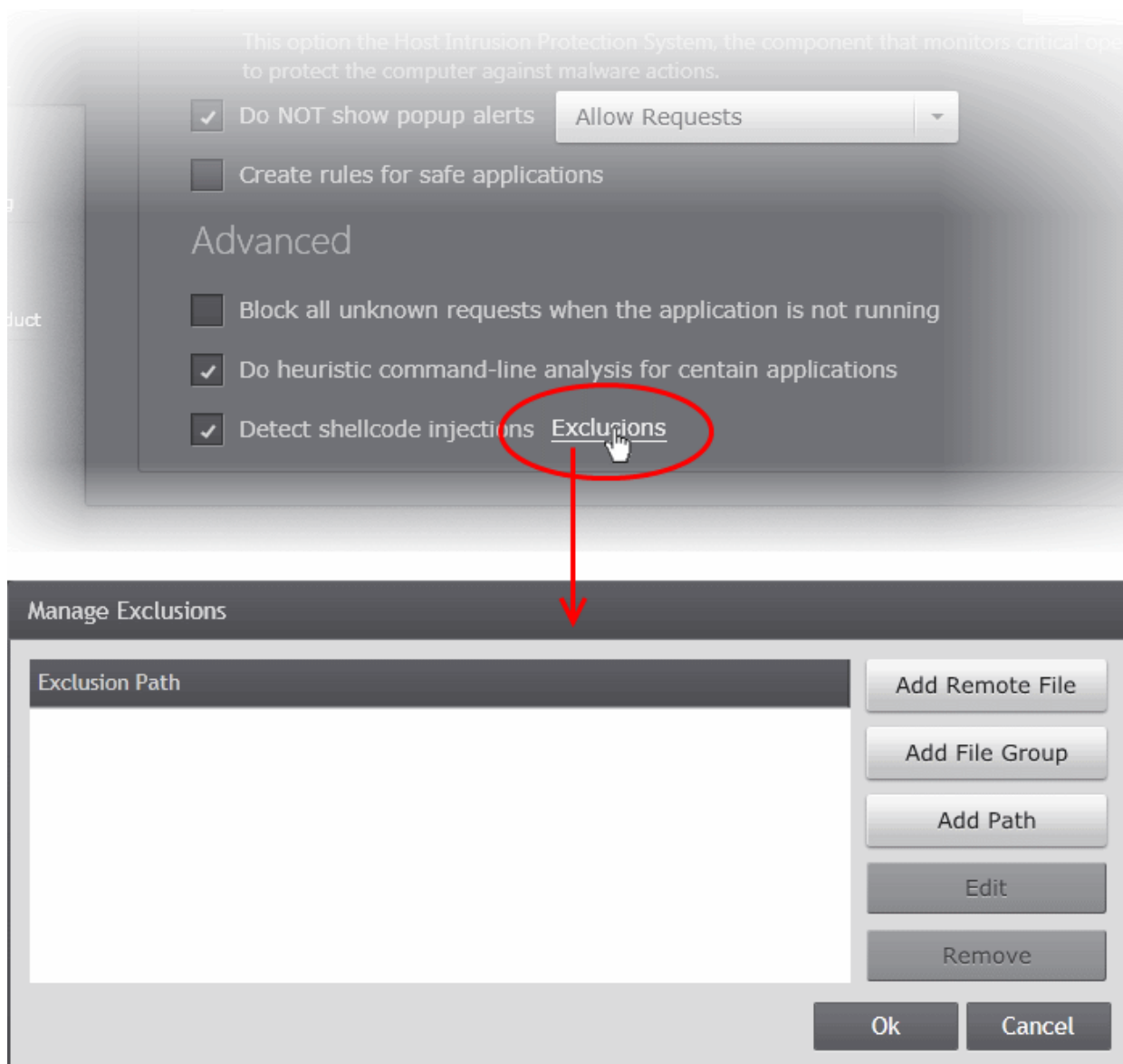
You can add files and folders to the 'Exclusions' list by specifying trustworthy file(s) stored in selected endpoint(s), specifying a file group or specifying a file path from standard Windows folders. The procedure is similar to adding exclusions for Antivirus Scans. Refer to the following descriptions in the section **Exclusions** for more details.

- **Adding a specific file from a selected endpoint**
- **Adding a File Group**
- **Adding File Path**

- To change or edit an item, select the item and click 'Edit'.

- To remove an item from the exclusions list, select the item and click 'Remove'.

- Click the 'Save' icon for your settings to take effect.

Sandbox

The Sandbox is an integral part of the Defense+ engine and is used to run potentially unsafe applications in an isolated environment to prevent damage to the endpoint and data stored in it. The Defense+ engine uses various analyses to determine whether an application loaded into the system memory is trusted, unrecognized or malware. You can define rules how these identified applications can be run in the Sandbox, that is,

- Run with restricted access to operating system resources

- Run completely isolated from your operating system and files on the rest of your computer

- Completely block from running

- Allow it to run outside the sandbox environment without any restriction.

For more information about defining rules, refer to the section **Configuring Rules for Auto-Sandbox**.

The Sandbox creates a new folder called Shared Space at the endpoint by default at 'C:/Program Data/Shared Space' for sharing files between it and the real computer system. The applications running inside the sandbox will be allowed to store their data in the shared space for future sessions. This data will can also be accessed by non-sandboxed applications.

The administrator can configure the Sandbox settings for the CES/CAS installations at the endpoints applied with the Policy from the 'Sandbox Settings' screen.

To access the Sandbox settings screen, click the 'Sandbox' tab in the 'Defense+ Settings' interface.

The Sandbox tab allows the administrator to:

- **Enable/Disable Auto-Sandbox**

- **Configure rules for auto-sandboxing applications**

- **Configure Shared Space Settings**

- **Configure Advanced Settings for Sandbox**

Enable/Disable Auto-Sandbox

- To enable Defense+ to auto-sandbox applications as defined in the Sandbox Rules, select Enable Auto-Sandbox checkbox.

Configuring Rules for Auto-Sandbox

The Sandbox rules determine whether a program should be allowed to run with full privileges, ignored, run restricted or run in fully virtualized environment. For easy identification, CES/CAS will show a green border around programs that are running in the sandbox at the endpoints.
Rules at the top of the table have a higher priority than those at the bottom and are applied first. In the event of a conflict between rules, the setting in the rule nearer to the top of the table will be applied.

CESM ships with a set of pre-defined auto-sandbox rules that are configured to provide maximum protection to the endpoint and is applied to each and every policy by default. In addition, the administrator can add custom rules and manage the rules from the Sandbox screen.

The Sandbox displays the configured rules as a table:

Sandbox Rules - Table of Column Descriptions	
Column Heading	**Description**
Action	Displays the operation that the sandbox should perform on the target files if the rule is triggered.
Target	The files, file groups or specified locations on which the rule will be executed.
Reputation	The trust status of the files to which the rule should apply. The possible values are: • 'Malware' • 'Trusted' • 'Unrecognized'.
Enable Rule	Allows you to enable/disable the rule

The table below provides the configuration settings for the pre-defined rules:

Rule	Action	Target	Restriction Level	Rating	Source			Log Action	Limit Maximum memory	Limit Program Execution Time	Quarantine
					Created by	Located on	Downloaded from				
1	Block	File Group - All Applications	N/A	Malware	Any	Any	Any	On	N/A	N/A	On
2	Block	File Group - Suspicious Locations	N/A	Any	Any	Any	Any	On	N/A	N/A	Off
3 Applicable only for Windows 8.0 and 8.1	Ignore	All Metro Apps	Off	Any	Any	Any	Any	On	N/A	N/A	N/A
4	Run Virtual	File Group - All Applications	Off	Unrecognized	Any	Any	Internet	On	Off	Off	N/A
					Any	Network Drive	Any				
					Any	Removable Drive	Any				
5	Run Virtual	File Group - All Applications	Off	Unrecognized	File Group - Web Browsers	Any	Any	On	Off	Off	N/A
					File Group - Email Clients	Any	Any				
					File Group – File Downloaders	Any	Any				
					File Group – Pseudo-File Downloaders						
6	Run	File Group -	Off	Unrecogn	Any	Any	Any	On	Off	Off	N/A

	Virtual	Shared Spaces		ized									

The administrator can add new rules for automatically running specified programs inside the sandbox at the endpoints to which the policy is applied.

An Auto-sandbox rule can be created for:

- An individual target application at a specific endpoint by specifying the file path of the executable file;

- An individual target application at several endpoints by specifying its common file path or the Hash value of the executable file;

- All applications in a File Group.

The target(s) can be filtered by specifying 'Source', 'Reputation' and 'Options'. They are, however, optional, so the administrator can create a very simple rule to run an application in the sandbox just by specifying the action and the target application.

To add a new rule

- Click 'Add' from the 'Sandbox' interface. The 'Add New Sandbox' Rule dialog will appear.
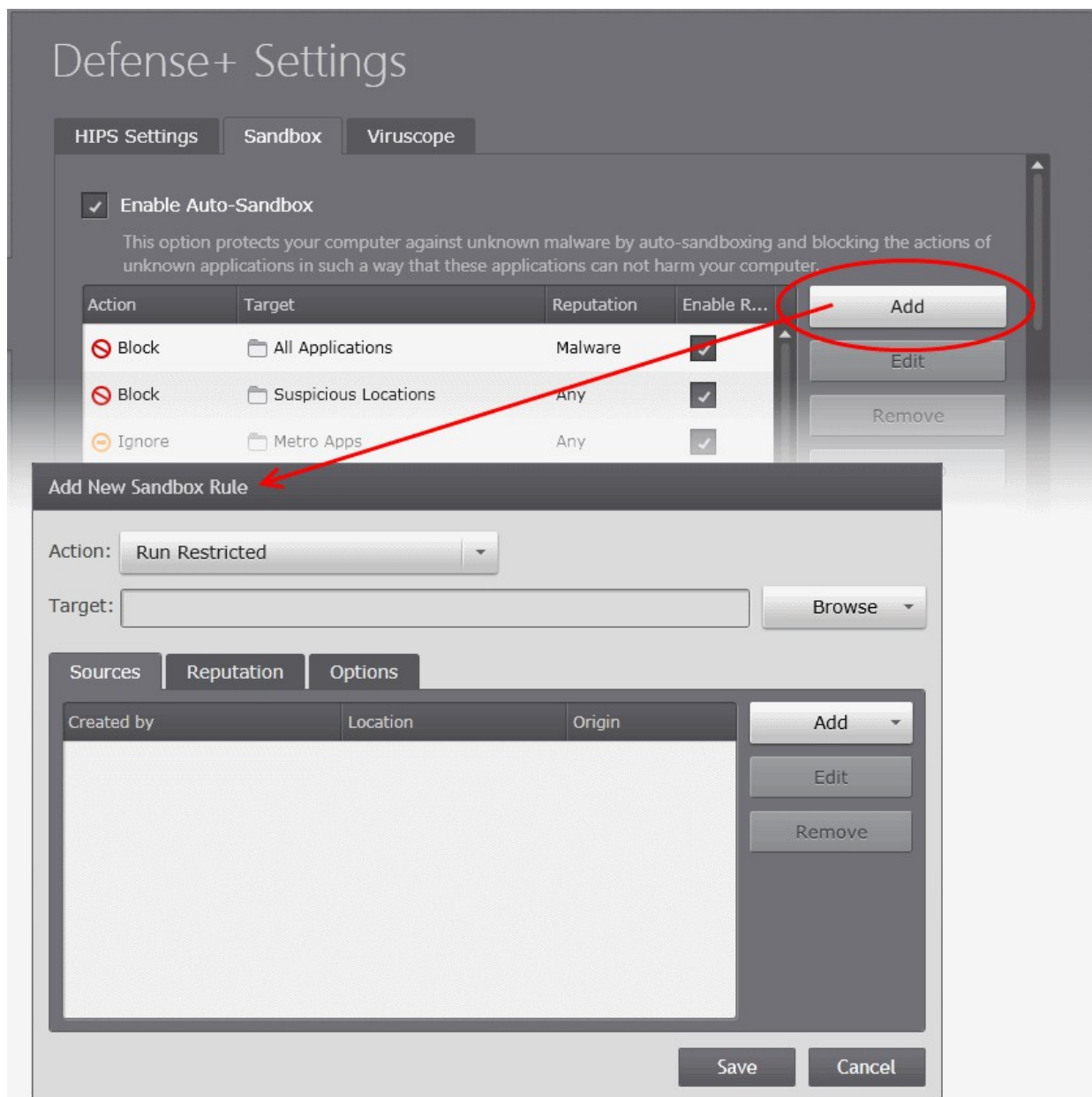
The creation of a new rule from the Add New Sandbox Rule dialog involves the following five steps. Each step is explained in

detail after the brief descriptions:

- **Step 1 - Select the Action**
- **Step 2 - Select the Target Application(s)**
- **Step 3 - Select the Sources** (Optional)
- **Step 4 - Select the File Rating** (Optional)
- **Step 5 - Configure the sandbox settings for the selected targets** (Optional)

If you want to just specify a target application and an action for the rule, just follow Step 1 and Step 2 and click 'Save' in the 'Add New Sandbox Rule' dialog. The default values for Sources and Reputation will be 'Any' and for Options it will be 'Log when this action is performed'.

Step 1 - Select the Action

The 'Action' drop-down allows you to choose whether or not the sandbox has to allow the application to run and the restriction level to be th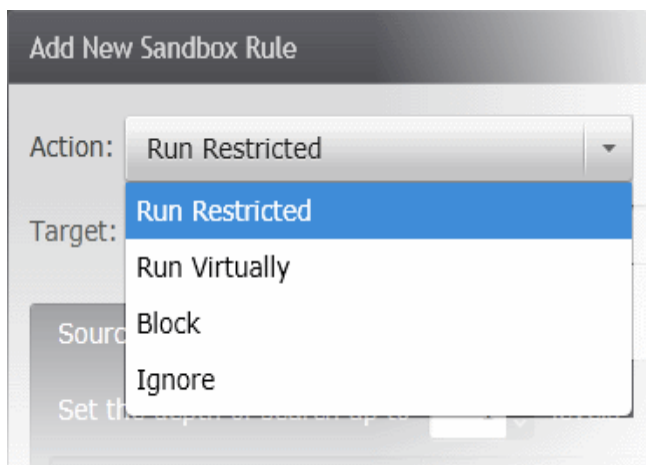e applied. The restriction level determines the privileges to be assigned to the auto-sandboxed application to access the other software and hardware resources of the endpoint computer. The options available are:

- **Run Restricted** - The application is allowed to run and access the Operating System files and resources as per the Restriction Level set under the 'Options' tab, in **Step 5 - Configure the sandbox settings for the selected targets**
- **Run Virtually** - The application will be run in a virtual environment completely isolated from your operating system and files on the rest of your computer.
- **Block** - The application is not allowed to run at all.
- **Ignore** - The application will not be sandboxed and allowed to run with all privileges.

Step 2 - Select the Target Application(s)

The next step is to select the target application to which the auto-sandbox rule is to be applied. Click the 'Browse' button beside the Target field.
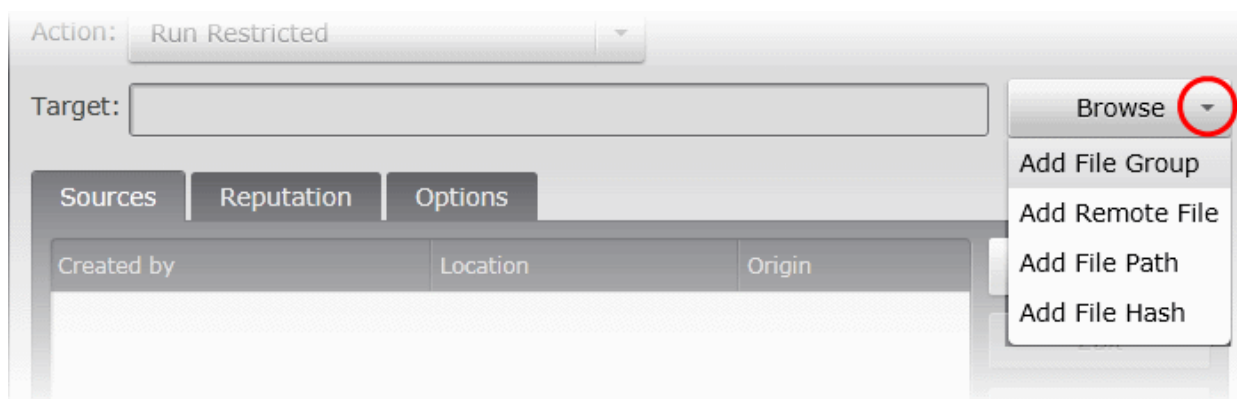
The administrator can add the target application(s) in four ways:

- **Adding a File Group**
- **Adding a specific file from a selected endpoint**
- **Adding File Path**
- **Specifying a File Hash**

Adding a File Group

File groups are handy, predefined groupings of one or more file types. Choosing File Groups allows the administrator to add a category of pre-set files or folders. For example, selecting 'Executables' would exclude all files with the extensions .exe .dll .sys .ocx .bat .pif .scr .cpl . Other such predefined categories available include 'Windows System Applications' , 'Windows Updater Applications' , 'Start Up Folders' etc. CESM also enables the administrator to add custom File Groups for the policy from the File Rating Interface. Refer to the description under **Managing File Groups** in the section **Configuring File Rating Settings** for more details.

To add a file group

- Click 'Add File Group'
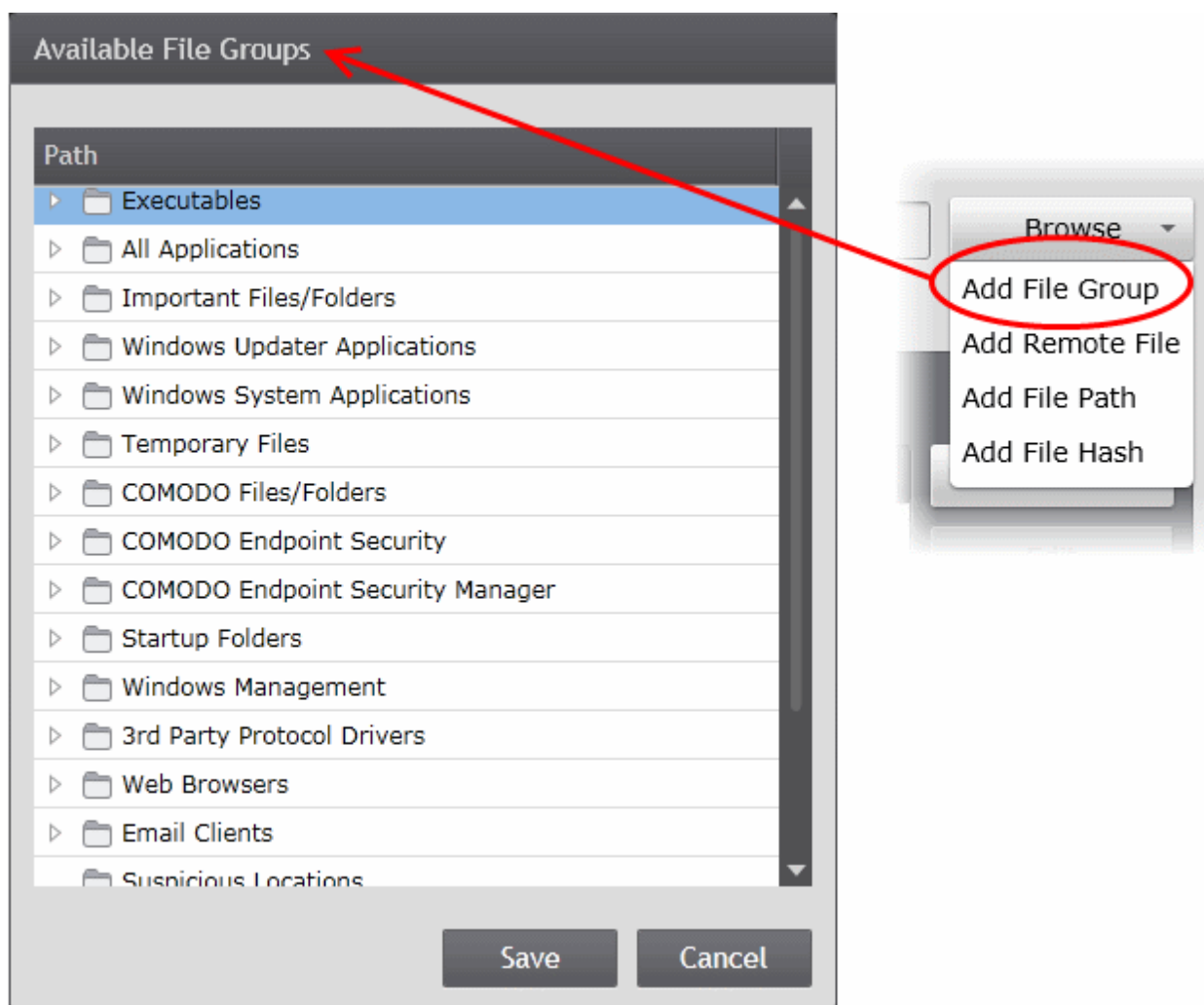
- Choose the 'File Group' from the 'Available File Groups' dialog and click Save.

Adding a specific file from a selected endpoint

The administrator can add specific individual files from selected endpoints applied with the policy, so that the added files will be auto-sandboxed as per the rule.

To add a specific file from a selected endpoint
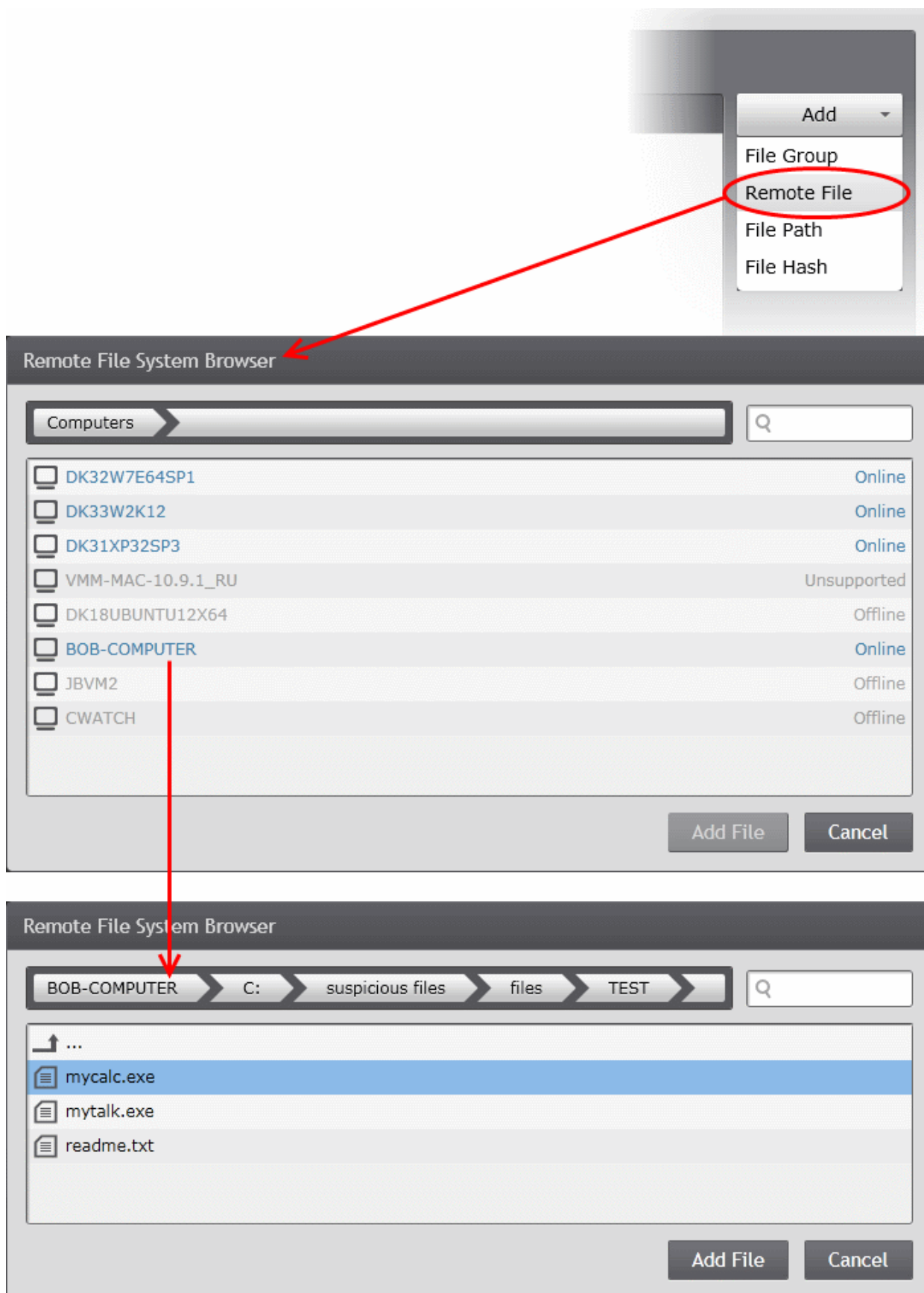
- Click 'Add Remote File'

The list of endpoints will be displayed.

- Double click on the endpoint, navigate to the file path and select the file.

Note: The Endpoint needs to be online for navigation through the file path in it.

- Click 'Add File'.
- Click the 'Save' icon to include the file as the target to the rule.

Adding a File Path

The administrator can add executable files as the target by selecting a standard folder and entering the path in the text field or by entering the entire common path.

To add a file path

- Click 'Add File Path'.
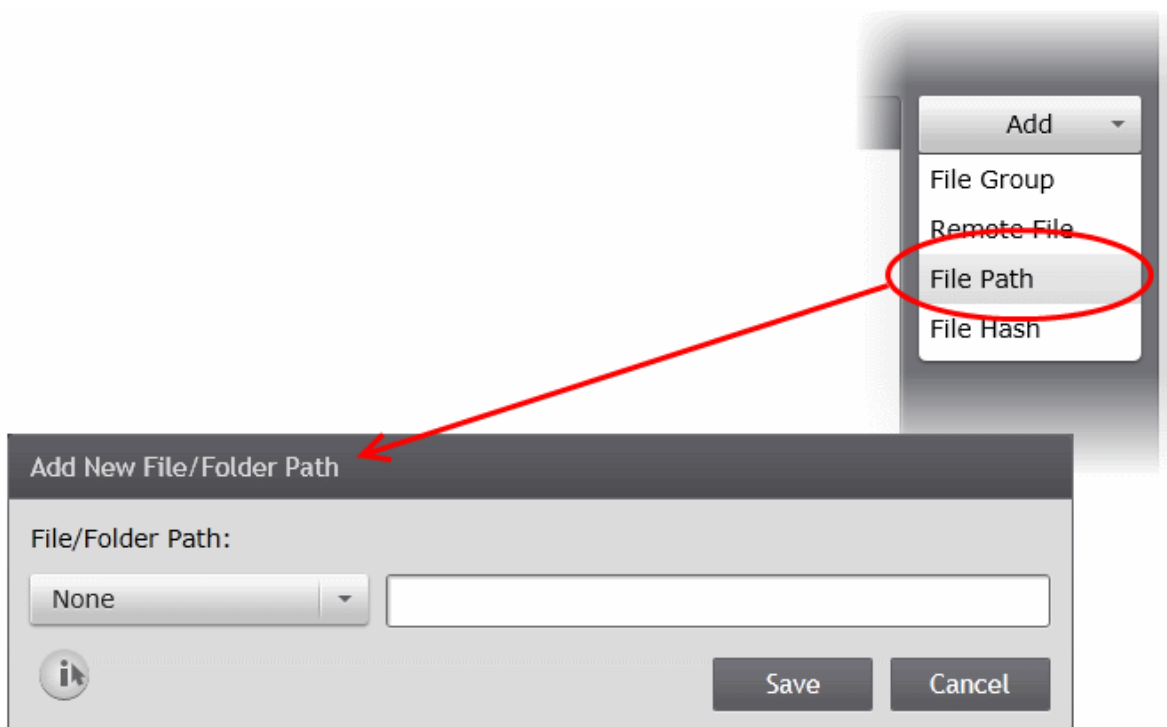
The 'Add New File/Folder Path' dialog will appear.

- Select the standard folder from the drop-down and enter the path/file name in the text box or enter the full folder/file path in the text box.
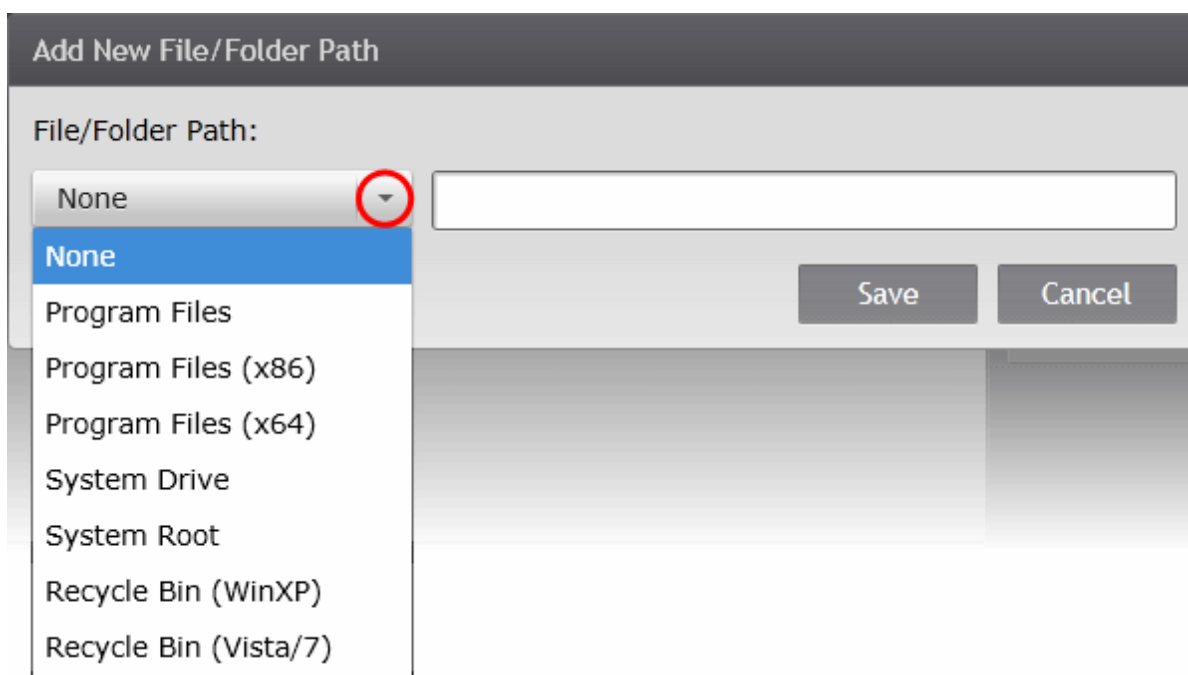
- Click 'Save' in the 'Add New File/Folder Path' dialog to add the file as the target to the rule.

Adding File Hash

The administrator can add a program as a target by specifying the SHA1 File Hash value of the executable file. CESM will monitor all the endpoints to which the policy is applied and if the executable file with the same hash value attempts to execute in any of the endpoint(s) the rule will be triggered and the program will be auto-sandboxed as per the rule.

The Hash value can be entered in two ways:

- CESM has a built-in SHA1 Hash calculator. The administrator can specify an executable file by selecting an endpoint on which the application is installed and select the file. CESM will automatically calculate the Hash value of it.

- If the hash value is already available, the administrator can directly enter the hash value

To add a file hash

- Click 'Add File Hash'. The 'Add New File Hash' dialog will appear.
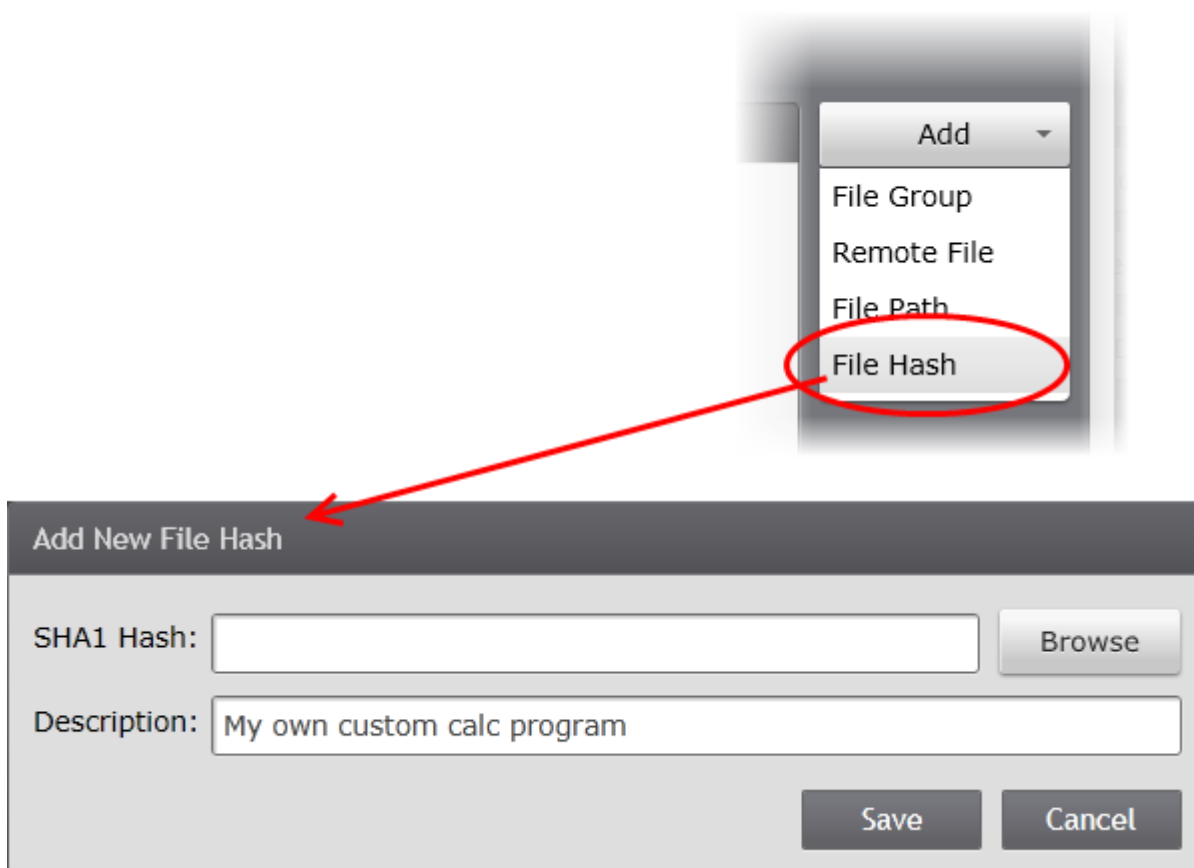
- To specify an executable from an endpoint, click Browse, choose the endpoint and navigate to the executable file and click Add File. The Hash value will be automatically entered.
- If you already have the hash value of the program calculated using a third-party Hash Calculator, enter the hash value in the SHA1 Hash field

- Enter a short description for the file in the Description field. This description will be displayed in the Target field of the rule.

- Click Save. The target will be added.

Step 3 - Select the Sources

If you want to include a number of items for a rule but want the rule to be applied for items from certain sources only, you can specify the sources in this step. For example, if you include all executables in the Target but want the rule to be applied for executables that were downloaded from the Internet only, then the filter can be applied in the Sources. Another example is if you want to run unrecognized files from a network share, you have to create an ignore rule with All Applications as target and source located on network drives.

To add a source

- Click the 'Add' button to choose the source file that has created the application set as target in Step 2. The process of adding the source file is similar to adding a file for target. Refer to the description **above** for more details.

  - For example, if the file was downloaded from Internet using a web browser, you can choose the File Group 'Web Browsers'.
  - If you are unsure of the source, choose 'All Applications' file group.

  The source will be added to the 'Created By' column.

- Choose the Location in which the application is stored from the 'Location' drop-down. The options available are:
  - Any - The rule will apply to the target application located on the local drive or on a removable drive of the endpoint or on a network drive.
  - Local Drive - The rule will apply only to the target application located on the local drive of the endpoint.
  - Removable Drive - The rule will apply only to the target application located on the removable drive connected to the endpoint.
  - Network Drive - The rule will apply only to the target application located on a network drive but executed at the endpoint.
- Choose the Origin of the executable. The available options are:
  - Any - The rule will apply to the target application downloaded, copied or moved from anywhere.
  - Internet - The rule will apply only to the target application downloaded from Internet.
  - Intranet - The rule will apply only to the target application downloaded from Intranet.

Step 4 - Select the File Rating

The administrator can narrow down the scope of applications to which the rule needs to be applied by specifying the File Rating and the age of the target files from the 'Reputation' tab.

- To specify a reputation, select the 'Select file rating' checkbox and choose the file rating from the drop-down. The available options are:

  - **Trusted** - Applications that are signed by trusted vendors and files installed by trusted installers are categorized as Trusted files. Refer to the sections **Configuring File Rating Settings**

  - **Unrecognized** - Files that are scanned against the Comodo safe files database not found in them are categorized as Unrecognized files. Refer to the section **Viewing and Managing Unrecognized Files** for more information.

  - **Malware** - Files are scanned according to a set procedure and categorized as malware if not satisfying the conditions.

- To filter only the files that have been created before or after a certain time for auto-sandboxing, specify the age of the files:

  - Select the 'Match files that are created 'More than/Less than' 'NN' 'Hours/Days' checkbox,

  - To select the files whose age is less than the specified time period, choose 'Less than' from the first drop-down and specify the time period using the next two drop-downs

  - To select the files whose age is more than the specified time period, choose 'More than' from the first drop-down and specify the time period using the next two drop-downs

Step 5 - Configure the sandbox settings for the selected targets

The 'Options' tab allows the administrator to configure granular settings for the execution of the auto-sandboxed application.

The options available depend on the action chosen in Step 1.

Action	Available Options

Ignore	• **Log when this action is performed** - Whenever this rule is triggered, the event will be added to the logs.
	
	• **Don't apply the selected action to child processes** - Child processes are the processes initiated by the applications, such as launching some unwanted app, third party browsers plugins / toolbars that was not specified in the original setup options and / or EULA. CES treats all the child processes as individual processes and forces them to run as per the file rating and the Sandbox rules.
	
	    • By default, this option is not selected and the ignore rule is applied also to the child process of the target application(s).
	
	    • If this option is selected, then the Ignore rule will be applied only for the target application and all the child processes initiated by it will be checked and Sandbox rules individually applied as per their file rating.

Block	• **Log when this action is performed** - Whenever this rule is triggered, the event will be added to the logs. • **Quarantine Program** - If chosen, the intercepted program will be automatically moved to quarantine. Refer to the section **Viewing and Managing Quarantined Items** for more information.
Run Virtually Run Restricted	• **Log when this action is performed** - Whenever this rule is triggered, the event will be added to the logs. • **Set Restriction Level to** - The administrator can choose whether or not the restriction level is to be applied to the programs run inside the sandbox by selecting or deselecting this checkbox. For 'Run Restricted' action, the option is selected by default. If selected, the administrator can choose the restriction level to be applied from the drop-down. The options available are:

	• **Partially Limited** - The application is allowed to access all operating system files and resources like the clipboard. Modification of protected files/registry keys is not allowed. Privileged operations like loading drivers or debugging other applications are also not allowed. (Default)
	• **Limited** - Only selected operating system resources can be accessed by the application. The application is not allowed to execute more than 10 processes at a time and is run without Administrator account privileges.
	• **Restricted** - The application is allowed to access very few operating system resources. The application is not allowed to execute more than 10 processes at a time and is run with very limited access rights. Some applications, like computer games, may not work properly under this setting.
	• **Untrusted** - The application is not allowed to access any operating system resources. The application is not allowed to execute more than 10 processes at a time and is run with very limited access rights. Some applications that require user interaction may not work properly under this setting.
	• **Limit maximum memory consumption to** - Enter the upper limit of size of system memory (in MB) that the process can use.
	• **Limit program execution time to** - Enter the maximum time in seconds for which the program can be allowed to run. On lapse of the time, the program will be automatically terminated.

- Click 'Save' in the Add New Sandbox Rule dialog to add the rule.

- Once created, the rules can be edited or deleted at any time from the same interface.

- To edit a rule, select the rule and click Edit. The Edit Sandbox Rule dialog will appear. The dialog is similar to Add New Sandbox Rule dialog. Refer to the description of **adding a sandbox rule** for more details.

- To remove a rule, select the rule and click 'Remove'.

- To change the priority of a rule, select the rule and click 'Move Up' or 'Move Down' buttons.

- To remove the custom rules and revert the predefined rules to default configuration, click 'Reset to Default'.

Configuring Shared Space Settings

'Shared Space' is a dedicated area at each endpoint that sandboxed applications are permitted to write to and which can also be accessed by non-sandboxed applications (hence the term 'Shared Space'). For example, any files or programs you download via a sandboxed browser that you wish to be able to access from your real system should be downloaded to the shared space. This is located by default at 'C:/Program Data/Shared Space'.

The Shared Space at the endpoint can be accessed in the following ways:

- Clicking the 'Shared Space' shortcut on the computer desktop

- Clicking 'Shared Space' button on the CES interface

- Opening 'Sandbox Tasks' from the Tasks interface then clicking 'Open Shared Space'

- By default, sandboxed applications can access folders and files on the 'real' system but cannot save any changes to them. However, you can define exceptions to this rule by using the 'Do not virtualize access to...' links.

The 'Shared Space' settings area in the Sandbox interface allows the administrator to configure the exceptions:
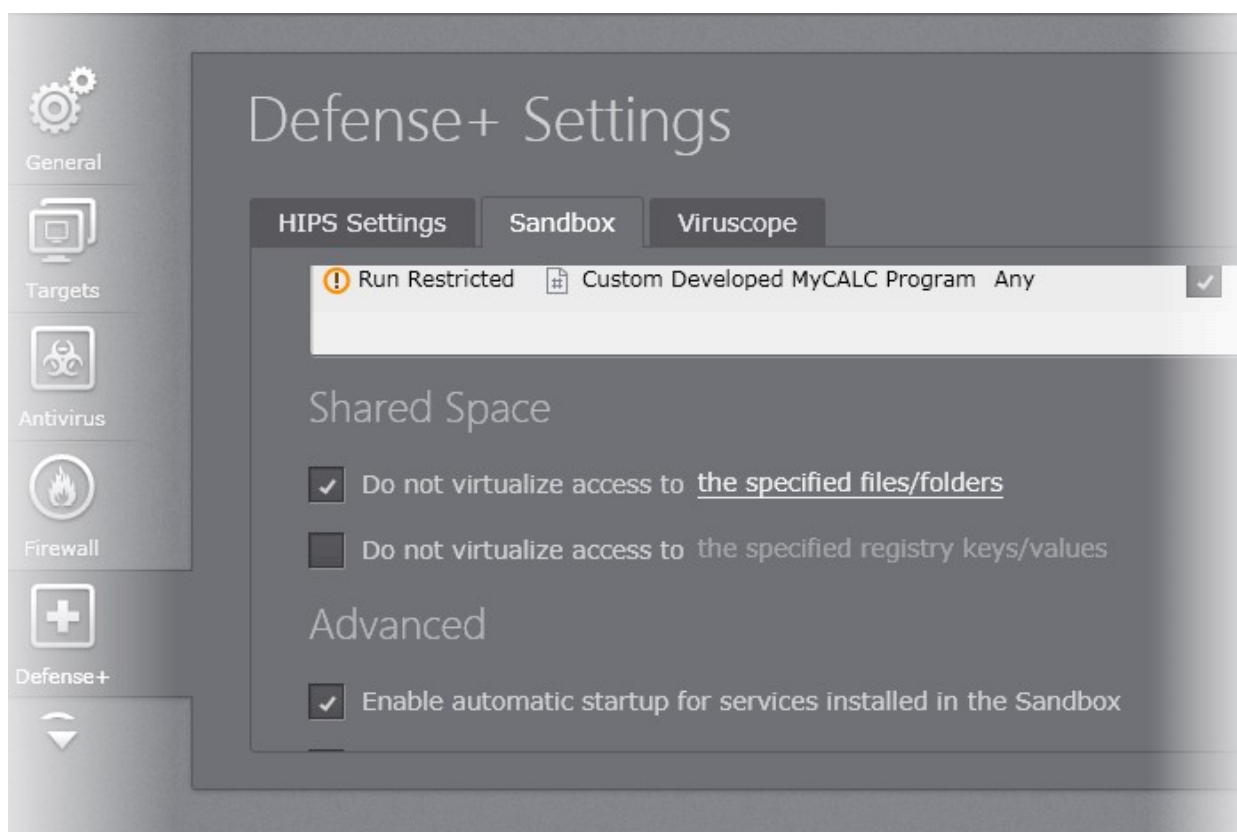
To define exceptions for files and folders

- Enable the 'Do not virtualize access to the specified files/folders' check-box then click the the specified files/folders link. The 'Manage Exclusions' dialog will appear.
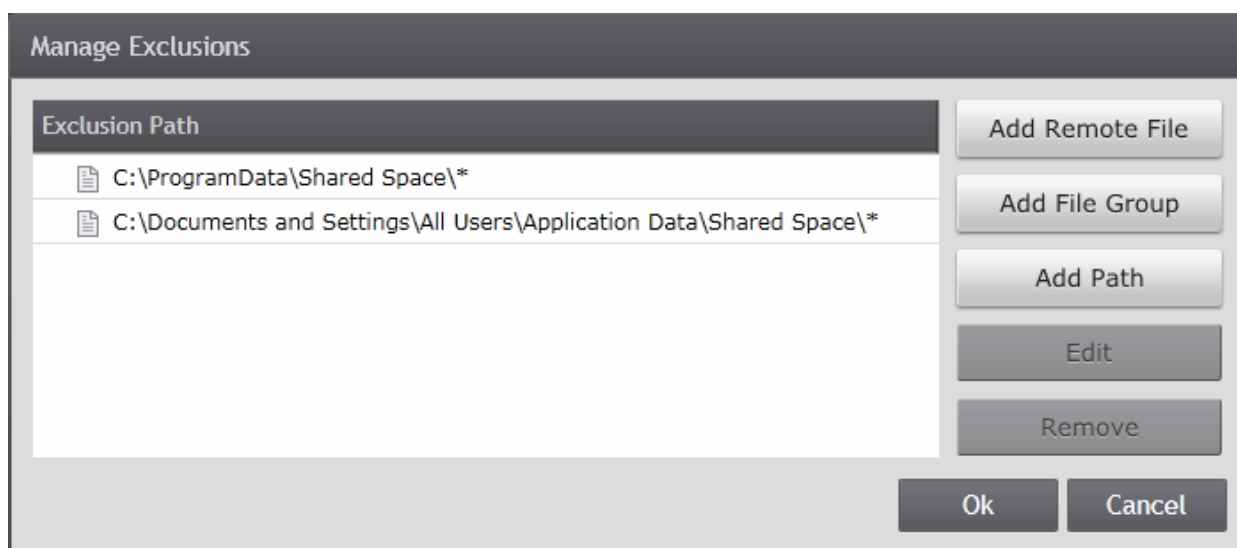

- You can add files and folders to the 'Exclusions' list by specifying trustworthy file(s) stored in selected endpoint(s), specifying a file group or specifying a file path from standard Windows folders. The procedure is similar to adding exclusions for Antivirus Scans. Refer to the following descriptions in the section **Exclusions** for more details.

  - **Adding a specific file from a selected endpoint**
  - **Adding a File Group**
  - **Adding File Path**

To define exceptions for specific Registry keys and values

- Enable the 'Do not virtualize access to the specified registry keys/values' check-box then click the the specified

---

registry keys/values link. The 'Manage Exclusions' dialog will appear.
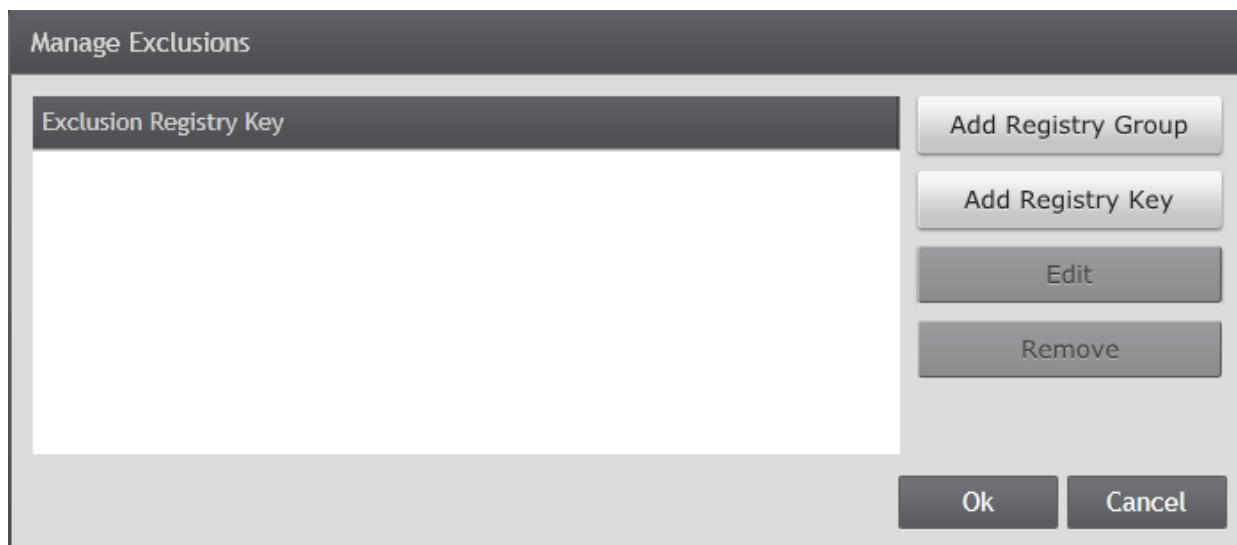
The administrator can add the Registry key in the following ways:

- **Adding a Registry Group**
- **Adding a Registry Key**

Adding a Registry Group

Registry groups are predefined batches of one or more registry keys that can be re-used for different settings under Defense+. Choosing Registry Groups allows the administrator to exclude the whole bunch of the keys and values from virtualization and enable them to be accessed by the programs running inside the sandbox. Refer to the description under **Managing Registry Groups** in the section **Configuring File Rating Settings** for more details on creating and managing predefined and custom Registry groups.

To add a Registry group

- Click 'Add Registry Group'
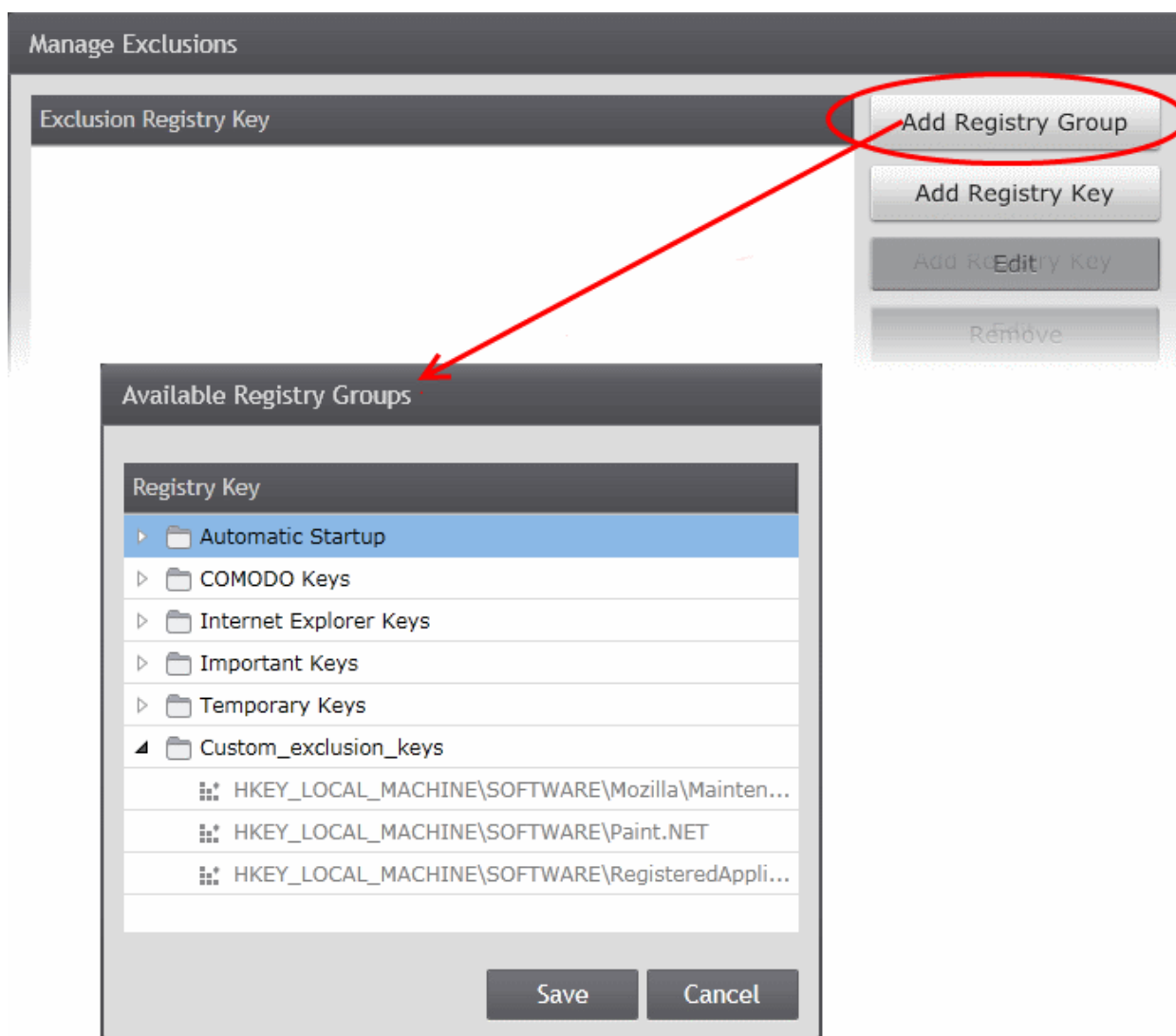
The 'Available Registry Groups' dialog will appear with a list of predefined and custom Registry groups. The administrator can expand a group to view the member keys by clicking the right arrow ▷ beside the file group name.
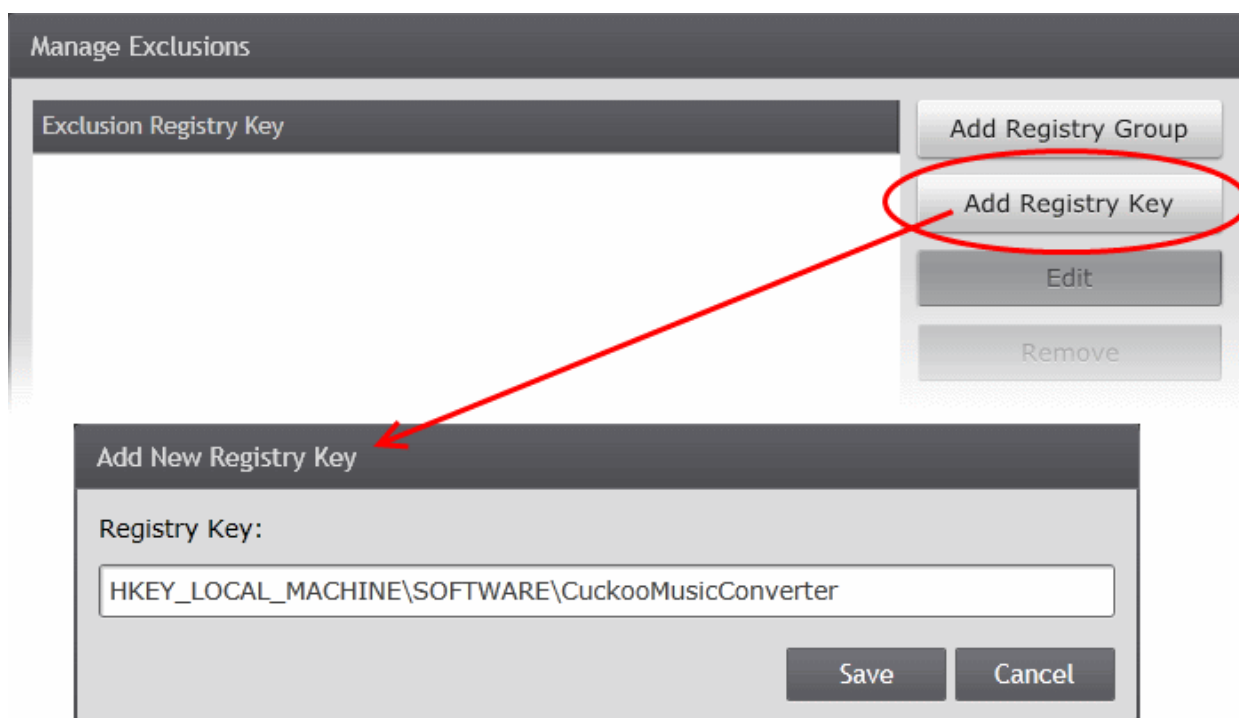
- Select the Registry group and click 'Save'.

- Repeat the process for adding more Registry groups.

Adding a Registry Key

The administrator can add specific standard keys to be excluded from virtualization by directly entering the Registry Key path.

To add a Registry Key

- Click 'Registry Key'.

The 'Add New Registry Key' dialog will appear.

- Enter the full Registry key path in the text box and click 'Save'.

- Repeat the process for adding more Registry keys.

## Configuring Advanced Settings for Sandbox

The Advanced Settings area allows the administrator to configure Sandbox alert settings as well as to enable automatic startup services for programs installed in the Sandbox.

- **Enable automatic startup for services installed in the sandbox** - By default, CES installation at the endpoint does not permit sandboxed services to run at Windows startup. Select this check-box to allow them to do so at the endpoints applied with the policy. **(Default = Enabled)**

- **Show highlight frame for virtualized programs** - If enabled, CES displays a green border around the windows of programs that are running inside the sandbox at the endpoint. **(Default = Enabled)**

The following example shows an .odt document opened with a sandboxed version OpenOffice Writer:
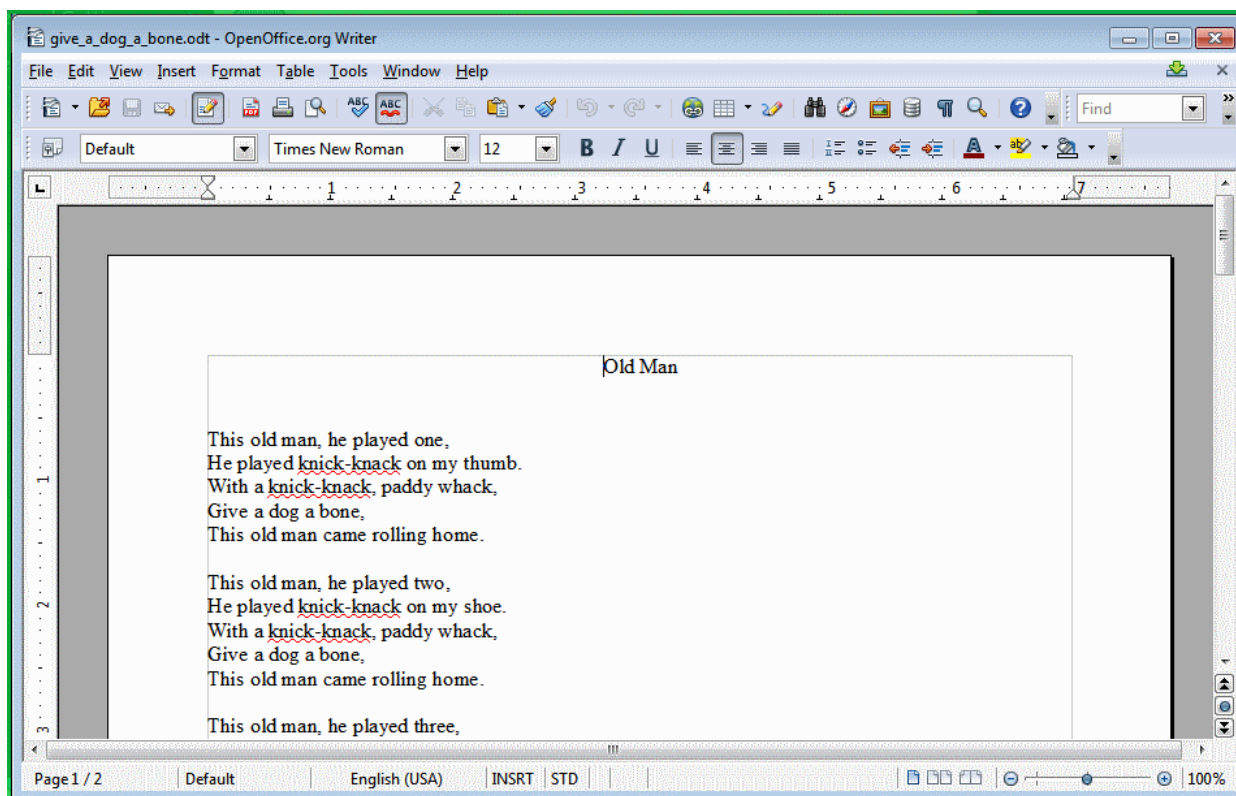
- • **Detect programs which require elevated privileges** - If enabled, the Sandbox displays alerts when an installer or updater requires administrator or elevated privileges to run at the endpoint. An installer that is allowed to run with elevated privileges is permitted to make changes to important areas of the endpoint, such as the registry.
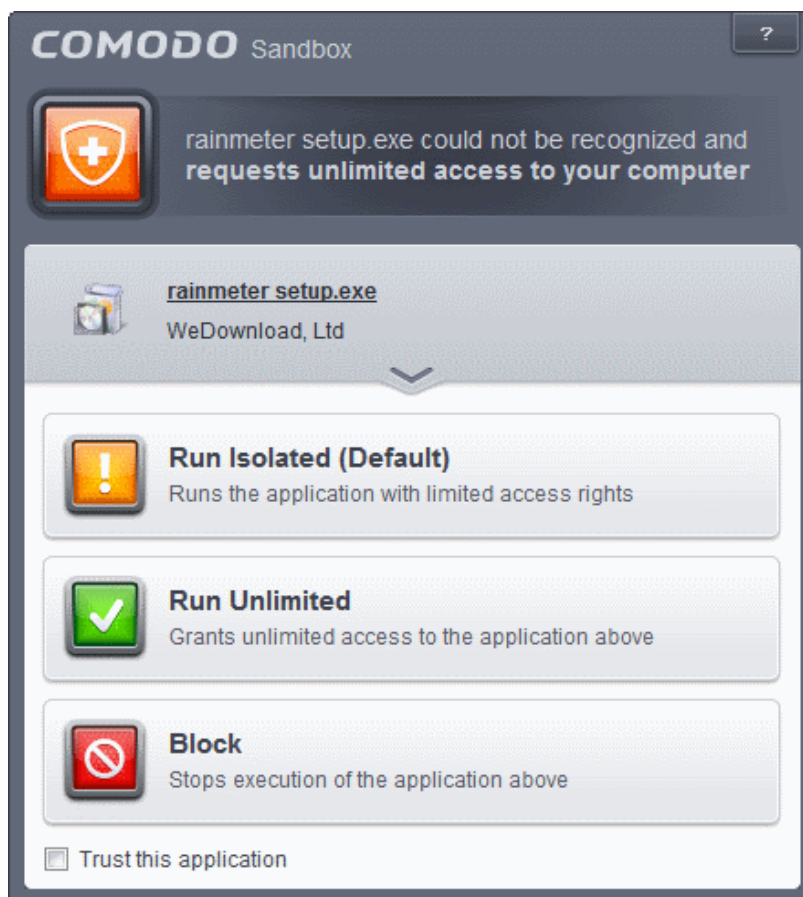
The enduser can decide on whether or not to allow the installer or update based on their assessment, from the alert itself. *(Default=Enabled)*

Refer to the online help page at **http://help.comodo.com/topic-84-1-604-7354-Understanding-Security-Alerts.html** for more details on security alerts displayed at the endpoints.

- **Show privilege elevation alerts for unknown programs** - If enabled, the Sandbox displays alerts when a new or unrecognized program, application or executable requires administrator or elevated privileges to run. The end user can decide on whether or not to allow the unknown application based on your assessment, from the alert itself. *(Default=Enabled)*

- Click the Save icon for the configuration changes to the Sandbox to take effect.
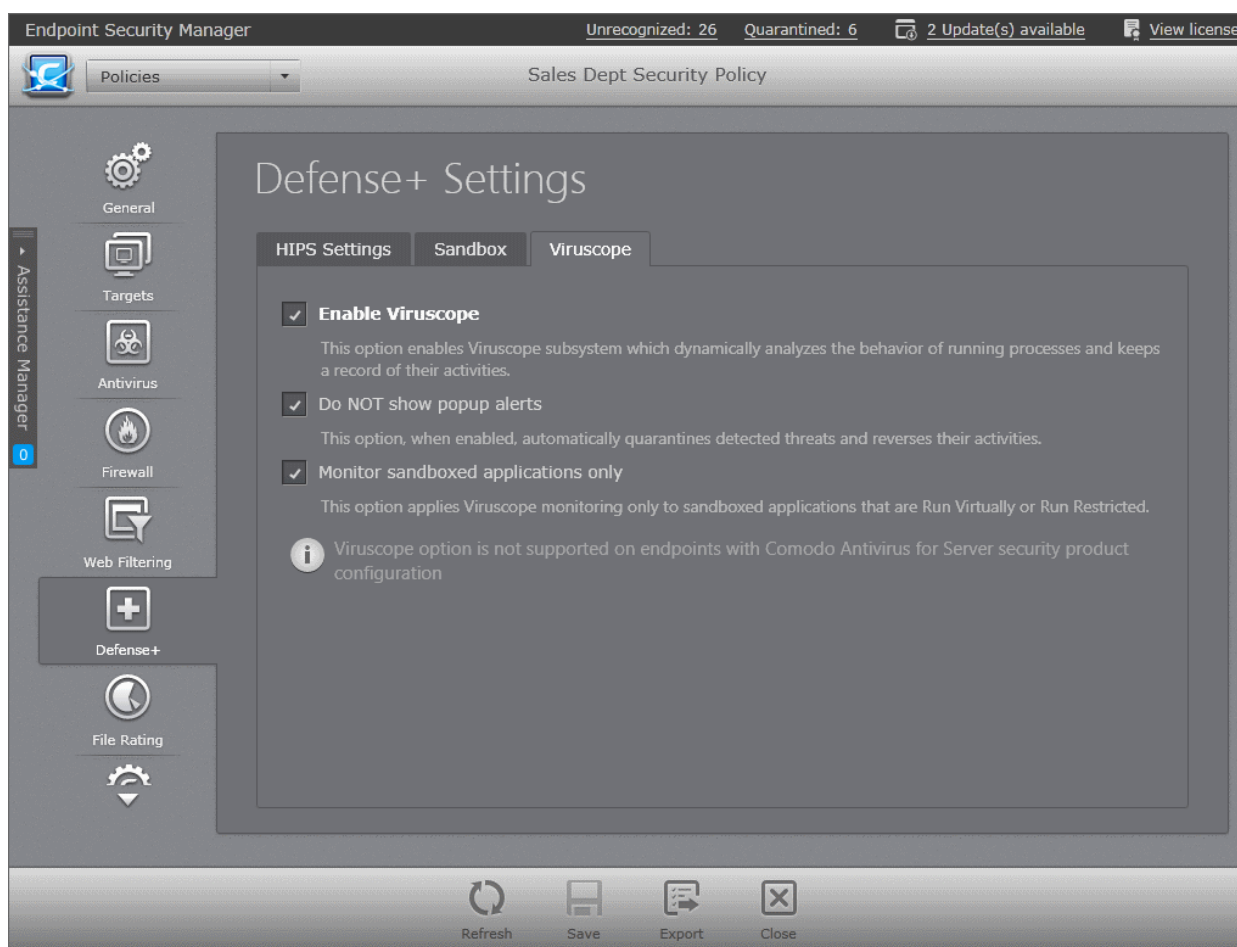
Viruscope

The Viruscope component of Defense+ monitors the activities of processes running at the endpoints and generates alerts if they take actions that could potentially threaten your privacy and/or security. Apart from forming yet another layer of malware detection and prevention, the sub-system represents a valuable addition to the core process-monitoring functionality of the Defense+ by introducing the ability to reverse potentially undesirable actions of software without necessarily blocking the software entirely. This feature can provide more granular control over otherwise legitimate software which requires certain actions to be implemented in order to run correctly.

Viruscope alerts give the end user with the opportunity to quarantine the process & reverse its changes or to let the process go ahead. Be especially wary if a Viruscope alert pops up 'out-of-the-blue' when you have not made any recent changes to your computer.
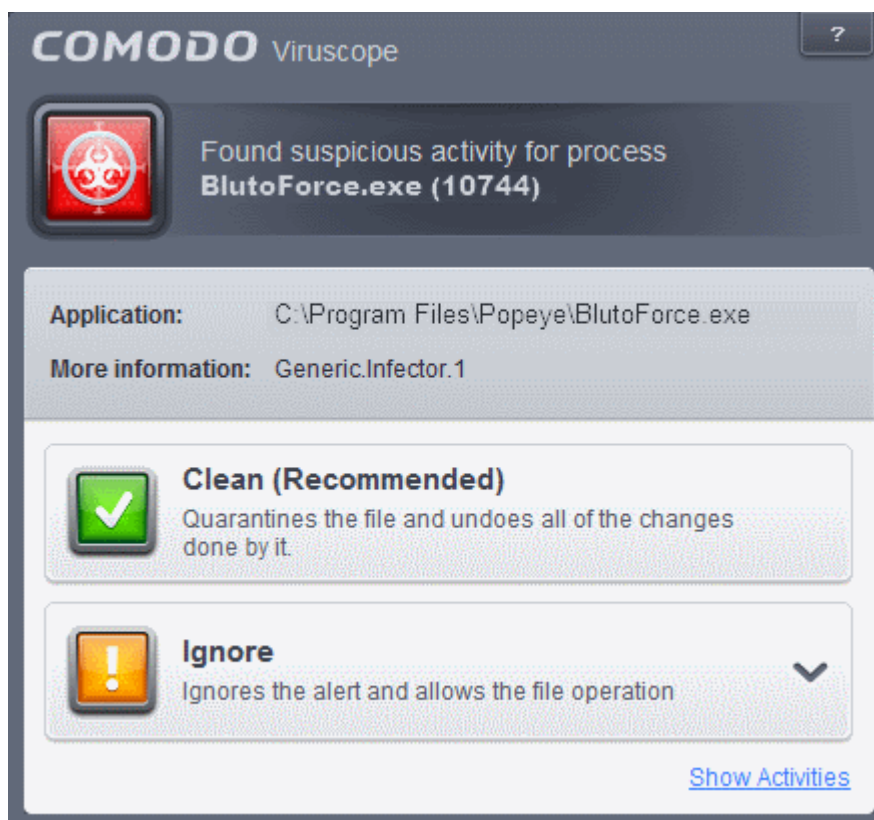
The 'Viruscope' tab in the Defense+ Settings interface enables the administrator to enable and configure the Viruscope settings for the policy.

- • **Enable Viruscope (Recommended)** - Allows you to enable or disable Viruscope. If enabled, the Viruscope monitors the activities of all the running processes and generates alerts on suspicious activities. **(Default = Enabled)**

- • **Do NOT show popup alerts** - Allows you to configure whether or not to show Viruscope alerts when a suspicious activity is recognized. Choosing 'Do not show popup alerts' will minimize disturbances but at some loss of user awareness. If you choose not to show alerts then detected threats are automatically quarantined and their activities are reversed. (Default = Enabled)

- • **Monitor sandboxed applications only** - By default, Viruscope will monitor only the processes pertaining to auto-sandboxed applications or applications manually added to run inside the sandbox. If you want Viruscope to monitor all the processes running at the endpoint de-select this option. (Default = Enabled)

For more details on the Defense+ Settings, see the of CES - Defense+ Settings online help page at **http://help.comodo.com/topic-84-1-604-7470-Defense+-Settings.html**.

5.2.7. Configuring File Rating Settings

The CES/CAS rating system is a cloud-based file lookup service (FLS) that ascertains the reputation of files on your computer. Whenever a file is first accessed, CES/CAS will check the file against our master whitelist and blacklists and will award it trusted status if:

- • The application is from a vendor included in the Trusted Software Vendors list;

- • The application is included in the extensive and constantly updated Comodo safelist;

- • The application/file is awarded 'Trusted' status in the local File List.

Trusted files are excluded from monitoring by HIPS - reducing hardware and software resource consumption. On the other hand, files which are identified as malicious will be awarded 'Malicious' rating and denied all access rights from other processes or users - effectively cutting them off from the rest of the system. The malicious files are also added to the global 'Blocked Files' list and are denied access at all the endpoints. Files which could not be recognized by the rating system are awarded 'Unrecognized' status and added to the global 'Unrecognized Files' list. You can review files on the unrecognized files list and their activities, the endpoints at which they are discovered, remove files identified as malware from the endpoints or remove a

file from the Unrecognized Files list, if it is a false-positive from the Unrecognized Files interface. For more details on viewing and managing global 'Files List', refer to the section **Files Managment**.

The 'File Rating' Settings area allows the administrator to configure the file rating settings for the policy, manually assign ratings to executable files and manage Trusted Vendor list. Also, the administrator can create and manage File Groups and Registry Groups that can be used for defining exclusions from Antivirus scans, and Defense+ monitoring settings.

> **Note**: The 'File Rating Settings' interface allows the administrator to view and edit the file rating settings for custom policies and to view the configuration for the predefined policies. Predefined policies cannot be edited.
>
> The 'File Rating' Settings interface is available only for 'Windows Workstation' Policy and 'Windows Servers' Policy types.

- To open the File Rating interface, click on the 'File Rating' icon ⊙ in the left pane.

The following sections provide explanations on:

- **Configuring File Rating Settings**
- **Rating Files**
- **Managing Trusted Vendors List**
- **Managing File Groups**
- **Managing Registry Groups**

File Rating Settings

The File Rating Settings screen allows you to configure the overall behavior of File Rating feature of CES/CAS at the endpoints applied with the policy.

- **Enable Cloud Lookup** - Allows you to enable or disable File Rating.(**Default and recommended =Enabled**)

> **Note**: CES uses Ports 4446 and 4447 of the endpoint computers for TCP and UDP connections to the cloud. Comodo advises to maintain these ports free and not assigned to other applications, if this option is enabled.

- **Analyze unknown files in the cloud by uploading them for instant analysis** - Instructs CES/CAS to upload files whose trustworthiness could not be assessed by cloud lookup to Comodo for analysis immediately. The experts at Comodo will analyze the file and add to the whitelist or blacklist according to the analysis. (**Default =Enabled**)

- **Trust applications signed by trusted vendors** - When this option is enabled, CES/CAS will award trusted status to the executables and files that are digitally signed by vendors in the Trusted Vendors list using their code signing certificates. (**Default =Enabled**)

- **Trust files installed by trusted installers** - When this option is enabled, CES/CAS will consider the executable and files stored by applications that are assigned with Installer or Updater rule under HIPS Rules or the applications. (**Default =Enabled**)

- **Detect potentially unwanted applications** - When this check box is selected, CES/CAS identifies the applications that:

  - A user may or may not be aware is installed on their computer, and/or
  - May have functionality and objectives that are not clear to the user.

    Example: Potentially Unwanted Applications (PUAs) include adware and browser toolbars. PUAs are often installed as an additional extra when the user is installing an unrelated piece of software. Unlike malware, many PUA's are 'legitimate' pieces of software with their own EULA agreements. However, the 'true' functionality of the software might not have been made clear to the end-user at the time of installation. For example, a browser toolbar may also contain code that tracks a user's activity on the Internet. (**Default =Disabled**)

    On detecting a PUA, the CES/CAS installation at the endpoint raises an alert for the user to decide whether or not to run it and add it to the logs.

- **Do NOT show popup alerts** - This option allows you to configure whether or not to show file rating alerts when malware is encountered. Choosing 'Do not show popup alerts' will minimize disturbances but at some loss of user awareness. If you choose not to show popup alerts then you have a choice of default responses that CES should automatically take - either 'Block Requests' or 'Allow Requests'. (**Default =Disabled**)

Rating Files

The 'Rating Files' interface allows the administrator to manually add files with an administrator defined file rating for the policy. CES/CAS installations on endpoints using this policy will allow or block the files based on the administrator defined rating. The ratings that can be assigned to files are:

- **Trusted**
- **Unrecognized**
- **Malicious**

Trusted Files

Files added to the list with the 'Trusted' rating are automatically given Defense+ trusted status. If an executable is unknown to the Defense+ safe list then, ordinarily, it and all its active components generate HIPS alerts when they run. Of course, the end-user could choose the 'Treat this as a Trusted Application' option at the alert but it is often more convenient to classify entire directories of files as 'Trusted Files'.

For the files added manually, it generates a hash or a digest of the file using a pre-defined algorithm and saves in its database. On access to any file, its digest is created instantly and compared against the list of stored hashes to decide on whether the file has 'Trusted' status. By this way, even if the file name is changed later, it will retain its Trusted status as the hash remains same.

The administrator can define a personal safe list of files to complement the default Comodo safe list.

By adding executables to this list (including sub folders containing many components) you can reduce the amount of alerts that HIPS generates whilst maintaining a higher level of Defense+ security. This is particularly useful for developers that are creating new applications that, by their nature, are as yet unknown to the Comodo safe list.

Unrecognized Files

Once added to the file list, CES/CAS first scans against the Comodo certified safe files database and awards a file rating accordingly. If a file is unknown, it is given 'Unrecognized' rating for administrator to review and potentially set their own rating.

Blocked Files

Files that are awarded 'Blocked' rating will not be allowed to run on endpoints to which the policy is applied.

The 'Rating Files' tab allows the administrator to create custom list of applications with their own rating for selectively allowing or blocking them at the endpoints based on their ratings.

- To open the 'Rating Files' interface, click the 'Rating Files' tab in the 'File Rating' settings screen.
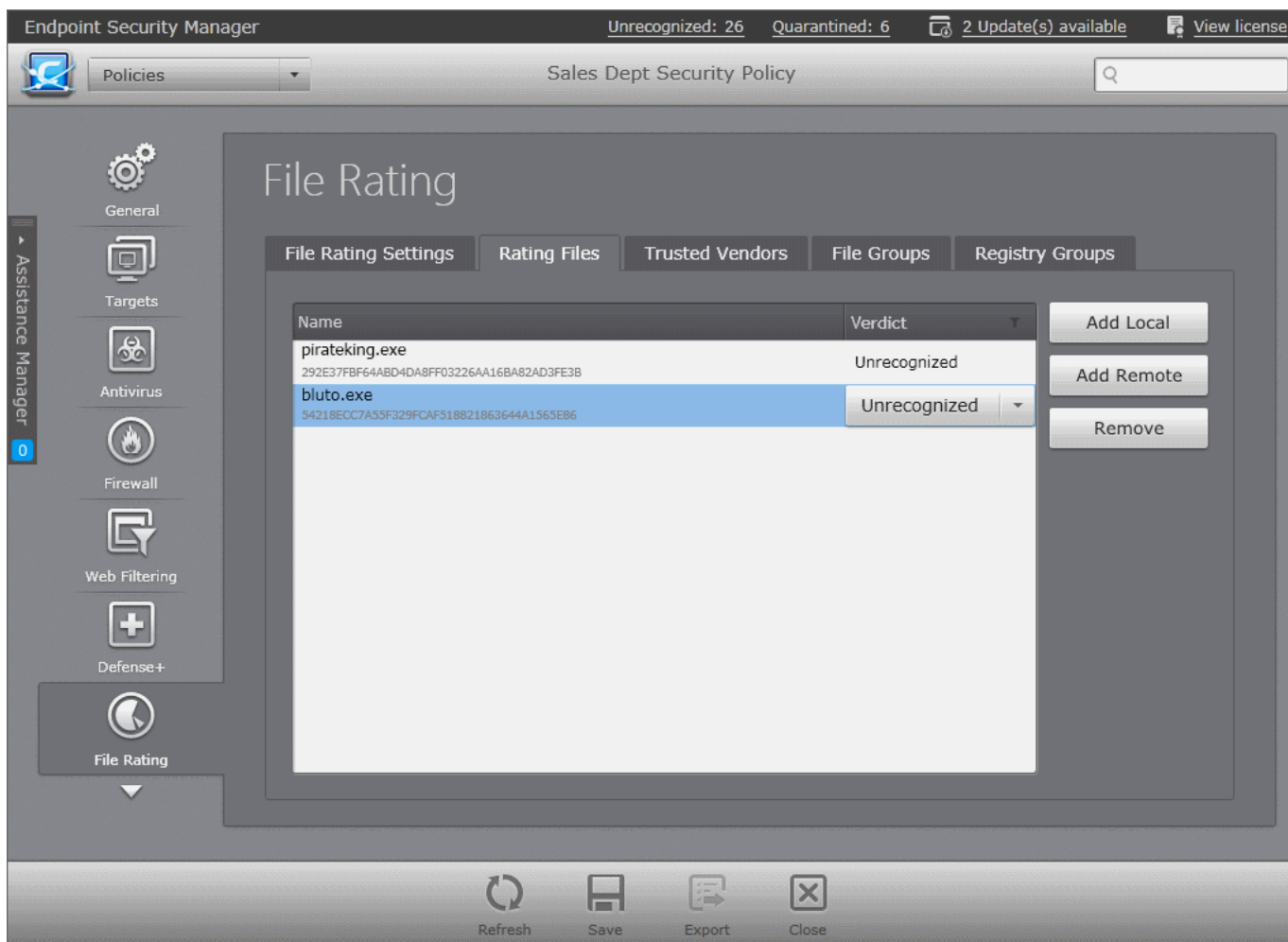
The 'Rating Files' interface displays a list of manually added files along with their ratings:

Rating Files - Table of Column Descriptions	
Column Header	**Description**
Name	Displays the name of the file and its file hash.
Verdict	Indicates the rating assigned to the file.

Filtering Options

You can filter the entries based on the ratings.

- To filter the list. click the funnel icon at the right of the 'Verdict' column header.
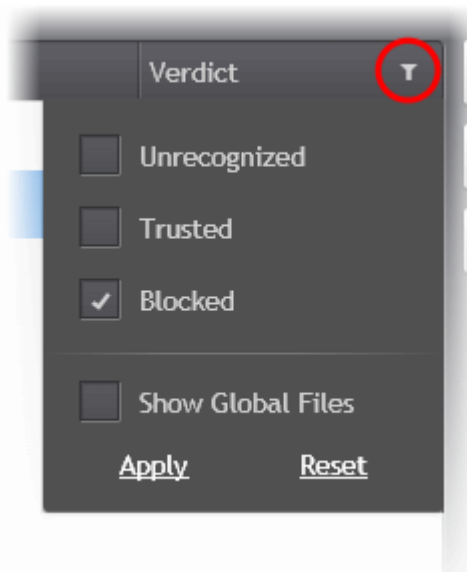
- Select the verdict to filter the list and click 'Apply'.

- To remove the filters, click the funnel icon and click 'Reset'.

- Selecting 'Show Global Files' displays files that were added to the global file list with the chosen rating, in addition to the files added for the policy in the 'Rating Files' interface. For more details on the managing the global file list, refer to the section **Files Management**.

From this interface, the administrator can:

- **Manually add files and assign rating**

- **Remove files from the list**

Adding Files to the Rating Files List

Administrators can manually add files to the list from the local machine or from machines connected to CESM. Upon addition of a file, CESM performs an instant cloud lookup and displays the file rating as per the global files list. The administrator can then manually choose a custom rating, if the rating from file lookup service needs to be changed.

To add new file(s) to Files list

- To add files from the computer through which the console is accessed, click the 'Add Local' button and navigate too the executable file to be added to the 'File List' and click 'Open'.

- To add files from other endpoints that are connected to CESM, click the 'Add Remote' button, select the endpoint, navigate to the file(s) that you want to add and click 'Add File'.

The File will be added to the list with the result from the cloud lookup in the 'Verdict' column.
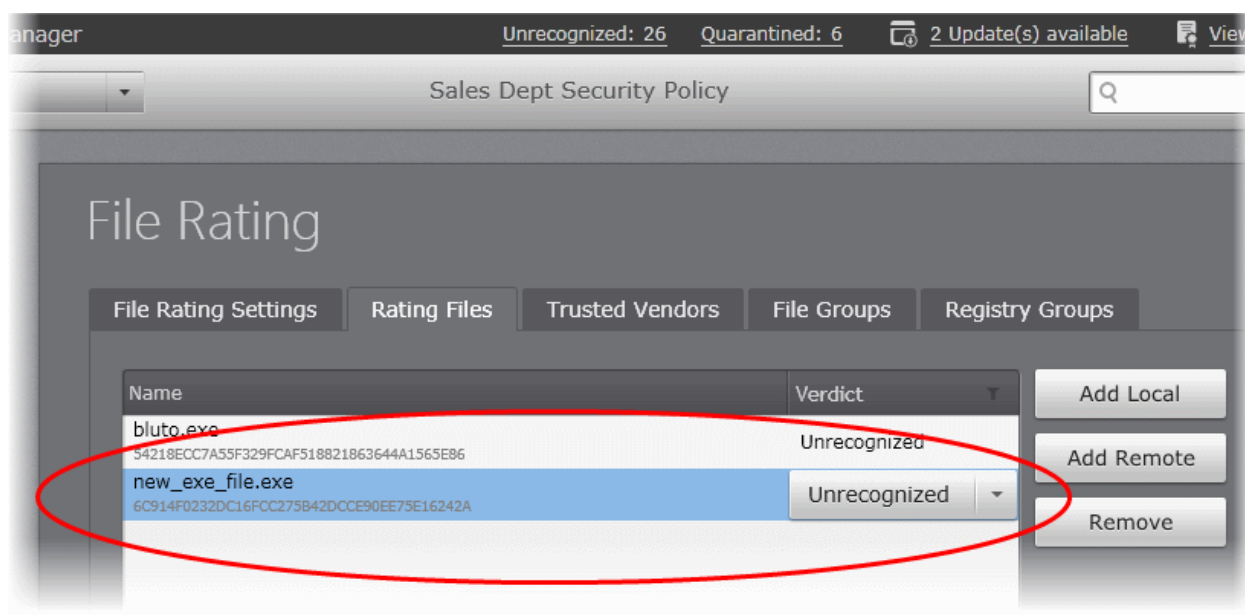
- To change the rating, click on the drop-down arrow beside the verdict an choose the rating from the drop-down.
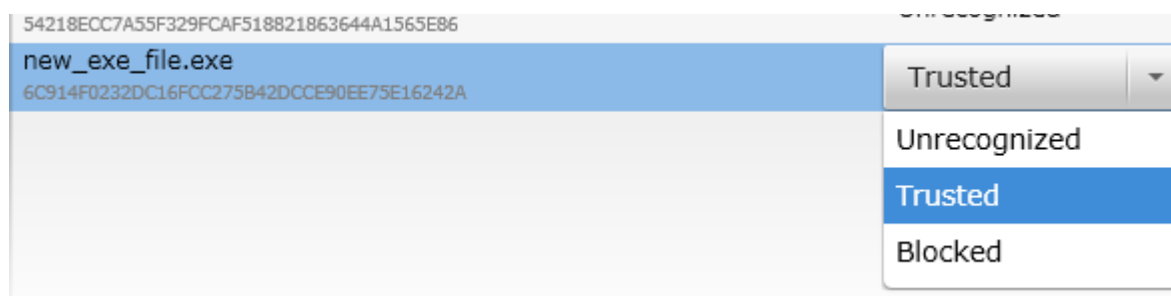
- Click 'Save' from the 'File Rating' interface for your configuration to take effect.

Removing files from Files List

In order for the CES/CAS to allow or block a file based on their default file rating, the administrator can remove the file from the Rating Files list, by selecting it and clicking 'Remove'.

Managing Trusted Vendors List

In CES/CAS, there are two basic methods in which an application can be treated as safe. Either it has to be part of the 'Safe List' (of executables/software that is known to be safe) or that application has to be signed by one of the vendors in the 'Trusted Vendor List'.

A software application can be treated as a 'Trusted' one if it is published by a Trusted Software publisher/vendor. To ensure the authenticity, the publisher/vendor digitally sign their software using a **code signing certificate** obtained from a Trusted Certificate Authority (CA). Ensuring whether a software/application is signed by a vendor ensures that the software is trusted. Refer to the Background details given below for more information.
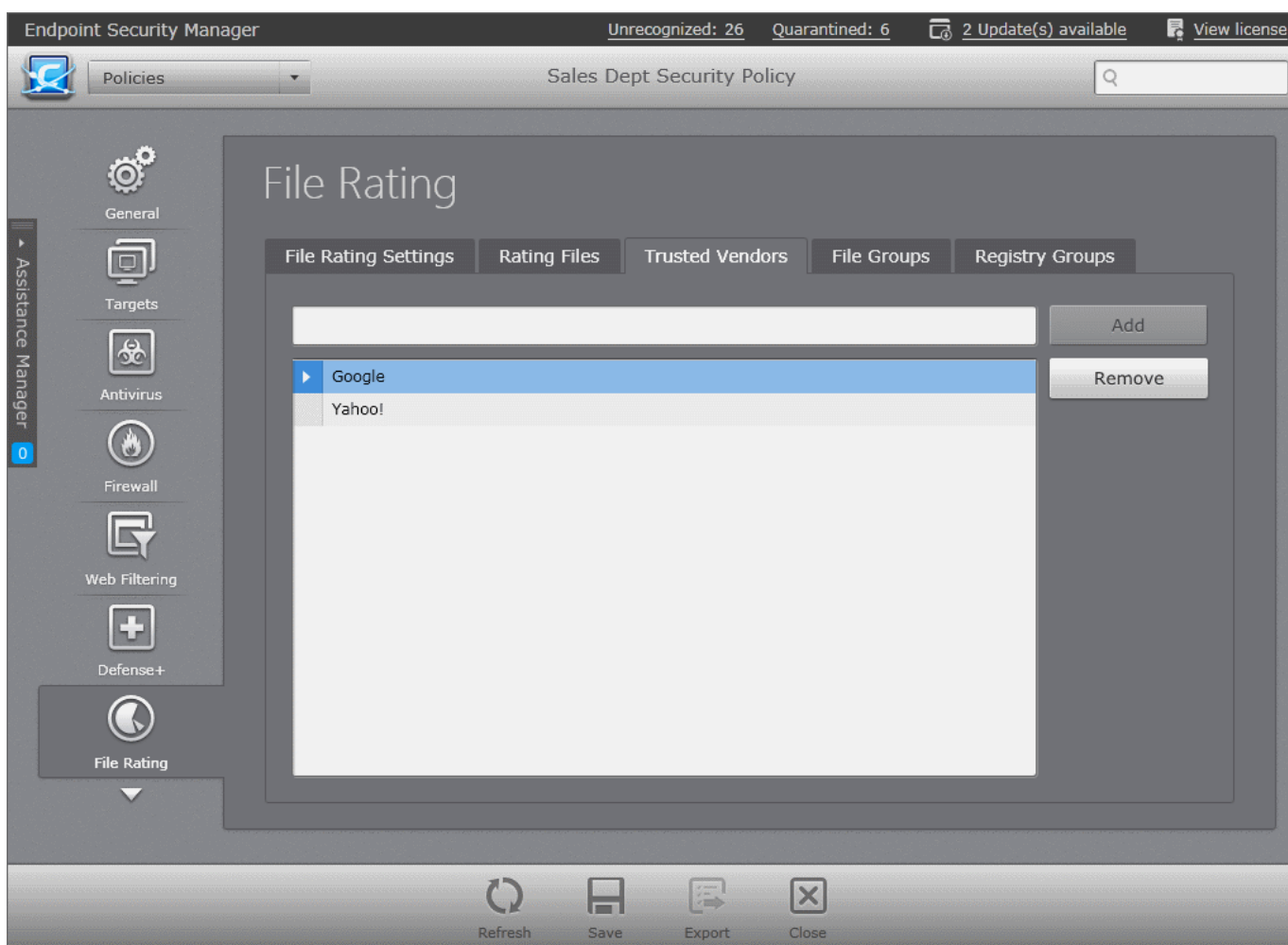
Background

Many software vendors digitally sign their software with a code signing certificate. This practice helps end-users to verify:

- **Content Source**: The software they are downloading and are about to install really comes from the publisher that signed it.

- **Content Integrity**: That the software they are downloading and are about to install has not be modified or corrupted since it was signed.

In short, users benefit if software is digitally signed because they know who published the software and that the code hasn't been tampered with - that are are downloading and installing the genuine software.

The 'Vendors' that digitally sign the software to attest to it's probity are the software publishers. These are the company names you see listed in the first column in the graphic above.

However, companies can't just 'sign' their own software and expect it to be trusted. This is why each code signing certificate is counter-signed by an organization called a 'Trusted Certificate Authority'. 'Comodo CA Limited' and 'Verisign' are two examples of a Trusted CA's and are authorized to counter-sign 3rd party software. This counter-signature is critical to the trust process and a Trusted CA only counter-signs a vendor's certificate after it has conducted detailed checks that the vendor is a legitimate company.

If a file is signed by a Trusted Software Vendor and the user has enabled 'Trust Applications that are digitally signed by Trusted Software Vendors' then it will be automatically trusted by CES/CAS (if you would like to read more about code signing certificates, see **http://www.instantssl.com/code-signing/**).

One way of telling whether an executable file has been digitally signed is checking the properties of the .exe file in question.

- Browse to the folder containing the .exe file.

- Right click on the .exe file.

- Select 'Properties' from the menu.

- Click the tab 'Digital Signatures (if there is no such tab then the software has not been signed).

This displays the name of the CA that signed the software.

Select the certificate and click the 'Details' button to view digital signature information. Click 'View Certificate' to inspect the actual code signing certificate.

The Trusted Vendors tab in the File rating settings interface allows the administrator to add vendors to the list for the policy.

To add trusted vendors

- Enter the name of the vendor as given in the code signing certificate in the text field.

- Click the 'Add' button.

The vendor will be added to the list.

If you want to remove a vendor from the list, select it and click the 'Remove' button.

- Click 'Save' for any changes to the settings to take effect.

Managing File Groups

File Groups are handy, predefined groupings of one or more file types, which makes it easy to add them for various functions such as adding them to Exclusions for AV scans, HIPS monitoring, auto-sandbox rules and so on. CESM ships with a set of predefined File Groups that are available for all the policies and if required administrators can add new File Groups, edit and manage all the groups for the custom policies.

The 'File Groups' tab in the 'File Rating' settings interface allows the administrator to view, create and manage pre-defined and custom file groups for a policy. The custom file group created for one policy will be available for various settings within the policy and will not be available for other policies.
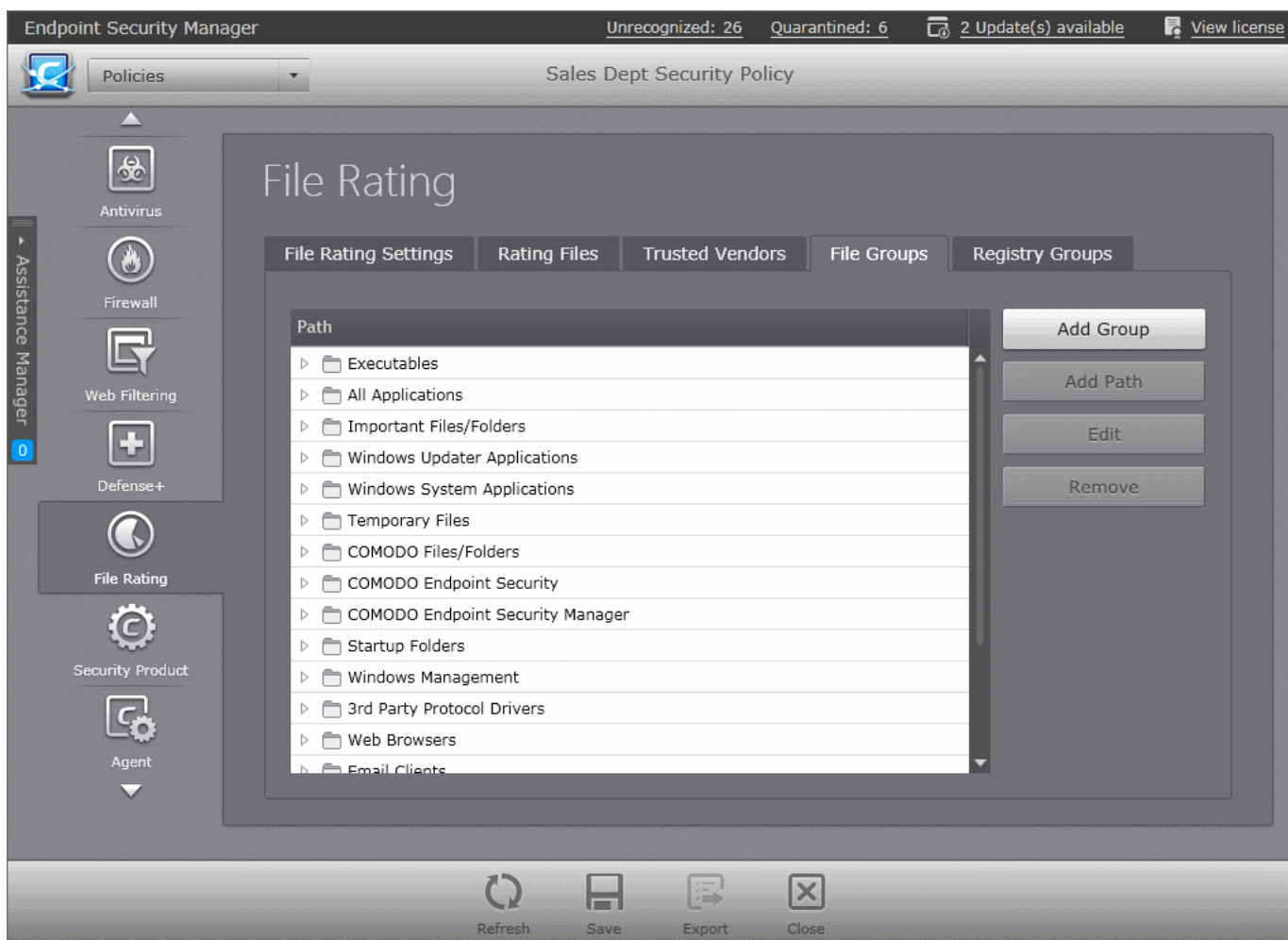
The administrator can expand a group to view the member files by clicking the right arrow ▷ beside the file group name.

New file groups can be added by specifying a name for the group and adding files by selecting them from standard Windows folders or entering their common file path.

To add a new custom file group

- Click 'Add Group' in the 'File Groups' interface. The 'Group Name' text box will appear.
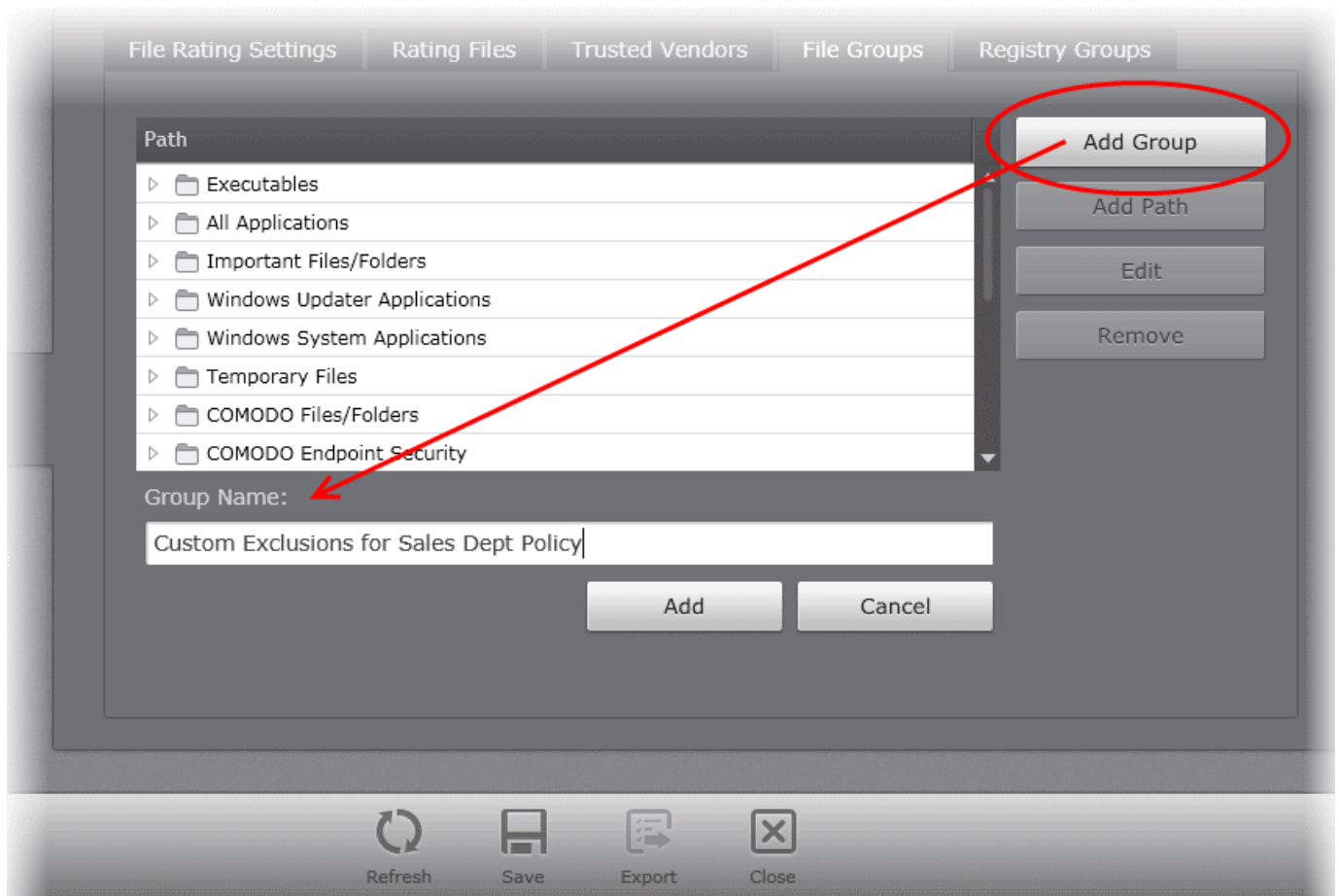
- Enter a name shortly describing the group and click 'Add'. The Group will be created and added.

The next step is to add files to the group.

- Select the new group and click 'Add Path'. The File/Folder Path field will appear with a drop-down and a text field.
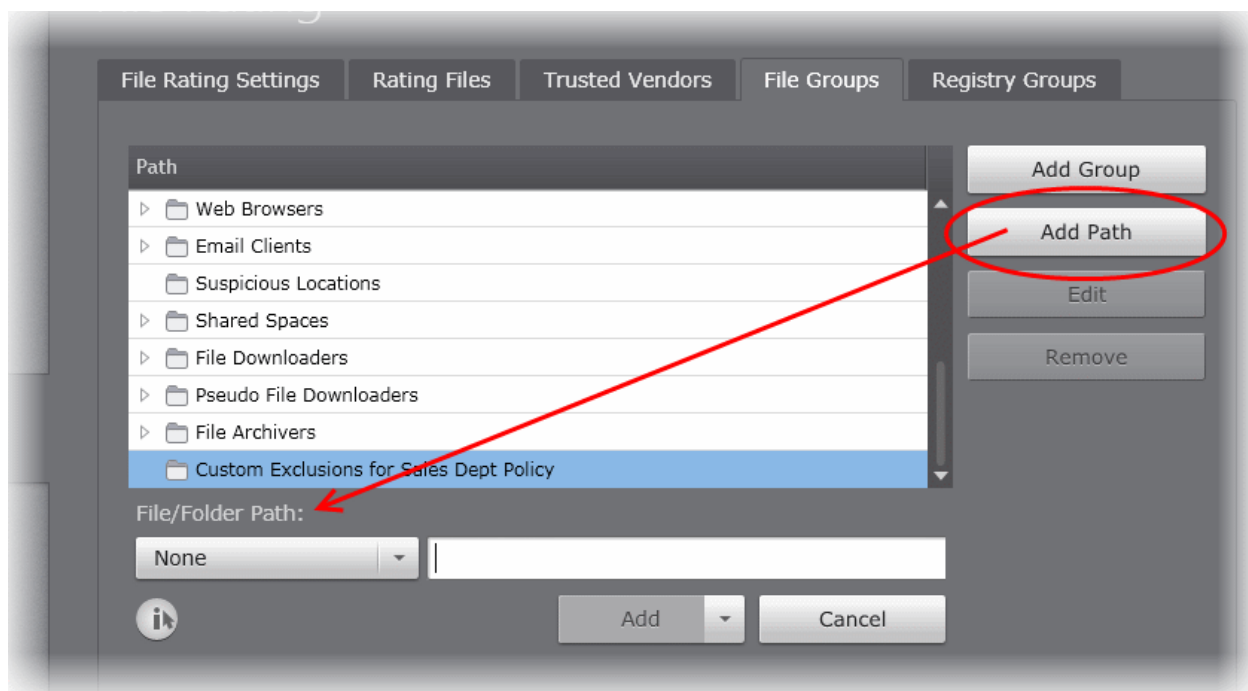
- Select the standard folder from the drop-down and enter the path/file name in the text box or enter the full folder/file path in the text box.
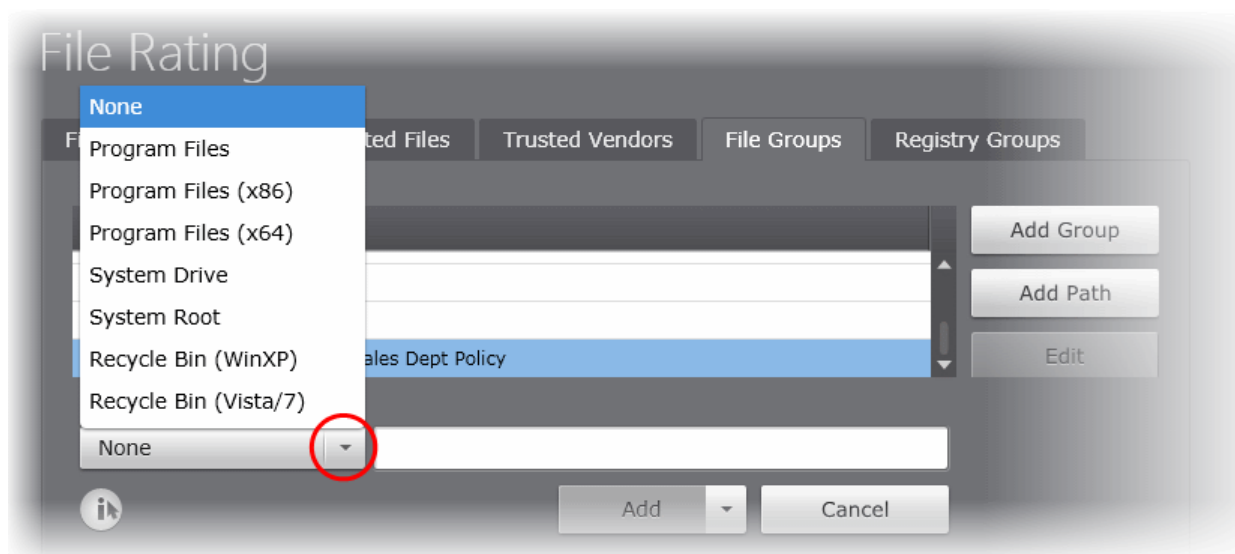
- Click Add. The file will be added to the group.

- Repeat the process to add more files to the group.

Editing a File Group

- To change a group name, select the group click Edit and enter the new name in the Group Name text box

- To add a new member file to a group, select the group and click Add Path and follow the steps as explained **above**.

- To edit the path of member files in a group, select the group, expand the group by clicking the right arrow ▷ beside the file group name, select the file and click the 'Edit'. Follow the steps as explained **above**.

- To remove a file group, select the group and click 'Remove'.

- To remove a member file in a group, select the group, expand the group by clicking the right arrow ▷ beside the file group name, select the file and click the 'Remove'.

Managing Registry Groups

Registry groups are predefined batches of one or more registry keys. Creating Registry group for a policy allows the administrator to add the group for exclusions for sandbox rules, enabling programs running inside the sandbox to access the keys and values in the group. CESM ships with a set of predefined Registry Groups that are available for all the policies and if required administrators can add new Registry Groups, edit and manage all the groups for the custom policies.

The 'Registry Groups' tab in the 'File Rating' settings interface allows the administrator to view, create and manage pre-defined and custom Registry groups for a policy. The custom Registry group created for one policy will be available for the settings within the policy and will not be available for other policies.
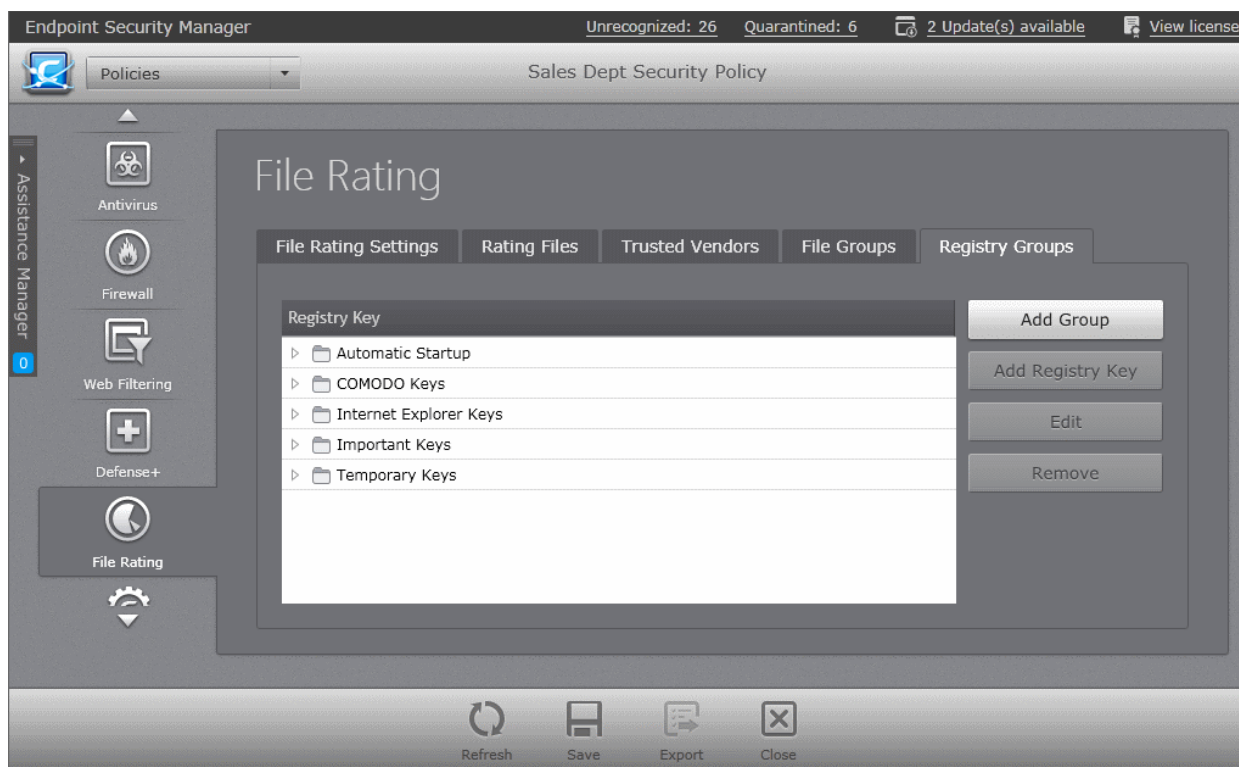
The administrator can expand a group to view the member keys by clicking the right arrow ▷ beside the Registry group name.

New Registry groups can be added by specifying a name for the group and adding keys to it in two steps.

To add a new custom Registry group

- Click 'Add Group' in the 'Registry Groups' interface. The 'Group Name' text box will appear.
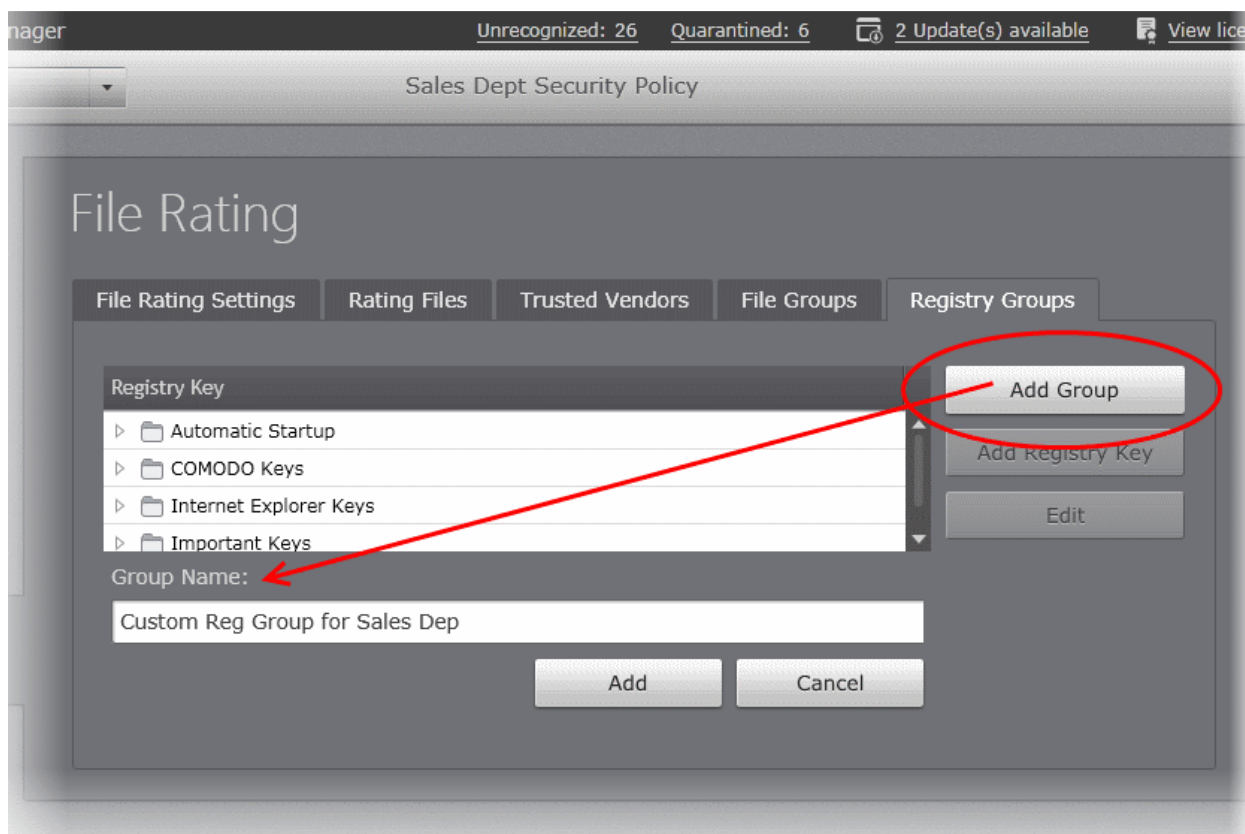
- Enter a name shortly describing the group and click 'Add'. The Group will be created and added.

The next step is to add keys to the group.

- Select the new group and click 'Add Registry Key'. The Registry Key field will appear.
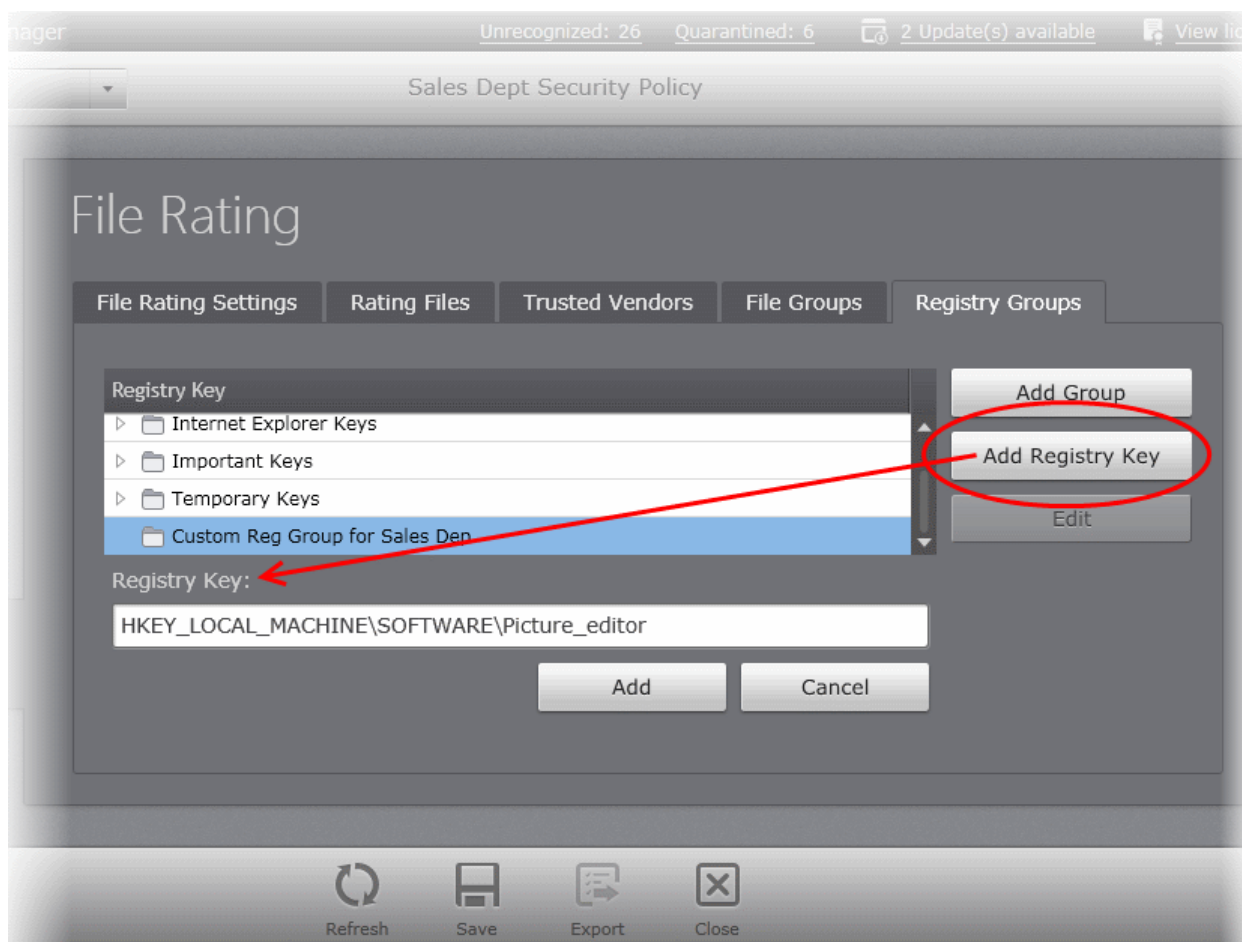
- Enter the full Registry key path in the text box.
- Click 'Add'. The key will be added to the group.
- Repeat the process to add more keys to the group.

Editing a File Group

- To change a group name, select the group click 'Edit' and enter the new name in the Group Name text box
- To add a new member key to a group, select the group and click 'Add Registry Key' and follow the steps as explained **above**.
- To edit a key in a group, select the group, expand the group by clicking the right arrow ▷ beside the group name, select the key and click the 'Edit'. Follow the steps as explained **above**.
- To remove a Registry group, select the group and click 'Remove'.
- To remove a member key in a group, select the group, expand the group by clicking the right arrow ▷ beside the group name, select the key and click the 'Remove'.

For more details on the File Rating Settings, , see the of CES - File Rating Settings online help page at **http://help.comodo.com/topic-84-1-604-7472-Manage-File-Rating.html**

5.2.8. Configuring General Security Product Settings

In the General Security Product Settings screen, administrators can configure various options related to the operation of Comodo Endpoint Security products like user interface settings, scheduled program updates, parental control, server to download the updates from and the Log settings.

Note: The 'General Security Product Settings' interface allows the administrator to view and edit various options for

CES/CAS/CAVM for the custom policies, and to view the configuration for the predefined policies. Predefined policies cannot be edited.

The following sections explain in detail on:

- **General Security Product Settings for Windows Workstations and Servers with CES/CAS installed**
- **General Security Product Settings for Mac based computers with CAVM installed**

General Security Product Settings for Windows Workstations and Servers Policy Types

To open the General Security Product Settings interface, click on the 'Security Product' icon [icon] in the left pane.

The 'General Security Product Settings' interface allows the administrator to configure the following:

- **User Interface**
- **Updates**
- **Proxy and Host Settings**
- **Log Settings**

User Interface Settings

The 'User Interface' tab allows the administrator to enable / disable CES/CAS notification messages and / or messages from Comodo Message Center and access to Shared Space folder from the desktop.

- **Show messages from COMODO Message Center** - If enabled, Comodo Message Center messages will periodically appear at the managed endpoints. They contain news about product updates, occasional requests for feedback, info about other Comodo products you may be interested to try and other general news. (*Default = Disabled*)

- **Show notification messages** - These are the CES/CAS system notices that appear in the bottom right hand corner of a user's desktop (just above the tray icons). They inform users about actions that CES/CAS is taking such as running an application in the sandbox. Notifications from the real-time antivirus scanner will also be displayed unless you have de-selected the 'Do not show antivirus alerts' check box in Antivirus > Real-time Scan. Leave this box disabled if you do not want system messages to be shown on endpoints. *(Default = Disabled)*

- **Show desktop widget** - The CES/CAS desktop widget displays at-a-glance information about CES/CAS security status, number of background tasks and shortcuts to open browsers inside the sandbox. The widget also acts as a shortcut to open the CES/CAS main interface, the Task Manager, the browsers and so on. If you do not want the widget to be displayed on the desktop of the endpoints, clear this checkbox.(*Default = Disabled*).

- **Show Shared Space shortcut on the desktop** - 'Shared Space' is a dedicated area on the local drive of the endpoint created by CES. Applications sandboxed by CES are permitted to write data into the dedicated area, so that they can also be accessed by non-sandboxed applications (hence the term 'Shared Space'). For example, any files or programs you download via a sandboxed browser that you wish to be able to access from your real system should be downloaded to the shared space. This is located by default at 'C:/Program Data/Shared Space'. By default, a shortcut for the user to access the shared space is created in the desktop. If you do not want the shortcut to be created, de-select this option. (*Default = Enabled*).

Note: The Sandboxing feature is available only on the CES, installed on Windows workstations. Hence this option is available only for Windows Workstations Policy type and not in Windows Servers Policy type.

- Click 'Save' for your settings to take effect.

Update Settings

The 'Updates' area allows the administrator to configure the frequency for the CES/CAS program to check for virus database updates.
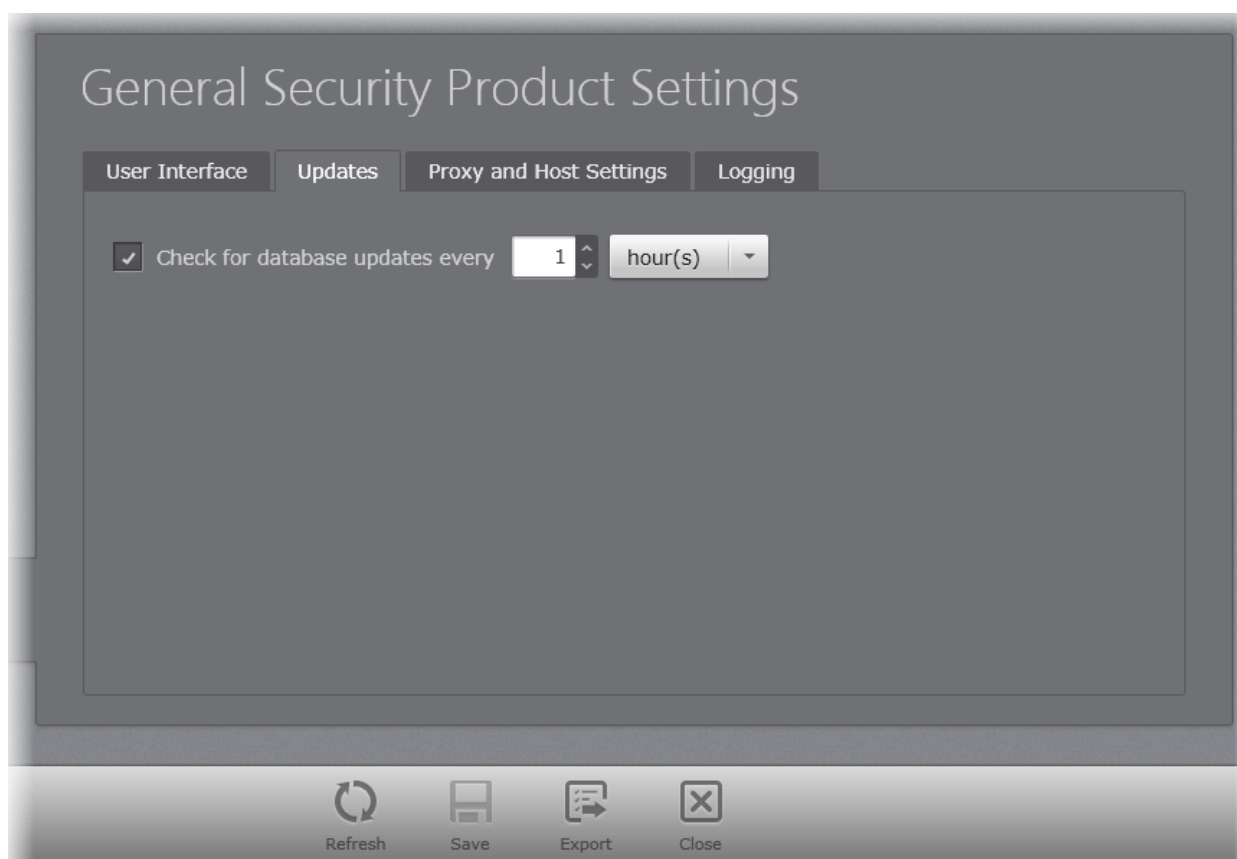
- • **Check Database updates every NN hours** - If this is option is enabled, CES/CAS automatically checks for program and virus database updates from the servers specified in the Proxy and Host Settings screen. Comodo recommends automatic update checks are enabled to ensure your system enjoys maximum protection against the latest threats. (***Default=Enabled***). You can also specify the intervals at which the CES/CAS should check for the updates. (***Default = 1 hour***)

- • Click the 'Save' icon for your settings to take effect.

Proxy and Host Settings

The Proxy and Host Settings screen allows administrators to select the host from which the updates are to be downloaded by the CES/CAS installations at the endpoints. By default, CES/CAS will directly download updates from Comodo servers. However, advanced users and network admins may wish to first download updates to a proxy/staging server and have individual CES/CAS installations collect the updates from there. The 'Proxy and Host Settings' interface allows you to point CES/CAS at this proxy/staging server. This helps conserve overall bandwidth consumption and accelerates the update process when large number of endpoints are involved.

> **Note**: Configuring a proxy server for individual CES/CAS installations to download the AV database and program updates requires the proxy cache service enabled for CESM. The Administrator should have enabled the service while choosing the 'Installation Preferences' during the CESM installation. Refer to the section **Installing and Configuring the Service** for more details.
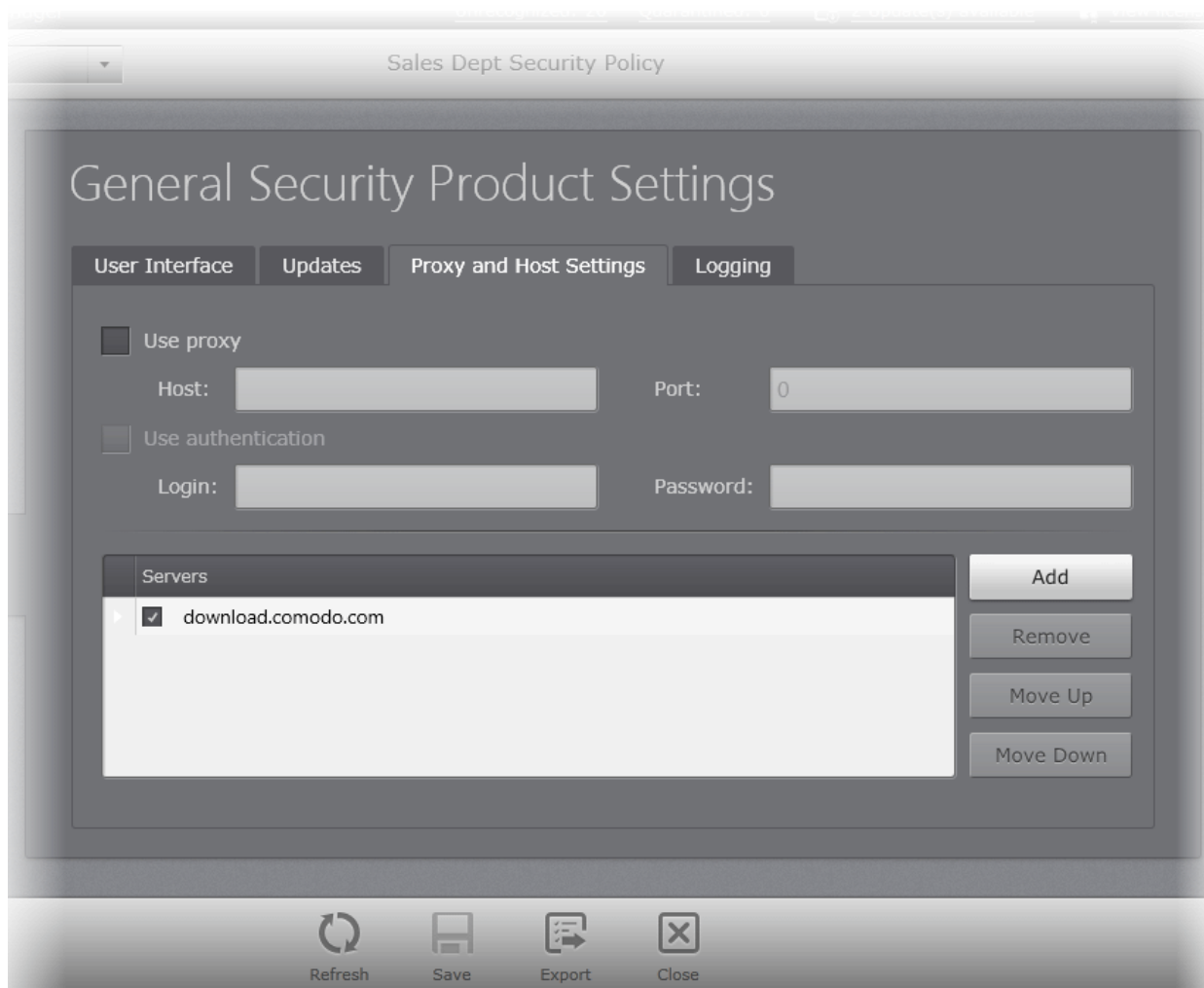
- Select '**Use proxy**' check box if you want CES/CAS to use the Proxy Server.

    - Enter the host name and port numbers. If the proxy server requires access credentials, select the 'Use Authentication' check-box and enter the login / password accordingly.

You can add multiple servers from which updates are available. To do this, click the 'Add' button beside the 'Servers' column then enter the address in the server field.

- Activate or deactivate each update server by selecting or deselecting the check-box alongside it

- Use the 'Move Up' and 'Move Down' buttons to specify the order in which each server should be consulted for updates. CES/CAS will commence downloading from the first server that contains new updates.

- Click the 'Save' icon for your settings to take effect.

Log Settings

CESM has the ability to store the log files from the CES/CAS installations at the endpoints at different locations, it can even forward the logs to an external Syslog server. The administrator can choose the location of their easier access to view the logs.

The Logging tab in the General Security Product Settings interface allows the administrator to configure the locations at which the log files from the CES/CAS installations at the endpoints are to be stored as per the policy and maximum file size settings for the log files.
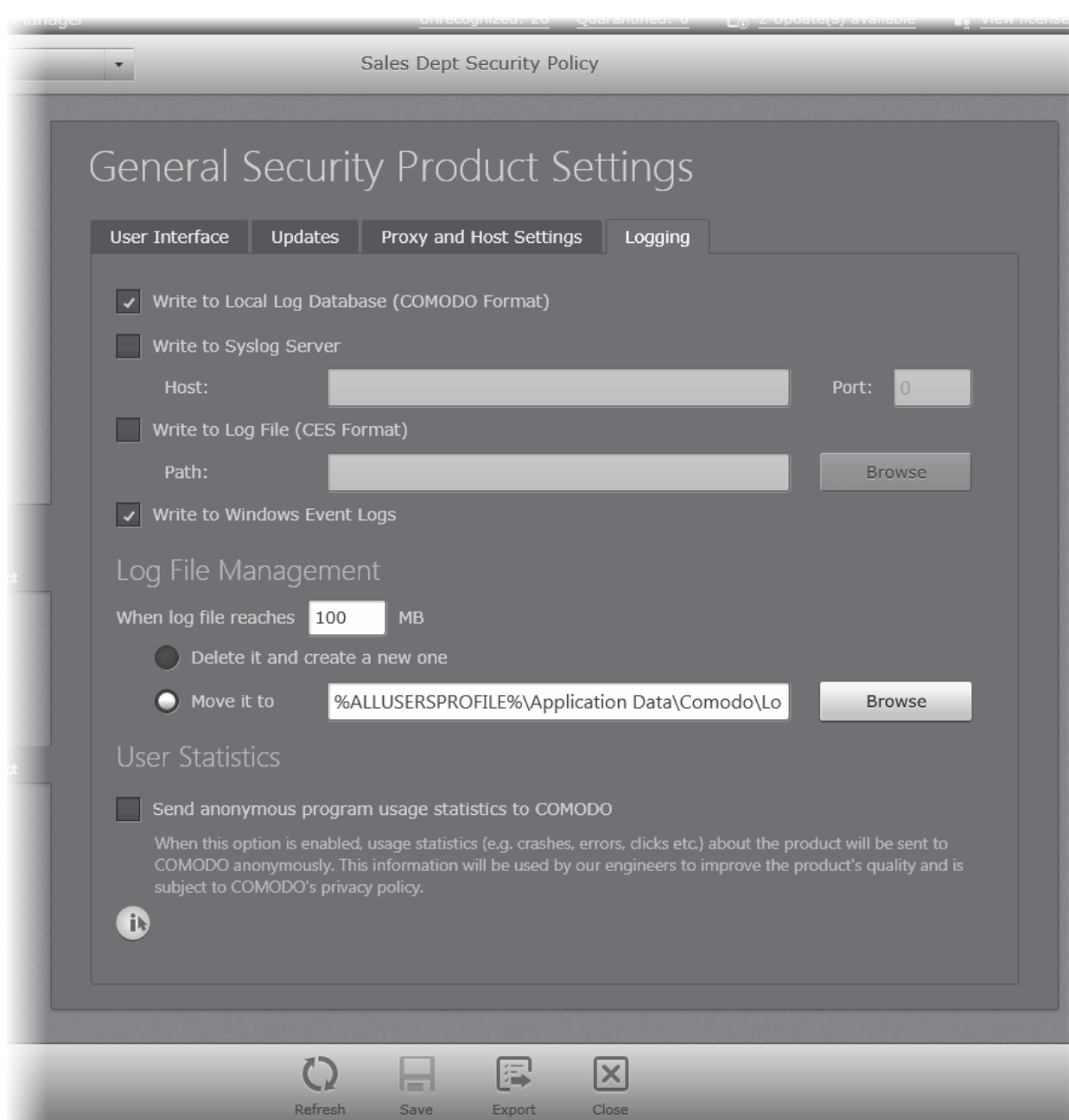
- **Write to Local Log Database** - Instructs CESM to store the log files in the local storage of the endpoint in Comodo format so that they can be viewed from the CES/CAS installation. The Log storage depends on the log file management settings configured in the '**Log File Management**' settings area in the same interface. (**Default = Enabled**).

- **Write to Syslog Server** - Instructs CESM to forward the log files to an external Syslog Server integrated with the CESM sever. Enter the IP address/hostname of the Syslog server in the Host text field and enter the port through which Syslog server listens to CESM in the 'Port' field (default port = 514). (***Default = Disabled***)

- **Write to Log file (CES) Format** - Instructs CESM to store the log files in at a specified location in an endpoint connected to the server in Common Log Format (CES) format, also known as NCSA Common Log Format, which is standardized text file format. In selecting this option, click Browse, select the Endpoint and navigate to the log file to which the logs are to be added. (***Default = Disabled***)

- **Write to Windows Event Logs** - Instructs CESM to store the log events to the Windows Event Logs. (***Default = Disabled***)

Log File Management

- **If the log file's size exceeds (Mb)** - Enables the administrator to specify behavior when the Local Log Database (Comodo Format) log file reaches a certain size. You can decide on whether to maintain log files of larger sizes or to discard them depending on your future reference needs and the storage capacity of your hard drive.

- Specify the maximum limit for the log file size (in MB) in the text box beside 'If the log file's size exceeds (MB)' *(Default = 100MB).*

- If you want to discard the log file if it reaches the maximum size, select **'Delete it and create a new one'.** Once the log file reaches the specified maximum size, it will be automatically deleted from your system and a new log file will be created with the log of events occurring from that instant *(Default = Enabled).*

- If you want to save the log file even if it reaches the maximum size, select **'Move it to'** and select a destination folder for the log file *(Default = Disabled).*

User Statistics

- **Send anonymous program usage statistics to COMODO** - Comodo collects collects the usage details from millions of CES/CAS users to analyze their usage patterns for the continual enhancement of the product. On selecting this option, the CES installations at the endpoints will collect details on how the end-users use the application and send them periodically to Comodo servers through a secure and encrypted channel. Also your privacy is protected as this data is sent anonymous. This data will be useful to the engineers and developers at Comodo to identify the areas to be developed further for delivering the best Internet Security product. Disable this option if you do not want your usage details to be sent to Comodo. *(Default = Disabled)*

- Click the 'Save' icon for your settings to take effect.

General Security Product Settings for Mac General Policy Type

- To open the General Security Product Settings interface, click on the 'Security Product' icon ⚙ from the left pane.

The 'General Security Product Settings' interface allows the administrator to configure the following:

- **General Settings**
- **Parental Control**
- **Updates**

General Settings

The 'General' tab allows the administrator to enable / disable automatic program and virus database updates and display of notification messages from CAVM.
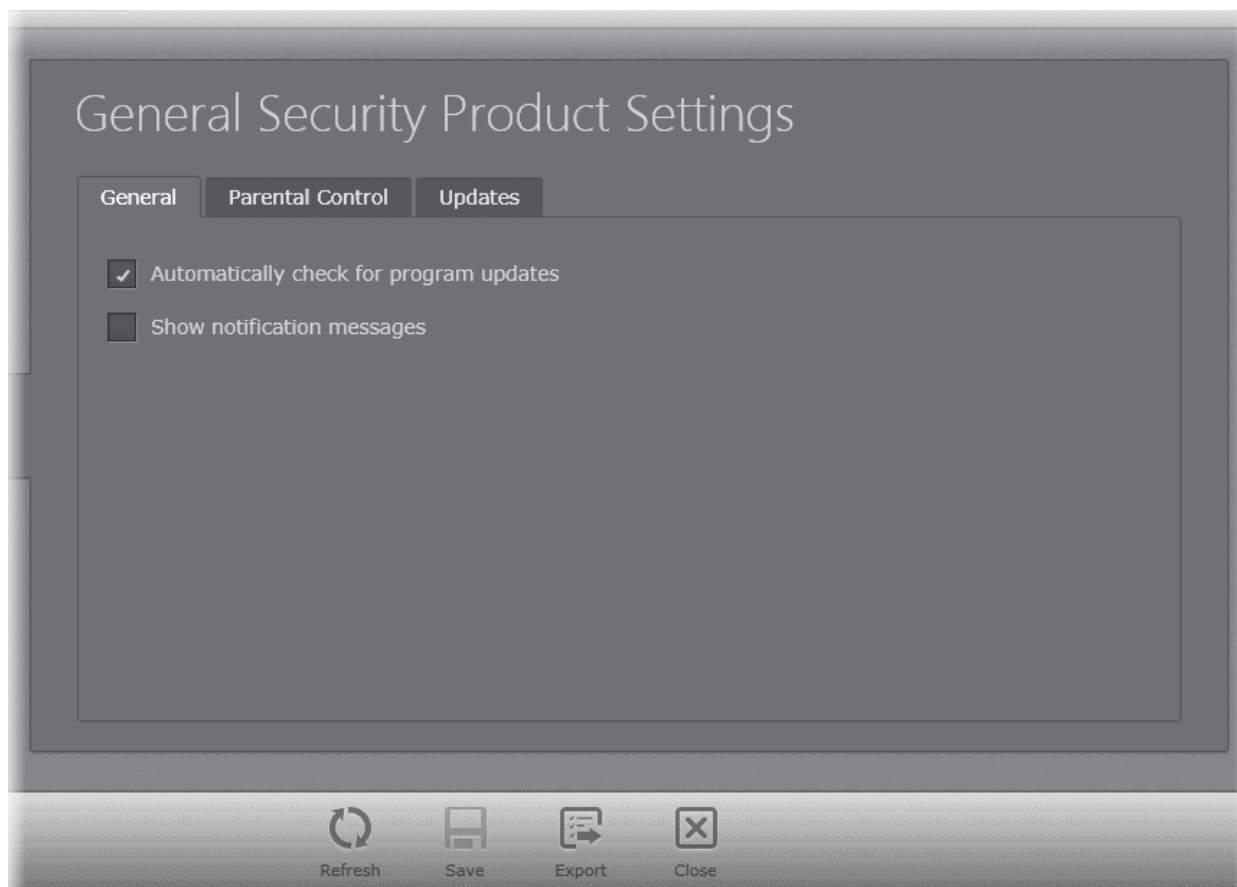
- **Automatically check for program updates** - If this is option is enabled, CAVM automatically checks for program and virus database updates and download them. You can also specify which servers to use for updates in the 'Updates' screen. Comodo recommends automatic update checks are enabled to ensure your system enjoys maximum protection against the latest threats.(*Default=Enabled*)

- **Show notification messages** - Messages from CAVM appear in the bottom right hand corner of a user's desktop (just above the tray icons). They inform users about actions that CAVM is taking. Notifications from the real-time antivirus scanner will also be displayed unless you have de-selected the 'Do not show antivirus alerts' check box in Antivirus > Real-time Scan. Leave this box disabled if you do not want system messages to be shown on endpoints. (*Default = Disabled*)

Parental Control

The 'Parental Control' tab enables the administrator to provide password protection for the local configuration of the CAVM.
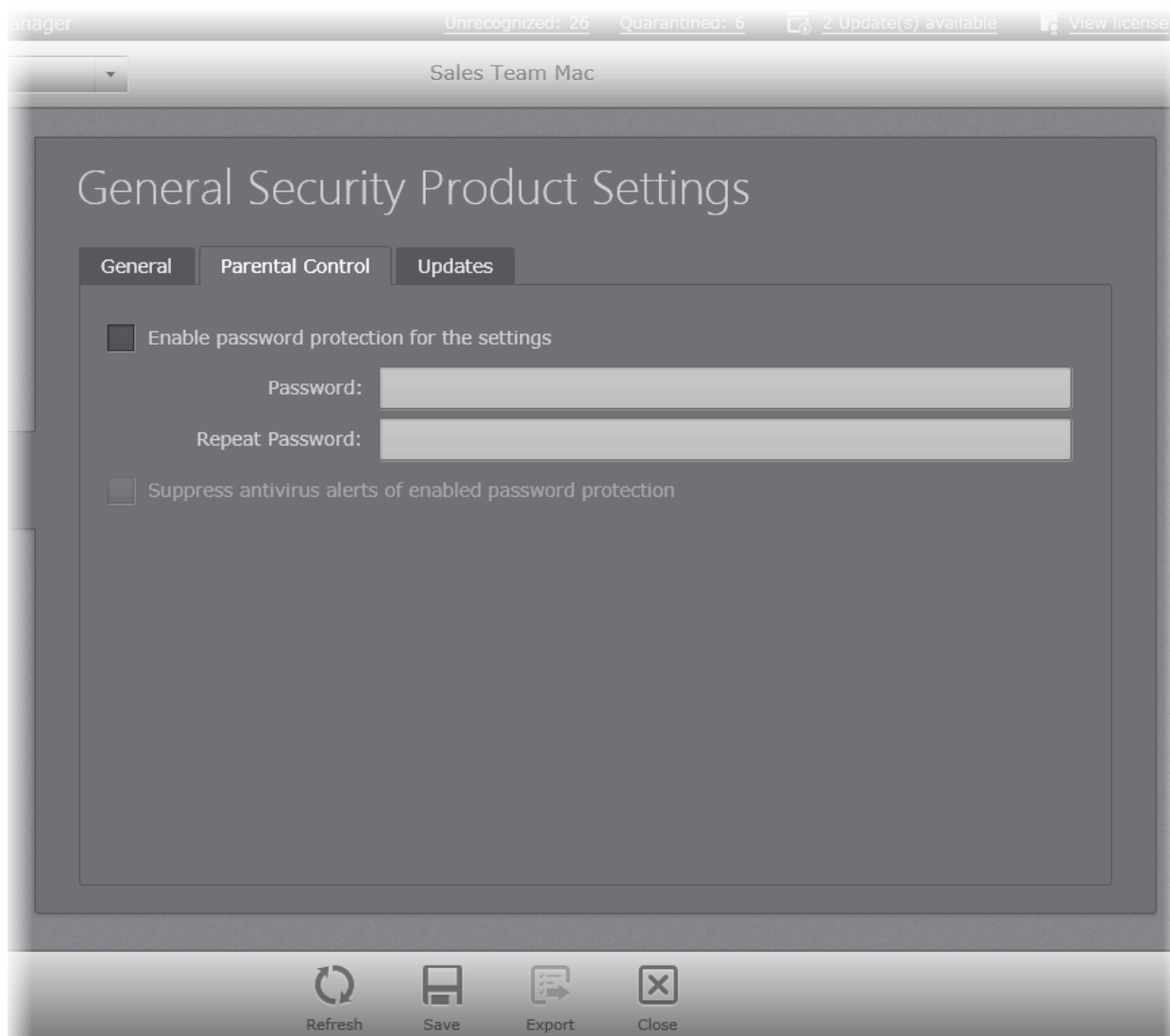
- • **Enable Password protection for settings** - If this option is selected, the user at the endpoint can change the settings of the CAVM installation only after entering the password specified in this field. Enter the password and reenter it for confirmation in the respective fields if this option is selected. (***Default = Disabled***)

- • **Suppress antivirus alerts of enabled password protection** - On an attempt to change a configuration of CAVM at the endpoint, an alert will be generated, prompting the user/administrator to enter the password. On entering the password, the user/administrator will be able to locally change the configuration. If you do not want to display the alert and hence prohibit changes to be done at the local installation, select this option. (***Default = Disabled***)

Updates

The 'Updates' tab enables the administrator to specify the server from which the CAVM installation at the endpoints can download the program and virus database updates.
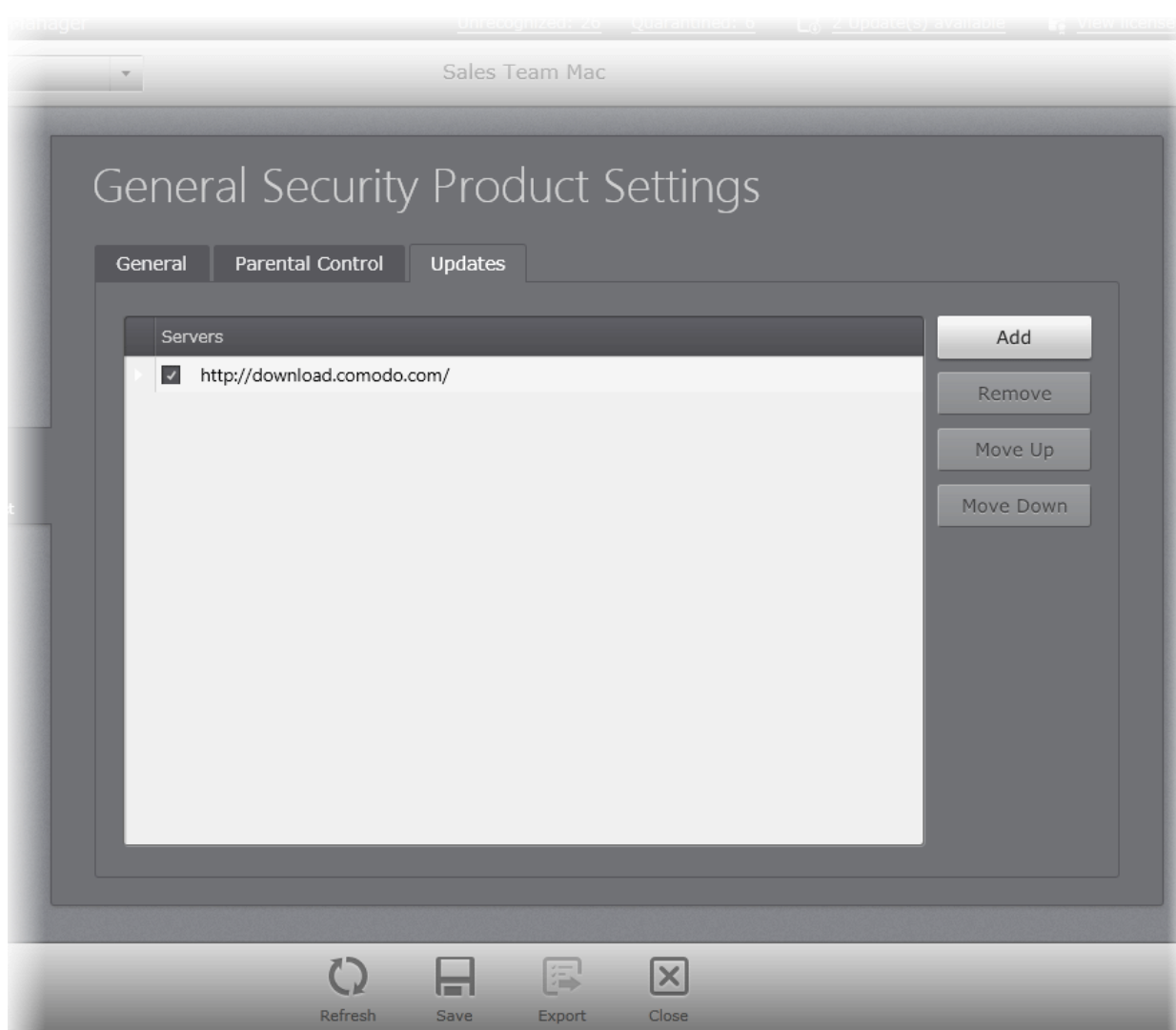
You can add multiple servers from which updates are available. To do this, click the 'Add' button beside the 'Servers' column then enter the address in the server field.

- Activate or deactivate each update server by selecting or deselecting the check-box alongside it

- Use the 'Move Up' and 'Move Down' buttons to specify the order in which each server should be consulted for updates. CAVM will commence downloading from the first server that contains new updates.

- Click the 'Save' icon for your settings to take effect.

5.2.9. Configuring Agent Settings

In the Agent Settings screen, administrators can edit the Agent settings for the selected policy.

> **Note**: The 'Agent Settings' interface allows the administrator to view and edit the agent settings for the custom policies, and to view the settings for the predefined policies. Predefined profiles cannot be edited.

To open the Agent Settings interface, click on the 'Agent' icon in the left pane. The Agent Settings screen will be displayed.
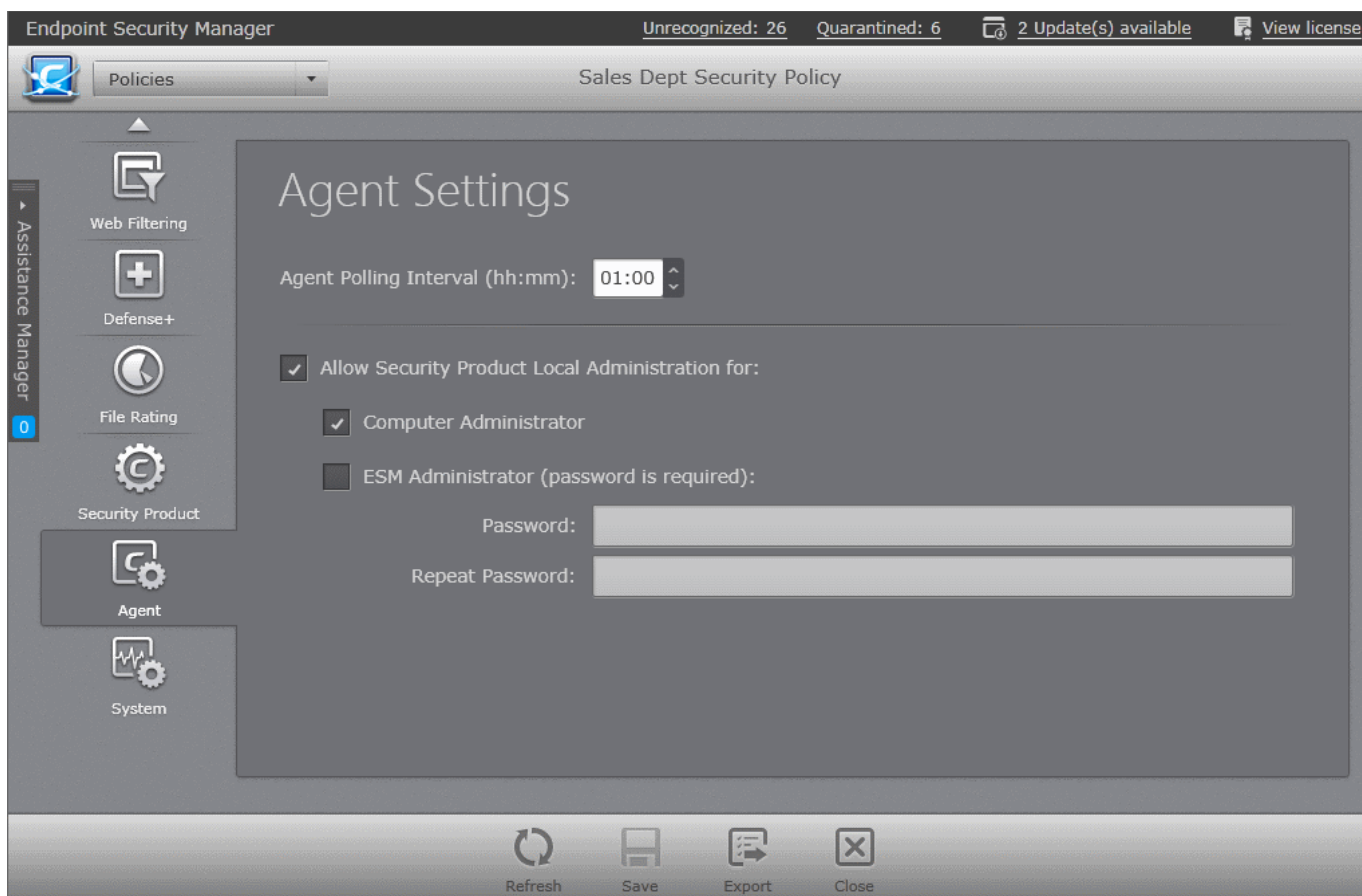
- **Agent polling interval** - The administrator can set the time interval (in hours and minutes) for the agent to periodically check whether the CES/CAS/CAVM at the target computer is compliant with the applied security policy. The result will be dynamically displayed in the 'Computers' interface. (Default = 1 hour, up to but not including 24 hours).

- **Allow Security Product Local Administration for**- Configures the agent to allow the CES/CAS installation at the target machine to be switched to local administration mode should the user desire to change the security settings. The administrator may choose to not allow the user to alter the security settings in his/her computer, so as to not lead to a security hole in the network. On selecting the 'Allow Local Administration' check box, the administrator should specify how the access to local administration has to be restricted by selecting an option from the following check boxes:

  - **Computer administrator** - Selecting this option will require the computer user to either have administrative credentials or enter credentials while switching CES/CAS at the target machine to local administration mode.

  - **ESM Administrator** (password is required) - Allows the administrator to specify a password in the text box below this option. This password should be entered for switching the CES/CAS to local administration mode.

Note: The option 'Allow Security Product Local Administration for' is not available for Mac General Policy type.

- Click 'Save' for any changes to take effect.

5.2.10.   Configuring System Settings

The System Settings screen allows the administrator view and configure the system settings like power management, connectible devices management and system resource monitoring settings deployed on to the target computers as per the policy.

Note: The 'System Settings' interface allows the administrator to view and edit the system settings for the custom policies, and only to view the settings for the predefined policies. Predefined profiles cannot be edited.

To open the System Settings interface, click on the 'System' icon [icon] in the left pane. The System Settings screen with Monitoring Configuration interface will be displayed.
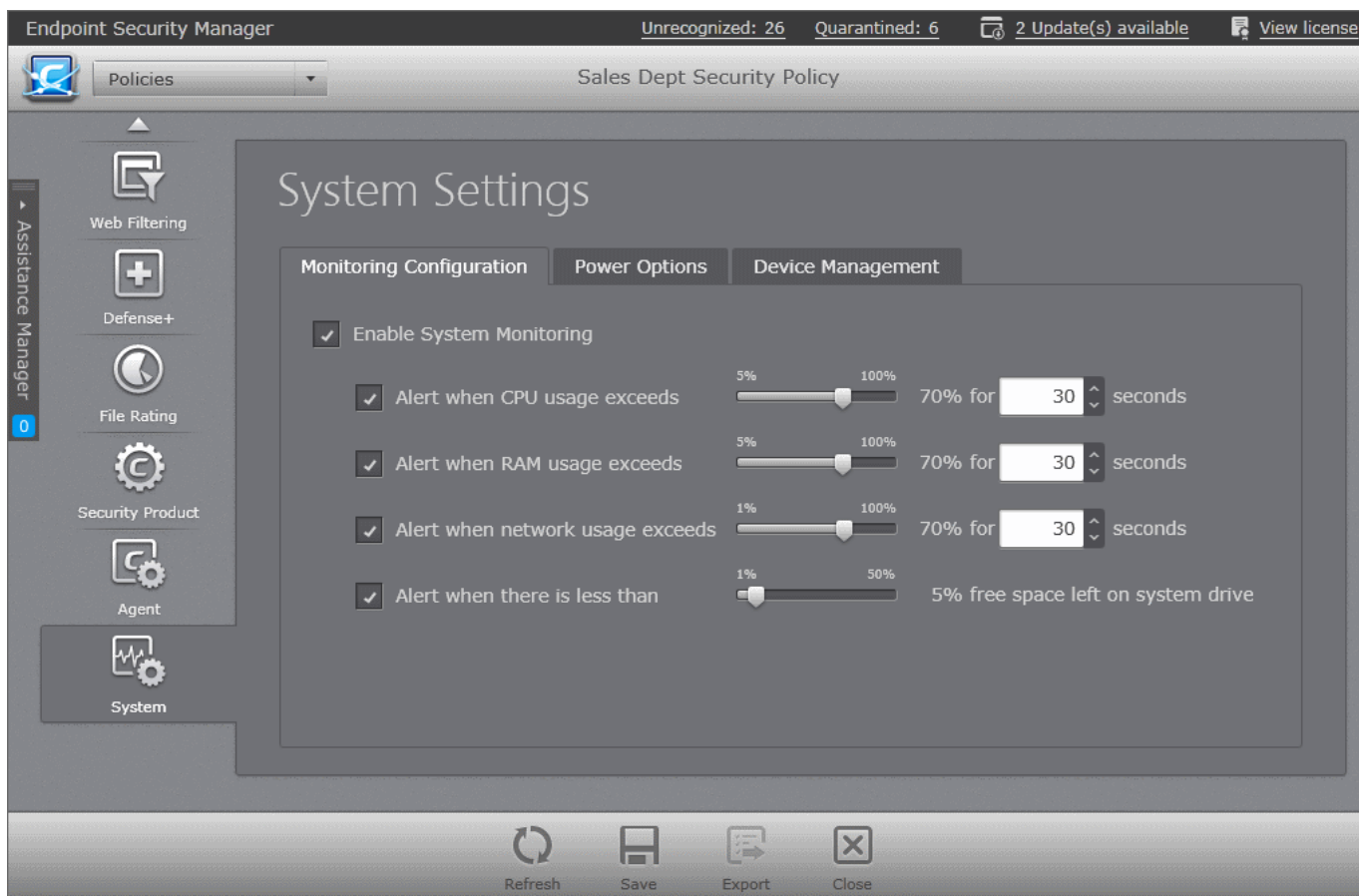
System Monitoring Configuration

CESM can watch the system resource usages like CPU usage, system memory usage, network data traffic and disk space usage in the managed endpoints. If the usage levels exceed the thresholds set by the policy applied to an endpoint, and alert will be generated and the endpoint will be indicated as 'Overloaded' in the Computers area. The administrators can view the alerts generated under the Computer Properties > Monitoring Alerts pane, for taking measures to keep the system resource usage within limits and for troubleshooting purposes, should any problem arises at the endpoint. Refer to the section **Viewing System Monitoring Alerts** for more details.

The 'Monitoring Configuration' tab enables the administrator to enable/disable system resource monitoring, and configure the thresholds for various monitored parameters.

- **Enable System Monitoring** - Allows you to enable or disable system resource monitoring.

    - **Alert when CPU exceeds NN% usage for TT seconds** - Generates alert when the CPU usage at the target computer is continuously larger than the percentage specified in the slider for the time (in seconds) specified in the time drop-down combo box. The administrator can specify the maximum CPU usage allowance in the slider and the period in the drop-down combo box. (Default = 70% for 30 seconds)

    - **Alert when RAM exceeds NN% usage for TT seconds** - Generates alert when the system memory usage at the target computer is continuously larger than the percentage specified in the slider for the time (in seconds) specified in the time drop-down combo box. The administrator can specify the maximum system memory usage allowance in the slider and the period in the drop-down combo box. (Default = 70% for 30 seconds)

    - **Alert when network usage exceeds NN% usage for TT seconds** - Generates alert when the data traffic from/to the endpoint is continuously larger than the network utilization percentage specified in the slider, for the time (in seconds) specified in the time drop-down combo box. The administrator can specify the network usage limit in the slider and the period in the drop-down combo box. (Default = 70% for 30 seconds)

    - **Alert when there is less than NN% free space left on system drive** - Generates alert when the remaining space in the hard disk drive partition on which the Operating System is installed, reduces below the

percentage of total partition size, specified in the slider. The administrator can specify the minimum amount of free space to be maintained in the system drive through the slider. (Default = 5%)

Power Options

The administrator can set the power management settings like idle time out period for display, hard disks, system standby and system hibernation under the Power Options tab.
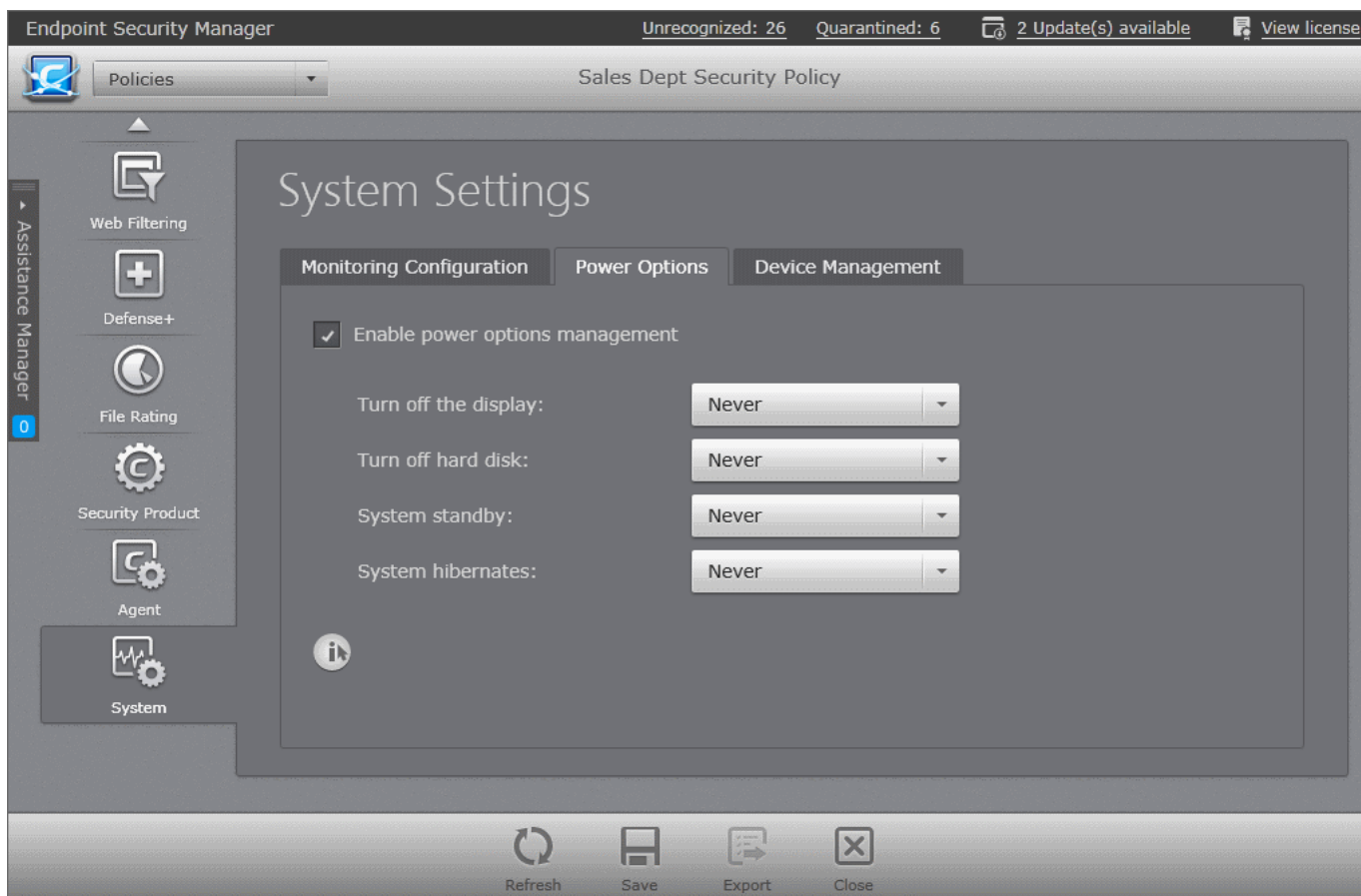
- **Enable power options management** - Allows the administrator to configure power settings. On selecting the 'Enable power options management' check box, the administrator can specify the power settings from the options below:

    - **Turn off the display** - Allows the administrator to select the period after which the display will be switched off.
    - **Turn off hard disk** - Allows the administrator to select the period after which the hard disk will be turned off.
    - **System standby** - Allows the administrator to select the period after which the system will go into standby mode.
    - **System hibernates** - Allows the administrator to select the period after which the system will go into hibernate mode.

The above power settings are applicable only for plugged-in to mains (AC) settings and will not apply to on-battery power settings.

Devices Management

The administrator can configure restrictions for connecting external storage devices and using external memory media under the Device Management tab.

Note: The Device Management Settings are not available for Mac General Policy Type.
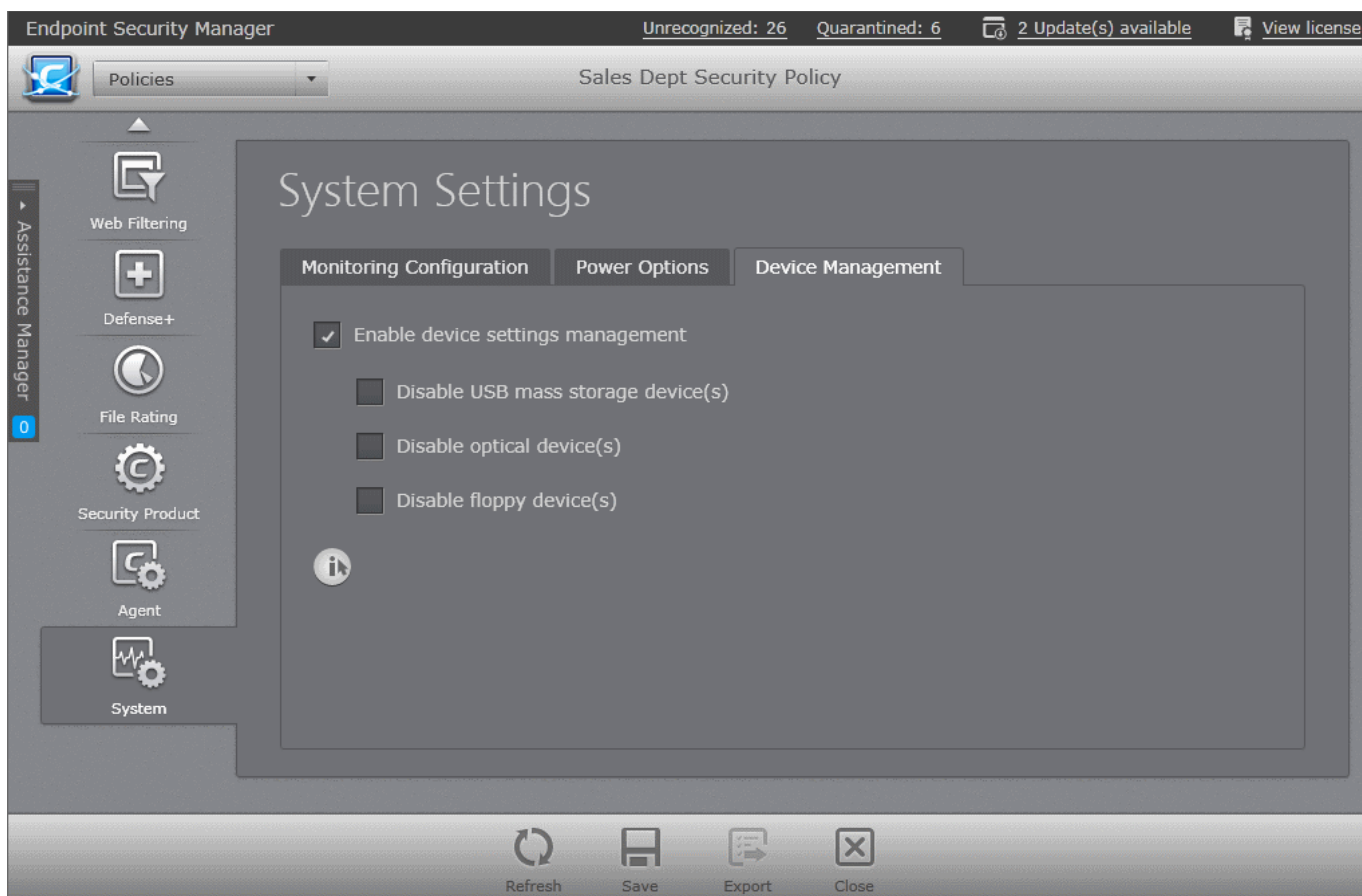
- **Enable device settings management** - The administrator can configure device settings by the selecting this check box and from the options below:
    - **Disable USB mass storage devices(s)** - Selecting this option will disable USB mass storage devices at the target computers.
    - **Disable optical device(s)** - Selecting this option will disable optical devices at the target computers. This will take effect only after reboot of the the target computers.
    - **Disable floppy device(s)** - Selecting this option will disable floppy devices at the target computers.
- Click the 'Save' icon for any changes to take effect.

5.3. Re-applying Security Policies to Endpoint Groups

Newly created security policies or edited polices can be assigned or reassigned to endpoint groups or endpoints in multiple ways.

Re-applying policies to endpoint groups:

- From the '**Policies**' area - Administrators can reassign polices to different endpoint groups from this interface also. Select the policy that you want to reassign to a group and use any of the following options:
    - Right click options in the Policies interface. (Refer to the section **Selecting Target Groups** for more details).
    - Policy Target screen of the selected group. (Refer to the section **Selecting Target Groups** for more details).
    - Using the Policy icon in the Groups interface (Refer to the section **Selecting Target Groups** for more details).

- From the '**Groups**' area - Administrators can reassign polices to different endpoint groups from this interface. Select the group that you want to reassign a policy and use any of the following options:
    - Right click options in the Groups interface. (Refer to the section **Viewing and Managing Groups** for more details).
    - General screen of the selected group.(Refer to the section **Viewing and Managing Groups** for more details).
    - Using the Policy icon in the Groups interface. (Refer to the section **Viewing and Managing Groups** for more

details).

Re-applying policies to endpoints:

- From the '**Computers**' area - Administrators can reassign polices to different endpoints from this interface. Select the endpoint that you want to reassign a policy and use any of the following options:
    - Right click options in the Computers interface.
    - Advanced screen of the Computers interface. (Refer to the section **Viewing and Managing Group and Security Policy Details** for more details).
    - Using the Policy icon in the Computers interface.

6. Viewing and Managing Quarantined Items

CES/CAS/CAVM installations at the managed endpoints automatically move programs, executables and files identified as potential threats from real-time and on-demand scans to quarantine within the respective endpoint. The total number of items in quarantine in the network is displayed beside the 'Quarantined' shortcut link at the title bar of the CESM console interface and is updated each time an item is moved to quarantine in a managed endpoint.
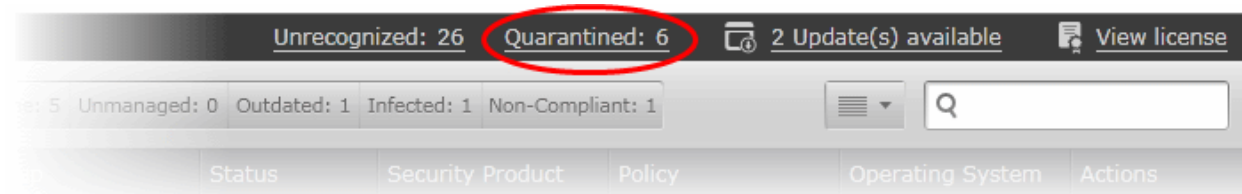
The administrator can view a consolidated list of all the items quarantined by all the CES/CAS/CAVM installations from the Quarantine area, can analyze the trustworthiness of the items and delete them permanently or restore them to their original location from this interface. If the item is a false positive, the administrator can add the file to the trusted files list of selected policy(ies).

Note: The administrator can view the list of items moved to quarantine on individual endpoints from the 'Endpoint Security' pane of the 'Computer Properties' interface. Refer to the section **Viewing and Managing Endpoint Security Software** for more details.

To open the 'Quarantine' area, choose 'Quarantine' from the drop-down at the top left

Tip: The Quarantine area can also be accessed by clicking the 'Quarantined' shortcut link from the title bar.
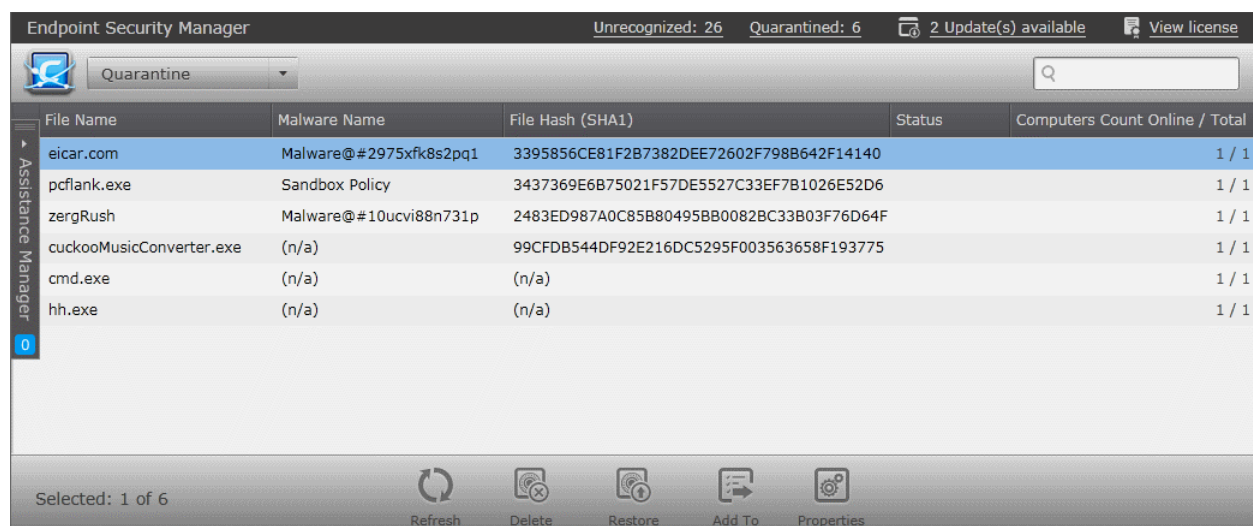
The 'Quarantine' Area - Table of Column Descriptions	
Column Heading	**Description**
File Name	Displays the name of the file of the quarantined item.
Malware Name	Displays the name of the malware contained in the quarantined file.
File Hash (SHA1)	Displays the hash value of the file moved to quarantine, derived using SHA1 hash algorithm.
Status	Indicates the current status of restore or removal actions currently executed on the item.
Computers Count Online/Total	The numerator indicates the number of currently online endpoint computers on which the item was quarantined and the denominator indicates the total number of endpoint computers on which the item was quarantined

Filter Options

The search field in the gray stripe allows the administrator to search for a specific malware or file by entering its name partially or fully.

Managing Quarantined Items

To view the details of a selected item, select the item and click 'Properties' or right click on the item and choose 'Properties' from the context sensitive menu.

The 'Quarantine Properties' interface will be displayed:

The interface contains two areas:

- **General** - Displays the general information on the quarantined item.
- **Computers** - Displays the list of endpoints up on which the item was identified and allows the administrator to restore or delete the item application from the selected endpoints.

General Properties Screen

The 'General Properties' screen can be displayed by clicking the 'General' tab from the left hand side navigation.
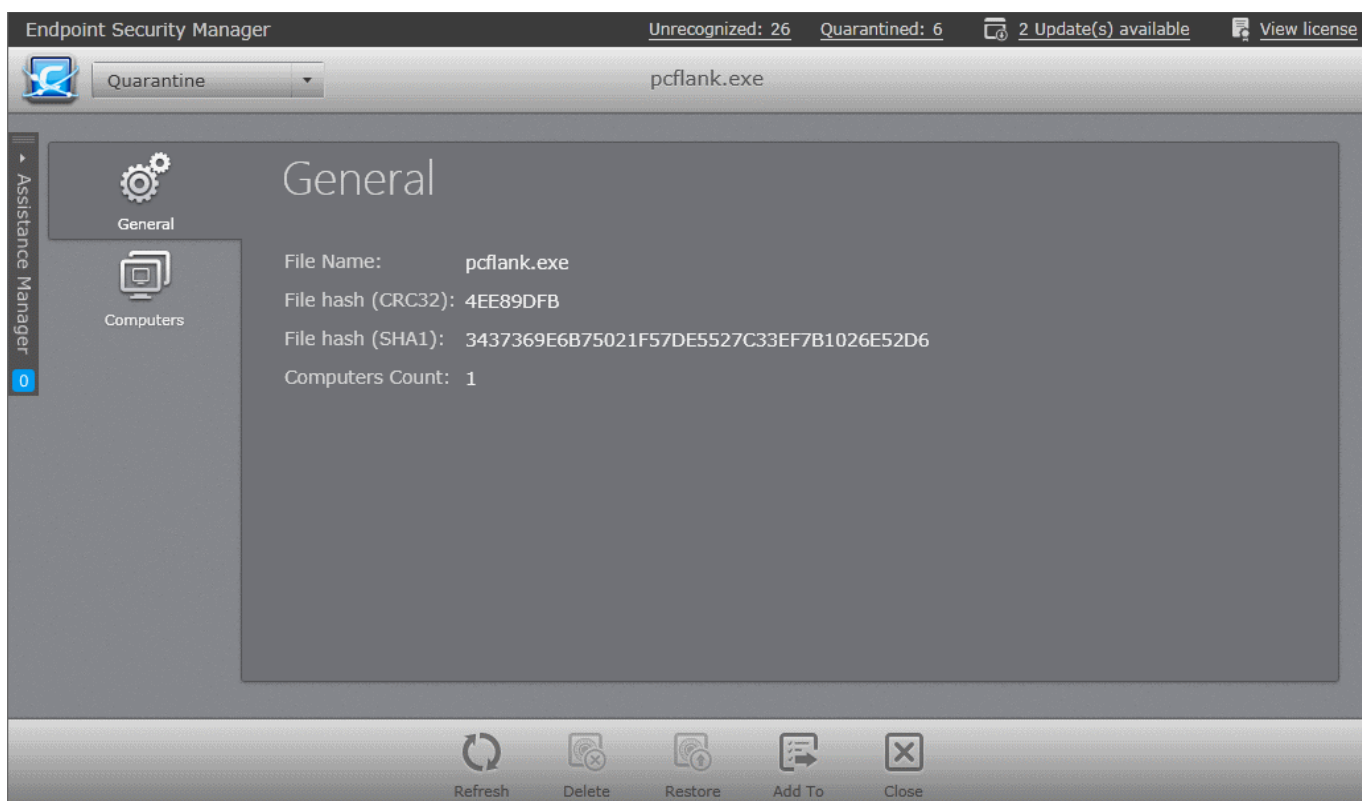
The General Properties screen displays the details on file name, file hash value and the total number of endpoints on which the item was identified.

Computers Screen

The 'Computers' screen can be opened by clicking the 'Computers' tab in the 'Quarantine Properties' interface.

The 'Computers' screen displays the list of endpoints on which the item was identified and allows the administrator to permanently remove the file from the selected endpoints if it is an unwanted one or restore the file, to its original location on the selected endpoint if it is trustworthy.

To remove the item from selected endpoints

1. Select the endpoints by selecting the checkboxes beside them
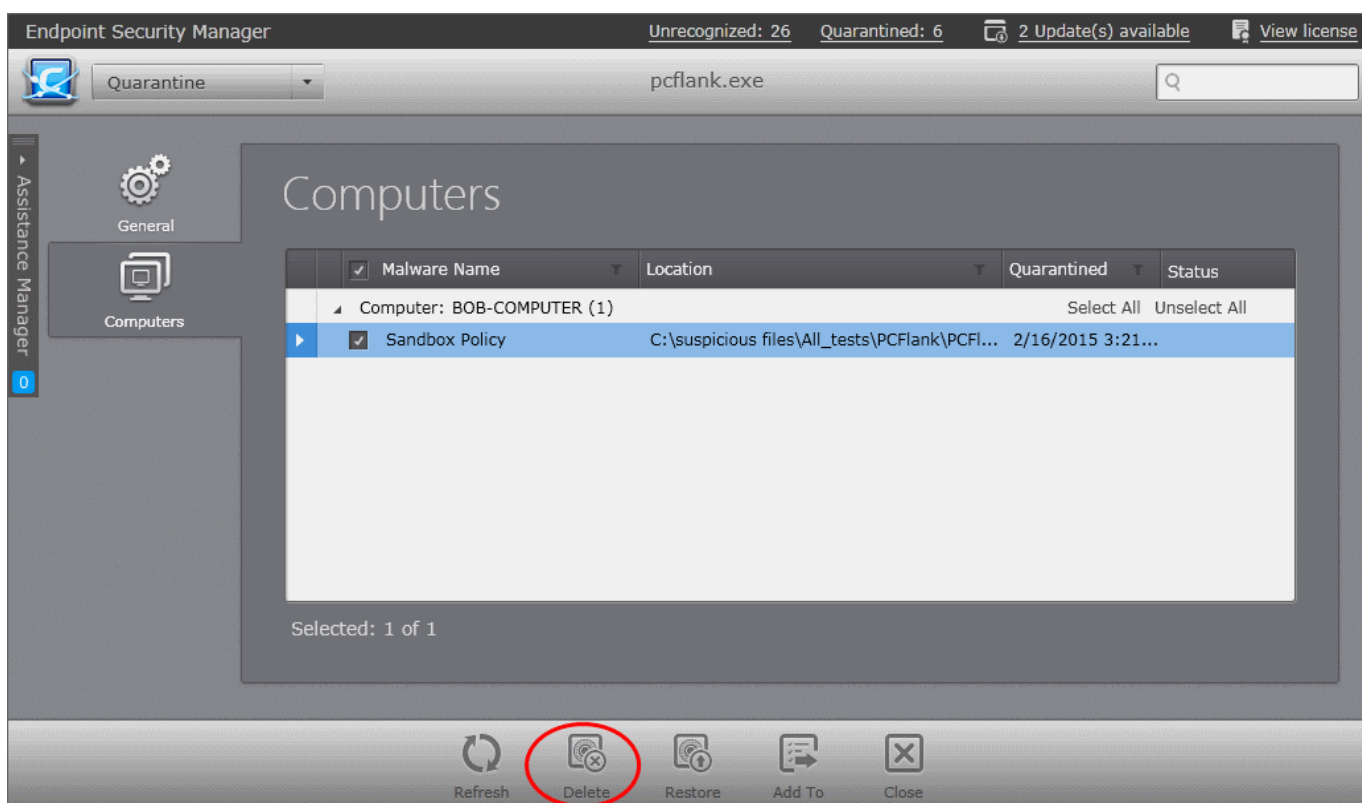
2. Click 'Delete'.

The file containing malware will be permanently removed from the selected endpoints immediately.

> **Tip**: To remove the item from all the endpoints simultaneously, you can select the item(s) by and clicking the checkbox beside Malware Name at the top or 'Select All' and click 'Delete' from the Quarantine interface.

To restore the item in selected endpoints

1. Select the endpoints by selecting the checkboxes beside them
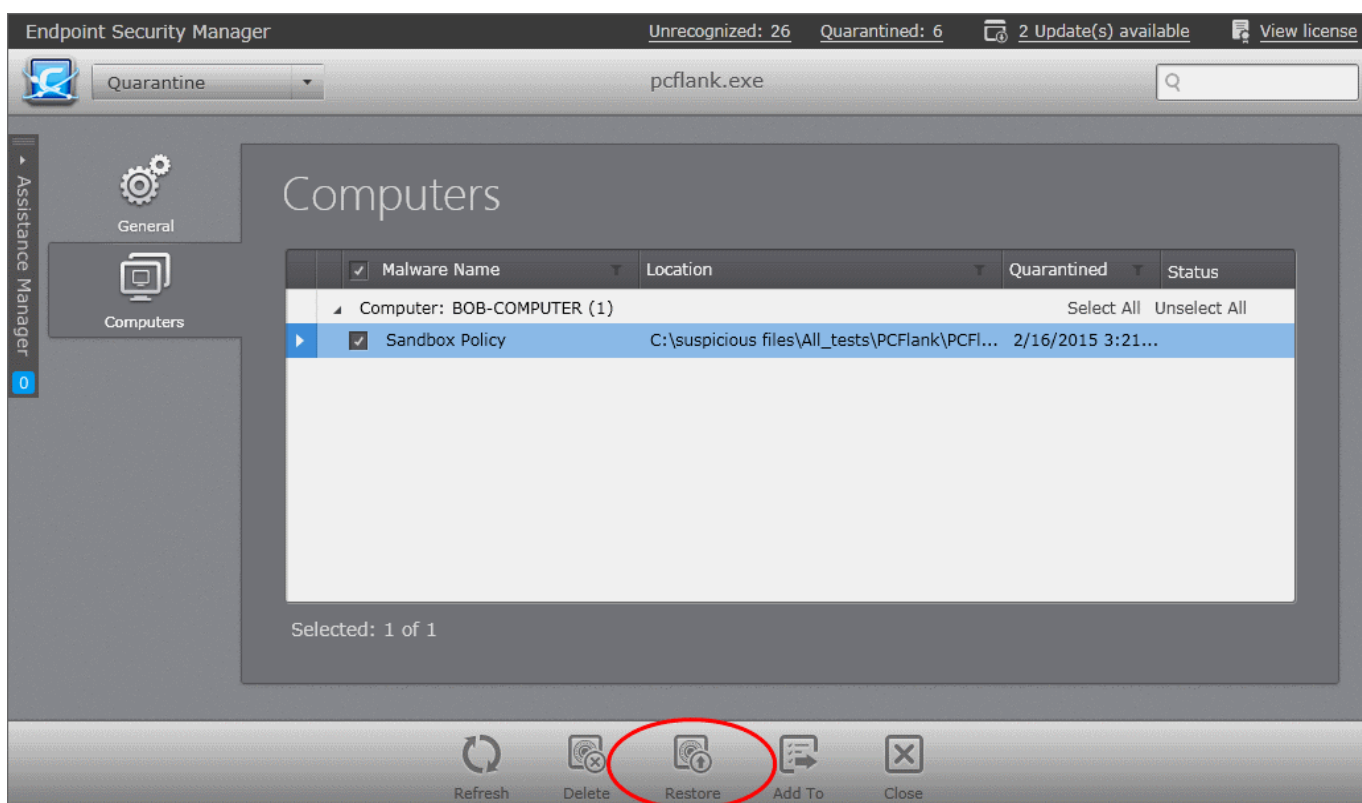
2. Click 'Restore'.

The file will be restored to its original location in the endpoint immediately.

> **Tip**: To restore the items to their original locations in all the endpoints simultaneously, you can select the item(s) by and clicking the checkbox beside Malware Name at the top or 'Select All' and click 'Restore' from the Quarantine interface.

Adding Quarantined Files to Trusted Files list or Blocked Files List

If a quarantined file is identified as trustworthy by the administrator, the file can be added with 'Trusted' status to the custom files list of selected policies or to the global 'Trusted Files' list. Files added as trusted will be skipped from real-time, on-demand and scheduled antivirus scans at the endpoints or endpoint groups for which the policy is applied, till the next AV database update.

> **Tip**: If a file is to be excluded from all types of AV scans in future, the administrator can add the file to the Exclusions list from **Policy Properties** > **Antivirus** > **Excluded paths** pane. Refer to the section **Exclusions** for more details.

On the other hand, if a quarantined file is identified as a malware, the administrator can move it to the global 'Blocked Files' list to block the file from being executed at any endpoint managed by CESM.

**To move a file to trusted files list or blocked files list**

•   Select the file(s) and click 'Add to'.

> **Tip**: You can select multiple files simultaneously by pressing and holding the 'Ctrl' or 'Shift' keys in the key board.

•   Alternatively, right click on the selected file and choose 'Add to'.
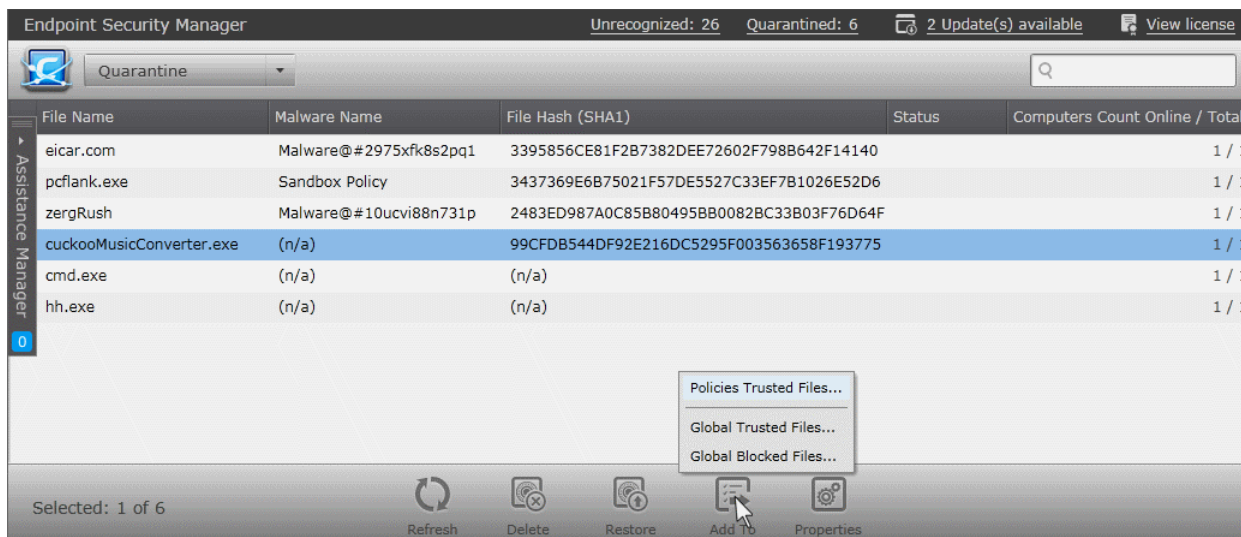
- To add the file(s) as Trusted to the custom files list of selected policies, choose 'Policies Trusted Files', select the policies and click 'Add'. For the changes to take effect immediately at the endpoints applied with the policy, select the 'Apply policy immediately' checkbox before clicking 'Add'.
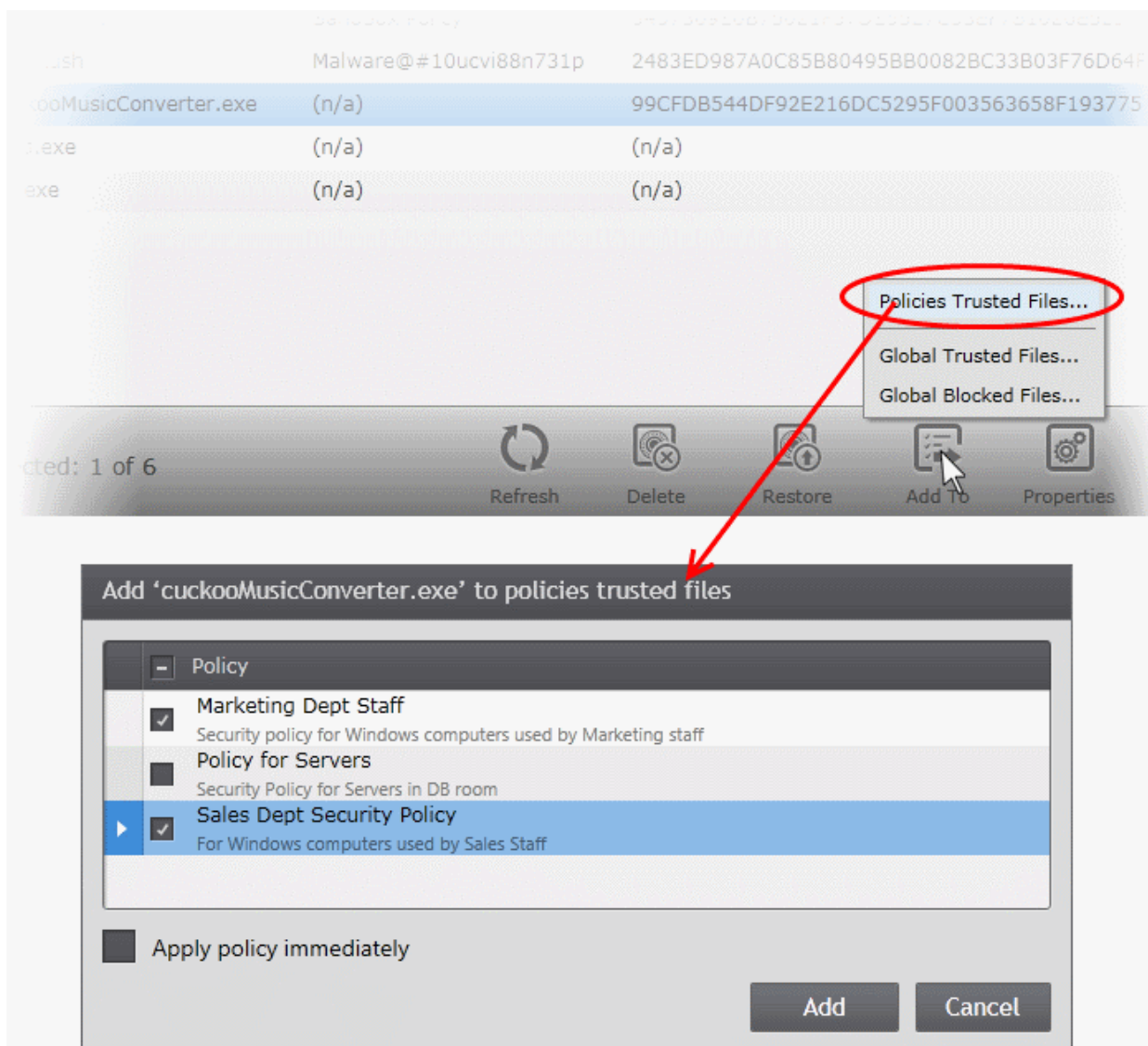
For more details on custom file list of a policy, refer to the description of **Rating Files** in the section **Configuring File Rating**

Settings.

- To add the file to the global 'Trusted Files' List, choose 'Global Trusted Files'. The file will be immediately added to the 'Trusted Files' list accessible through 'Files Management' > 'Trusted Files'. Refer to the section **Trusted Files** for more details.

- To add the file to the global 'Blocked Files' List, choose 'Global Blocked Files'. The file will be immediately added to the 'Blocked Files' list accessible through 'Files Management' > 'Blocked Files ' and will be blocked from running from any of the endpoints managed by CESM. Refer to the section **Blocked Files** for more details.

7.Viewing and Managing Sandboxed Applications

The Sandbox component of CES/CAS on each endpoint provides an isolated environment in which suspicious, unknown/unrecognized or unstable programs are run. Sandboxed applications are not permitted to access files or user data on the host machine.

The CES/CAS installations at each managed endpoint run selected applications at the endpoints inside the sandbox when:

- The application is auto-sandboxed based on the Sandbox rules defined in the Policy applied to the individual endpoint or the group to which the endpoint belongs. Refer to the description under **Sandbox Settings** in the section **Configuring Defense+ Settings** for more details on setting the Sandbox Rules for a policy.

- The application is auto-sandboxed based on the Sandbox rules configured at the CES/CAS installation at the endpoint

- The user at the endpoint runs a program inside the Sandbox on a 'one-off' basis. This is helpful to test the behavior of new executables that have they downloaded or for applications that they are not sure that you trust.

The total number of programs, executables and applications that are currently running inside sandbox at all the managed endpoints is displayed next to the on the 'Sandboxed' at the title bar and is updated each time a program is run inside the sandbox in a managed endpoint.
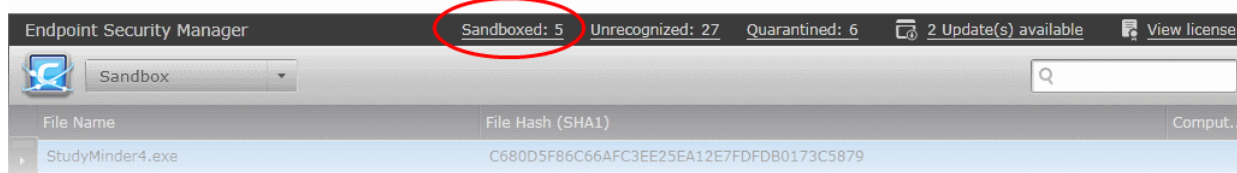
The administrator can view a consolidated list of all the programs currently running inside the sandbox at all the endpoints, irrespective of whether they are auto-sandboxed or manually run inside the sandbox from the 'Sandbox' area. The administrator can analyze the trustworthiness of the programs and can add them to the trusted files list of selected policy(ies), so that they will not be auto-sandboxed at the endpoints for which the policy is applied.

To open the 'Sandbox' area, choose 'Sandbox' from the drop-down at the top left

Tip: The 'Sandbox' area can also be accessed by clicking the 'Sandboxed' shortcut link in the title bar of the CESM console interface.
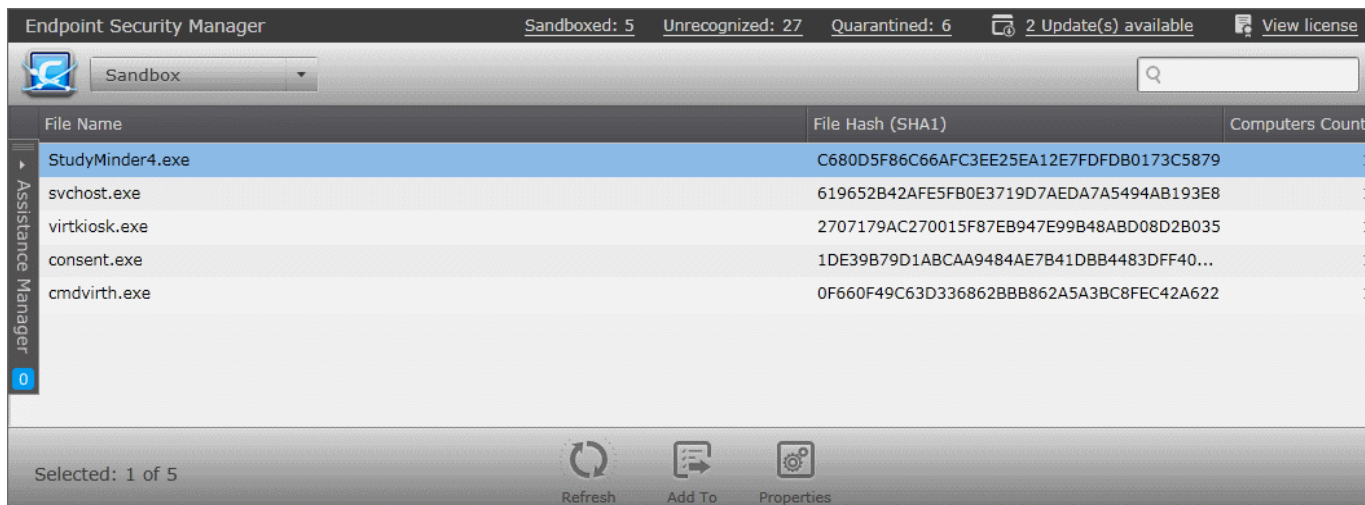
The 'Sandbox' Area - Table of Column Descriptions	
Column Heading	**Description**
File Name	Displays the name of the executable file run inside the sandbox.
File Hash (SHA1)	Displays the hash value of the file, derived using SHA1 hash algorithm.
Computers Count	Indicates the number of endpoint computers on which the program/executable/application is run inside the sandbox.

Filter Options

The search field in the gray stripe allows the administrator to search for a specific sandboxed application by entering its name partially or fully.

Managing Sandboxed Applications

To view the details of a selected sandboxed application, select the application and click 'Properties' or right click on the application and choose 'Properties' from the context sensitive menu.
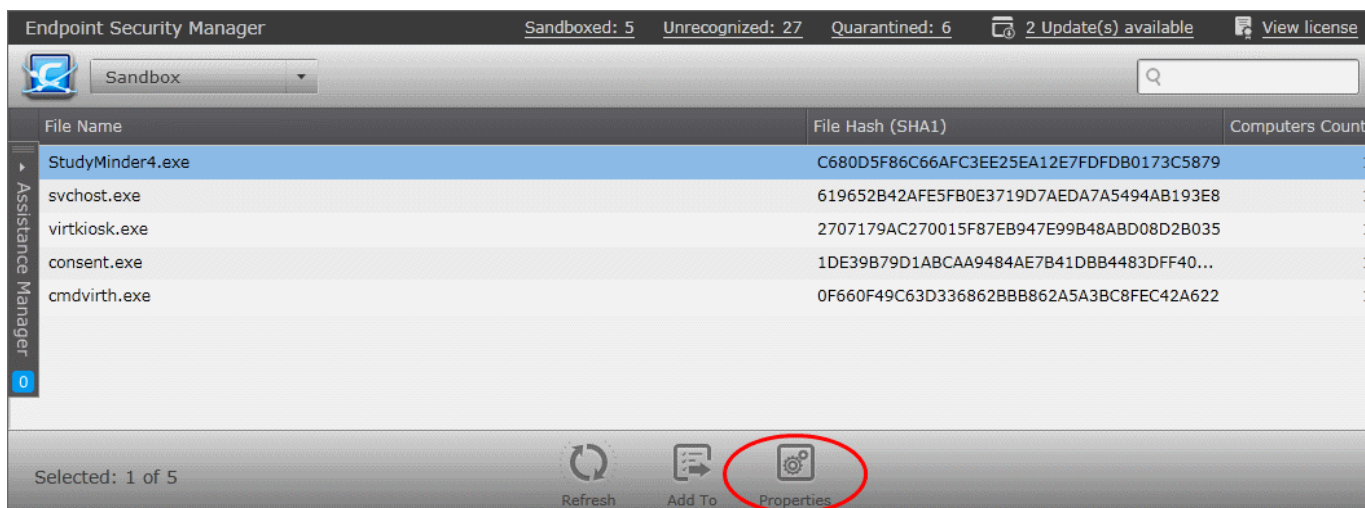
The Sandbox Application Properties interface will be displayed:
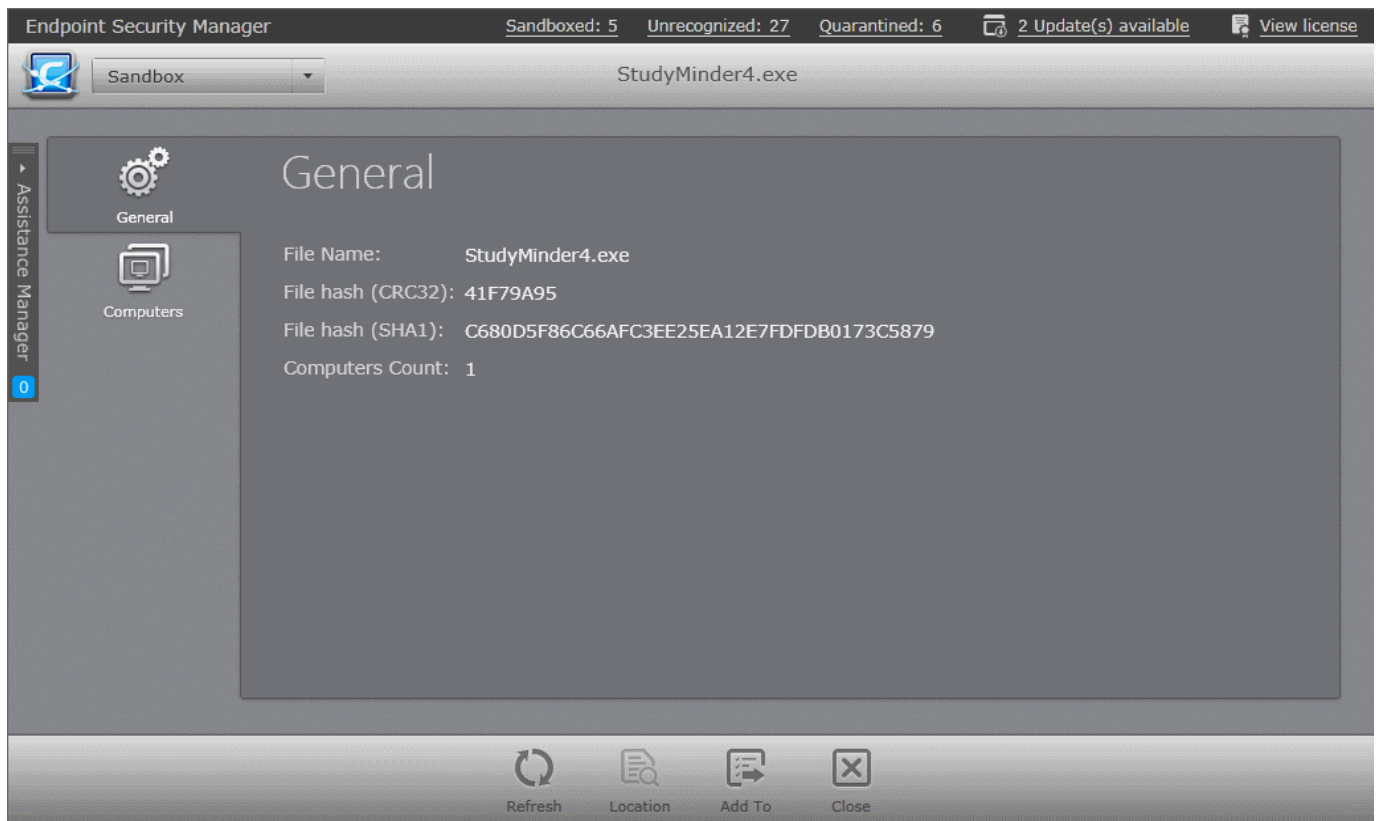
The interface contains two areas:

- **General** - Displays the general information on the sandboxed application.
- **Computers** - Displays the list of endpoints in which the application is running inside the sandbox and allows the administrator to view the location of the application in the selected endpoints.

General Properties Screen

The General Properties screen can be displayed by clicking the 'General' tab from the left hand side navigation.
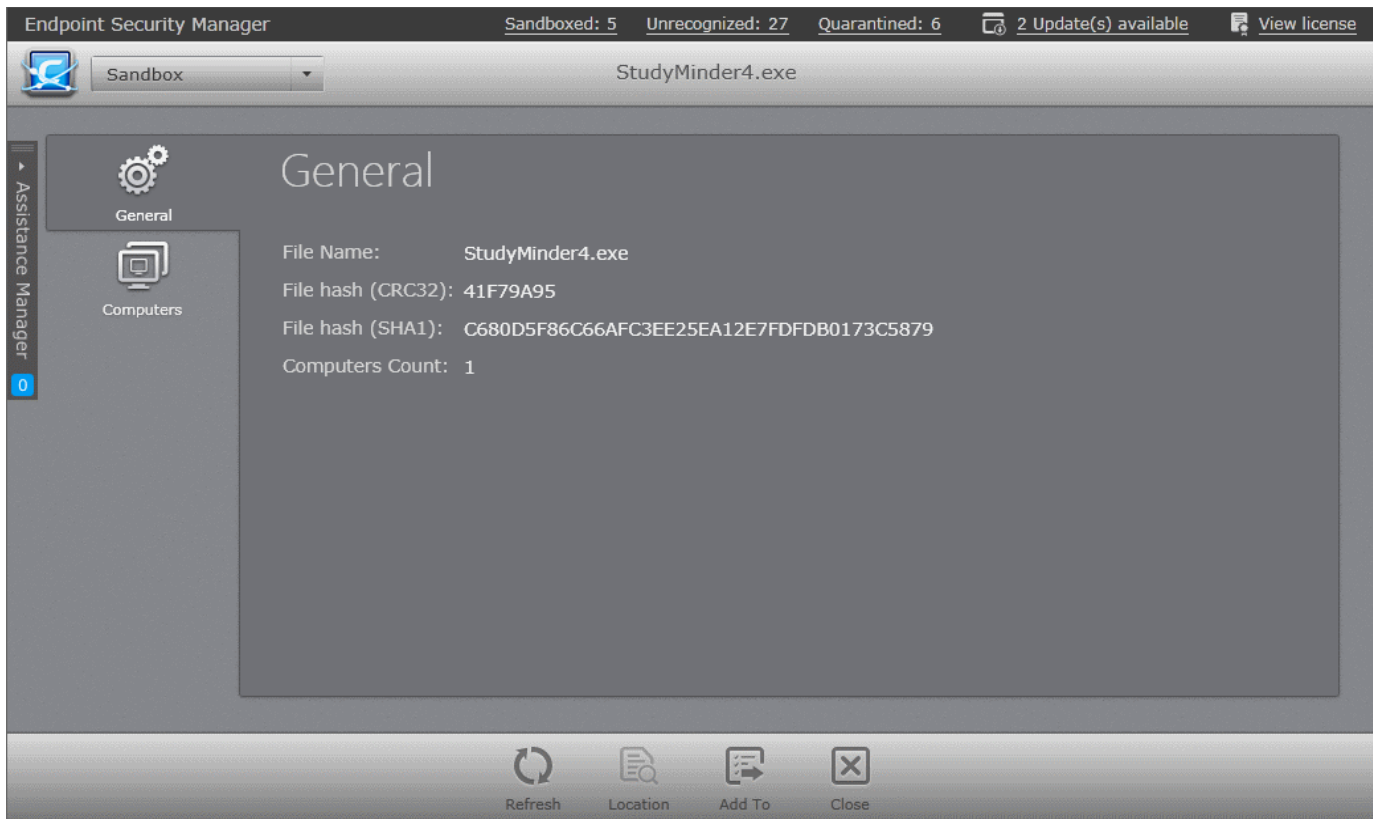
The General Properties screen displays the details on file name, file hash value and the total number of endpoints on which the application is running inside the sandbox.

Computers Screen

The 'Computers' screen can be opened by clicking the 'Computers' tab in the 'Sandbox Application Properties' interface.

The 'Computers' screen displays the list of endpoints on which the item was identified and allows the administrator to view the location of the application in the selected endpoints.
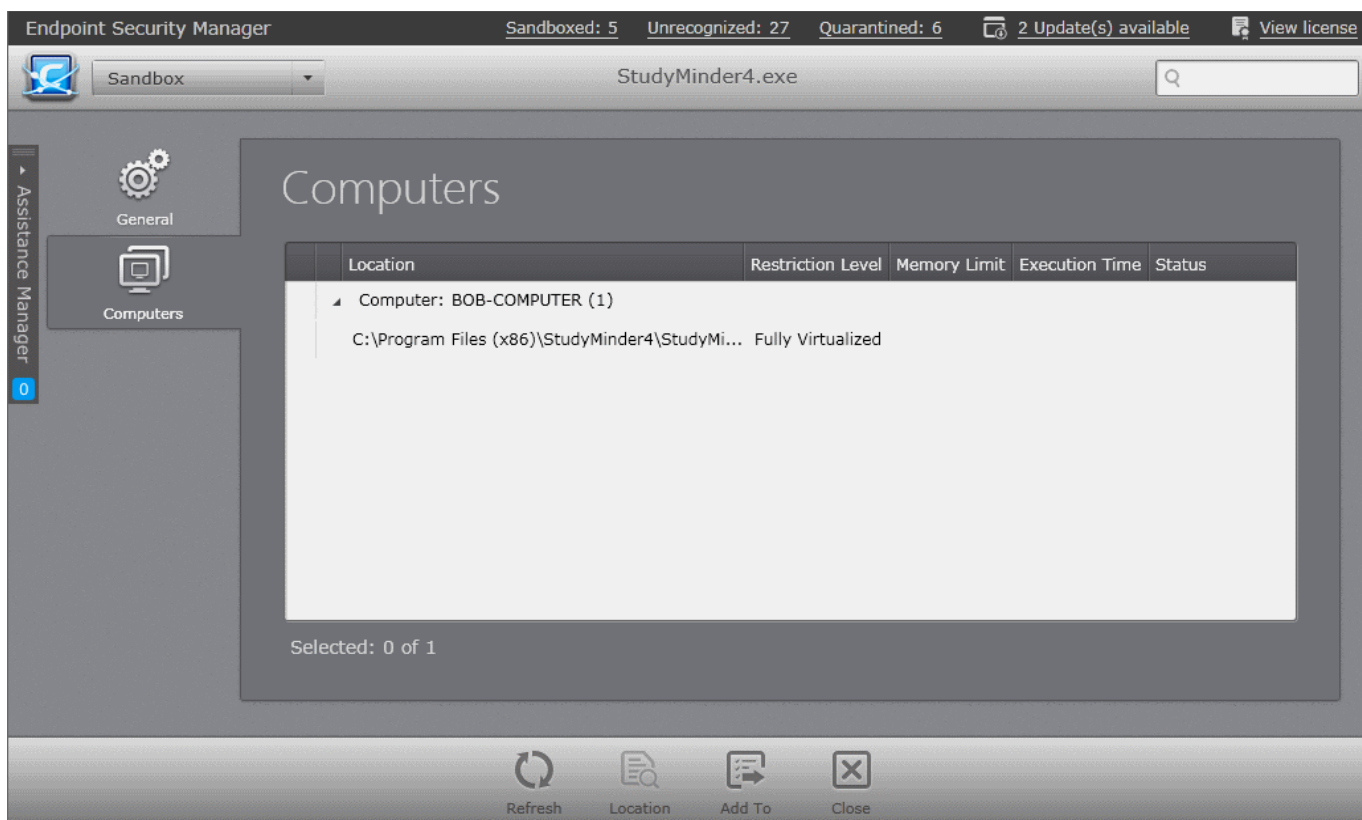
To view the location of the application

1. Select the endpoints. You can select multiple endpoints simultaneously by pressing and holding the 'Ctrl' or 'Shift' keys in the key board.

2. Click 'Location'.

The File System interface will open for the selected endpoint pointing the location from which the application is run. Refer to the section **Viewing and Managing Drives and Storage** for more details.

Adding Trustworthy applications to Trusted Files list or Blocked Files List

If a sandboxed application file is identified as trustworthy by the administrator, the executable can be added with 'Trusted' status to the custom files list of selected policies or to the global 'Trusted Files' list. Files added as trusted will not be auto-sandboxed at the endpoints to which the policy is applied. The executable file can also be added to the global Trusted Files list,so that the application will not be auto-sandboxed at any of the managed endpoints in the network.

On the other hand, if a sandboxed application is not trustworthy, the administrator can move it to the global 'Blocked Files' list to block the file from being executed at any endpoint managed by CESM.

 To move application(s) file to trusted files list or blocked files list

• Select the file(s) and click 'Add to'.

Tip: You can select multiple files simultaneously by pressing and holding the 'Ctrl' or 'Shift' keys in the key board.

• Alternatively, right click on the selected file and choose 'Add to'.
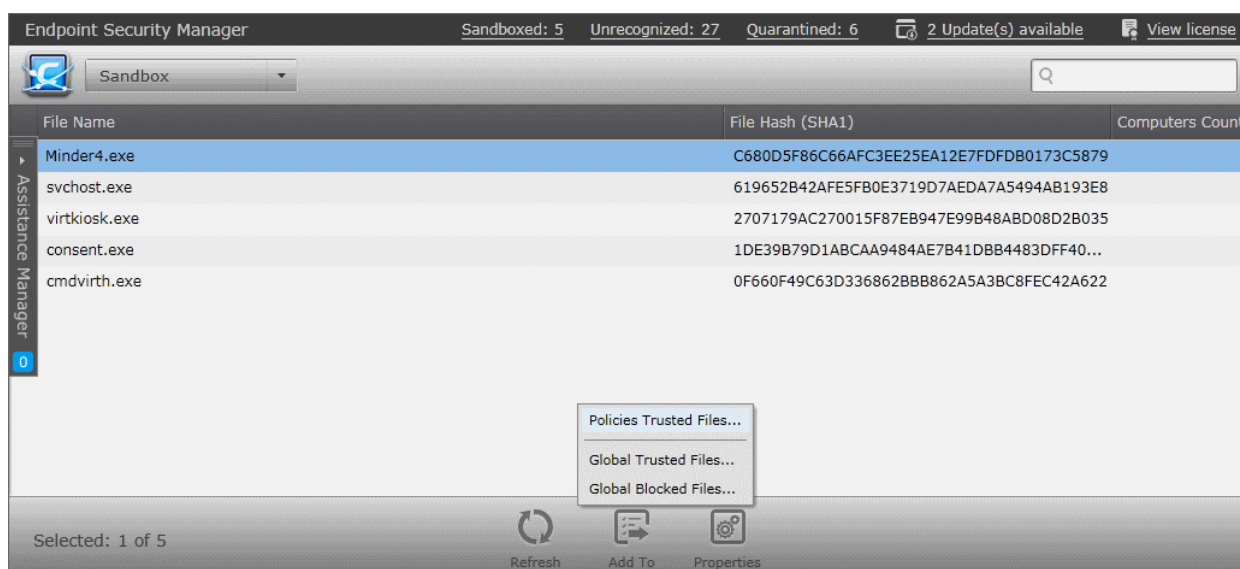
- To add the executable(s) as Trusted to the custom files list of selected policies, choose 'Policies Trusted Files', select the policies and click 'Add'. For the changes to take effect immediately at the endpoints applied with the policy, select the 'Apply policy immediately' checkbox before clicking 'Add'.
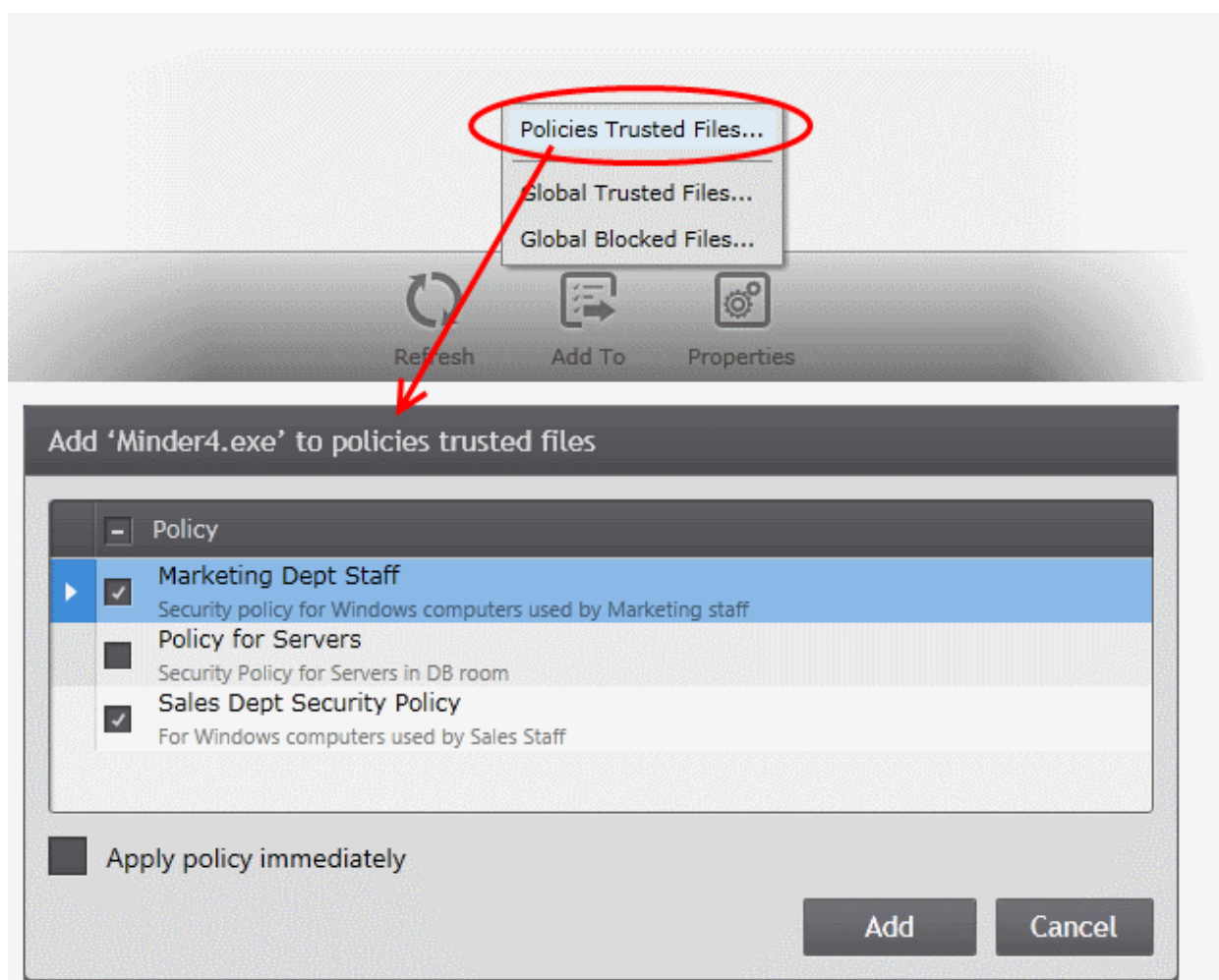
For more details on custom file list of a policy, refer to the description of **Rating Files** in the section **Configuring File Rating Settings**.

- To add the executable to the global 'Trusted Files' List, choose 'Global Trusted Files'. The executable file will be immediately added to the 'Trusted Files' list accessible through 'Files Management' > 'Trusted Files'. Refer to the section **Trusted Files** for more details.

- To add the executable to the global 'Blocked Files' List, choose 'Global Blocked Files'. The executable file will be immediately added to the 'Blocked Files' list accessible through 'Files Management' > 'Blocked Files ' and will be blocked from running from any of the endpoints managed by CESM. Refer to the section **Blocked Files** for more details.

8.Files Management

The HIPS component of CES/CAS installations at managed endpoints watches all file system activity on your computer. Every new executable file introduced to the computer, is first scanned against the Comodo certified safe files database. If they are not safe, they are rated as 'Unrecognized'. Apart from new executables, any executables that are modified are also rated as 'Unrecognized Files'.

The 'Unrecognized Files' is specifically important for Policies in which HIPS is set to 'Clean PC Mode'. In Clean PC Mode, the files in 'Unrecognized Files' are NOT considered clean. For more information, please refer to the description of '**Clean PC Mode**' in the section **Configuring Defense+ Settings**.

The 'Files Management' interface enables the administrator to view a consolidated list of all the items that are rated as 'Unrecognized' by all the CES/CAS installations at the endpoints. The administrator can analyze the trustworthiness of the items and move the files to global trusted files list or global blocked files list.

In addition, the administrator can manually add executable files to the global 'Unrecognized' Files list, 'Trusted Files' list and 'Blocked Files' depending on the nature of the files.

The files added to the 'Trusted Files' list are automatically given Defense+ trusted status and are allowed to run without generating any alert. File added to the 'Blocked' Files list are prohibited to run at all the endpoints.

To open the 'Files Management' interface, choose 'Files Management' from the drop-down at the top left.

The interface contains three tabs:

- **Unrecognized** - Displays the list of files reported as Unrecognized by the CES/CAS installations at the endpoints. The administrator can manually add files to the 'Unrecognized Files' list and move items to global 'Trusted Files' list or global 'Blocked Files' list, depending on the trustworthiness of the files from this interface. Refer to the section **Viewing and Managing Unrecognized Files** for more details.

- **Trusted Files** - Displays the global 'Trusted Files' list . The administrator can manually add files or move items to this list from Unrecognized Files list. Refer to the section **Viewing and Managing Trusted Files List** for more details.

- **Blocked Files** - Displays the global 'Blocked Files' list . The administrator can manually add files or move items to this list from Unrecognized Files list. Refer to the section **Viewing and Managing Blocked Files** List for more details.

8.1. Viewing and Managing Unrecognized Files

The total number of items in 'Unrecognized Files' list on all the managed endpoints is displayed next to the 'Unrecognized' in the title bar and is updated each time an item is discovered at an endpoint or manually added to the list.
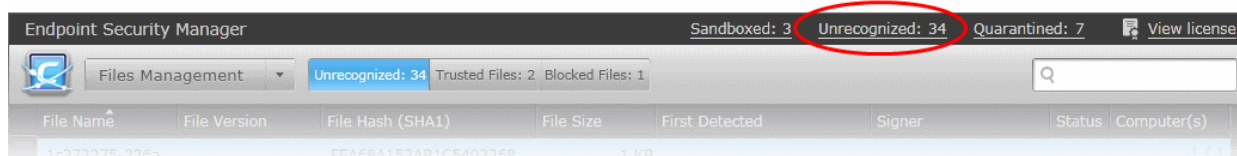
The 'Unrecognized Files' displays a consolidated list of unrecognized files reported by the CES/CAS installations at the endpoints.

- To open the 'Unrecognized Files' area, choose 'Files Management' from the drop-down at the top left and click the 'Unrecognized' tab.

Tip: The 'Unrecognized Files' area can also be accessed by clicking the 'Unrecognized' link at the title bar.

The 'Unrecognized Files' List - Table of Column Descriptions	
Column Heading	**Description**
File Name	Displays the name of the file of the 'Unrecognized' item.

File Version	Displays the version number of the executable file
File Hash (SHA 1)	Displays the hash value of the file derived using SHA1 hash algorithm.
File Size	The size of the unrecognized file in bytes.
First Detected	Precise date and time at which the item was discovered at an endpoint.
Signer	The vendor that has signed the code of the executable.
Status	Indicates whether the executable was blocked or allowed.
Computers Count Online/Total	The numerator indicates the number of currently online endpoint computers on which the item was accessed and the denominator indicates the total number of endpoint computers on which the item was identified.

Filter Options

The search field in the gray stripe allows the administrator to search for a specific item or file by entering its name in part or full.
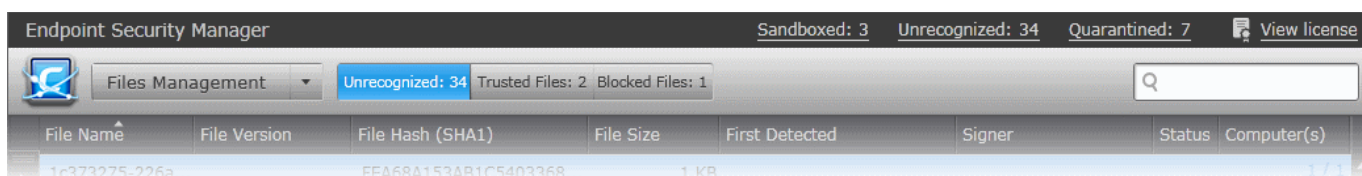
Managing Unrecognized Items

The Unrecognized Files interface allow you to:

- **View the details of files in the list**
- **Manually add files to the list**
- **Move selected files to global 'Trusted Files' or 'Blocked Files' list**
- **Removing files from the list and deleting files from the endpoints**

View the details of files in the list

- To view the properties of a file, select the item and click 'Properties', right click on the item and choose 'Properties' from the context sensitive menu or simply double click on the item.

The Properties interface for the selected item will be displayed: The interface contains two areas:

- **General** - Displays the general information on the selected item.
- **Details** - Displays the list of endpoints up on which the item was identified with its current activities at each endpoint.

General Properties Screen

The General Properties screen is displayed by default. To return to the 'General Properties' screen from Details screen, click the 'General' tab from the left hand side navigation.

The General Properties screen displays the details on file name, version, size, file hash values, the dates at which the item was first identified, last accessed and last modified and the digital signature details of the file.

Details Screen

The 'Details' screen can be opened by clicking the 'Details' tab in the 'Properties' interface.

The 'Details' screen displays the list of endpoints on which the item was identified and its activities at each endpoint. The administrator can view the processes executed by the file at each endpoint with the details on data handled by each process. The administrator can also view the location in the endpoint file system, from which the process is executed.

The list at the left hand side displays the computers at which the item was discovered. The table at the right hand side displays the processes executed by the file in the endpoint selected from the list as a tree structure. The process tree can be expanded by clicking the right arrow ▷ beside the process name in the table.

The 'Application Activities' - Table of Column Descriptions	
Column Heading	**Description**
Activity	Displays the name of the process executed by the application
PID	Displays the process identifier of the process
Data	Displays the file modified by the process

To identify the location from which the processes is executed select the process and click 'Location'.
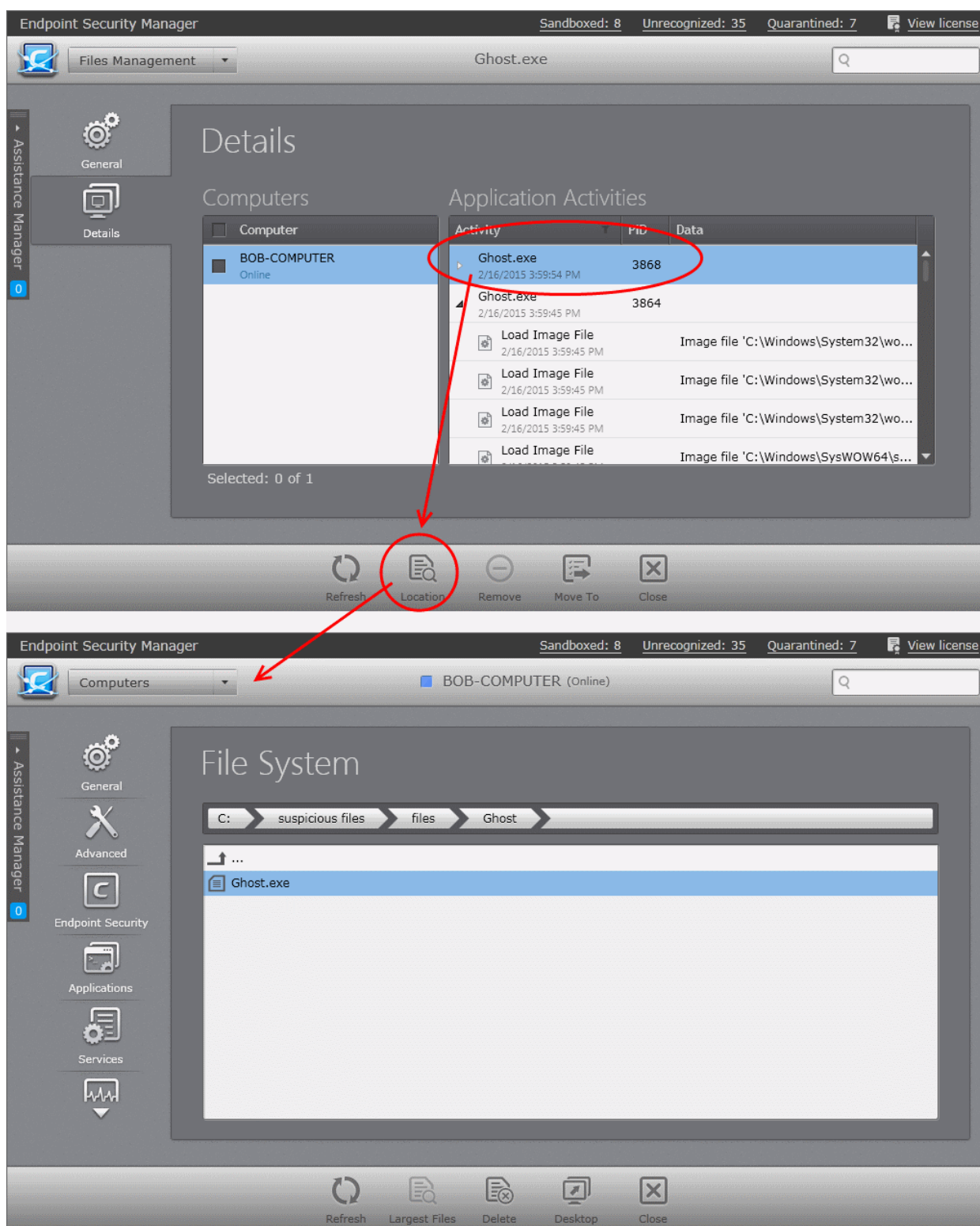
The **File System** interface of the endpoint will open with the location of the process highlighted.

Adding Files to the Unrecognized Files list

In addition to the files added to the 'Unrecognized Files' list by the CES/CAS installations at the endpoints, administrators can manually add files to the list. The files will be assigned the 'Unrecognized' rating and applied to all the policies and will be monitored and controlled at the endpoints with the restrictions as per the Defense+ settings of the respective policy.

Files can be added from the computer from which the console is accessed or from ant endpoint connected to CESM.

- To add a file from the computer from which the console is accessed, click 'Add' and choose 'Local File' or right click

inside the list and choose 'Add Local File' from the options.

- Navigate to the location of the file to be added, choose the file and click 'Open'.

- To add a file from an endpoint click 'Add', choose 'Remote File' from the options or or right click inside the list and choose 'Add Remote File' from the options.

  The list of endpoints will be displayed.

  - Double click on the endpoint, navigate to the file path and select the file.

Note: The Endpoint needs to be online for navigation through the file path in it.

- Click 'Add File'.

Moving Selected Files to Global 'Unrecognized Files' or 'Blocked Files' list

If an unrecognized item is identified as trustworthy by the administrator, the file can be added to the global 'Trusted Files' list, so that it is applied to all the policies. Files added to trusted file list will be skipped from real-time, on-demand and scheduled antivirus scans at the endpoints, till the next AV database update.

Tip: If a file is to be excluded from all types of AV scans in future, the administrator can add the file to the Exclusions list from **Policy Properties** > **Antivirus** > **Excluded paths** pane. Refer to the section **Exclusions** for more details.

If an unrecognized item is identified as a malware by the administrator, the file can be added to the global 'Blocked Files' list, so

that it is applied to all the policies. Files added to blocked files list will not be allowed to run at the endpoints.

- To move an item to the global 'Trusted Files' list, select the item, click 'Move to' and choose Trusted Files' or right click the item and choose 'Move to Trusted Files'. The file will be added to **Trusted Files** list.
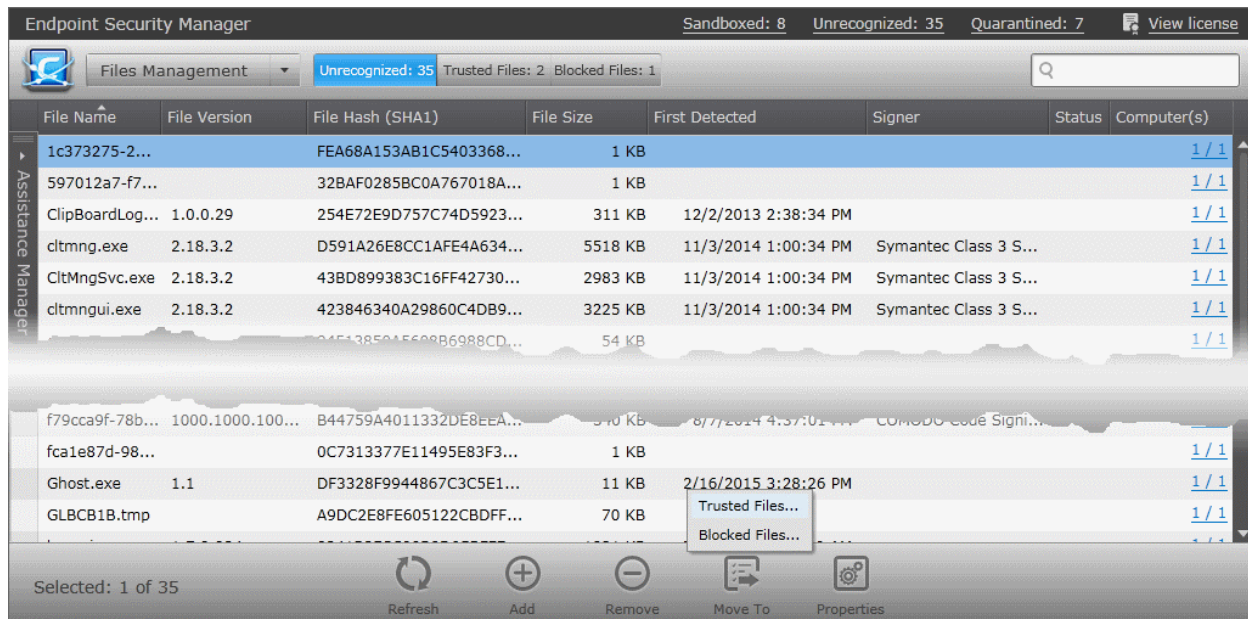
- To move an item to the global 'Blocked Files' list, select the item, click 'Move to' and choose 'Blocked Files' or right click the item and choose 'Move to Blocked Files'. The file will be added to '**Blocked Files**' list.

Removing files from the list and deleting files from the endpoints

If an unrecognized item is identified as a false-positive, the administrator can remove it from the 'Unrecognized Files' list. The item will only be removed from the list and not removed from the endpoint. If an unrecognized item is identified as a malware, the administrator can remove it from all the endpoints at once.

- To remove or delete an item. select the item from the list and click 'Remove' or right click on the item and choose 'Remove'.

The 'Remove Unrecognized File' dialog will appear.
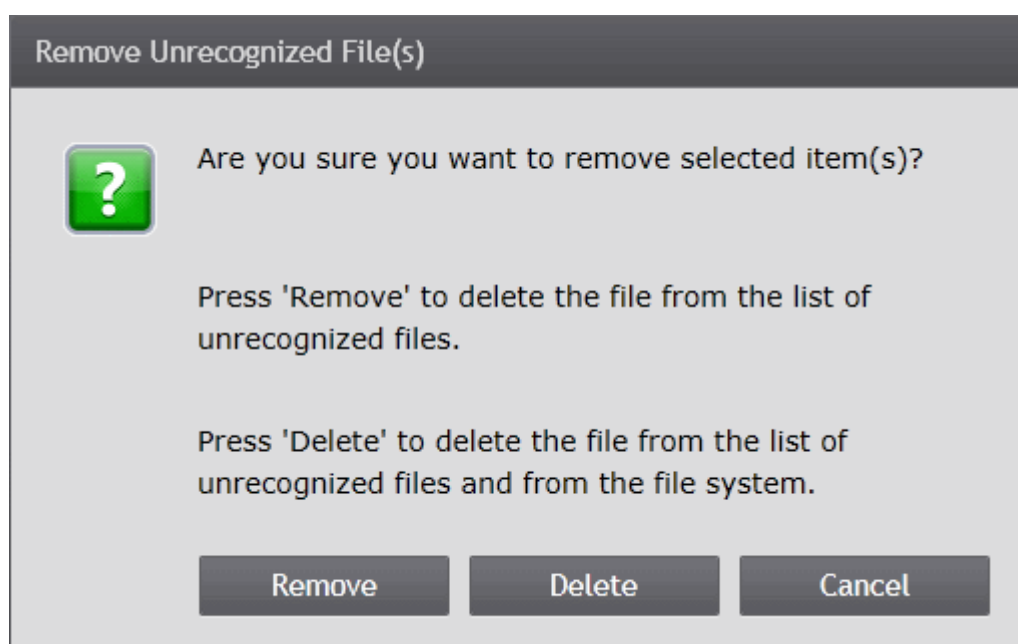
- To remove a false-positive item from the 'Unrecognized Files' list, click 'Remove'. The file will be removed from the list.

- To remove an item from all the endpoints, click 'Delete'. The file will be removed from the list and will be deleted from the local drives of all the endpoints at which it was discovered

8.2. Viewing and Managing Trusted Files List

Files added to the Trusted Files list are automatically given Defense+ trusted status. By adding trustworthy files to the global 'Trusted Files' list, the administrator can define a personal safe list of files to complement the default Comodo safe list. The files added to this list are assigned 'Trusted' rating and applied to all the policies.

By adding executables to this list (including sub folders containing many components) you can reduce the amount of alerts that HIPS generates whilst maintaining a higher level of Defense+ security at the endpoints. This is particularly useful for developers that are creating new applications that, by their nature, are as yet unknown to the Comodo safe list.

The 'Trusted Files' tab in the 'Files Management' interface allows the administrator to add files to and manage the global 'Trusted Files' list.

- To open the 'Trusted Files' area, choose 'Files Management' from the drop-down at the top left and click the 'Trusted Files' tab.

The 'Trusted Files' List - Table of Column Descriptions	
Column Heading	**Description**
File Name	Displays the name of the file of the 'Unrecognized' item.
File Version	Displays the version number of the executable file
File Hash (SHA 1)	Displays the hash value of the file derived using SHA1 hash algorithm.
File Size	The size of the unrecognized file in bytes.
First Detected	Precise date and time at which the item was discovered at an endpoint.
Signer	The vendor that has signed the code of the executable.

Filter Options

The search field in the gray stripe allows the administrator to search for a specific item or file by entering its name in part or full.

Managing Trusted Files List

The 'Trusted Files' interface allow you to:

- **View the details of files in the list**

- **Manually add files to the list**

- **Move selected files to 'Unrecognized Files' list or global 'Blocked Files' list**

- **Removing files from the list**

View the details of files in the list

- To view the properties of a file, select the item and click 'Properties', right click on the item and choose 'Properties' from the context sensitive menu or simply double click on the item.

The Properties interface for the selected item will be displayed: The interface contains two areas:

- **General** - Displays the general information on the selected item.

- **Details** - Displays the list of endpoints up on which the item was identified with its current activities at each endpoint.

General Properties Screen

The General Properties screen is displayed by default. To return to the 'General Properties' screen from Details screen, click the 'General' tab from the left hand side navigation.

The General Properties screen displays the details on file name, version, size, file hash values, the dates at which the item was first identified, last accessed and last modified and the digital signature details of the file.

Details Screen

The 'Details' screen can be opened by clicking the 'Details' tab in the 'Properties' interface.

The 'Details' screen displays the list of endpoints on which the item was identified and its activities at each endpoint. The administrator can view the processes executed by the file at each endpoint with the details on data handled by each process. The administrator can also view the location in the endpoint file system, from which the process is executed.

The list at the left hand side displays the computers at which the item was discovered. The table at the right hand side displays the processes executed by the file in the endpoint selected from the list as a tree structure. The process tree can be expanded by clicking the right arrow ▷ beside the process name in the table.

The 'Application Activities' - Table of Column Descriptions	
Column Heading	**Description**
Activity	Displays the name of the process executed by the application
PID	Displays the process identifier of the process
Data	Displays the file modified by the process

Adding Files to Trusted Files list

The files added to the 'Trusted Files' list will be assigned the 'Trusted' rating and applied to all the policies. Administrators can add items to the Trusted Files list in two ways:

1. Move files from Unrecognized File list and Blocked Files list. Refer to the explanation under **Moving Selected Files to Global 'Trusted Files' or 'Blocked Files' list** in the section **Viewing and Managing Unrecognized Files List** for more details.

2. Manually add files from the computer from which the console is accessed or from ant endpoint connected to CESM.

-   To add a file from the computer from which the console is accessed, click 'Add' and choose 'Local File' or right click inside the list and choose 'Add Local File' from the options.

    -   Navigate to the location of the file to be added, choose the file and click 'Open'.

- To add a file from an endpoint click 'Add', choose 'Remote File' from the options or right click inside the list and choose 'Add Remote File' from the options.

  The list of endpoints will be displayed.

  - Double click on the endpoint, navigate to the file path and select the file.

Note: The Endpoint needs to be online for navigation through the file path in it.

- Click 'Add File'.

Moving Selected Files to 'Unrecognized Files' List or Global 'Blocked Files' list

Items that are added to the 'Trusted Files' list by mistake can be moved to 'Unrecognized Files' list or global 'Blocked Files' list.

- To move an item to the 'Unrecognized Files' list, select the item, click 'Move to' and choose 'Unrecognized Files' or right click the item and choose 'Move to Unrecognized Files'.
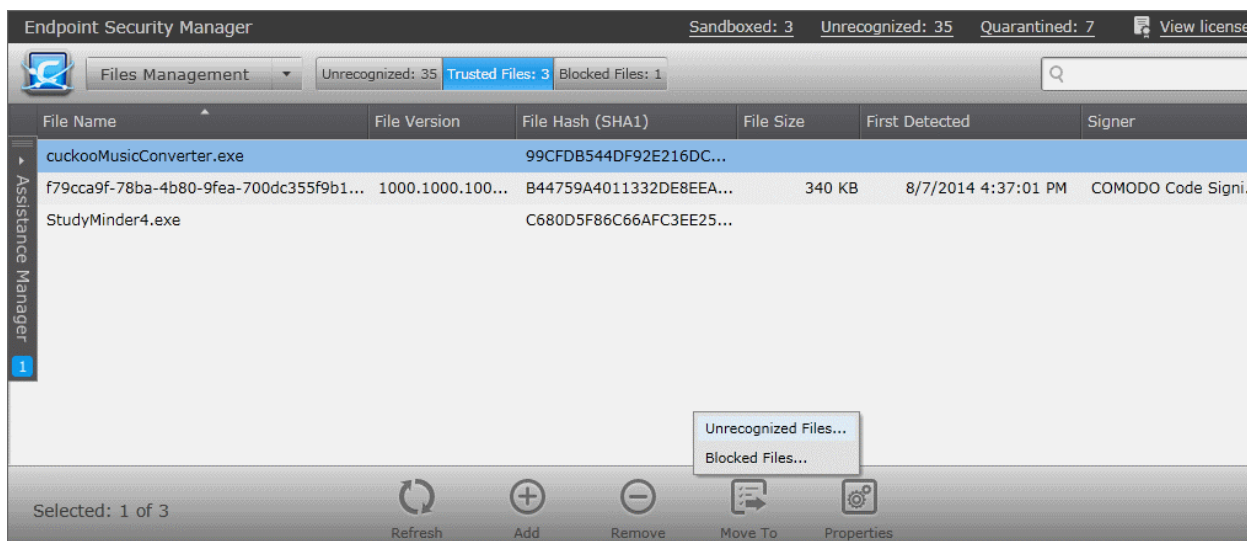
- To move an item to the global 'Blocked Files' list, select the item, click 'Move to' and choose 'Blocked Files' or right

click the item and choose 'Move to Blocked Files'. The file will be added to '**Blocked Files**' list.

Removing files from the Trusted Files list

If an item in the 'Trusted Files' list is identified not as trustworthy, the administrator can remove it from the list.

- To remove or delete an item. select the item from the list and click 'Remove' or right click on the item and choose 'Remove'.
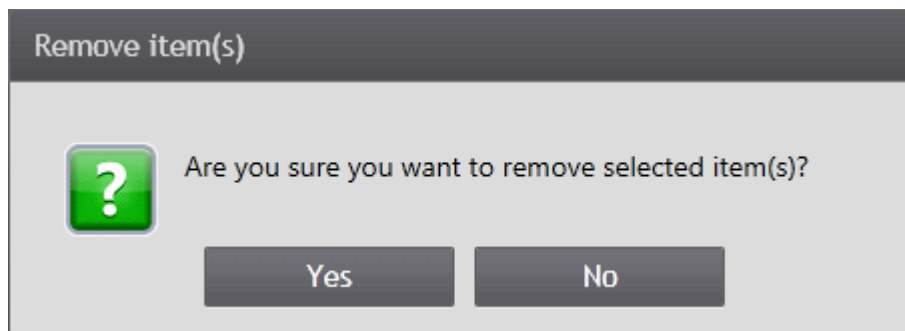
- Click 'Yes' in the confirmation dialog for removing the item from the list.

The file will only be removed from the list and not deleted from the endpoints at which it was discovered.

8.3. Viewing and Managing Blocked Files List

Files added to the global 'Blocked Files' list are automatically given 'Blocked' ranking and applied to all policies. These files will not be allowed to run at any of the endpoints managed by CESM.

The 'Blocked Files' tab in the 'Files Management' interface allows the administrator to add files to and manage the global 'Blocked Files' list.

- To open the 'Blocked Files' area, choose 'Files Management' from the drop-down at the top left and click the 'Blocked Files' tab.

The 'Blocked Files' List - Table of Column Descriptions	
Column Heading	**Description**
File Name	Displays the name of the file of the 'Unrecognized' item.
File Version	Displays the version number of the executable file

File Hash (SHA 1)	Displays the hash value of the file derived using SHA1 hash algorithm.
File Size	The size of the unrecognized file in bytes.
First Detected	Precise date and time at which the item was discovered at an endpoint.
Signer	The vendor that has signed the code of the executable.

Filter Options

The search field in the gray stripe allows the administrator to search for a specific item or file by entering its name in part or full.

Managing Blocked Files List

The 'Blocked Files' interface allow you to:

- **View the details of files in the list**
- **Manually add files to the list**
- **Move selected files to 'Unrecognized Files' list or global 'Trusted Files' list**
- **Removing files from the list**

View the details of files in the list

- To view the properties of a file, select the item and click 'Properties', right click on the item and choose 'Properties' from the context sensitive menu or simply double click on the item.

The Properties interface for the selected item will be displayed: The interface contains two areas:

- **General** - Displays the general information on the selected item.
- **Details** - Displays the list of endpoints up on which the item was identified with its current activities at each endpoint.

General Properties Screen

The General Properties screen is displayed by default. To return to the 'General Properties' screen from Details screen, click the 'General' tab from the left hand side navigation.

The General Properties screen displays the details on file name, version, size, file hash values, the dates at which the item was first identified, last accessed and last modified and the digital signature details of the file.

Details Screen

The 'Details' screen can be opened by clicking the 'Details' tab in the 'Properties' interface.

The 'Details' screen displays the list of endpoints on which the item was identified and its activities at each endpoint. The administrator can view the processes executed by the file at each endpoint with the details on data handled by each process. The administrator can also view the location in the endpoint file system, from which the process is executed.

The list at the left hand side displays the computers at which the item was discovered. The table at the right hand side displays the processes executed by the file in the endpoint selected from the list as a tree structure. The process tree can be expanded by clicking the right arrow ▷ beside the process name in the table.

The 'Application Activities' - Table of Column Descriptions	
Column Heading	**Description**
Activity	Displays the name of the process executed by the application
PID	Displays the process identifier of the process
Data	Displays the file modified by the process

Adding Files to Blocked Files list

The files added to the 'Blocked Files' list will be assigned the 'Blocked' rating and applied to all the policies and are prohibited from execution at all the managed endpoints. Administrators can add items to the Trusted Files list in two ways:

1. Move files from Unrecognized File list and Trusted Files list. Refer to the explanation under **Moving Selected Files to Global 'Trusted Files' or 'Blocked Files' list** in the section **Viewing and Managing Unrecognized Files List** for more details.

2. Manually add files from the computer from which the console is accessed or from ant endpoint connected to CESM.

• To add a file from the computer from which the console is accessed, click 'Add' and choose 'Local File' or right click inside the list and choose 'Add Local File' from the options.

• Navigate to the location of the file to be added, choose the file and click 'Open'.

- To add a file from an endpoint click 'Add', choose 'Remote File' from the options or right click inside the list and choose 'Add Remote File' from the options.

  The list of endpoints will be displayed.

  - Double click on the endpoint, navigate to the file path and select the file.

Note: The Endpoint needs to be online for navigation through the file path in it.

- Click 'Add File'.

Moving Selected Files to 'Unrecognized Files' List or Global 'Trusted Files' list

Items that are added to the 'Blocked Files' list by mistake or found trustworthy can be moved to 'Unrecognized Files' list or global 'Trusted Files' list.

- To move an item to the 'Unrecognized Files' list, select the item, click 'Move to' and choose 'Unrecognized Files' or right click the item and choose 'Move to Unrecognized Files'.
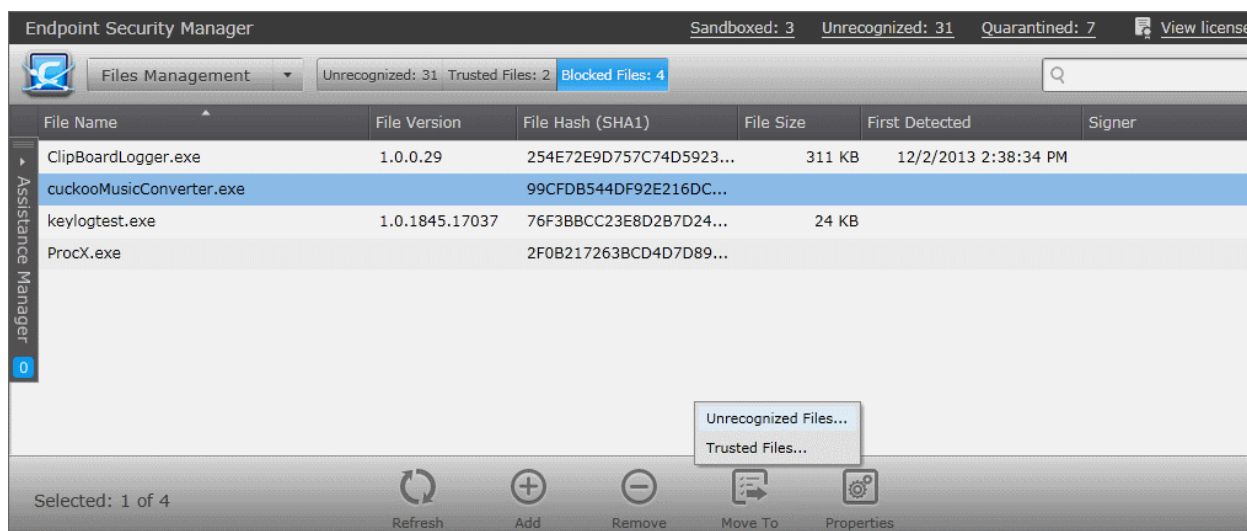
- To move an item to the global 'Trusted Files' list, select the item, click 'Move to' and choose 'Trusted Files' or right click the item and choose 'Move to Trusted Files'. The file will be added to '**Trusted Files**' list.

Removing files from the Blocked Files list

If an item in the 'Blocked Files' list is identified not a malware or need not be blocked any more, the administrator can remove it from the list.

- To remove or delete an item. select the item from the list and click 'Remove' or right click on the item and choose 'Remove'.
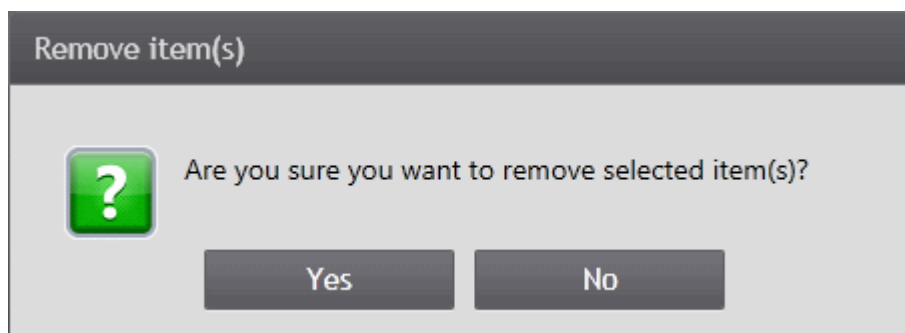
- Click 'Yes' in the confirmation dialog for removing the item from the list.

The file will only be removed from the list and not deleted from the endpoints at which it was discovered.

9.Viewing and Managing Installed Applications

CESM enables the administrator to have a great control over the applications installed on the endpoints. The administrator can view the list of applications and programs installed on all the endpoints running on different Operating Systems, with their version numbers and publisher details. If found suspicious, resource consuming or unnecessary, the administrator can uninstall

---

the application(s) from the selected endpoints.

The 'Applications' area displays the list of applications installed in all the endpoints connected to CESM.

To open the 'Applications' area, choose 'Applications' from the drop-down at the top left.

The Applications Area - Table of Column Descriptions	
Column Heading	**Description**
Application	Displays the name of the application.
Version	Displays the version number of the application.
OS Type	Displays the Operating System of the endpoint(s) on which the application is installed.
Publisher	Indicates the software vendor that has distributed the application.
Computers Count	Indicates the number of endpoint computers on which the application was detected.

Filter Options

The filter options in the gray stripe, gives at-a-glance statistics of the number of applications identified from computers running on different Operating Systems and allow the administrator to filter the computers based on the criteria.

The search field in the right allows the administrator to search for a specific application by entering its name partially or fully.

Managing Applications

To view the details of a selected application, select the application and click 'Properties' or right click on the application and choose 'Properties' from the context sensitive menu.
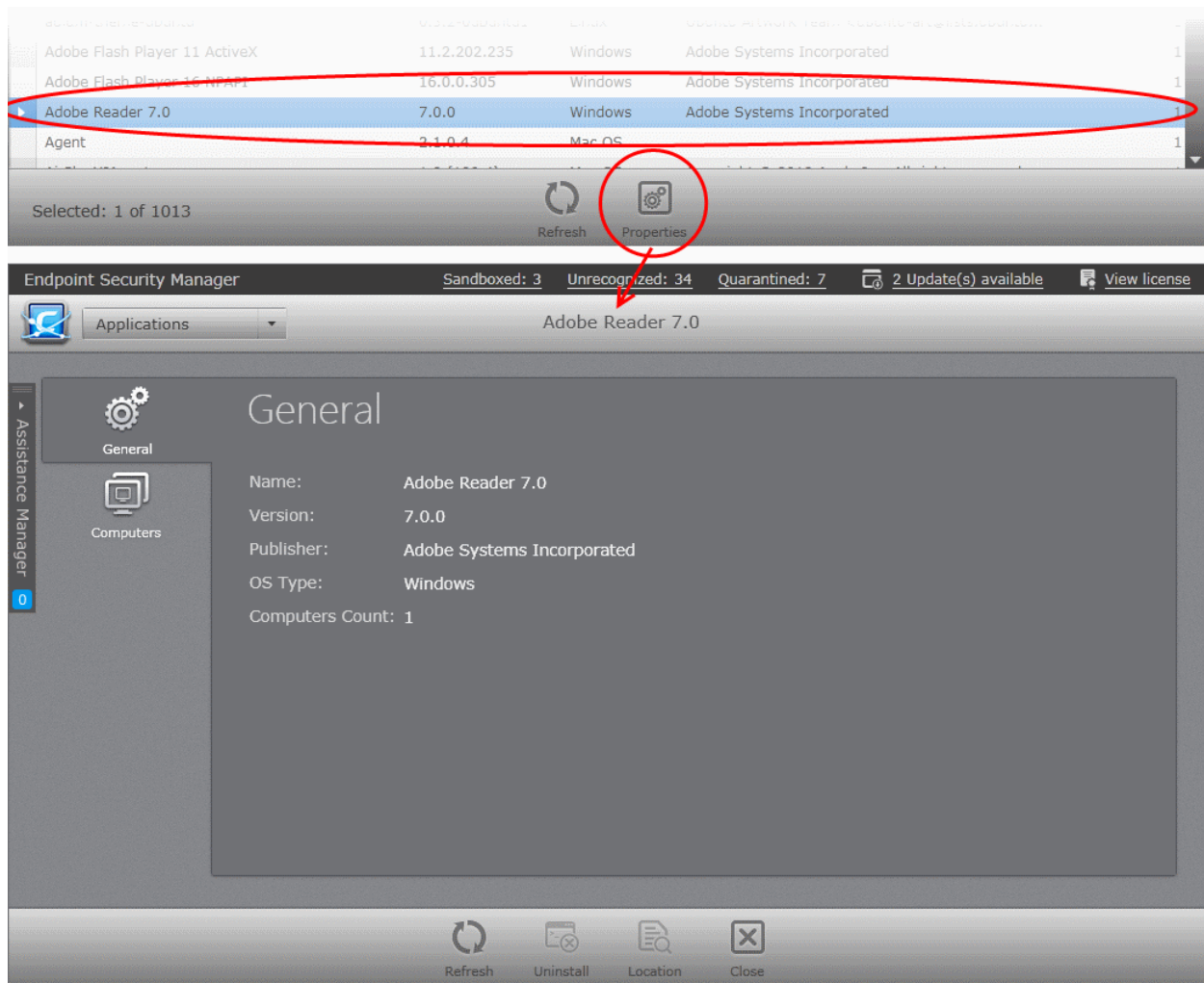
The Application Properties interface will open. The interface contains two areas:

- **General** - Displays the general information on the application.
- **Computers** - Displays the list of endpoints up on which the application was identified and allows the administrator to uninstall the application from the selected endpoints.

General Properties Screen

The General Properties screen can be displayed by clicking the 'General' tab from the left hand side navigation.
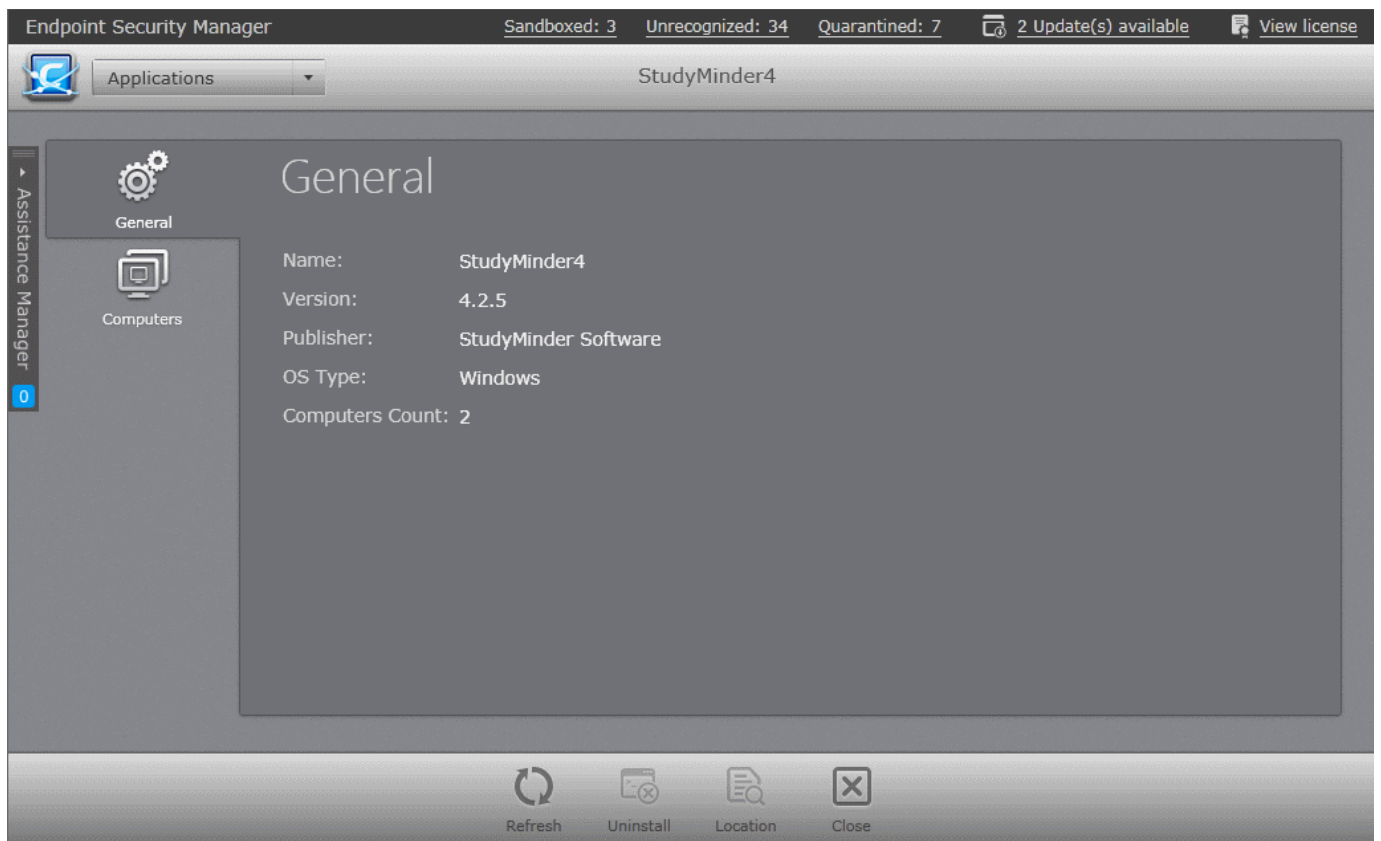
The General Properties screen displays the details on name, version number, publisher, OS and number of endpoints on which the application was identified.

Computers Screen

The 'Computers' screen can be opened by clicking the Computers tab in the 'Application Properties' interface.
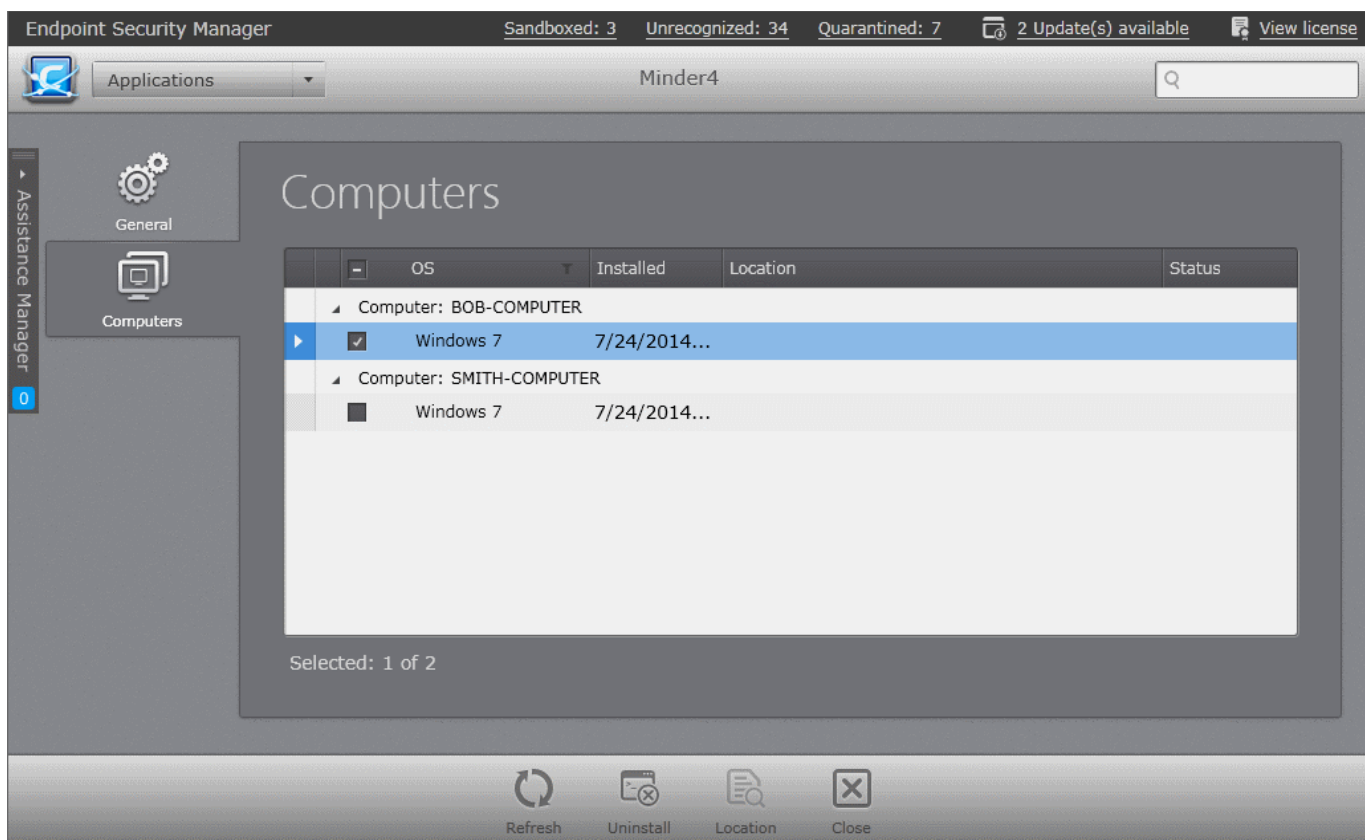
The 'Computers' screen displays the list of endpoints on which the application was identified and allows the administrator to identify the installation location of the application and uninstall the application, if it is an unwanted one.

To uninstall the application from selected endpoints

1.   Select the endpoints. To select all endpoints, click the checkbox beside 'OS' at the top or 'Select All' .
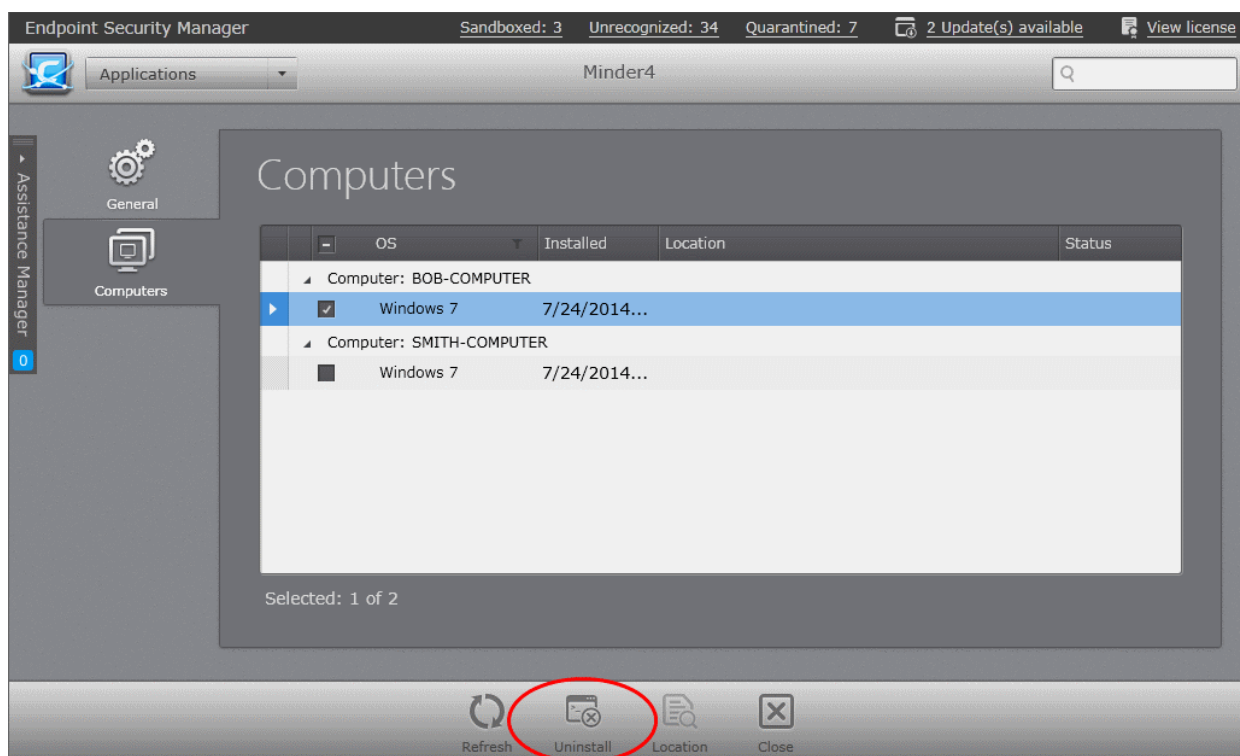
2.   Click 'Uninstall'.

The application will be uninstalled from the selected endpoints immediately.

Note: You can uninstall only MSI based applications from this interface.

To identify the installation location of the application

1. Select the endpoint
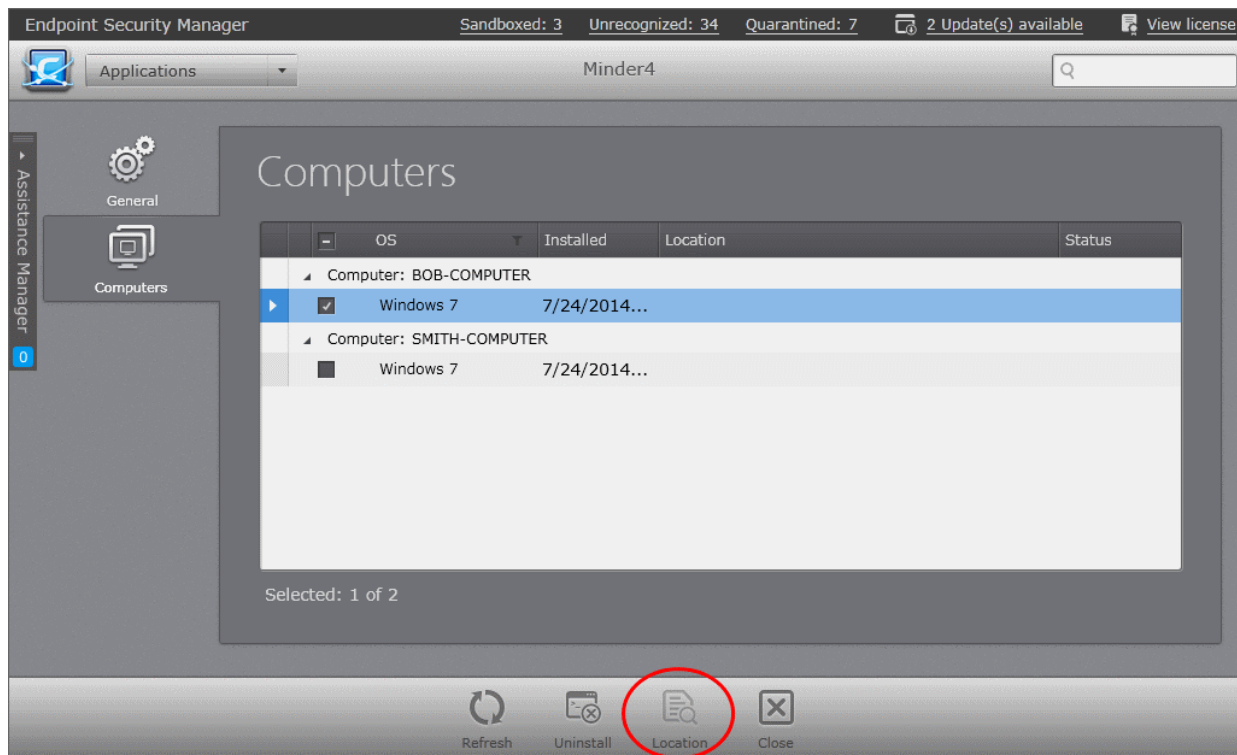
2. Click 'Location' at the bottom of the interface.

The 'File System' interface of the endpoint will open displaying the contents of installation folder of the application. Refer to the section **Viewing and Managing Drives and Storage** for more details.

10. Viewing and Managing Currently Running Processes

The 'Processes' area allows administrators to view and manage processes running on all endpoints. Administrator can use this feature to troubleshoot problems and terminate unnecessarily running processes if required.

To open the 'Processes' area, choose 'Processes' from the drop-down at the top left.

Column Heading	Description
Process	Displays the name of the process.
Description	Displays a short description of the process.
OS Type	Displays the Operating System of the endpoint(s) on which the process is running.
Company Name	Displays the vendor that has published the application
Location	Displays the location from which the process was initiated and run.
Status	Displays the list of all active processes on all endpoints. The status can be one of the following: • Terminating - The active process has been terminating. • Terminated - The active process has been terminated successfully. • Failed - The active process has been failed.
Computers Count	Indicates the number of endpoint computers on which the process is running

Filter Options

The filter options in the gray stripe, gives at-a-glance statistics of the number of processes identified from computers running on different Operating Systems and allow the administrator to filter the processes based on the criteria.

The search field in the right allows the administrator to search for a specific application by entering its name partially or fully.
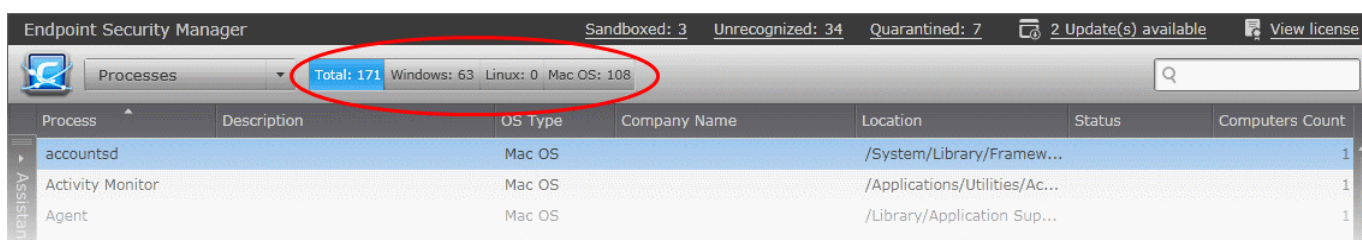
The administrator can terminate unsafe process(es)

- From all the endpoints at which it is currently running, by selecting the process(es) and clicking 'End process' at the bottom of the interface.

- At the selected endpoints from the Process Properties > Computers interface. Refer to the section **Managing Processes** for more details.

Managing Processes

The administrator can view the details of a processes and terminate unsafe processes from the Processes interface.

To view the details of a selected process

- Select a process from the list and click 'Properties' from the options at the bottom

- Right click on the process and select 'Properties' from the context sensitive menu

  or

- Double click on the process.

The Properties screen has two tabs:
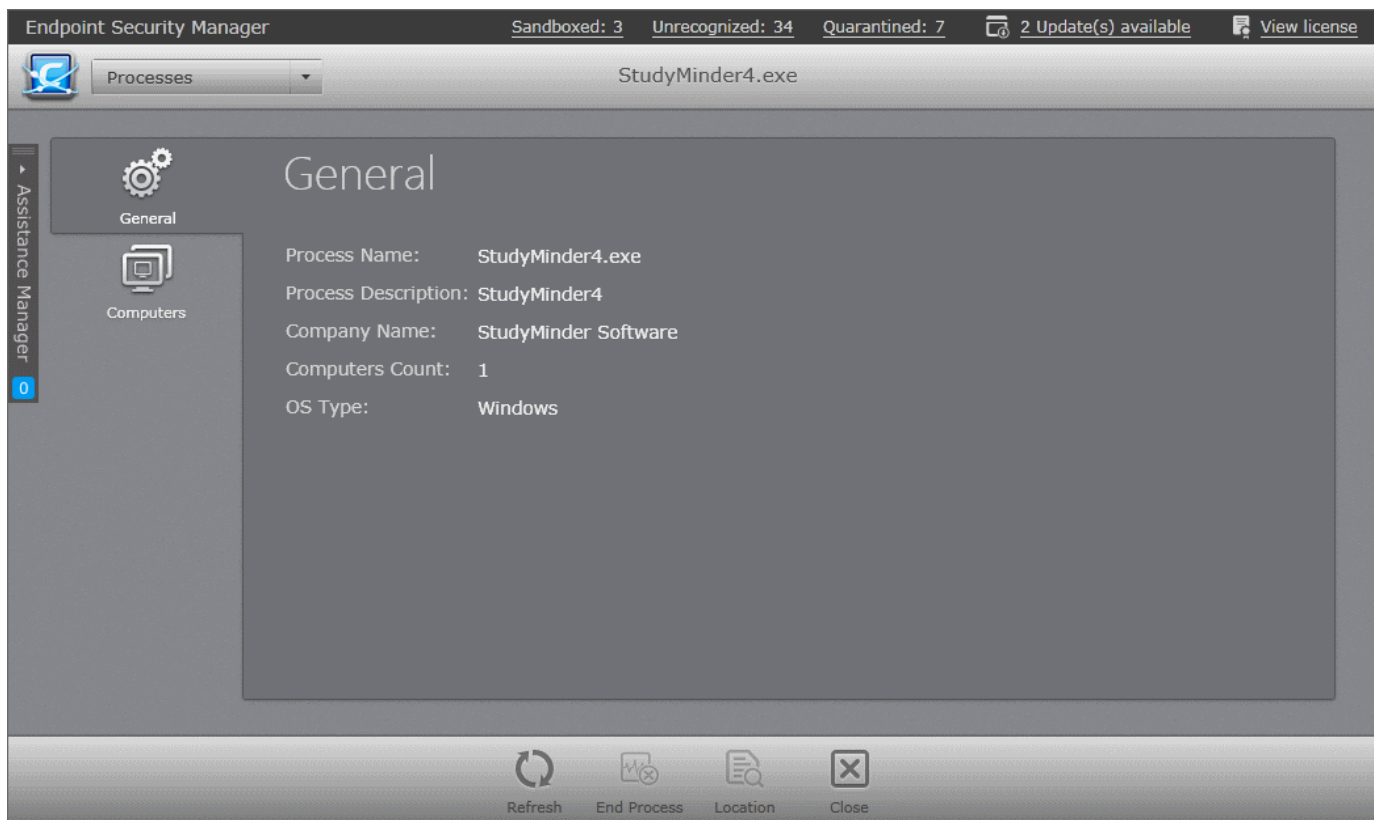
- **General** - Displays the name of the process name, a short description of the process, vendor of the executable that has initiated the process, number of computers at which the process is running and the Operating System of the endpoints on which the process is running.

- **Computers** - Displays the name of endpoints on which the process is running, their OS and status.
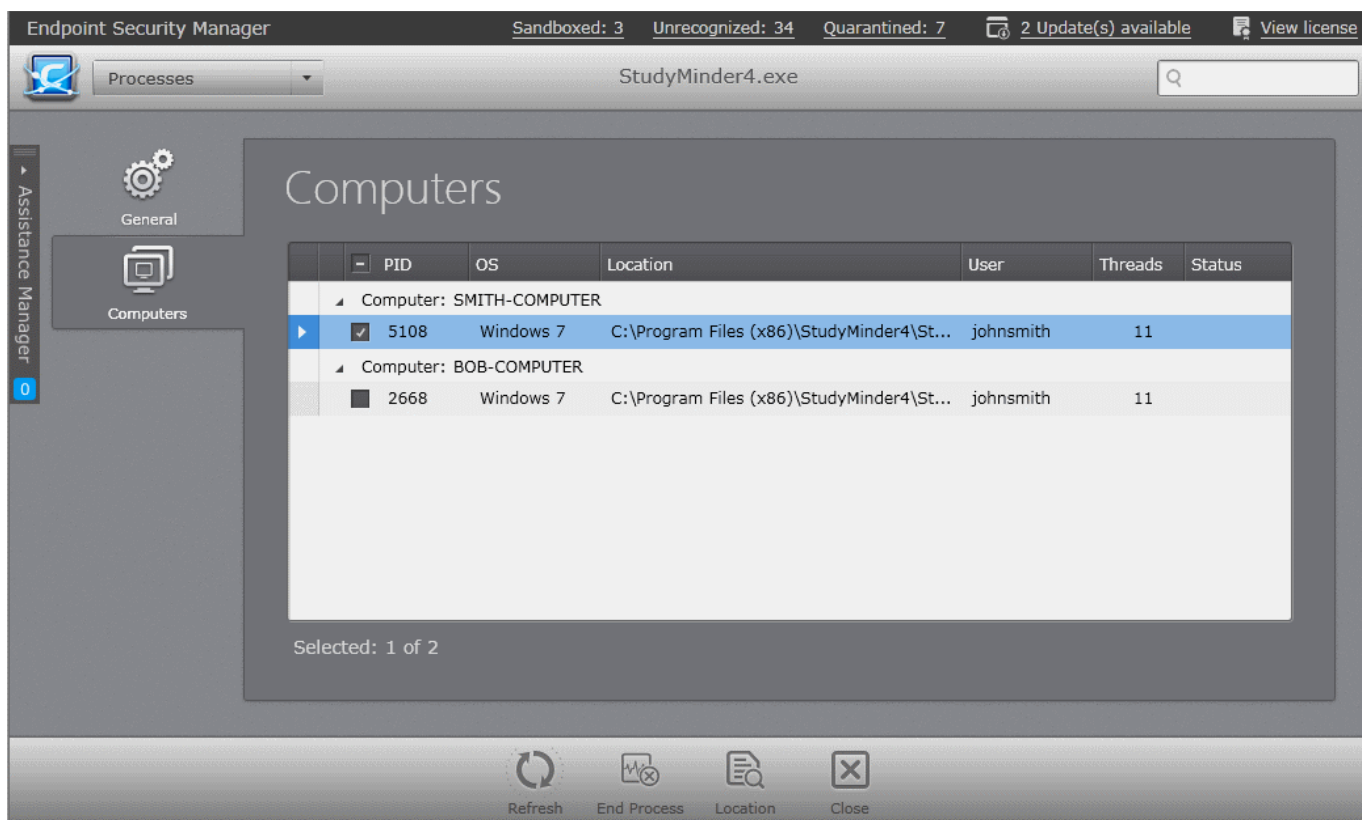
- To terminate the process from selected endpoints, select the endpoints and click End Process at the bottom of the interface.

- To view the location from where the process was initiated and running, select the endpoint and click Location at the bottom of the interface. The File System pane of the endpoint will open displaying the contents of installation folder of the application that has initiated the process. Refer to the section **Viewing and Managing Drives and Storage** for more details.

11.   Viewing and Managing Services

The 'Services' area allows administrators to view and manage Windows Services, Mac Services or Unix Daemons that are currently loaded on to all the Windows based, MacOS based or Linux based managed endpoints, with the number of computers on which the service is loaded. Administrator can use this feature to troubleshoot problems and start/stop the services if required.

To open the 'Services' area, choose 'Services' from the drop-down at the top left.

Column Heading	Description
Service	Displays the service key name.
Display Name	Displays the short name of the service.
OS Type	Displays the Operating System of the endpoint(s) on which the service is loaded.
Location	Displays the location of the application that that has initiated the service.
Status	Displays the running status of the service.
Computers Count	Indicates the number of endpoint computers on which the service is loaded.

Filter Options

The filter options in the gray stripe, gives at-a-glance statistics of the number of services identified from computers running on different Operating Systems and allow the administrator to filter the services based on the criteria.

The search field in the right allows the administrator to search for a specific service by entering its name partially or fully.

The administrator can stop a unwanted running service or start a stopped service:

- From all the endpoints, by selecting the services and clicking 'Stop' or 'Start' appropriately from the bottom of the interface.

- At the selected endpoints from the Service Properties > Computers interface. Refer to the section **Managing Services** for more details.

Managing Services

The administrator can view the details of a Service and Start or Stop it from the Service Properties interface.

To view the details of a selected Service

- Select the Service from the list and click 'Properties' from the options at the bottom

- Right click on the Service and select 'Properties' from the context sensitive menu

  or

- Double click on the Service.
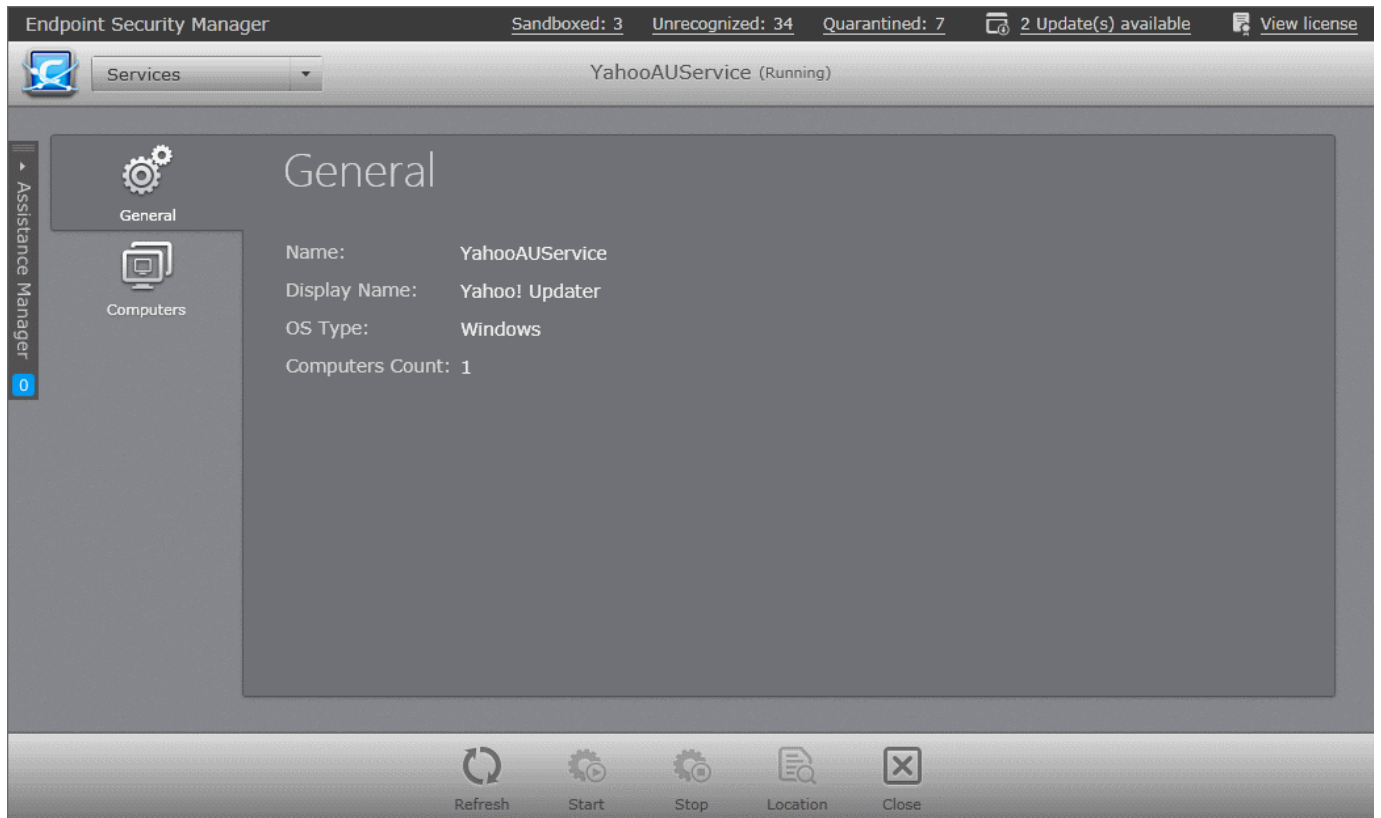
The Properties screen has two tabs:

- **General** - Displays the key name of the service, display name of the service and the Operating System and the number of computers at which the service is loaded.

- **Computers -** Displays the name of endpoints on which the service is loaded, their OS and running status.
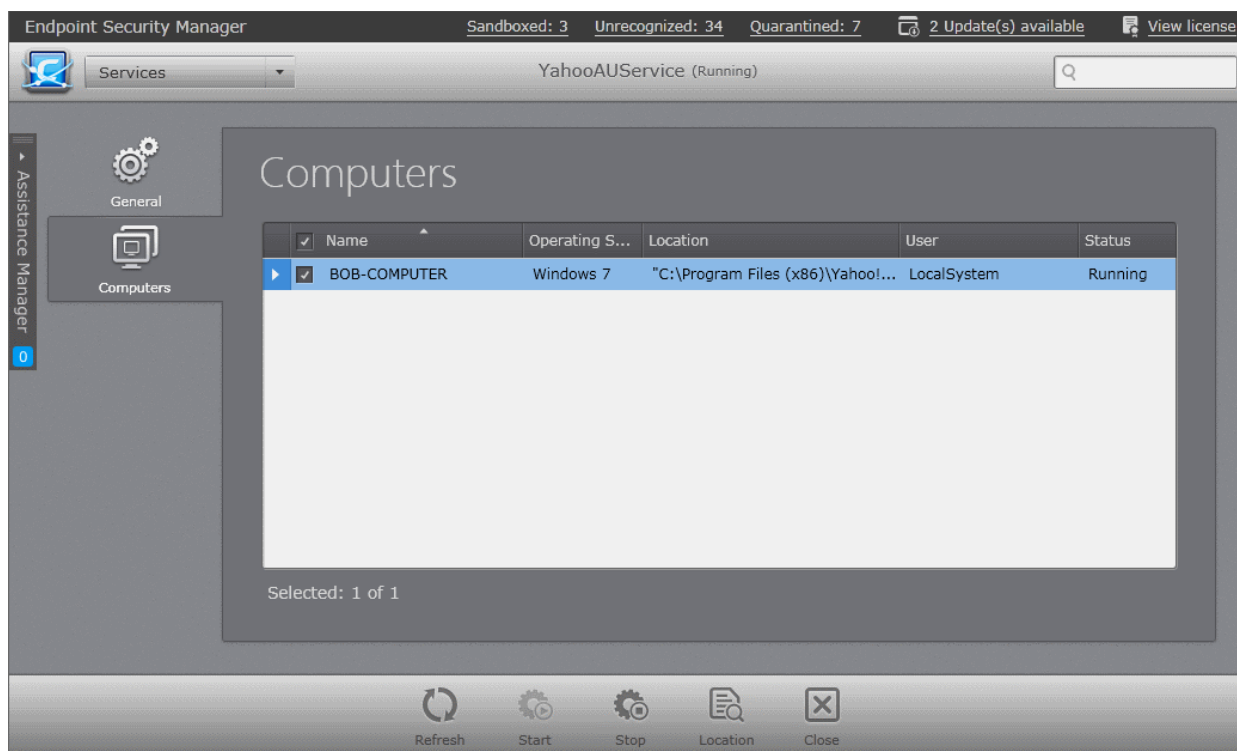
- To stop a running service from selected endpoint(s), select the computer(s) and click 'Stop' from the options at the bottom.

- To start a stopped service at selected endpoint(s), select the computer(s) and click 'Start' from the options at the bottom.

- To view the location of the application, program or OS component that has initiated the Service, select the endpoint and click Location at the bottom of the interface. The File System pane of the endpoint will open displaying the contents of installation folder of the application, program or OS component that has initiated the process. Refer to the section **Viewing and Managing Drives and Storage** for more details.

12.   The Reports Area

CESM Reports are highly informative, graphical summaries of the security and status of managed endpoints. Each type of report is fully customizable, features 'in-report' remediation and can be ordered for anything from a single machine right up to the entire managed environment. Reports can be exported to .pdf or spreadsheet. To open the Reports area, choose 'Reports' from the drop-down at top left.
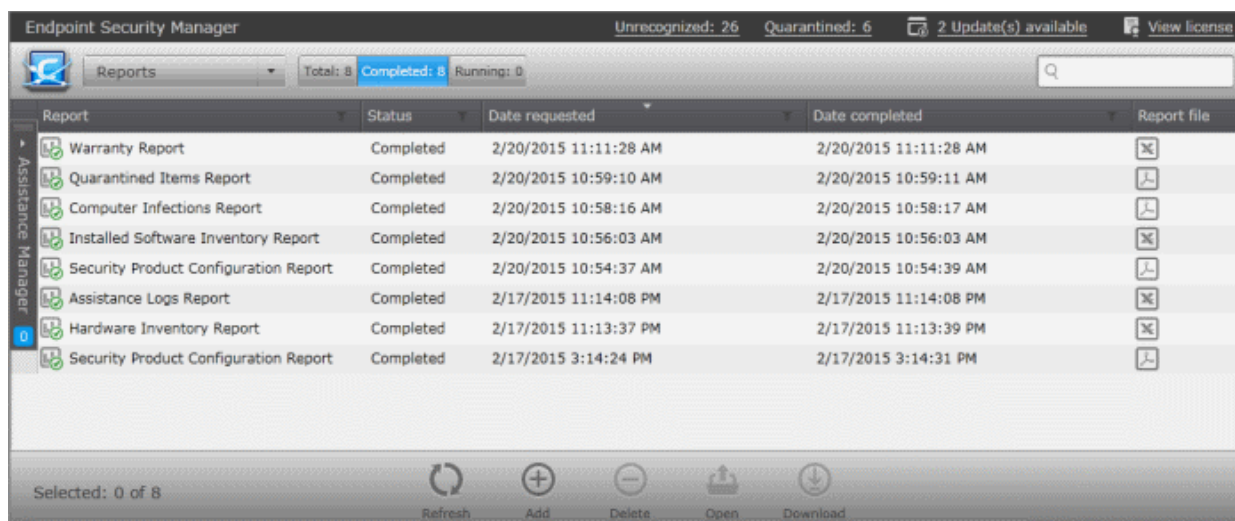
Column Heading	Description
Report	Indicates the type of the report requested/generated. For the complete list of Report types available from CESM, refer to the section **Report Types** given below.
Status	Indicates whether the report generation is 'Completed' or 'Running'.
Date Requested	Indicates the date and time of request for the report by the administrator.
Date Completed	Indicates the date and time of completion of report generation.
Report File	Enables the administrator to download the completed reports.

Administrators can generate reports for defined groups of endpoints, individual endpoints or selected endpoints. Clicking 'Add' at the bottom of the 'Reports' interface allows the administrator to select the report type and the select the endpoints from all the managed endpoints irrespective of the groups. Refer to the sections below for detailed explanations on each report type.

Report Types
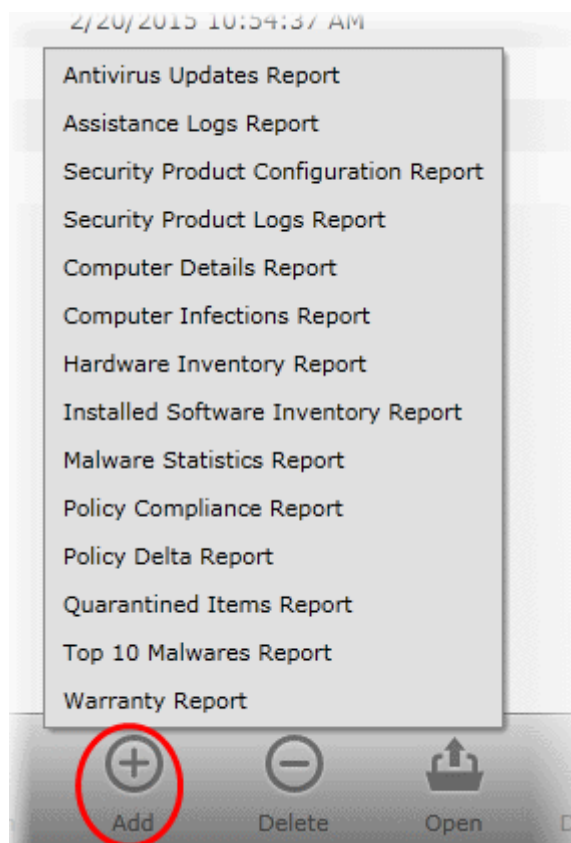
- **Antivirus Updates** - Information on versions of AV signature databases at the endpoints.

- **Assistance Logs** - Details of Assistance Manager sessions between users and administrators, including details of the chat.

- **Security Product Configuration** - Information on components of security product installed at the endpoints and their configuration status.

- **Security Product Log** - Logs of events related to security product at the endpoints.

- **Computer Details** - General information about target endpoint(s) such as operating environment and hardware details.

- **Computer Infections** - Information on malware discovered during the antivirus (AV) scans and not handled successfully (deleted, disinfected or quarantined) locally by the security product and the endpoints affected by them.

- **Hardware Inventory** - Provides information on computers such as name of the computer, its IP address, subnet mask, to which domain or workgroup it belongs and more.

- **Installed Software Inventory** - Provides information on software installed on endpoints such as operating systems, names of the software installed, their publishers' name, when the software were installed and more.

- **Malware Statistics** - Statistical information on the malware detected at various AV scans run on the target endpoint(s), with the actions taken against them.

- **Policy Compliance** - A summary of compliance of the endpoints to their assigned security policies and a detailed information on the security policies applied to the endpoints.

- **Policy Delta** - Provides a investigation report on the differences in components between the policy applied from the CESM server side and the actual state of the policy as in the target endpoint side to analyze reasons for an endpoint being non-compliant. This report can be generated only for endpoint with Non-Compliant status.

- **Quarantined Items** - Information on virus and other malware identified by AV scans and quarantined locally by CES.

- **Top 10 Malwares** - A list of top-ten malware discovered during the antivirus (AV) scans from the target endpoints during the specified time period.

- **Warranty** - Provides information about the security products installed on endpoints and their warranty statuses.

Filter Options

The filter options in the gray stripe, gives at-a-glance statistics of the reports requested, completed and under generation.

Clicking a category displays only the reports falling into that category.

The search field lets the administrator search for report(s) by endpoint or report completion/request date.
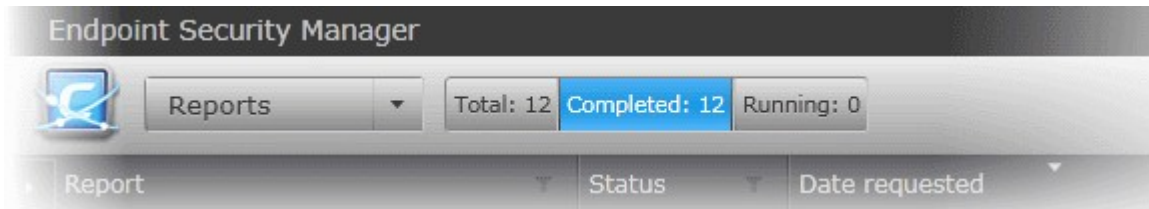
More filters can be applied by clicking the funnel icon beside the column heading.

- Click the filter icon �... in the 'Report' column header to search for a specific report type:
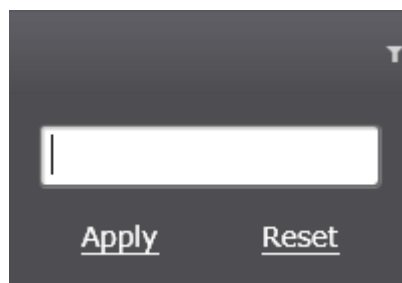
- Click the filter icon �... in the 'Status' column header to search for reports that were completed, running, failed or in queue.
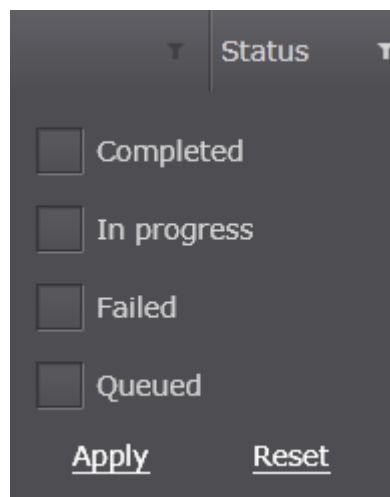
- Click the filter icon �... in the 'Date Requested' or 'Date completed' column header to search for reports that were requested or completed within a specific date range.
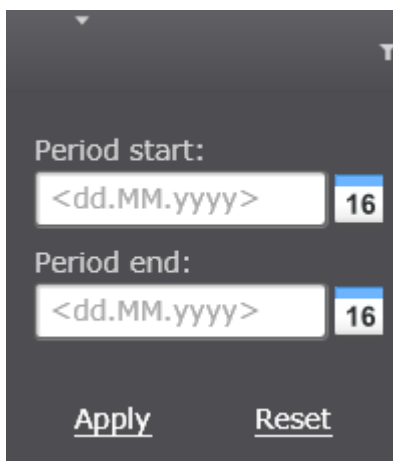
- Click 'Reset' to display all the items.

Generating a Report

Administrators can generate reports for defined groups of endpoints or individual endpoints. Group reports can be generated from the 'Groups' area, Reports for individual endpoints can be generated from the 'Computers' area.

To generate reports for a selected group

1. Open 'Groups' area by selecting 'Groups' from the drop-down at the top left.

2. Right click on a Group and choose 'Build Report'.

3. Choose the report type from the context sensitive menu.

or

- Select the Groups, select 'Report' from the bottom of the interface and choose the report type.
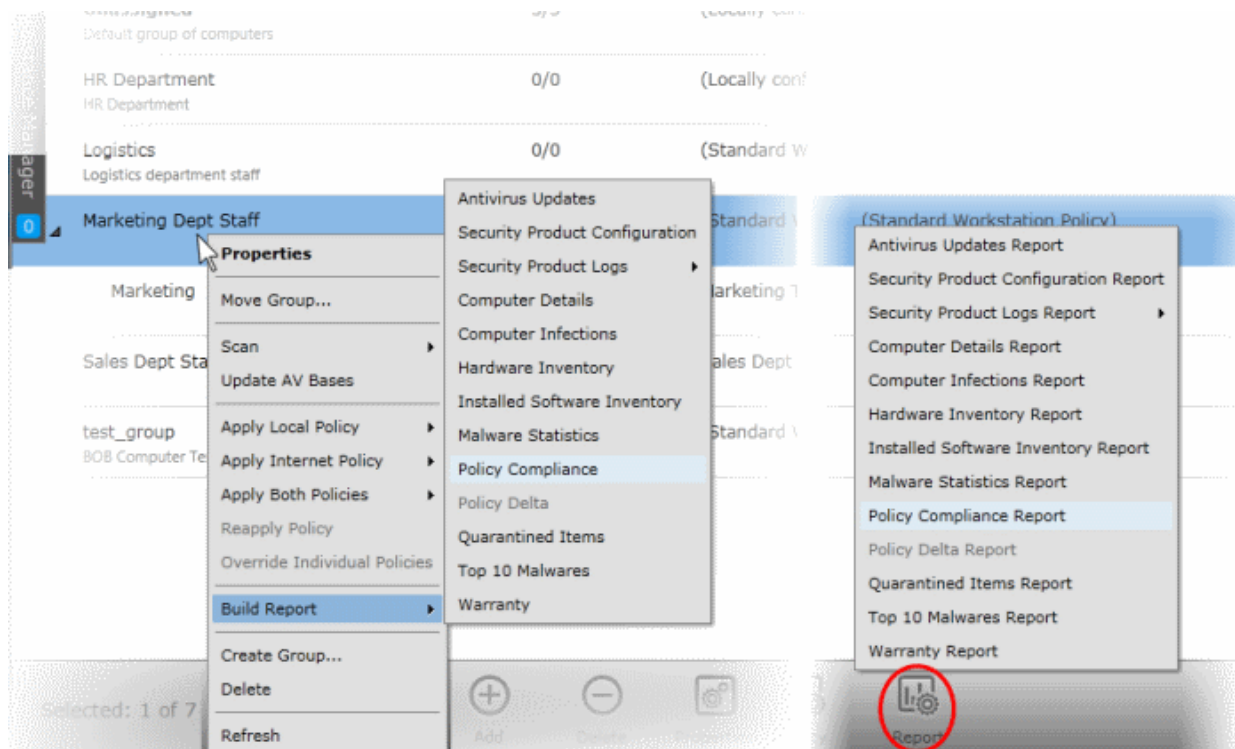
The report generation will be started or added to the queue. The progress will be displayed in the 'Reports' area. On completion, the report can be opened from the 'Reports' area. Refer to the sections below for detailed explanations on each report type.

To generate reports for a selected endpoint

1. Open 'Computers' area by selecting 'Computers' from the drop-down at the top left.

2. Right click on a computer and choose 'Build Report' and choose the report type from the context sensitive menu or Select the computer, click 'Report' on the bottom, and choose the report type.
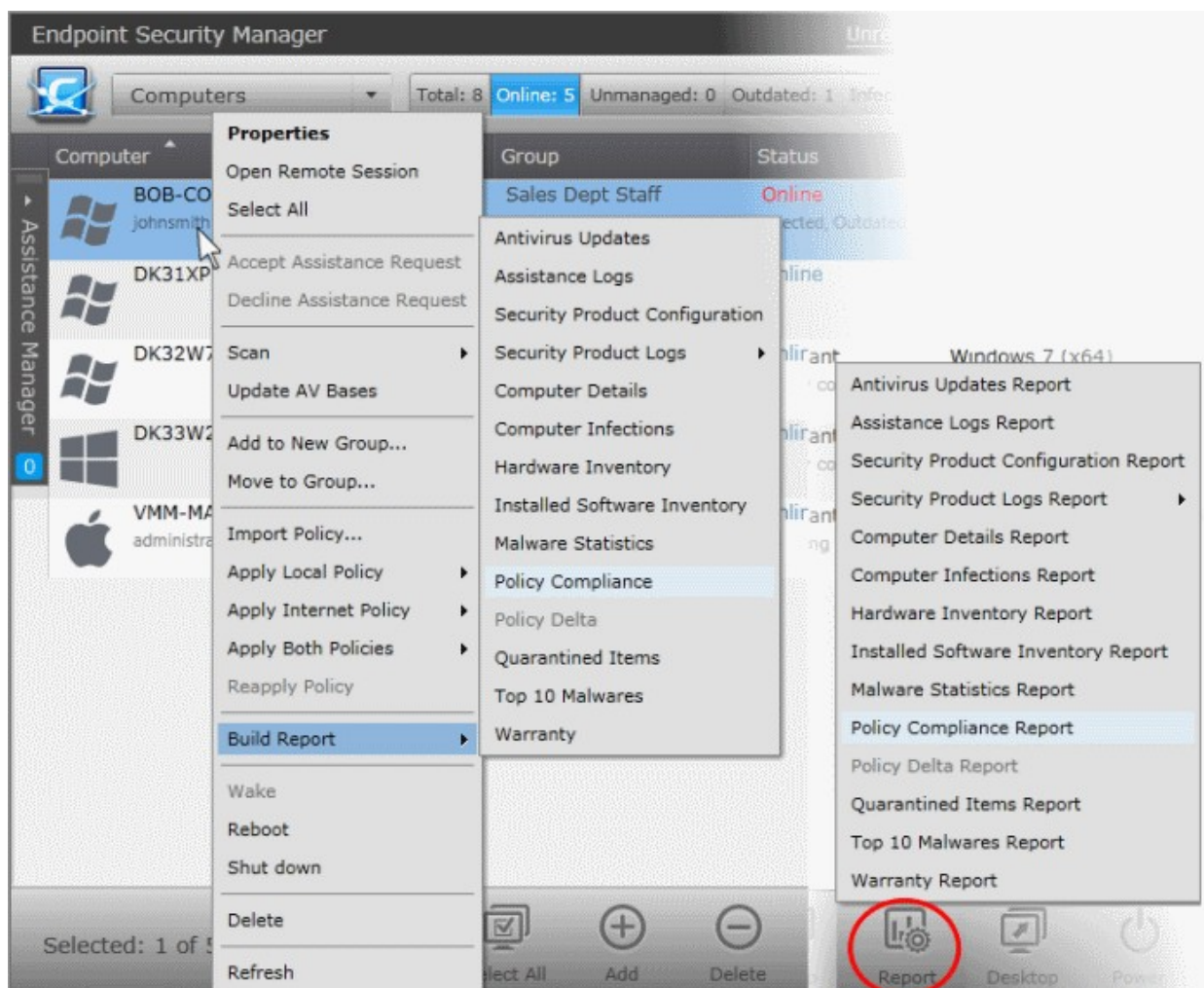
The report will now be generated. Progress will be displayed in the 'Reports' area. On completion, the report can be opened from the 'Reports' area. Refer to the sections below for detailed explanations on each report type.

Downloading the Report

If the administrator had opted for generating a downloadable report file in step 2 - Options, the report can be downloaded by clicking the download link beside the report in the 'reports' area or by selecting the report(s) and clicking the download icon at the bottom of the 'Reports' area or clicking the report file icon (or) under the Report File column. The administrator can choose the printable file to be generated in portable document (.pdf) or spreadsheet (.xls) format.

Viewing the Report

The administrator can view a generated report in the following ways:

- Selecting a report from the list and clicking 'Open' from the options at the bottom.

- Double clicking on the report

- Right clicking on a report and choosing 'Open' from the right click menu.

12.1.   Antivirus Updates Report

The Antivirus Updates report provides details on the antivirus (AV) signature database versions in the target computers and whether they are up-to-date. The report assists the administrators to decide on the target computers whose AV databases are to be updated and to run an Update AV base task on the computers. Comodo advises administrators to maintain the AV databases up-to-date in all the managed end-points to get protection against any threats discovered by our AV labs.

To generate a 'Antivirus Updates' report

  •   Open the 'Reports' area by choosing 'Reports' from the drop-down at the top left.

  •   Click 'Add' and choose 'Antivirus Updates Report'. The 'Create Antivirus Updates Report' wizard will start.
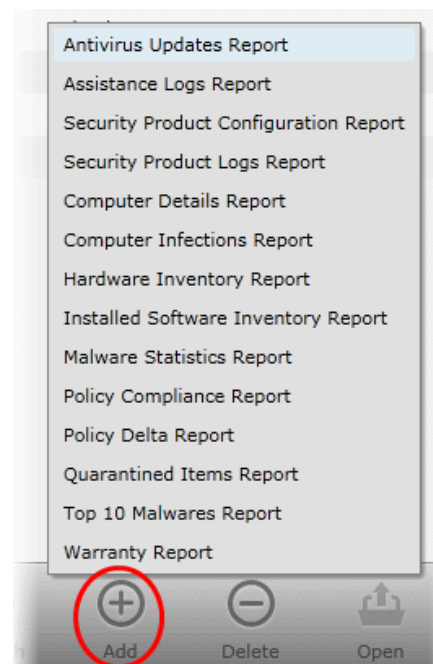
Step 1 - Selecting Targets

The list of all the endpoint computers connected to CESM is displayed.
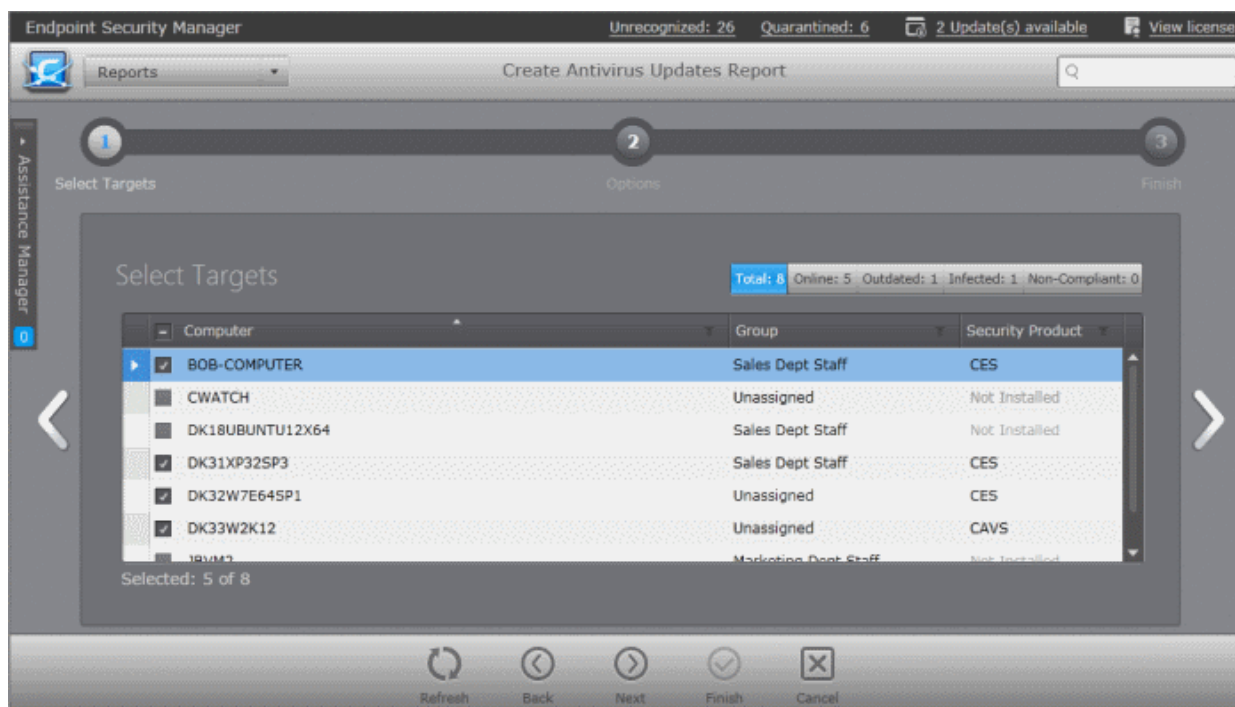
 •   Select the endpoint(s) for which you wish to generate the AV Updates report. The filter options in the header provides at-a-glance statistics of the computers in the network and allow the administrator to filter the computers based on the criteria. You can also filter the computers by clicking the funnel icon on the column headers.

  •   Click the right arrow or swipe the screen to the left to move to the next step.

Step 2 - Options

The second step allows you to configure the options for report generation.

  •   **Include computers with outdated virus databases only** - The report will ignore the endpoints that have

---

the most up-to-date AV signature database in the report and give details only on those having outdated databases.

- **Generate downloadable report file** - Select this option if you need to print or archive the report. You can choose the printable file to be generated in portable document (.pdf) or spreadsheet (.xls) format. On completion, the report generated can be downloaded to the administrator's computer.

- Select required options

- Click the 'Finish' icon to start generating the report.

The report generation will be started or added to the queue. The progress will be displayed in the 'Reports' area.

View the Report

The administrator can view the report at anytime after the completion.

To view the report

- Select the report from the list and click 'Open' from the options at the bottom.

- Double click on the report

  Or

- Right click on the report and choose 'Open' from the right click menu.

The report will contain the AV signature database update details at each endpoint selected in step 1.

- The summary pie chart in the upper portion provides an at-a-glance comparison report on numbers of computers that have outdated/up-to-date AV databases as compared to the latest database version indicated.

- Following the summary, details of each computer, with their IP Addresses and the installed AV database versions are displayed.

- • Click the print icon at the bottom to take print of the report.

Downloading the Report

If the administrator had opted for generating a downloadable report, it can be downloaded by selecting the Report in the 'Reports' area and clicking the download icon at the bottom or clicking the report file icon (or) under the Report File column.

12.2.   Assistance Logs Report

The Assistance Logs report provides details of chat sessions between between endpoint user and the administrator. The report includes UID of the sessions, name of the computer and its IP, name of the endpoint user and the name of the administrator. The actual chat details for each session is also included in the report.
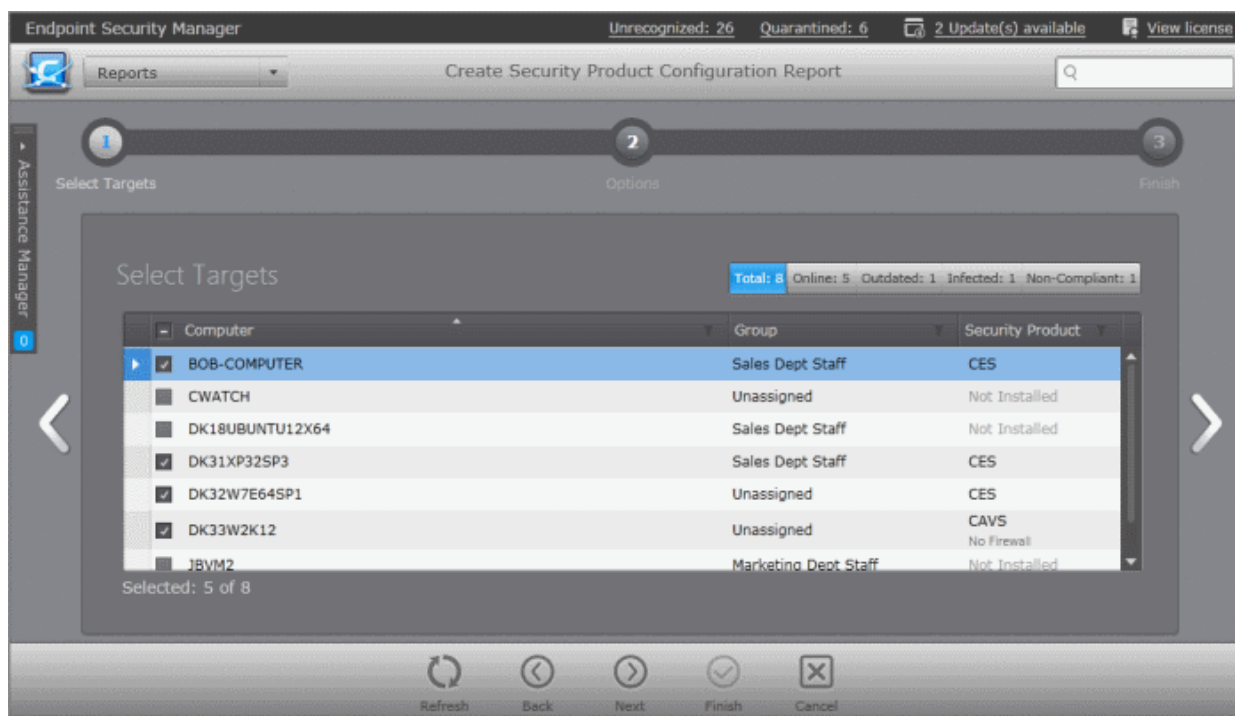
To generate a Assistance Logs report

- Open the 'Reports' area by choosing 'Reports' from the drop-down at the top left.

- Click 'Add' and choose 'Assistance Logs Report'. The 'Create Assistance Logs Report' wizard will start.
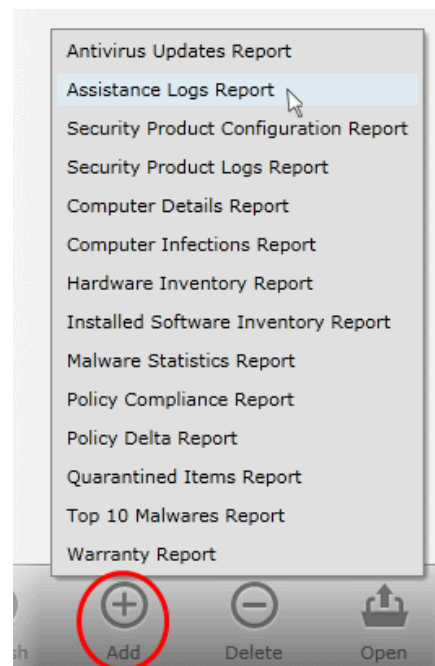
Step 1 - Selecting Targets

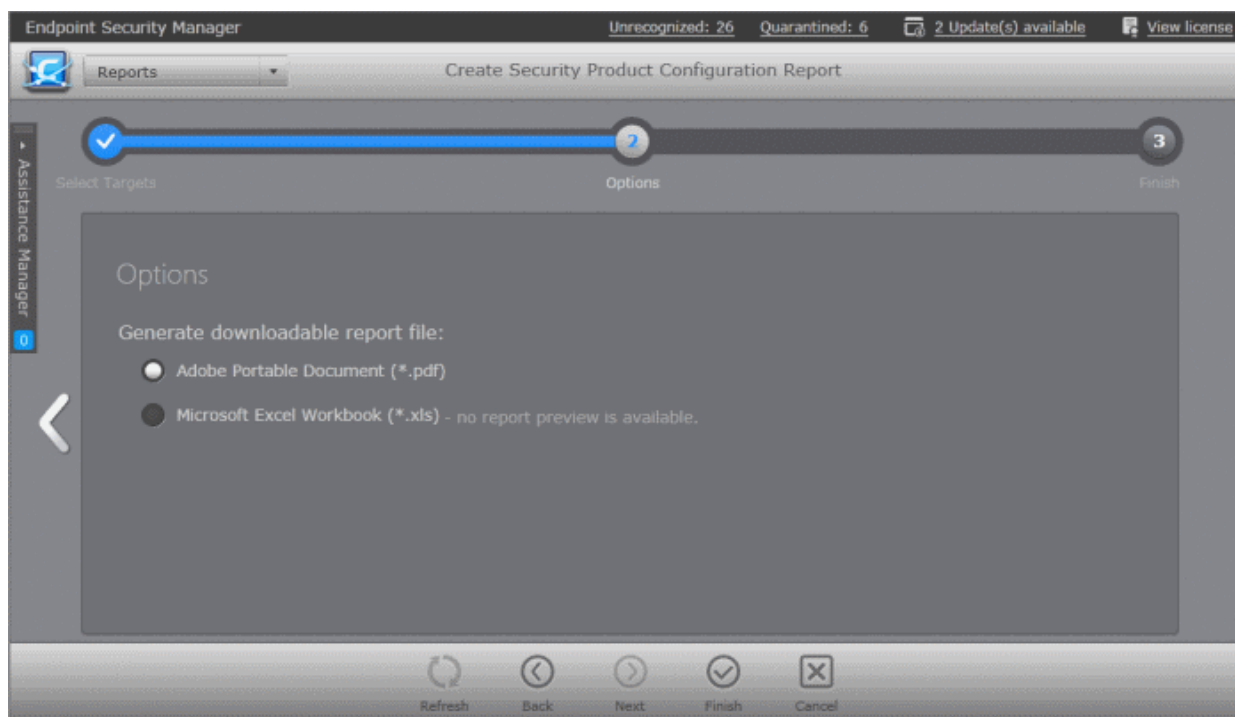The list of all the endpoint computers connected to CESM is displayed.
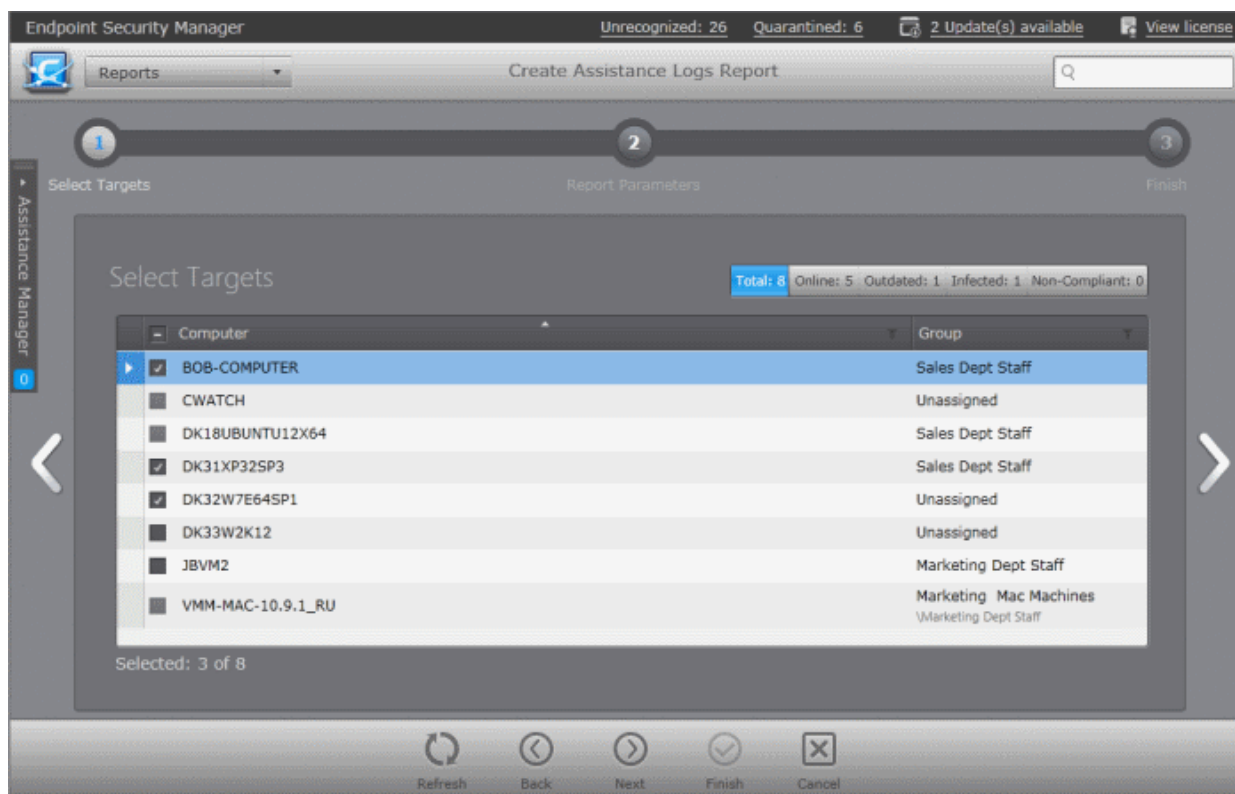
- Select the endpoint(s) for which you wish to generate the Assistance Logs report. The filter options in the header provides at-a-glance statistics of the computers in the network and allow the administrator to filter the computers based on the criteria. You can also filter the computers by clicking the funnel icon on the column headers.

- Click the right arrow or swipe the screen to the left to move to the next step.

Step 2 - Selecting the Report Period

The next step is to choose the time period for which the report should be generated.
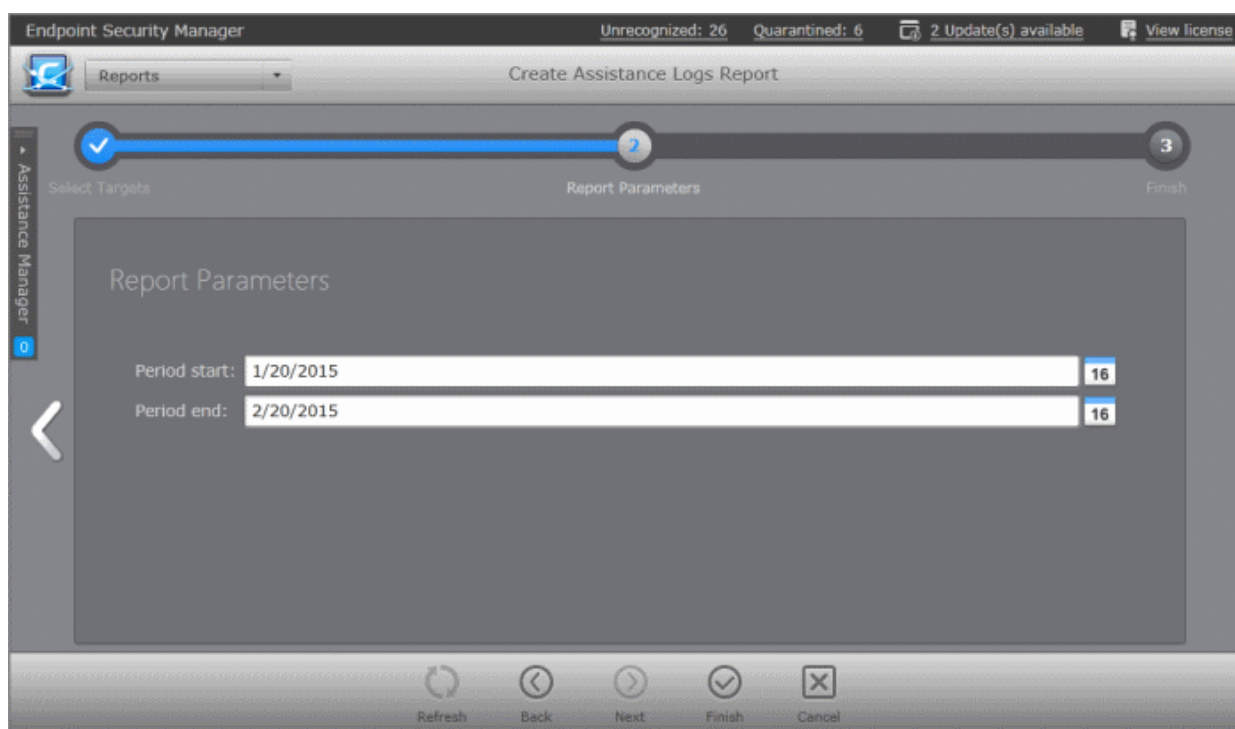
- • Specify the period start and end dates in the respective text fields in MM/DD/YYYY format. Alternatively, clicking the calendar icon at the right end of the text box displays a calendar to select the dates.
- • Click the 'Finish' icon to start generating the report.
- • The report generation will be started or added to the queue. The progress will be displayed in the 'Reports' area.

Downloading the Report

The report is available in spreadsheet format only and can be downloaded by selecting it in the

'Reports' area and clicking the download icon   at the bottom or clicking the report file icon under the Report File column.

12.3.   Security Product Configuration Report

The 'Security Product Configuration' report provides information on managed security software, like components of CES/CAS installed and their statuses on the target computers according to their applied policies.

To generate a Security Product Configuration report

- • Open the 'Reports' area by choosing 'Reports' from the drop-down at the top left.
- • Click 'Add' and choose 'Security Product Configuration Report'. The 'Create Security Product Configuration Report' wizard will start.

Step 1 - Selecting Targets

The list of all the endpoint computers connected to CESM is displayed.

- Select the endpoint(s) for which you wish to generate the Security Product Configuration report. The filter options in the header provides at-a-glance statistics of the computers in the network and allow the administrator to filter the computers based on the criteria. You can also filter the computers by clicking the funnel icon on the column headers.

- Click the right arrow or swipe the screen to the left to move to the next step.

Step 2 - Options

The second step allows you to configure the options for report generation.

- • **Generate downloadable report file** - Select this option if you need to print or archive the report. You can choose the printable file to be generated in portable document (.pdf) or spreadsheet (.xls) format. On completion, the report generated can be downloaded to the administrator's computer.
- • Select required options.
- • Click the 'Finish' icon to start generating the report.

The report generation will be started or added to the queue. The progress will be displayed in the 'Reports' area.

View the Report

The administrator can view the report at anytime after the completion.

To view the report

- • Select the report from the list and click 'Open' from the options at the bottom.
- • Double click on the report
  - • Or
- • Right click on the report and choose 'Open' from the right click menu.

The report contains the details on CES/CAS/CAVM versions and their components installed/activated on the endpoints selected in step 1.

- • The summary pie chart in the upper portion provides an at-a-glance information of security product versions installed in the selected endpoints.
- • The bar-graph displays a comparison of security product components installed and activated in the selected endpoints
- • Following is the graphical summary, details of each computer, with security product versions, installed and enabled components are displayed.

Endpoint Security Manager   Unrecognized: 26   Quarantined: 6   2 Update(s) available   View license
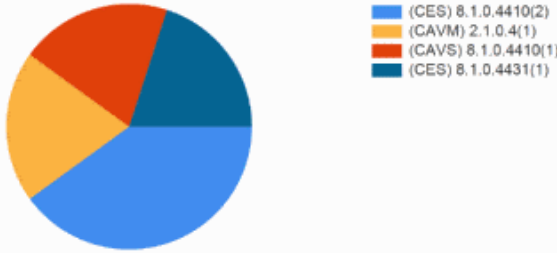
Reports   1 / 2

Security Product Configuration Report
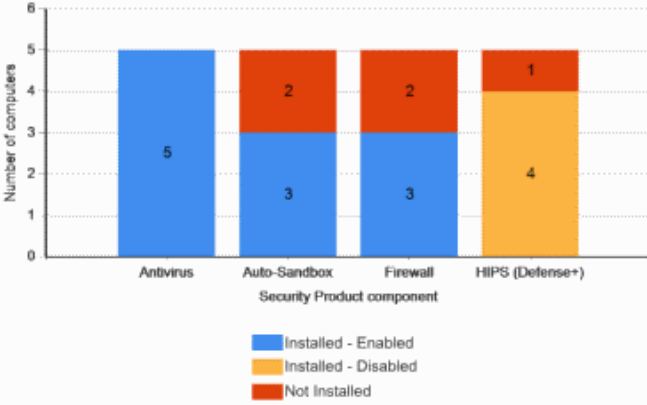
2/20/2015 1:50:11 PM

Security Product Configuration Report includes data from 5 computer(s)

Security Product Version Summary Chart

- (CES) 8.1.0.4410(2)
- (CAVM) 2.1.0.4(1)
- (CAVS) 8.1.0.4410(1)
- (CES) 8.1.0.4431(1)

Security Product Component Summary Chart

Number of computers

Antivirus	Auto-Sandbox	Firewall	HIPS (Defense+)
5	3 / 2	3 / 2	4 / 1

Security Product component

- Installed - Enabled
- Installed - Disabled
- Not Installed

Details:

Computer	Product	Version	Antivirus Installed	Antivirus Enabled	Auto-Sandbox Installed	Auto-Sandbox Enabled	Firewall Installed	Firewall Enabled	HIPS (Defense+) Installed	HIPS (Defense+) Enabled
VMM-MAC-10.9.1_RU	CAVM	2.1.0.4	✓	✓	✗	✗	✗	✗	✗	✗
dk33w2k12	CAVS	8.1.0.4410	✓	✓	✗	✗	✗	✗	✓	✗
BOB-COMPUTER	CES	8.1.0.4431	✓	✓	✓	✓	✓	✓	✓	✗
dk31xp32sp3	CES	8.1.0.4410	✓	✓	✓	✓	✓	✓	✓	✗
dk32w7e64sp1	CES	8.1.0.4410	✓	✓	✓	✓	✓	✓	✓	✗

Print   Close

- Click the print icon [icon] at the bottom to take print of the report.

Downloading the Report

If the administrator had opted for generating a downloadable report, it can be downloaded by selecting the Report in the 'Reports' area and clicking the download icon [icon] at the bottom or clicking the report file icon ([icon] or [icon]) under the Report File column.

12.4.   Security Product Logs Report

Each Comodo security product (CES/CAS/CAVM) installed on an endpoint maintains logs for each of the Antivirus, Firewall and Defense+ components (as applicable).

- **Antivirus** - The Antivirus component documents the results of all actions it performed in an extensive but easy to understand log report. A detailed scan report contains statistics of all scanned objects, settings used for each task and the history of actions performed on each individual file. Log entries are also generated during real-time protection, and after updating the anti-virus database and application modules.

- **Firewall** - The Firewall component records a history of all events/actions taken. Firewall 'Events' are generated and recorded for various reasons - including whenever an application or process makes a connection attempt that contravenes a rule in the Network Security Rulesets, or whenever there is a change in Firewall settings.

- **Defense+** - The Defense+ component records a history of all events/actions taken. Defense+ 'Events' are generated and recorded for various reasons. Examples include changes in Defense+ settings, when an application or process attempts to access restricted areas or when an action occurs that contravenes the Computer Security Rulesets.

Note: Comodo Antivirus for Server (CAS) contains only Antivirus and Defense+ components and maintain logs only AV and Defense+ events. Firewall Logs cannot be generated form the endpoints installed with CAS. Comodo Antivirus for Mac (CAVM) contains only Antivirus component and logs for Firewall and Defense+ events cannot be generated for Mac endpoints.

The Security Product Logs report shows the log of events stored in the target computers for the selected component. The administrator can generate different log report for each of the component for viewing and printing/archival purpose.

To generate a Security Product Logs report

- Open the 'Reports' area by choosing 'Reports' from the drop-down at the top left.

- Click 'Add' and choose 'Security Product Logs Report'. The 'Create Security Product Logs Report' wizard will start.

Antivirus Updates Report
Assistance Logs Report
Security Product Configuration Report
Security Product Logs Report
Computer Details Report
Computer Infections Report
Hardware Inventory Report
Installed Software Inventory Report
Malware Statistics Report
Policy Compliance Report
Policy Delta Report
Quarantined Items Report
Top 10 Malwares Report
Warranty Report

Add   Delete   Open

Step 1 - Select Report Type

The first step is to choose the security product component for which you want to generate a log report.

- Choose the component from Antivirus, Firewall and Defense+ and swipe the screen to the left or click the right arrow to move to step 2 - Selecting targets.
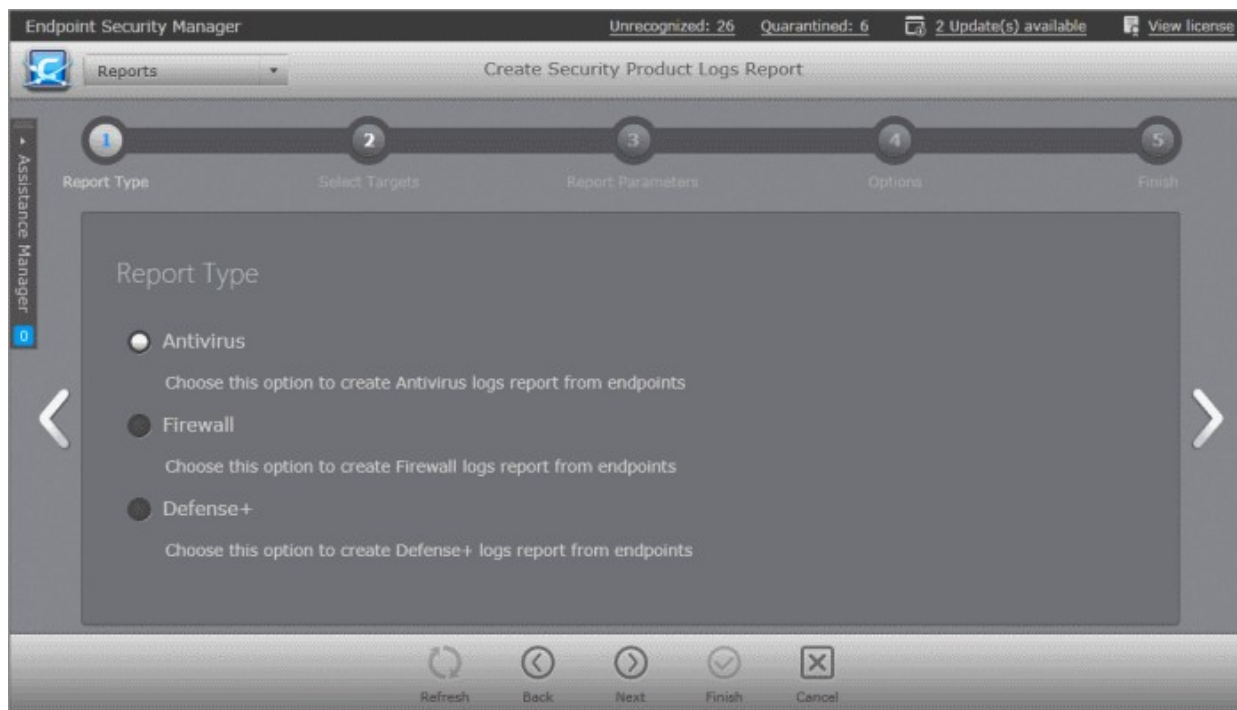
Step 2 - Selecting Targets

The list of all the endpoint computers connected to CESM is displayed.
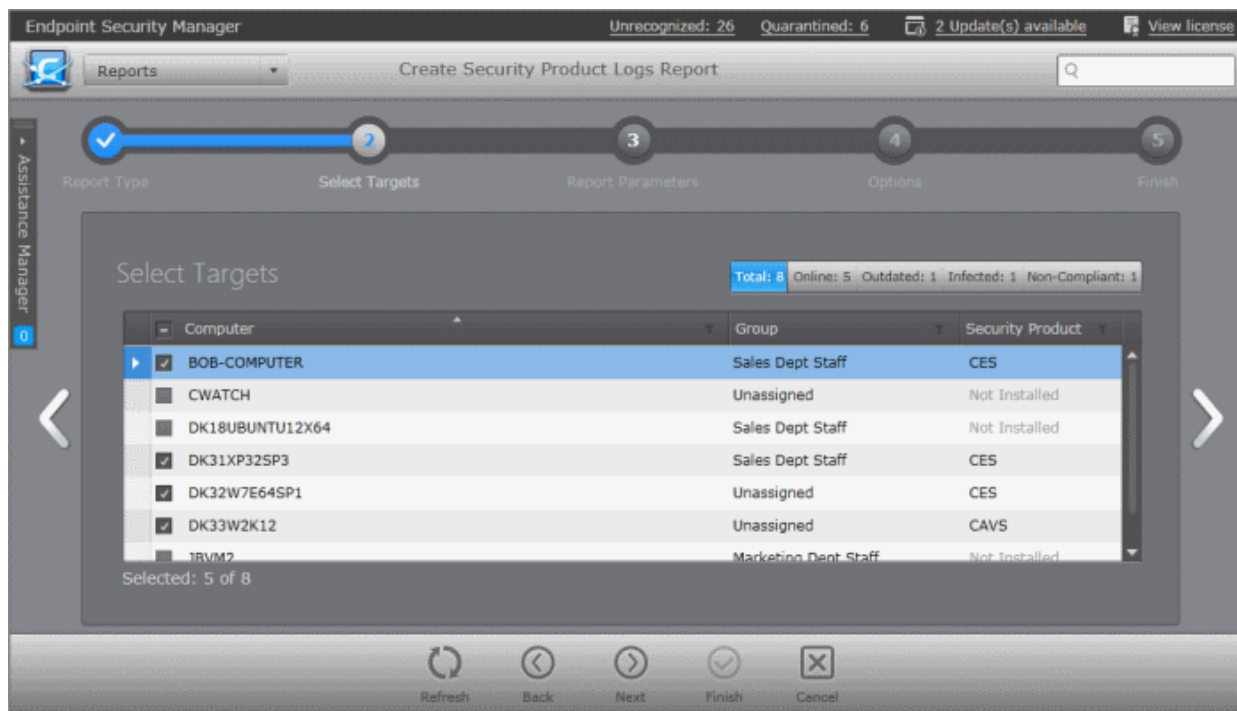
- Select the endpoint(s) for which you wish to generate the Security Product Logs report. The filter options in the header

provides at-a-glance statistics of the computers in the network and allow the administrator to filter the computers based on the criteria. You can also filter the computers by clicking the funnel icon on the column headers.

- Click the right arrow or swipe the screen to the left to move to the next step.

Step 3 - Report Parameters

The next step is to choose the time period, that the report should include the log saved during it.
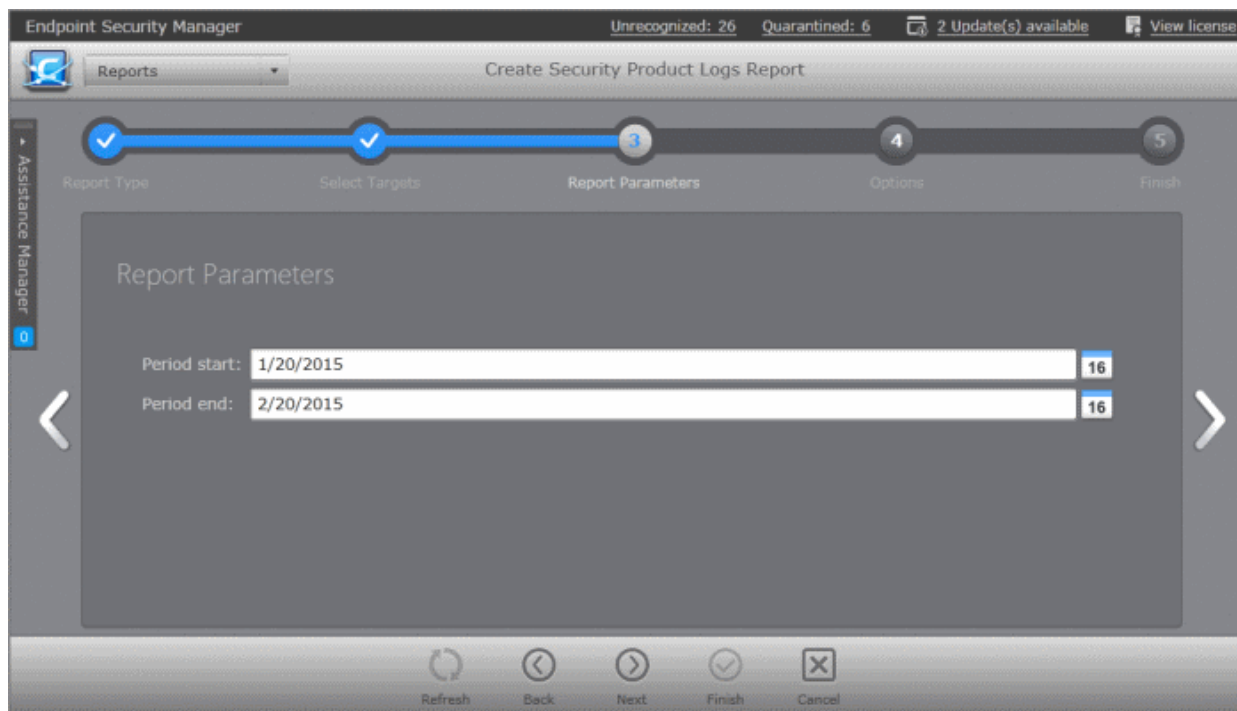
- Specify the period start and end dates in the respective text fields in MM/DD/YYYY format. Alternatively, clicking the calendar icon at the right end of the text box displays a calendar to select the dates.

Step 4 - Options

The fourth step allows you to configure the options for report generation.

- **Generate downloadable report file** - Select this option if you need to print or archive the report. You can choose the printable file to be generated in portable document (.pdf) or spreadsheet (.xls) format. On completion, the report generated can be downloaded to the administrator's computer.
- Select required options.

- Click the 'Finish' icon to start generating the report.

The report generation will be started or added to the queue. The progress will be displayed in the 'Reports' area.

View the Report

The administrator can view the report at anytime after the completion.

To view the report

- Select the report from the list and click 'Open'   from the options at the bottom.

- Double click on the report

    Or

- Right click on the report and choose 'Open' from the right click menu.

The report will contain the log entries for the component selected in step 1, recorded at the target endpoints selected at step 2 for the time period selected in step 3. If more than one computer is selected in step 2, the log reports are given for them one by one.

Examples of:

- **Antivirus Logs Report**
- **Firewall Logs Report** and
- **Defense+ Logs Report**

... are shown below.

Antivirus Logs Report

- The summary bar-graph in the upper portion provides an at-a-glance information of number of different AV events at the selected endpoints.

- Following the graphical summary, details of each AV event detected at each endpoint are displayed as a table.

  Column Descriptions

  - Computer Name - endpoint at which the event was logged.
  - OS Name - Operating system of the endpoint.
  - Malware Name - Name of the malware event that has been detected.
  - Location - Indicates the location where the application detected with a threat is stored.
  - Date - Indicates the date and time of the event.
  - Action - Indicates action taken against the malware through Antivirus.

Click the print icon at the bottom to take print of the report.

Firewall Logs Report
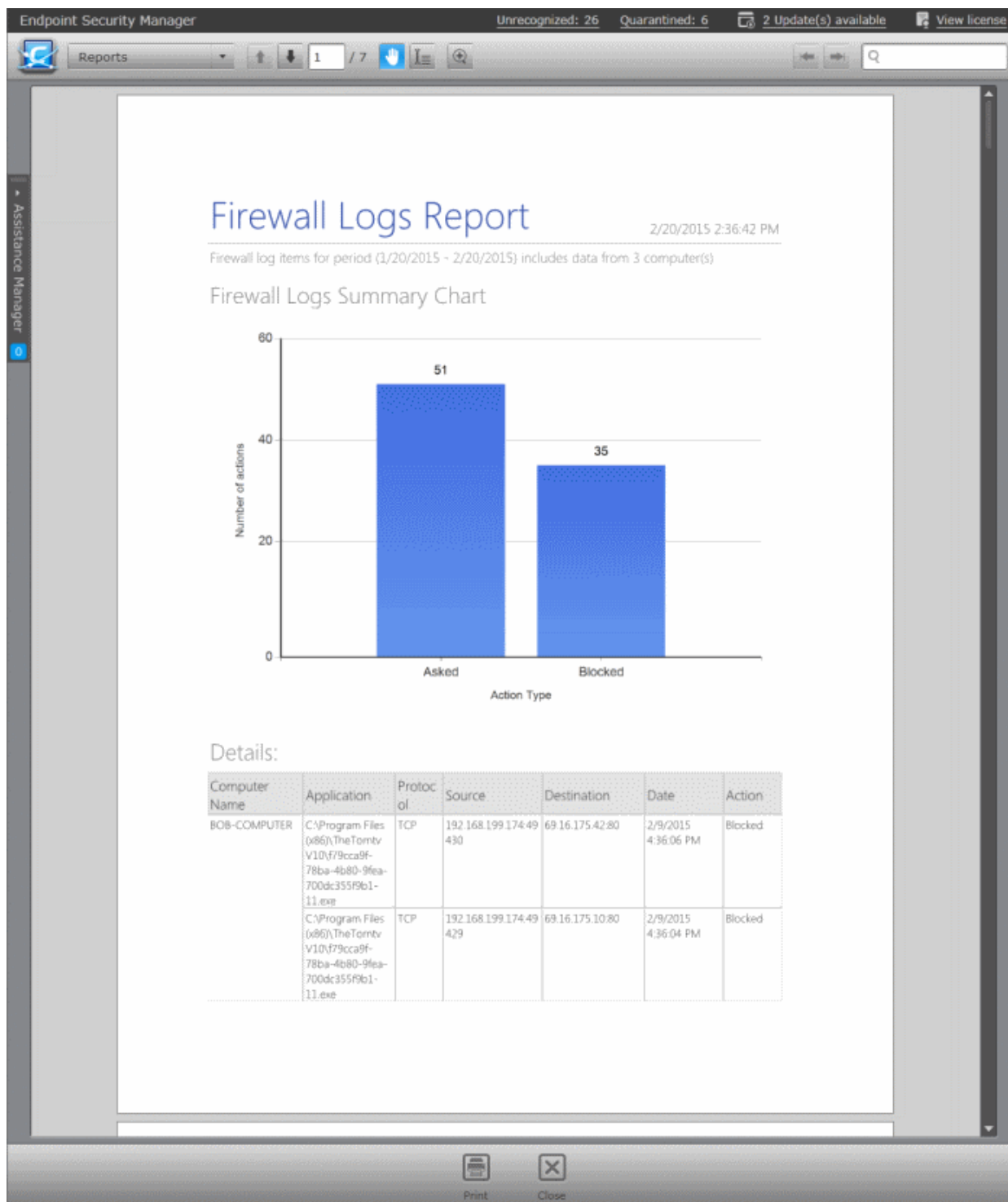
- The summary bar-graph in the upper portion provides 'at-a-glance' information about the number of different Firewall events at the selected endpoints.

- Following the graphical summary, details of each Firewall event detected at each endpoint are displayed as a table.

Column Descriptions

- Computer Name - Endpoint at which the event was logged.
- Protocol - The protocol of the connection attempt.
- Application - Name of the application or program that initiated the connection attempt.
- Source - The source IP and port combination of the connection attempt.
- Destination - The destination IP and port combination of the connection attempt.

- Date - Indicates the date and time of the event.
- Action - Indicates action taken against the connection attempt by the firewall.

Click the print icon [   ] at the bottom to take print of the report.

Defense+ Logs Report

- The summary bar-graph in the upper portion provides an at-a-glance information of number of different Defense+ events logged at the selected endpoints.
- Following the graphical summary, details of each Defense+ event detected at each endpoint are displayed as a table.

    Column Descriptions

    - Computer Name - Endpoint at which the event was logged.

- Application - Indicates which application or process propagated the event.
- Target - Represents the location of the target file.
- Date - Contains precise details of the date and time of the access attempt.
- Action - Indicates action taken by CES/CAS against the access attempt.

Click the print icon at the bottom to take print of the report.

Downloading the Report

If the administrator had opted for generating a downloadable report, it can be downloaded by selecting the Report in the 'Reports' area and clicking the download icon at the bottom or clicking the report file icon (or) under the Report File column.

12.5. Computer Details Report

The 'Computer Details' report provides information on the hardware configuration, network addresses, Operating System (OS) installed and installed programs (optional) of the selected target computer(s) in several pages. It also gives a comparison on OS versions installed, if you select multiple endpoints.

To generate a Computer Details report

- Open the 'Reports' area by choosing 'Reports' from the drop-down at the top left.

- Click 'Add' and choose 'Computer Details Report'. The 'Create Computer Details Report' wizard will start.
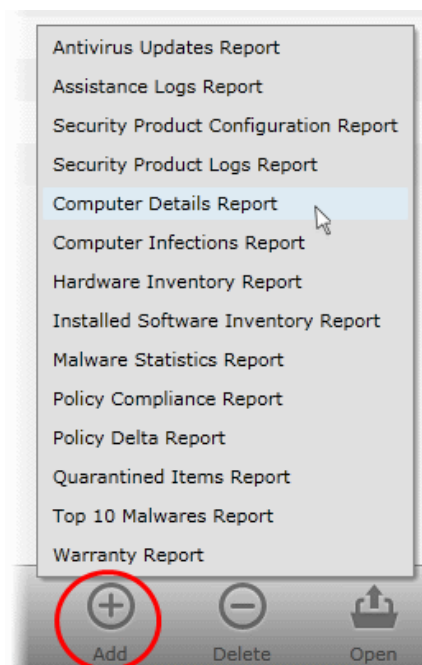
Step 1 - Selecting Targets

The list of all the endpoint computers connected to CESM is displayed.
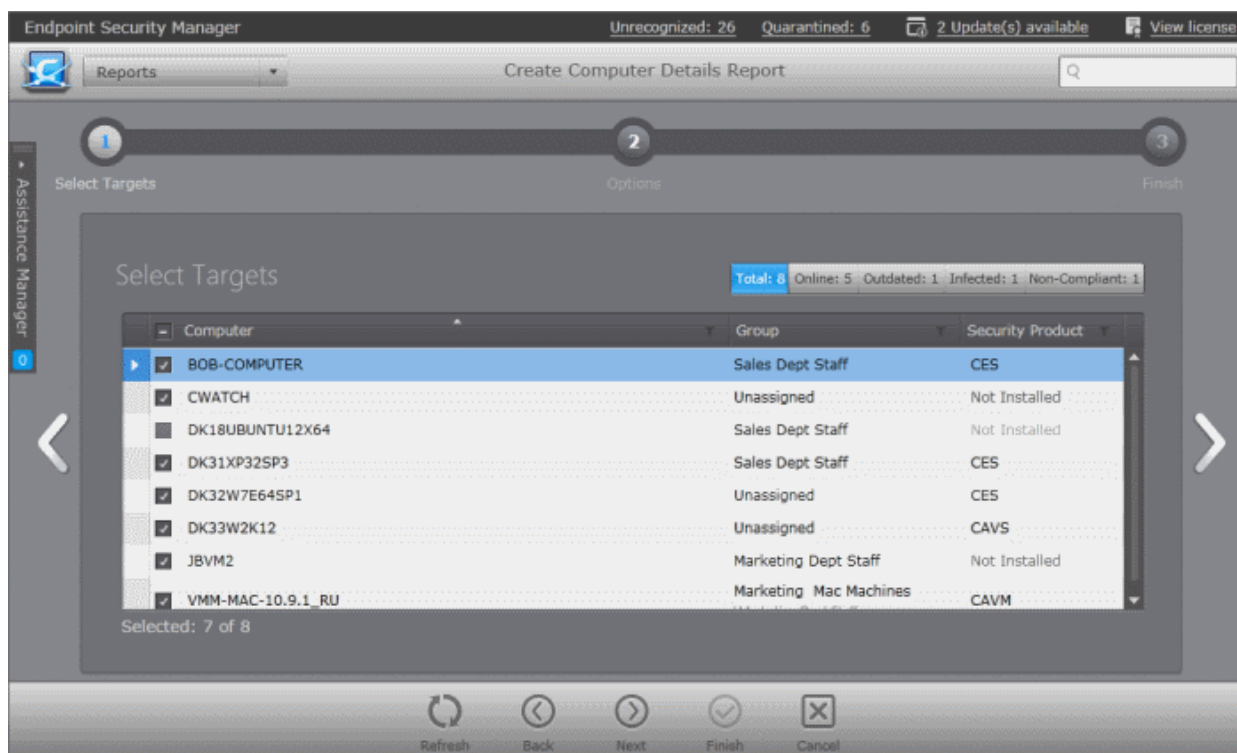
- Select the endpoint(s) for which you wish to generate the Computer Details report. The filter options in the header provides at-a-glance statistics of the computers in the network and allow the administrator to filter the computers based on the criteria. You can also filter the computers by clicking the funnel icon on the column headers.

- Click the right arrow or swipe the screen to the left to move to the next step.

Step 2 - Options

The second step allows you to configure the options for report generation.

- **Include software details into report** - Select this option if you want the details on the software installed on the target computer(s) to be included in the report.

- **Generate downloadable report file** - Select this option if you need to print or archive the report. You can choose the printable file to be generated in portable document (.pdf) or spreadsheet (.xls) format. On completion, the report generated can downloaded to the administrator's computer.

- Select required options

- Click the 'Finish' icon to start generating the report.

The report generation will be started or added to the queue. The progress will be displayed in the 'Reports' area.

View the Report
The administrator can view the report at anytime after the completion.

To view the report

- Select the report from the list and click 'Open'   from the options at the bottom.

- Double click on the report

    Or

- Right click on the report and choose 'Open' from the right click menu.

The report contains the hardware, software details of the endpoints selected in step 1 in several pages depending on the number of endpoints chosen.
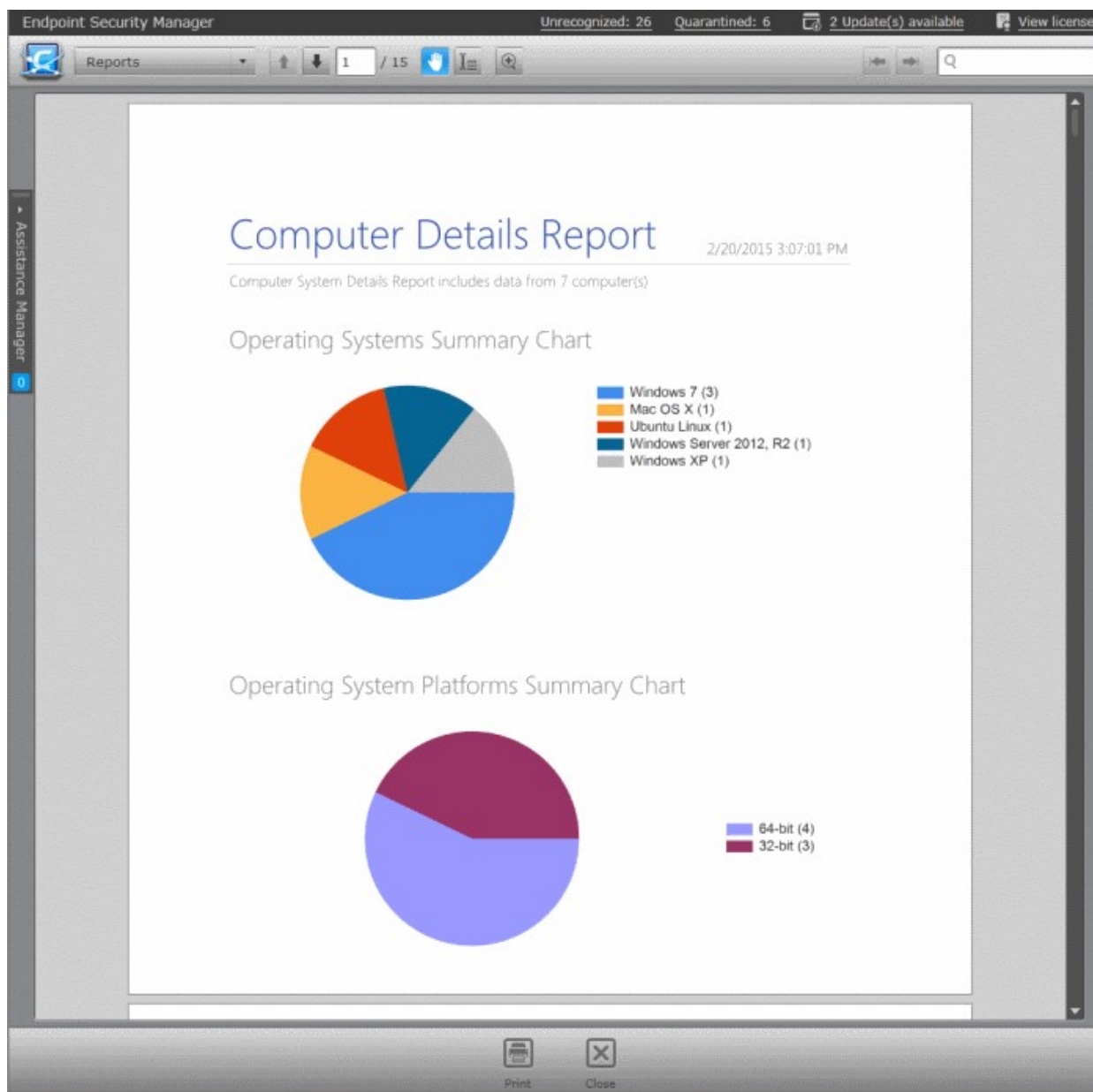
- The first page of the report contains pie charts providing a comparison of versions of Operating Systems (OS) of the selected target endpoints.

- The successive pages contains:

    - General Information including computer name, logged-on user and so on

    - Network Information including DNS name, domain, MAC address and so on

    - Operating System/Hardware Information

    - Installed Software … of each endpoint.

Click the print icon ![print icon] at the bottom to take print of the report.

Downloading the Report

If the administrator had opted for generating a downloadable report, it can be downloaded by selecting the Report in the

'Reports' area and clicking the download icon ![download icon] at the bottom or clicking the report file icon (![excel icon] or ![pdf icon]) under the

Report File column.

12.6. Computer Infections Report

The 'Computer Infections' report provides information on the number of target computers infected by malware. It details the malware detected by AV scans that have not been successfully handled (deleted, disinfected or quarantined) by the local installation of CES/CAS/CAVM.

To generate a Computer Infections report

- Open the 'Reports' area by choosing 'Reports' from the drop-down at the top left.

- Click 'Add' and choose 'Computer Infections Report'. The 'Create Computer Infections Report' wizard will start.
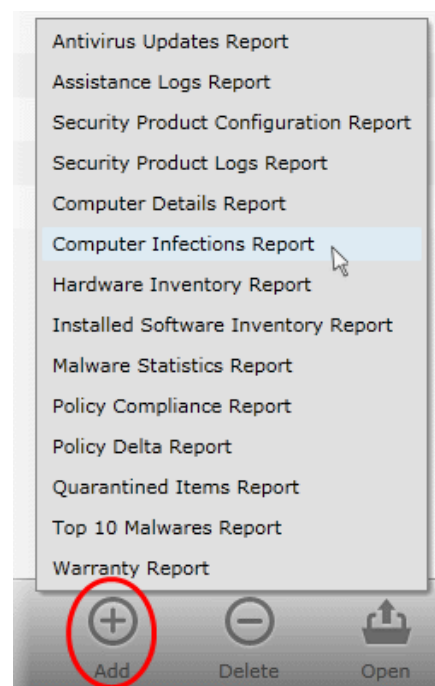
Step 1 - Selecting Targets

The list of all the endpoint computers connected to CESM is displayed.
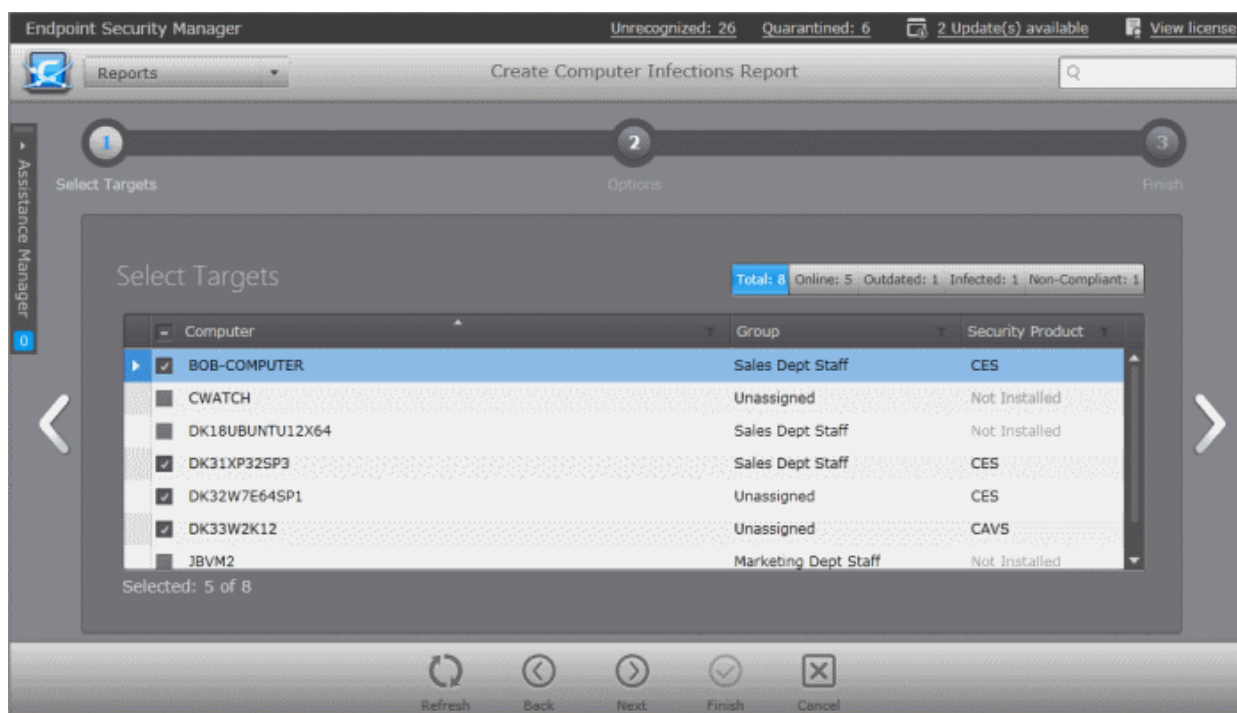
- Select the endpoint(s) for which you wish to generate the Computer Infections report. The filter options in the header provides at-a-glance statistics of the computers in the network and allow the administrator to filter the computers based on the criteria. You can also filter the computers by clicking the funnel icon on the column headers.

- Click the right arrow or swipe the screen to the left to move to the next step.

Step 2 - Options

The second step allows you to configure the options for report generation.

- • **Generate downloadable report file** - Select this option if you need to print or archive the report. You can choose the printable file to be generated in portable document (.pdf) or spreadsheet (.xls) format. On completion, the report generated can downloaded to the administrator's computer.

- • Select required options.

- • Click the 'Finish' icon to start generating the report.

The report generation will be started or added to the queue. The progress will be displayed in the 'Reports' area.

View the Report

The administrator can view the report at anytime after the completion.

To view the report

- • Select the report from the list and click 'Open' from the options at the bottom.

- • Double click on the report

    Or

- • Right click on the report and choose 'Open' from the right click menu.

- The report contains a pie chart showing the number of endpoints that are affected/not affected by malware.
- Following this is a list of affected computers along with their IP addresses, online/offline statuses and the name and location of malware detected on that computer.

Click the print icon at the bottom to take print of the report.

Downloading the Report

If the administrator had opted for generating a downloadable report, it can be downloaded by selecting the Report in the

'Reports' area and clicking the download icon at the bottom or clicking the report file icon (or) under the Report File column.

12.7.　　Hardware Inventory Report

The Hardware Inventory report provides complete details about the target endpoint(s) such as name of the computer, its IP address, since when the endpoint(s) are managed by CESM, the domain/workgroup they belong, MAC address, CPU, service pack and more.
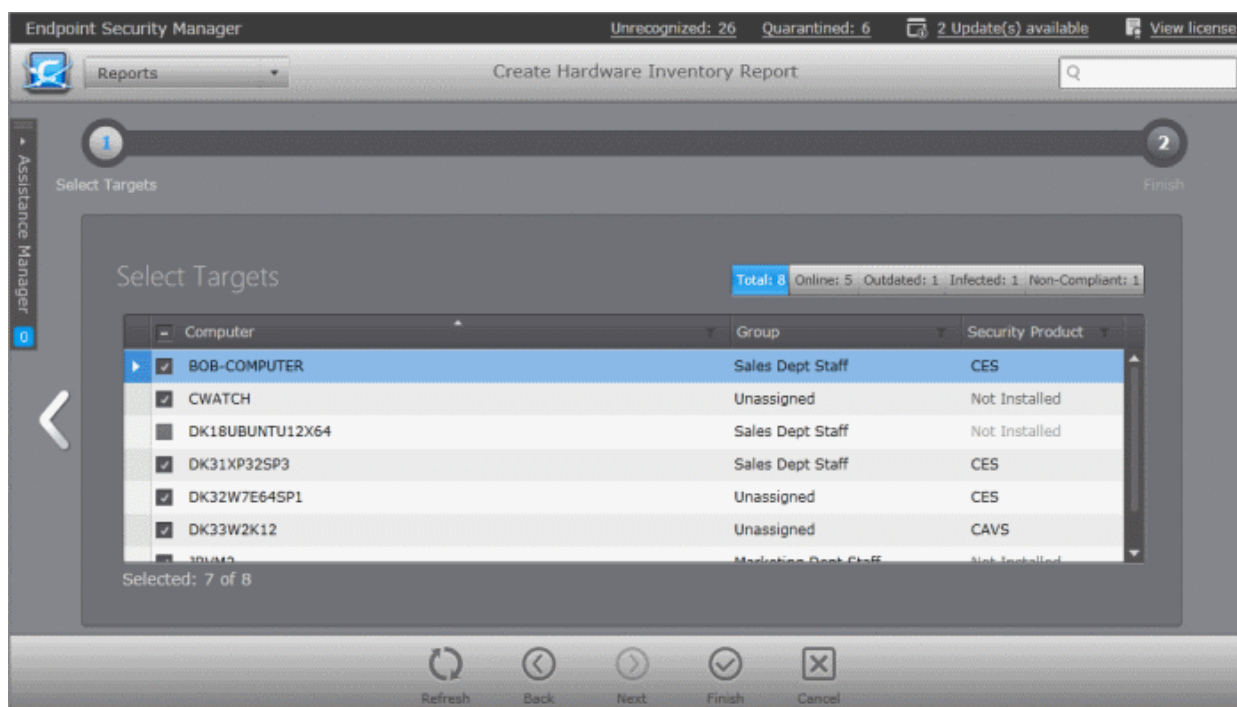
To generate a Hardware Inventory report

- Open the 'Reports' area by choosing 'Reports' from the drop-down at the top left.

- Click 'Add' and choose 'Hardware Inventory Report'. The 'Create Hardware Inventory Report' wizard will start.
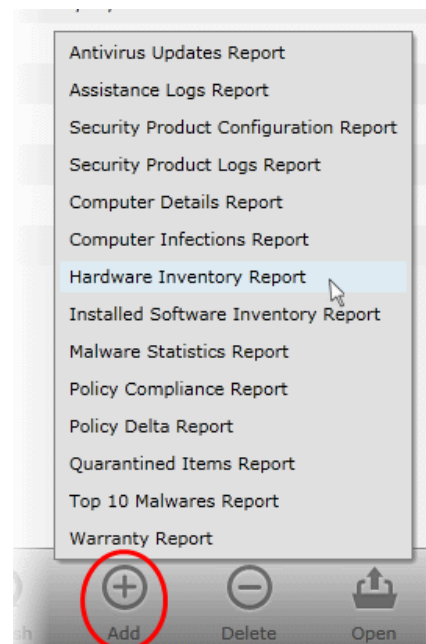
Step 1 - Selecting Targets

The list of all the endpoint computers connected to CESM is displayed.

- Select the endpoint(s) for which you wish to generate the Hardware Inventory report. The filter options in the header provides at-a-glance statistics of the computers in the network and allow the administrator to filter the computers based on the criteria. You can also filter the computers by clicking the funnel icon on the column headers.

- Click the 'Finish' icon to start generating the report.

- The report generation will be started or added to the queue. The progress will be displayed in the 'Reports' area.

Downloading the Report

The report is available in spreadsheet format only and can be downloaded by selecting it in the

'Reports' area and clicking the download icon [icon] at the bottom or clicking the report file icon [icon] under the Report File column.

12.8.   Installed Software Inventory Report

The Installed Software Inventory report provides complete details of software installed at the target endpoint(s) such as name of the software, its version, publisher name including copyright information and when it was installed. The report also contains name of the computer, operating system installed and its version details.
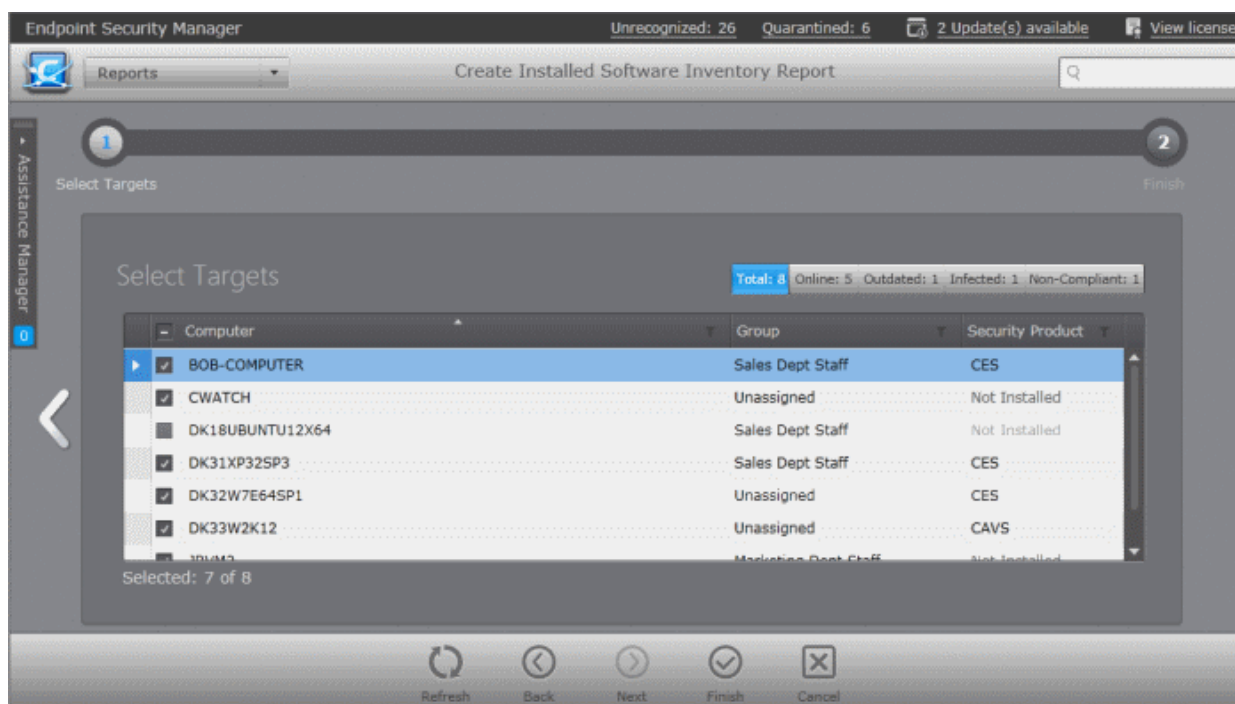
To generate a Installed Software Inventory report

• Open the 'Reports' area by choosing 'Reports' from the drop-down at the top left.

• Click 'Add' and choose 'Installed Software Inventory Report'. The 'Create Installed Software Inventory Report' wizard will start.
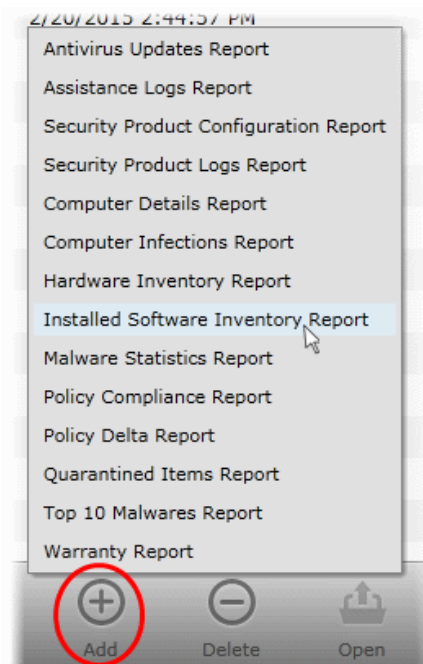
Step 1 - Selecting Targets

The list of all the endpoint computers connected to CESM is displayed.

- Select the endpoint(s) for which you wish to generate the Installed Software Inventory report. The filter options in the header provides at-a-glance statistics of the computers in the network and allow the administrator to filter the computers based on the criteria. You can also filter the computers by clicking the funnel icon on the column headers.

- Click the 'Finish' icon to start generating the report.

- The report generation will be started or added to the queue. The progress will be displayed in the 'Reports' area.

Downloading the Report

The report is available in spreadsheet format only and can be downloaded by selecting it in the

'Reports' area and clicking the download icon [icon] at the bottom or clicking the report file icon [icon] under the Report File column.

12.9. Malware Statistics Report

The Malware Statistics report provides a graphical representation of the total malware identified at the target endpoints and the actions taken against them by the installed security product during a selected period and a list of those malware with details on the target computers from which they are identified. The report enables the administrator to learn the trend of malware attacks that have occurred during a certain period of time.
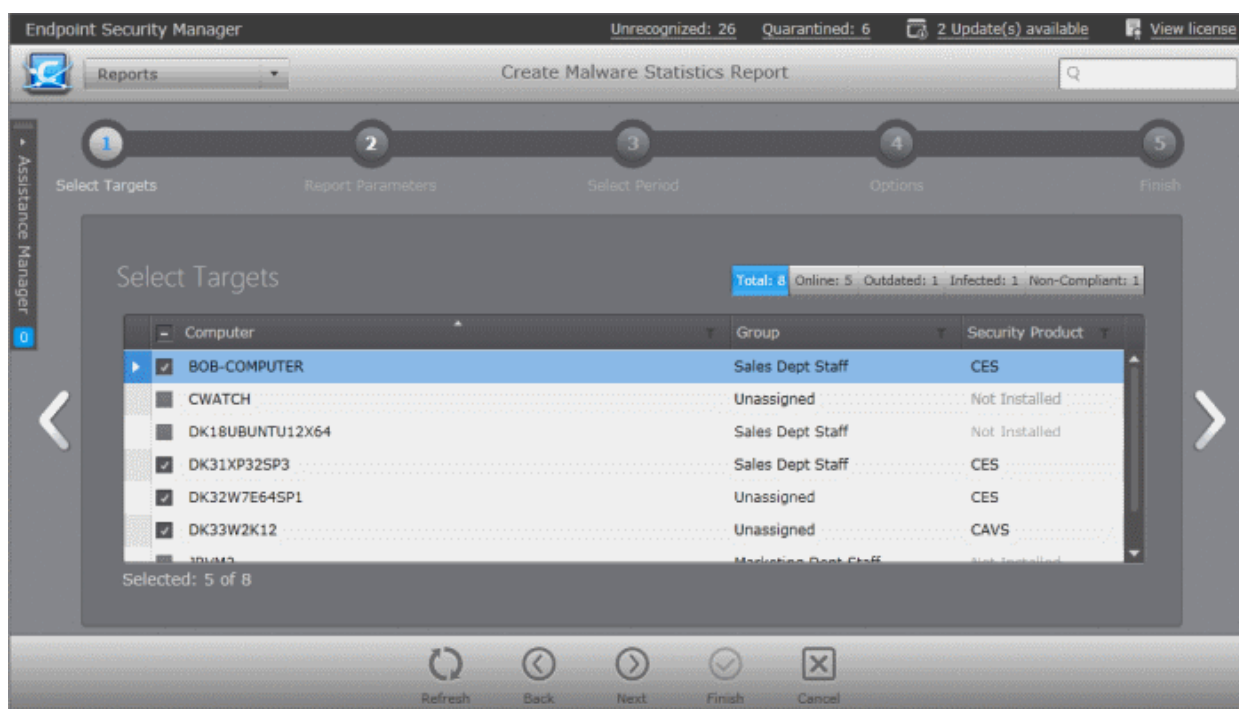
To generate a Malware Statistics report

- Open the 'Reports' area by choosing 'Reports' from the drop-down at the top left.

- Click 'Add' and choose 'Malware Statistics Report'. The 'Create Malware Statistics Report' wizard will start.
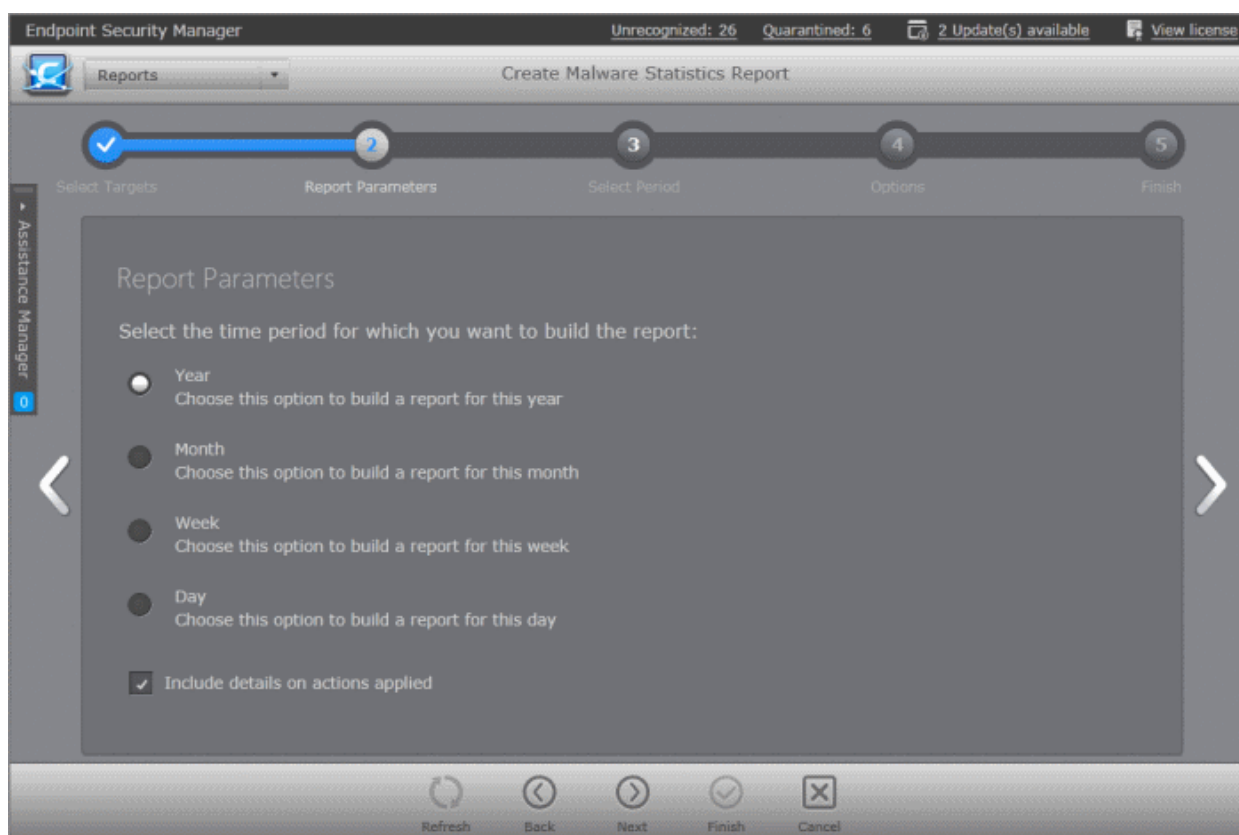
Step 1 - Selecting Targets

The list of all the endpoint computers connected to CESM is displayed.
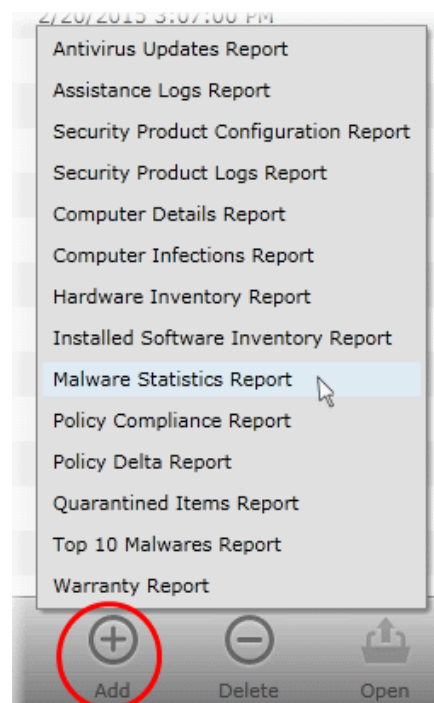
Step 2 - Selecting Report Duration and Options

The next step is to select the period for which you wish the report to be created.

- The time period options available are:
    - Year - Generates statistics from any year (from 1st January YYYY).
    - Month - Generates statistics from the beginning of a selected month in any year (from the 1st of the month). The month can be selected from a calendar in the next step 'Select Period'.

- Week - Generates statistics for any of the weeks between Sunday and Saturday. The week can be selected from a calendar in the next step 'Select Period'.

- Day - Generates statistics for any one day. The day can be selected from a calendar in the next step 'Select Period'.

Select the time period for which you wish to generate the statistics report.

- **Options**:

  - **Include details on actions taken** - Select this option if you want the Malware Statistics report t contain 'Details per computer' that gives details on each and every malware detected, its detection location and time and the action taken on it by the security product at the endpoint(s). The report will contain only graphical representations of the statistics of malware detected from various target computers if this option is not selected.

- Swipe the screen or click the right arrow to move to step 3 - Select Period.

Step 3 - Select Period

The next screen allows you to choose the specific time period as per the selection made in step 2.
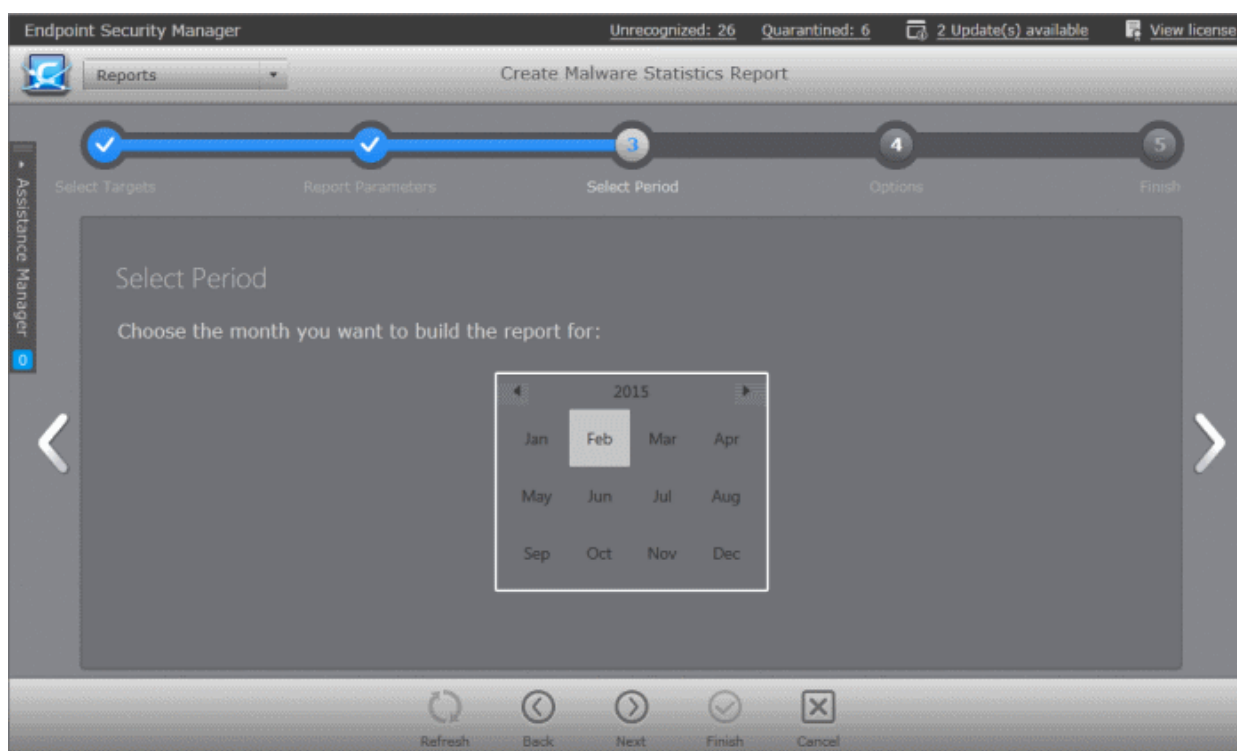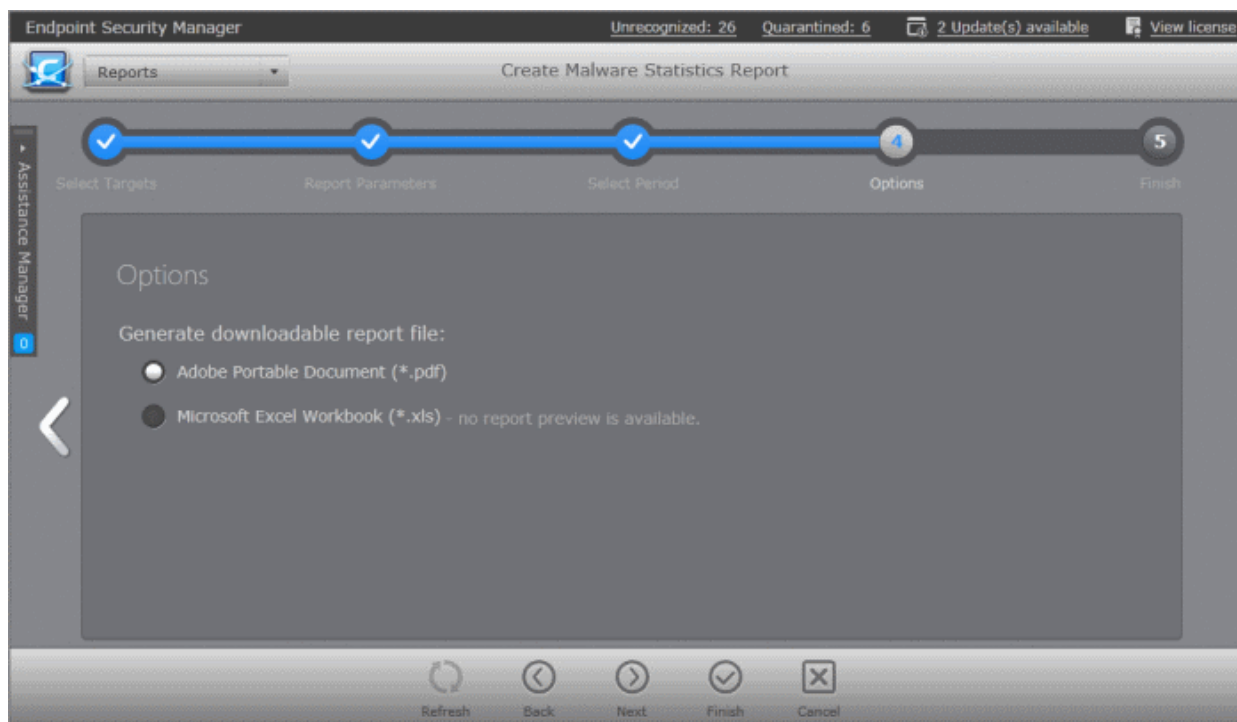

- Swipe the screen or click the right arrow to move to step 4 - Options.

Step 4 - Options

The next step allows you to configure the options for report generation.

- **Generate downloadable report file** - Select this option if you need to print or archive the report. You can choose the printable file to be generated in portable document (.pdf) or spreadsheet (.xls) format. On completion, the report generated can downloaded to the administrator's computer.

- Select required options.

- Click the 'Finish' icon to start generating the report.

The report generation will be started or added to the queue. The progress will be displayed in the 'Reports' area.

View the Report

The administrator can view the report at anytime after the completion.

To view the report

- Select the report from the list and click 'Open' from the options at the bottom.

- Double click on the report

  Or

- Right click on the report and choose 'Open' from the right click menu.

The report will contain a graphical representation malware statistics of the selected target computers for the selected time period. If the option 'Include details on actions taken' is chosen in step 2, the report will also contain 'Details per Computer' with granular details on the malware found at each endpoint and the action taken against them.

**Example 1 - Malware Statistics only**:
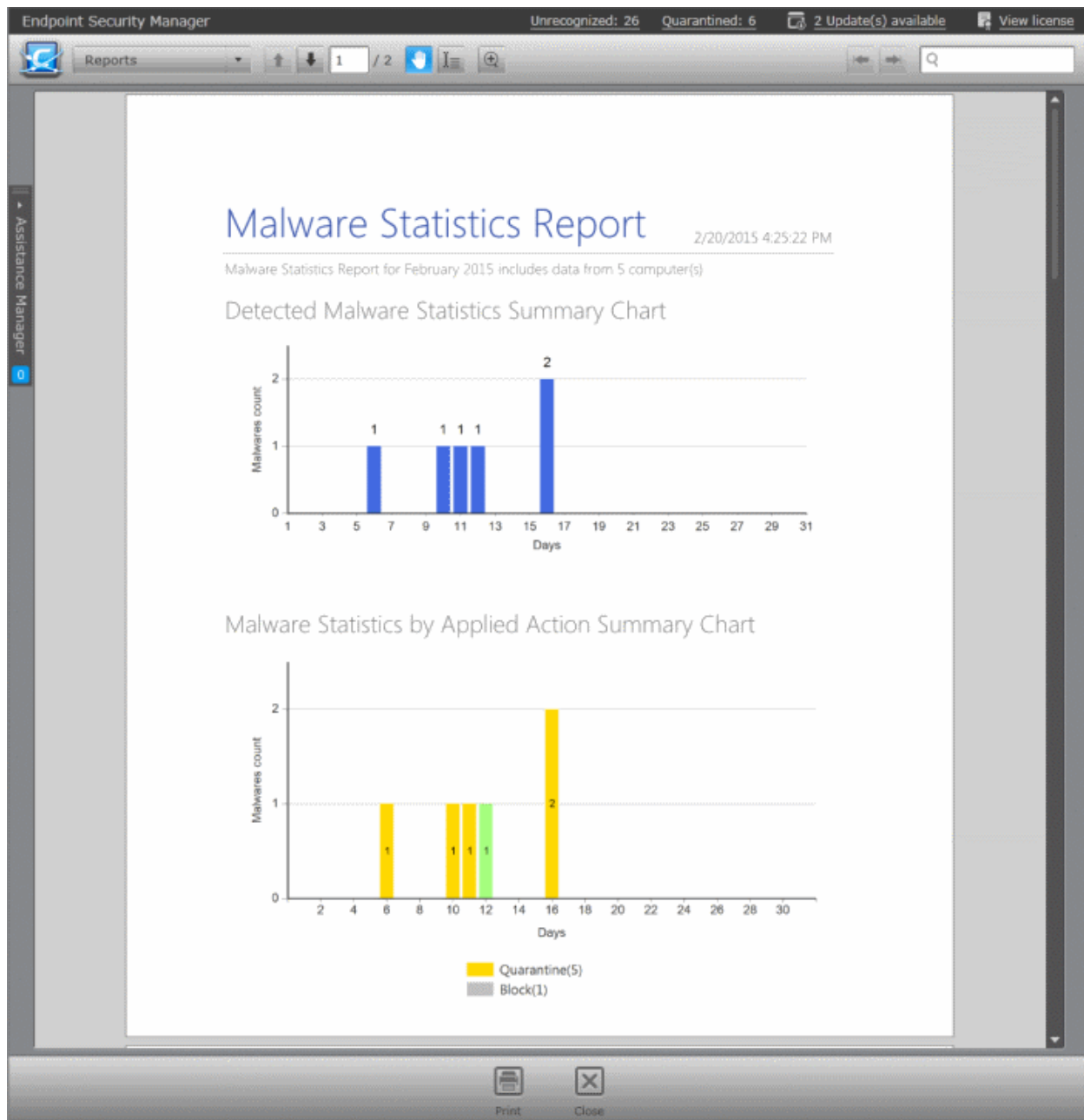
'Deleted', 'Ignored', 'Ask' and 'Quarantined' are the decisions taken by the security product in reaction to each piece of detected malware. The first chart indicates that a total of malware alerts were generated in the time period. The 2nd chart breaks down 10 alerts by the decisions taken by the security product.
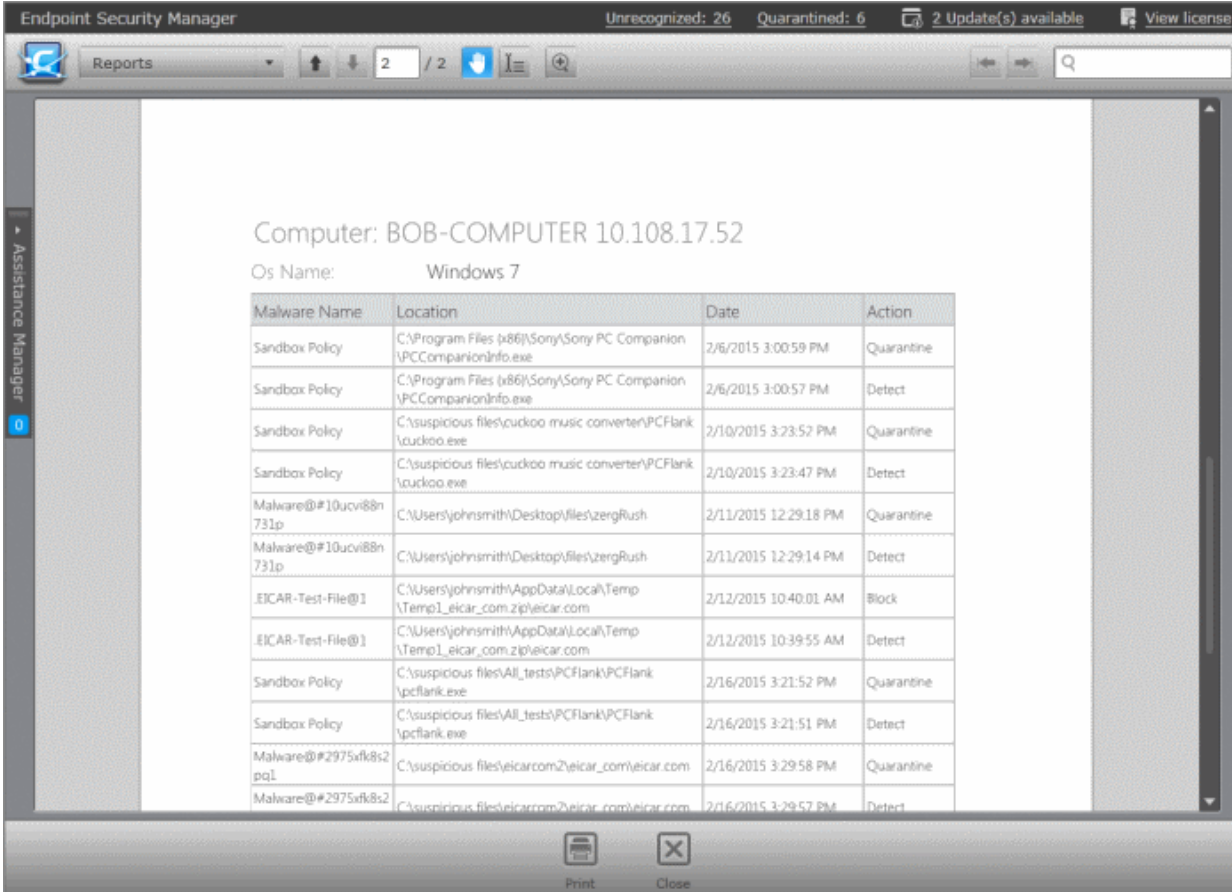
- Click the print icon at the bottom to take print of the report.

Example 2 - Malware Statistics report with Details per Computer:

The screenshot on the next page shows an example of 'Malware Statistics' Detailed Report. The detailed report shows the comparison graphs and details on the malware identified from the selected endpoints.
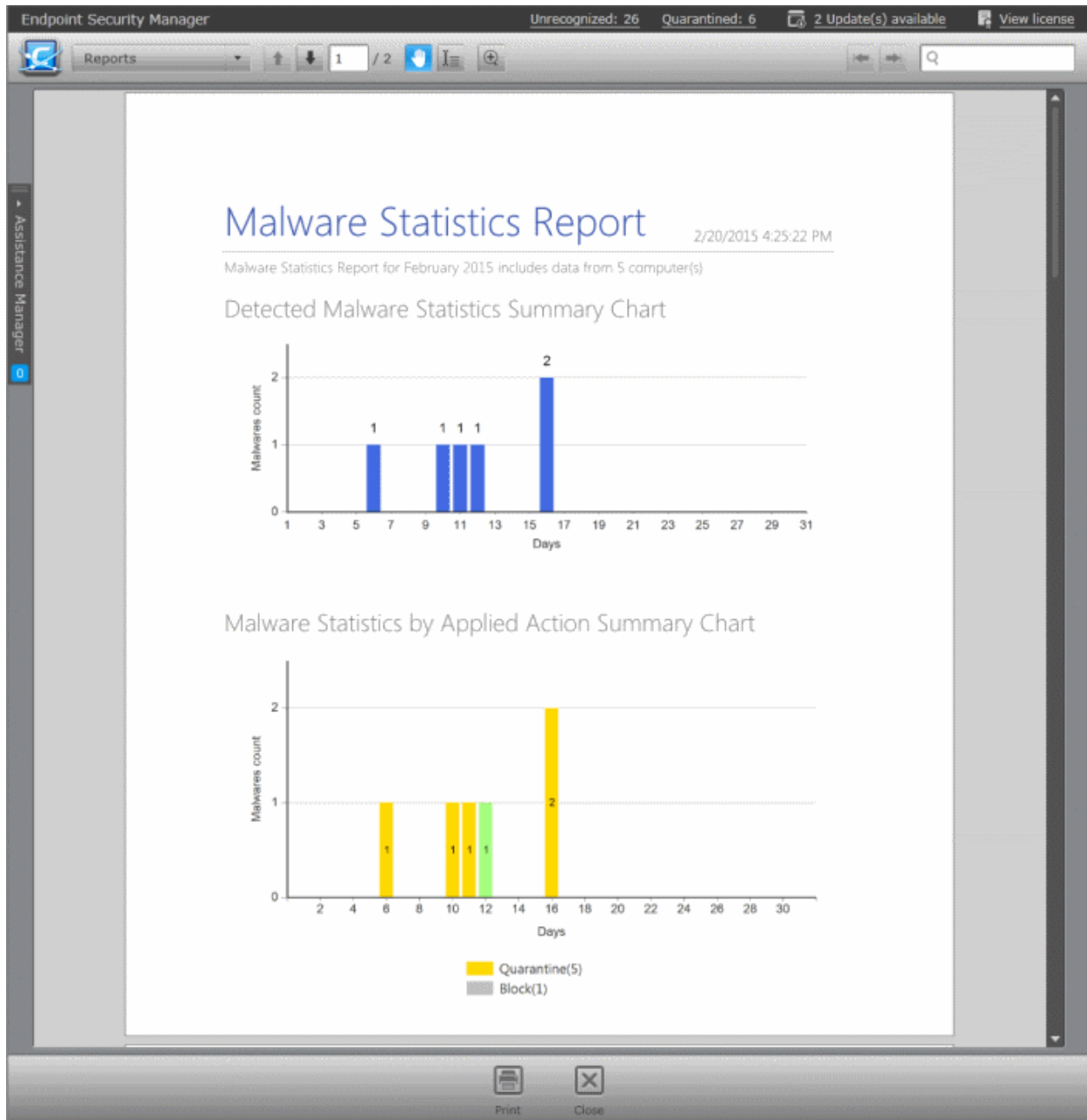
The first page shows the comparison graphs and the successive pages show details of each malware identified at each of the selected endpoint and action against it.

- Click the print icon at the bottom to take print of the report.

Downloading the Report

If the administrator had opted for generating a downloadable report, it can be downloaded by selecting the Report in the 'Reports' area and clicking the download icon at the bottom or clicking the report file icon (or) under the Report File column.

12.10.   Policy Compliance Report

Each target computer in CESM can receive a security policy that dictates the security settings of each of the security product (antivirus, firewall and Defense+ components for Windows OS; antivirus and firewall components for Windows Servers) of CES/CAS installed on it. The CES/CAS installation at the target endpoint will automatically be configured as per the applied policy when CES/CAS is in remote management mode.

If the end-user or the network administrator changes any of the security settings in their local installation of CES/CAS, the computer becomes 'non-compliant' with its designated (or 'applied') policy. But during the next polling time, the agent reapplies the policy automatically so that the the computer's status will return to 'compliant'. The administrator can also return a computer to 'compliant' state by reapplying the policy from the **Computer Properties > Advanced pane**.

The target computers applied with the 'Locally Configured' policy will always be retained in 'Compliant' status as CESM does not enforce any policy compliance on to them. Also, 'Locally Configured' policy allows the user to change the CES/CAS configuration settings locally and stores the changes dynamically. If the target computer is switched back to Local Configuration policy from any other CESM applied security policy, the last stored configuration is restored on to it.

Administrators are advised to regularly check whether imported computers are compliant with their assigned policy. Non-compliance can indicate unauthorized changes to power and/or device and/or CES/CAS security settings.

The Policy Compliance report provides a summary of the compliance of the target computers and details of computers which are non-compliant to the policy. The report also enables administrators to remediate non-compliant computers by resetting their CES/CAS security configuration and thus returning them to 'Compliant' status.

To generate a Policy Compliance report

• Open the 'Reports' area by choosing 'Reports' from the drop-down at the top left.

• Click 'Add' and choose 'Policy Compliance Report'. The 'Create Policy Compliance Report' wizard will start.
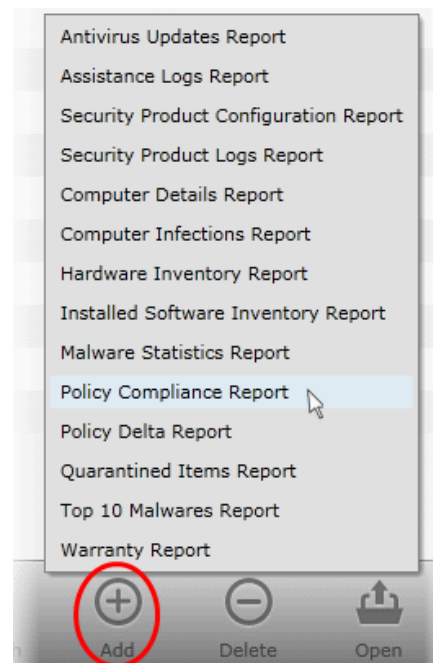
Step 1 - Selecting Targets

The list of all the endpoint computers connected to CESM is displayed.
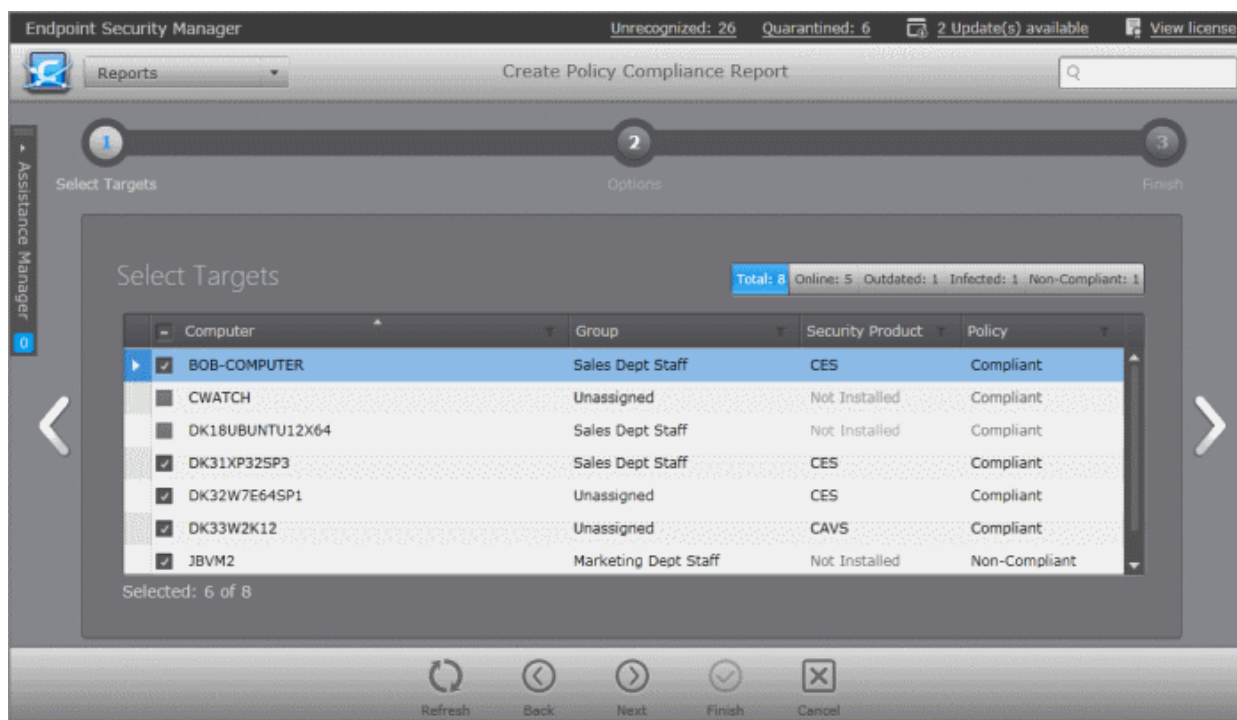
• Select the endpoint(s) for which you wish to generate the Policy Compliance report. The filter options in the header provides at-a-glance statistics of the computers in the network and allow the administrator to filter the computers based on the criteria. You can also filter the computers by clicking the funnel icon on the column headers.

• Click the right arrow or swipe the screen to the left to move to the next step.

Step 2 - Options

The second step allows you to configure the options for report generation.

• **Include only non-compliant computers** - The report will contains details of only the computers that are non-compliant.

- **Generate downloadable report file** - Select this option if you need to print or archive the report. You can choose the printable file to be generated in portable document (.pdf) or spreadsheet (.xls) format. On completion, the report generated can downloaded to the administrator's computer.
- Select required options.

- Click the 'Finish' icon to start generating the report.

The report generation will be started or added to the queue. The progress will be displayed in the 'Reports' area.

View the Report

The administrator can view the report at anytime after the completion.

To view the report

- Select the report from the list and click 'Open'   from the options at the bottom.

- Double click on the report

  Or

- Right click on the report and choose 'Open' from the right click menu.

- The first page of the report will contain a summary pie chart providing at-a-glance comparison on numbers of computers that are compliant, non-compliant and are pending to be applied with the policy.

- The following pages contain the details of each computer, with their associated group, IP addresses, applied Policy, compliancy status, last compliancy checked time, when the non-compliant computers went non-compliant.

Click the print icon at the bottom to take print of the report.

Downloading the Report

If the administrator had opted for generating a downloadable report, it can be downloaded by selecting the Report in the 'Reports' area and clicking the download icon at the bottom or clicking the report file icon (or) under the Report File column.

12.11.   Policy Delta Report

The Policy Delta report provides a summary of differences in the configuration of CES/CAS at 'Non-Compliant' endpoints with respect to the security policy applied to them. During report generation, CESM compares two configurations (source policy on the server side and target policy on the endpoint) component by component and provides details on the items that differ from the applied policy. The details in the report are helpful to the administrator for investigating the changes made to CES/CAS settings in the target computer and the reason(s) the computer received its non-compliant status.

To generate a Policy Delta report

- Open the 'Reports' area by choosing 'Reports' from the drop-down at the top left.

- Click 'Add' and choose 'Policy Delta Report'. The 'Create Policy Delta Report' wizard will start.
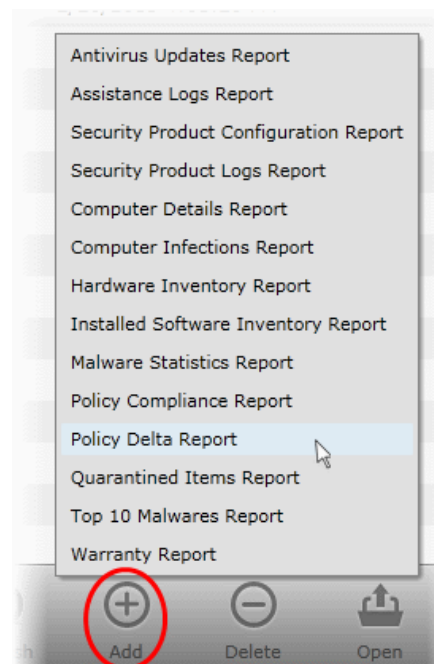
Step 1 - Selecting Targets

The list of all the endpoint computers connected to CESM is displayed.
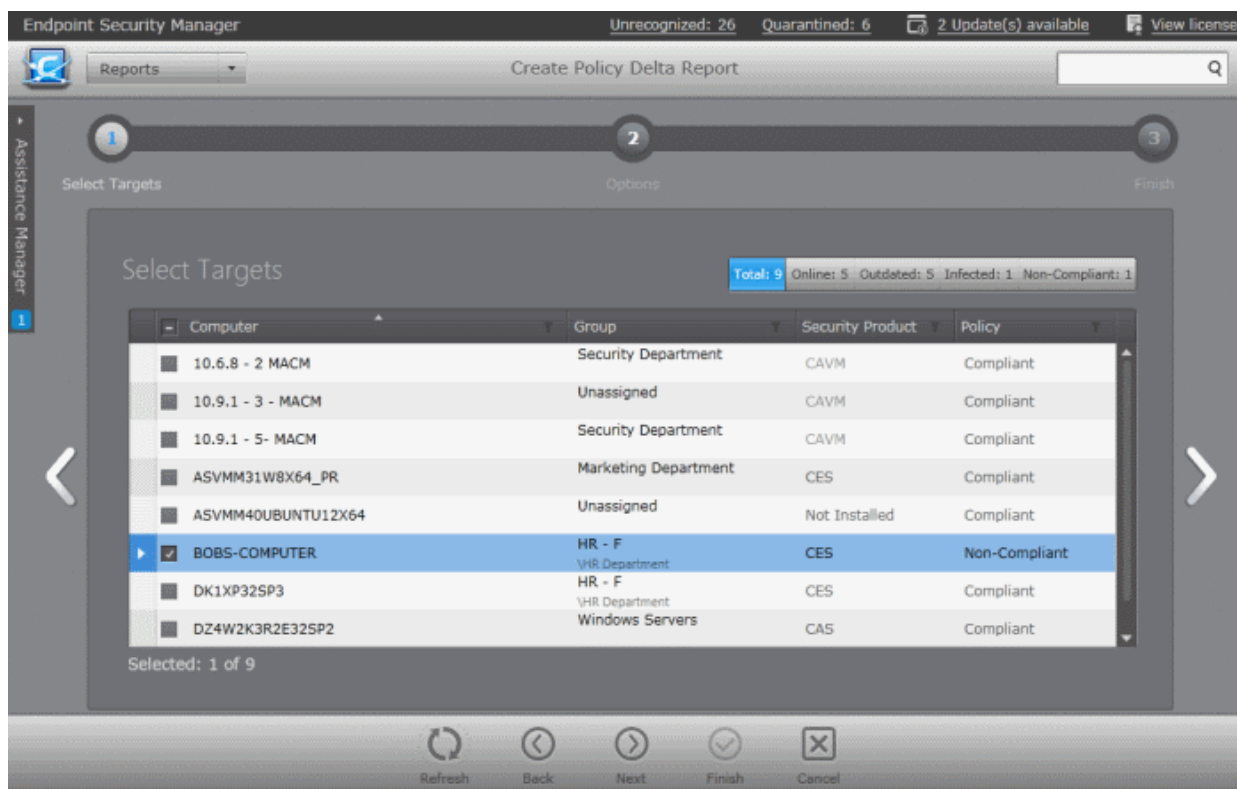
- Select the endpoint(s) for which you wish to generate the Policy Delta report. You can select only endpoints with 'Non-Compliant' status. The filter options in the header provides at-a-glance statistics of the computers in the network and

---

allows administrators to filter computers based on specific criteria. You can also filter by clicking the funnel icon on the column headers.

- Click the right arrow to move to the next step.

Step 2 - Options

The second step allows you to configure the options for report generation.

- **Generate downloadable report file** - Select this option if you need to print or archive the report. You can choose the printable file to be generated in portable document (.pdf) or spreadsheet (.xls) format. On completion, the report generated can downloaded to the administrator's computer.

- Select required options

- Click the 'Finish' icon to start generating the report.

The report generation will be started or added to the queue. The progress will be displayed in the 'Reports' area.

View the Report

The administrator can view the report at anytime after the completion.

To view the report

- Select the report from the list and click 'Open' from the options at the bottom.

- Double click on the report

  Or

- Right click on the report and choose 'Open' from the right click menu.

The first page of the report contains bar-graph summary of changes in components of CES/CAS in the selected computers. This is followed by the list non-compliant computers along with details about the changed components.

- Click the print icon at the bottom to take print of the report.

Downloading the Report

If the administrator had opted for generating a downloadable report, it can be downloaded by selecting the Report in the 'Reports' area and clicking the download icon at the bottom or clicking the report file icon (or) under the Report File column.

12.12. Quarantined Items Report

The 'Quarantined Items' report provides details about malware detected and successfully quarantined on target computers. The report also allows the administrator to remove quarantined items or to restore them to their original locations after analyzing the report.

Note: For the local CES/CAS/CAVM installations at the endpoints to quarantine the threats detected during scanning, the policy applied to them should have been derived from a computer in which CES/CAS/CAVM has been configured to automatically quarantine the threats identified from various scans. For more details on configuring CES/CAS/CAVM refer to the online help guide at **http://help.comodo.com/**.

To generate a Quarantined Items report

- Open the 'Reports' area by choosing 'Reports' from the drop-down at the top left.

- Click 'Add' and choose 'Quarantined Items Report'. The 'Create Quarantined Items Report' wizard will start.
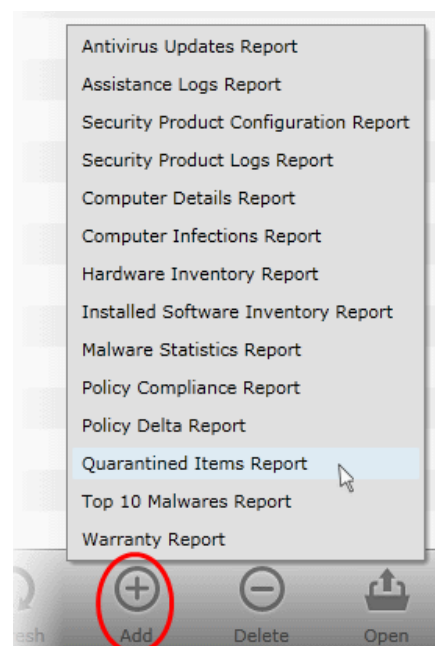
Step 1 - Selecting Targets

The list of all the endpoint computers connected to CESM is displayed.
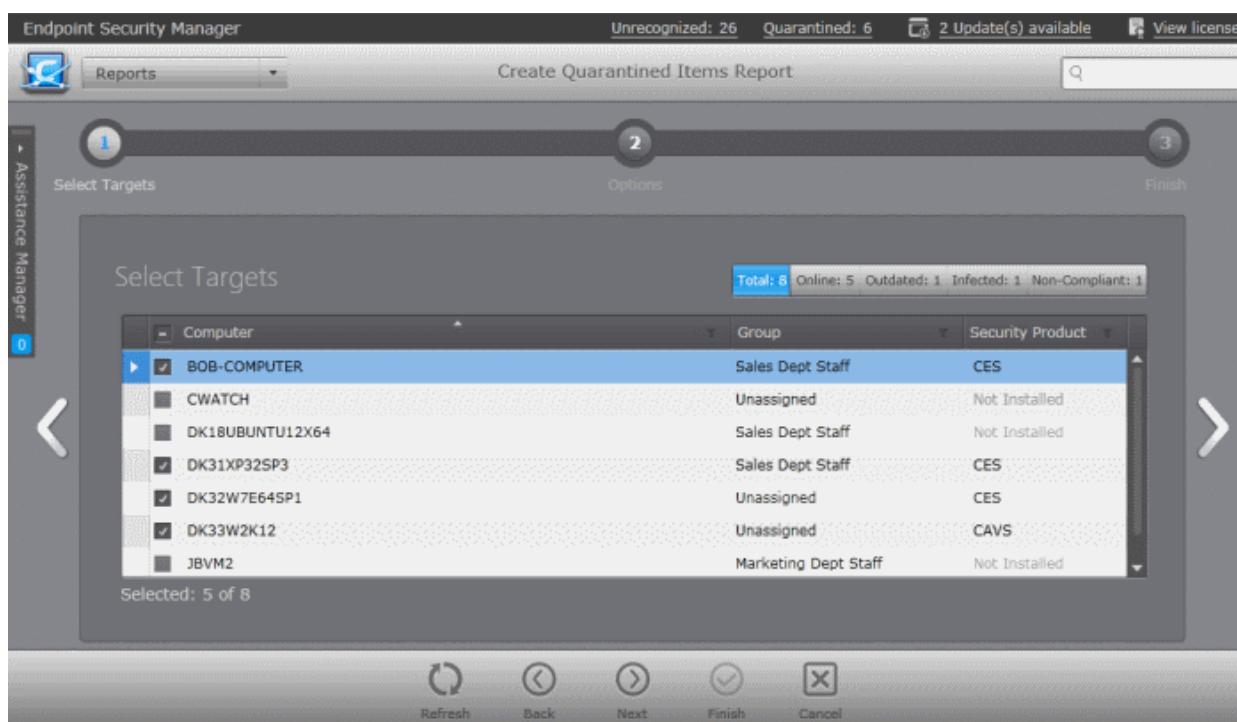
- Select the endpoint(s) for which you wish to generate the Quarantined Items report. The filter options in the header provides at-a-glance statistics of the comput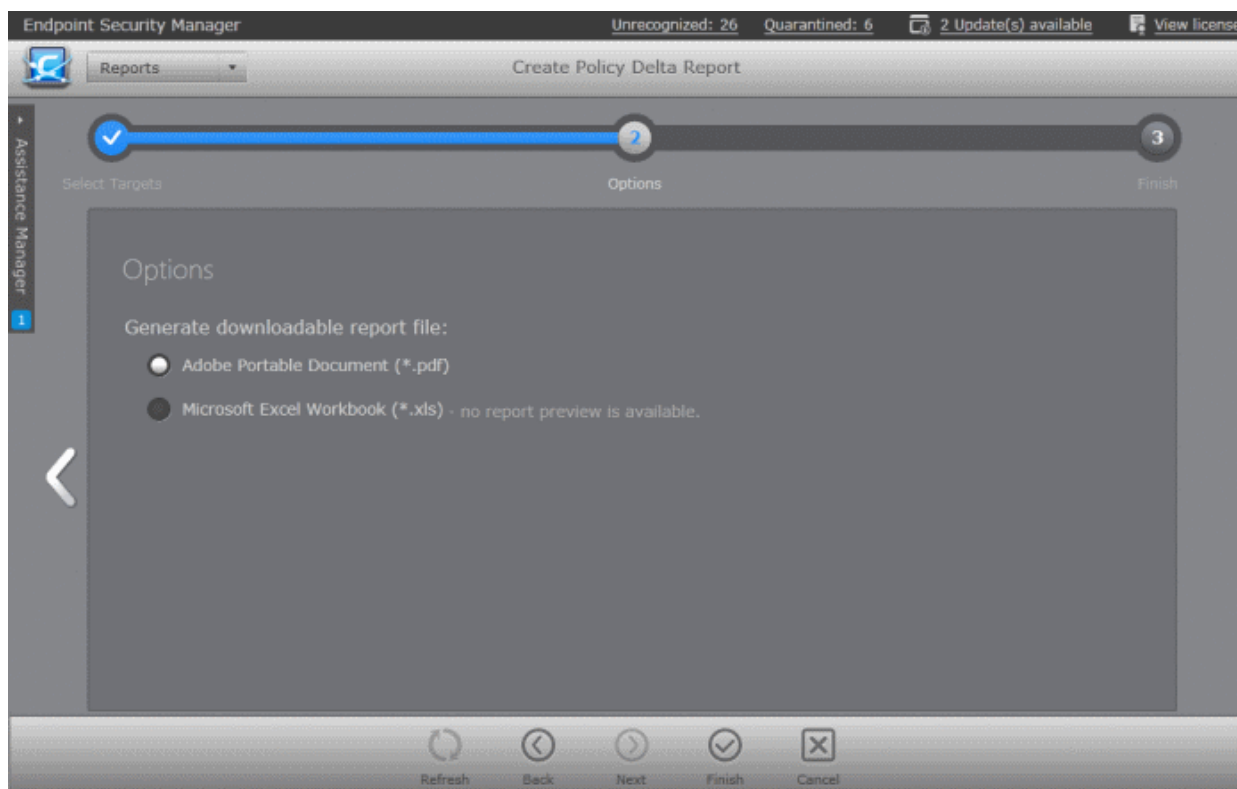ers in the network and allow the administrator to filter the computers based on the criteria. You can also filter the computers by clicking the funnel icon on the column headers.

- Click the right arrow or swipe the screen to the left to move to the next step.

Step 2 - Options

The second step allows you to configure the options for report generation.

- **Generate downloadable report file** - Select this option if you need to print or archive the report. You can choose the printable file to be generated in portable document (.pdf) or spreadsheet (.xls) format. On completion, the report generated can downloaded to the administrator's computer.

- Select required options

- Click the 'Finish' icon to start generating the report.

The report generation will be started or added to the queue. The progress will be displayed in the 'Reports' area.

View the Report

The administrator can view the report at anytime after the completion.

To view the report

- Select the report from the list and click 'Open'   from the options at the bottom.

- Double click on the report

    Or

- Right click on the report and choose 'Open' from the right click menu.

The report contains a pie-chart summary of quarantined items at endpoints of different groups and a table showing the malware quarantined at each endpoint selected in step 1.

- Click the print icon [icon] at the bottom to take print of the report.

Downloading the Report

If the administrator had opted for generating a downloadable report, it can be downloaded by selecting the Report in the

'Reports' area and clicking the download icon [icon] at the bottom or clicking the report file icon ([icon] or [icon]) under the Report File column.

12.13.   Top 10 Malwares Report

The 'Top 10 Malwares' report provides information on the malware that has most affected endpoints on the network. CESM ranks the malware identified at various target computers based on their number of appearances. The 'Top 10 Malwares' report gives details on the malware that are at the first ten positions. The report enables the administrator to learn on what type of malware the network is prone to and to take necessary actions to safeguard the network against them.

To generate a Top 10 Malwares report

-   Open the 'Reports' area by choosing 'Reports' from the drop-down at the top left.

-   Click 'Add' and choose 'Top 10 Malwares Report'. The 'Create Top 10 Malwares Report' wizard will start.
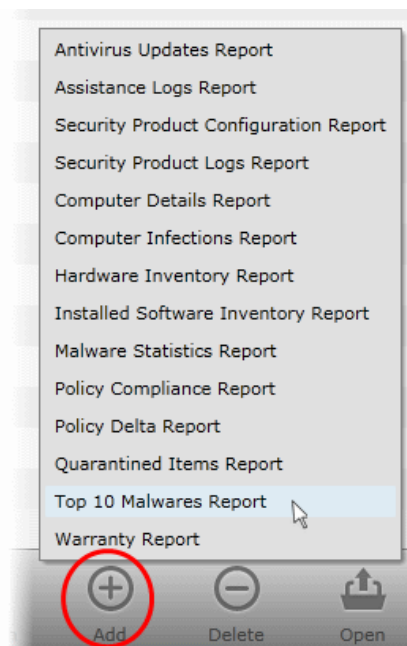
Step 1 - Selecting Targets
The list of all the endpoint computers connected to CESM is displayed.
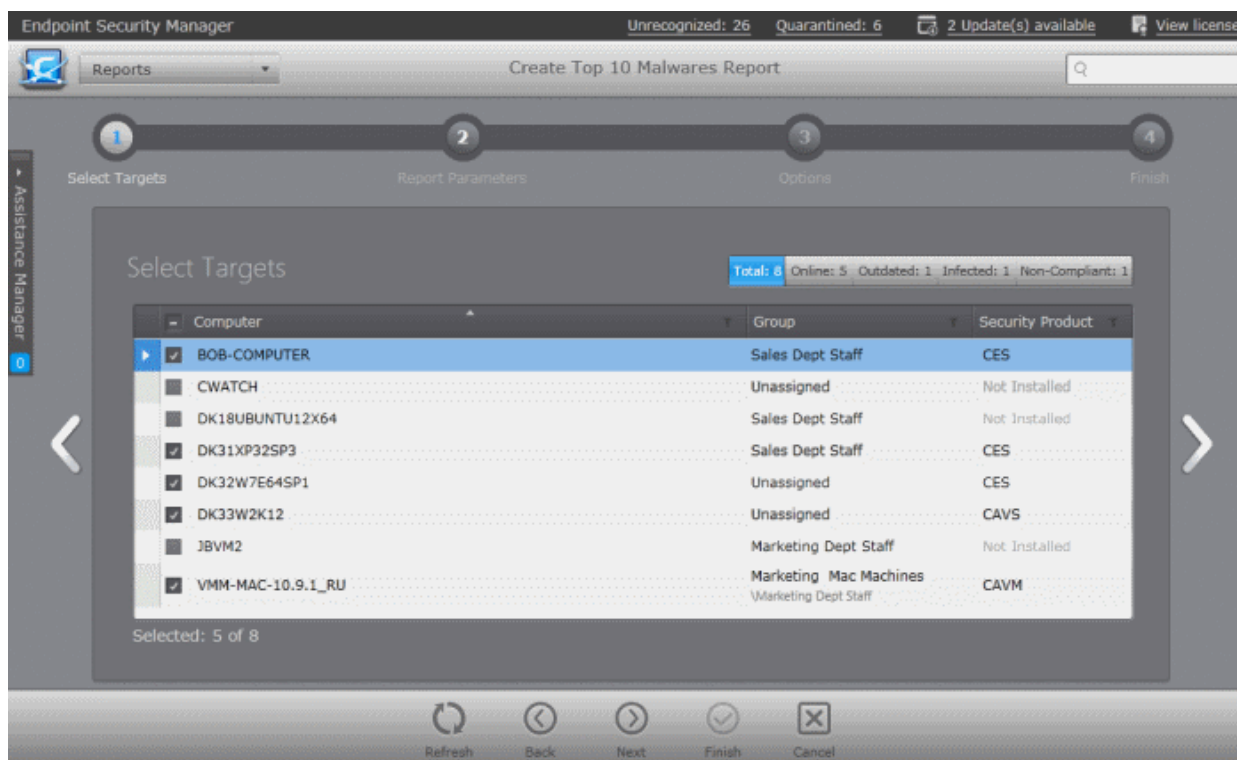
-   Select the endpoint(s) for which you wish to generate the Top 10 Malwares report. The filter options in the header provides at-a-glance statistics of the computers in the network and allow the administrator to filter the computers based on the criteria. You can also filter the computers by clicking the funnel icon on the column headers.

-   Click the right arrow or swipe the screen to the left to move to the next step.

Step 2 - Selecting the Report Period

The next step is to choose the time period that the report should include the top 10 malwares identified.
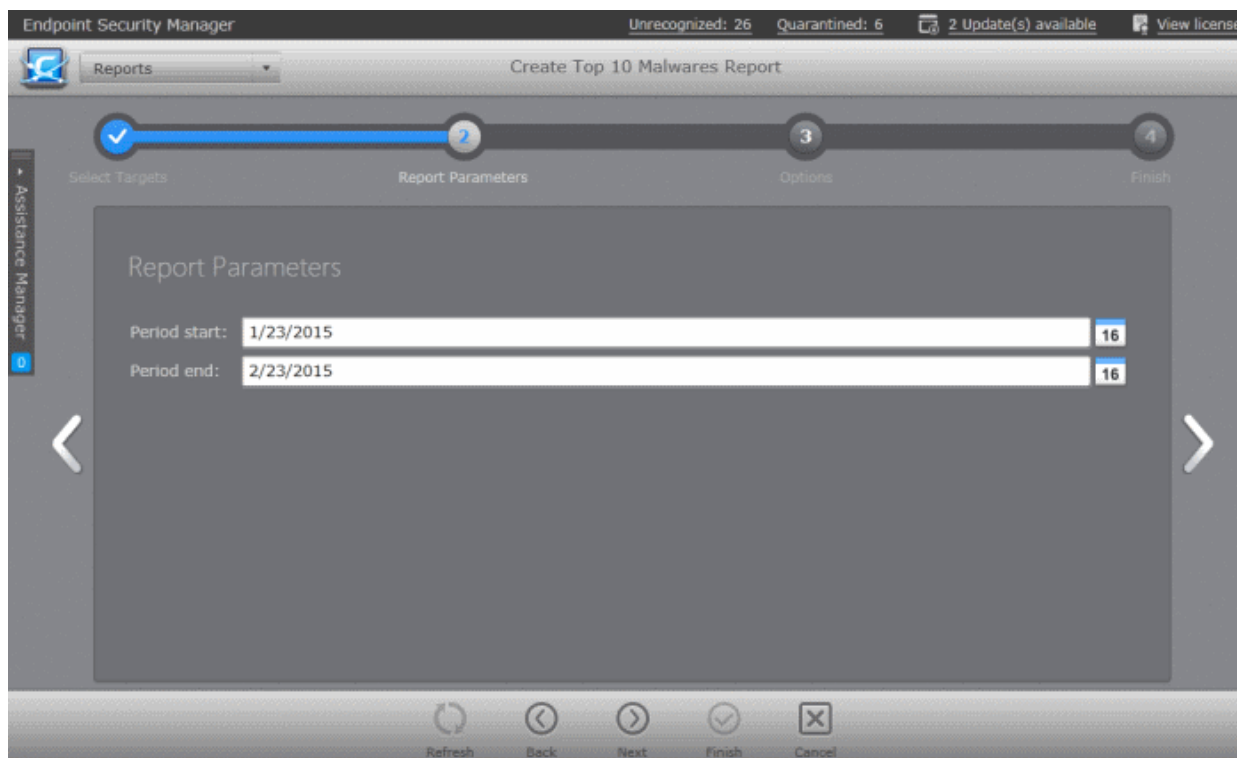
- Specify the period start and end dates in the respective text fields in MM/DD/YYYY format. Alternatively, clicking the calendar icon at the right end of the text box displays a calendar to select the dates.

- Click the right arrow to move to the next step.

Step 3 - Options

The next step allows you to configure the options for report generation.

- **Generate downloadable report file** - Select this option if you need to print or archive the report. You can choose the printable file to be generated in portable document (.pdf) or spreadsheet (.xls) format. On completion, the report generated can be downloaded to the administrator's computer.

- Select required options

- Click the 'Finish' icon to start generating the report.

The report generation will be started or added to the queue. The progress will be displayed in the 'Reports' area.

View the Report

The administrator can view the report at anytime after the completion.

To view the report

- Select the report from the list and click 'Open'   from the options at the bottom.

- Double click on the report

  Or

- Right click on the report and choose 'Open' from the right click menu.

The report contains a bar graph representation of comparison of the malware in terms of their number of occurrences and a list of top 10 malwares with details on number of appearances and the target computer(s) at which the malware is detected.

- Click the print icon at the bottom to take print of the report.

Downloading the Report

If the administrator had opted for generating a downloadable report, it can be downloaded by selecting the Report in the 'Reports' area and clicking the download icon at the bottom or clicking the report file icon (or) under the Report File column.

12.14.   Warranty Report

The Warranty report provides information about the security products installed on endpoints such as CES, CAS, CAVM and their warranty statuses. The report includes name of the computer and its IP, status of security product warranty installed on each endpoint and their activation date, name of the security product installed on endpoints and other details such as AV database, when the AV scan was run and more.


To generate a Warranty report

- Open the 'Reports' area by choosing 'Reports' from the drop-down at the top left.

- Click 'Add' and choose 'Warranty Report'. The 'Create Warranty Report' wizard will start.
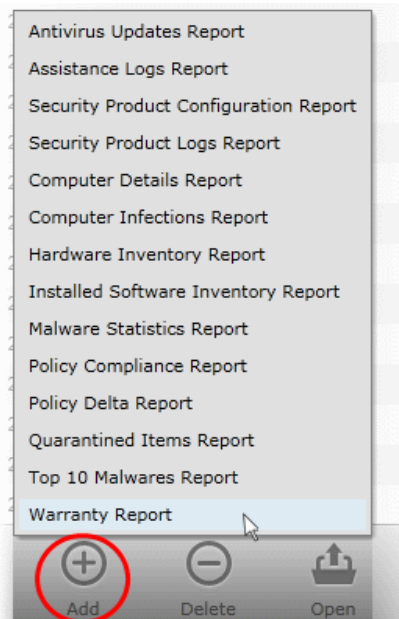

Step 1 - Selecting Targets

The list of all the endpoint computers connected to CESM is displayed.
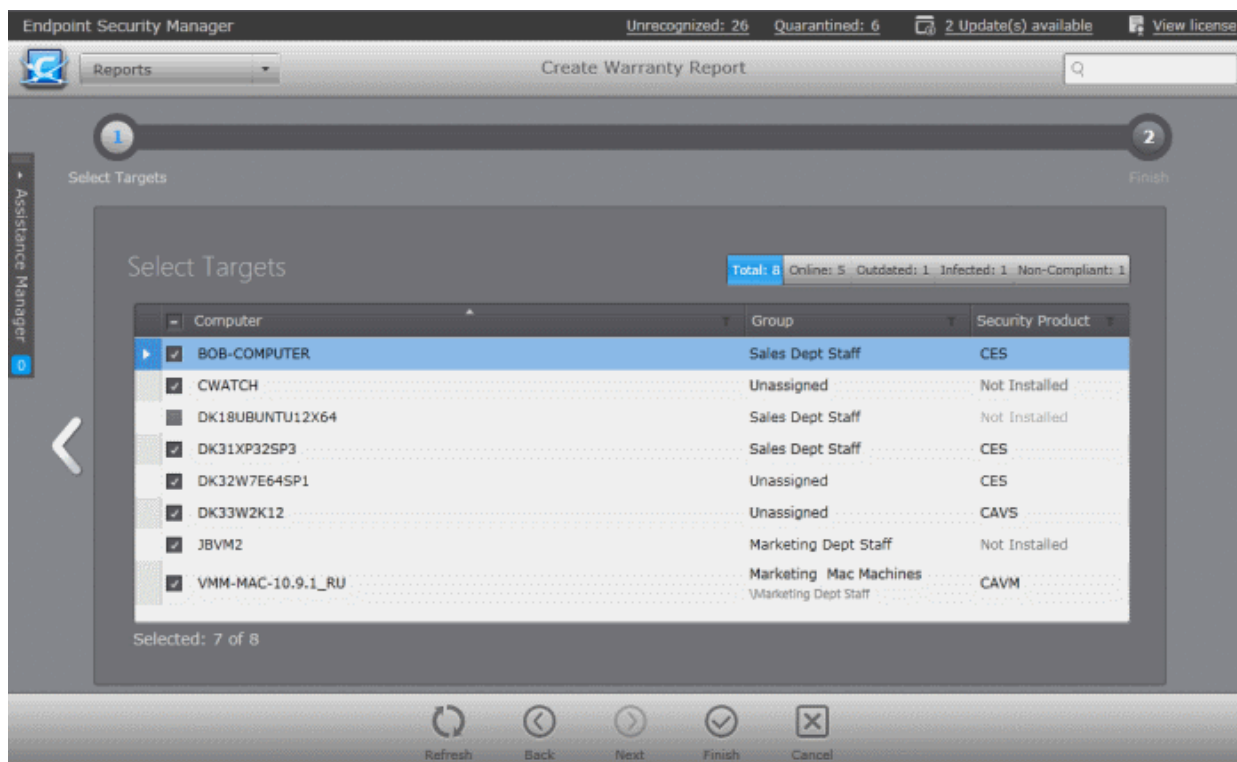
- Select the endpoint(s) for which you wish to generate the Warranty report. The filter options in the header provides at-a-glance statistics of the computers in the network and allow the administrator to filter the computers based on the criteria. You can also filter the computers by clicking the funnel icon on the column headers.

- Click the 'Finish' icon to start generating the report.

- The report generation will be started or added to the queue. The progress will be displayed in the 'Reports' area.

Downloading the Report

The report is available in spreadsheet format only and can be downloaded by selecting it in the
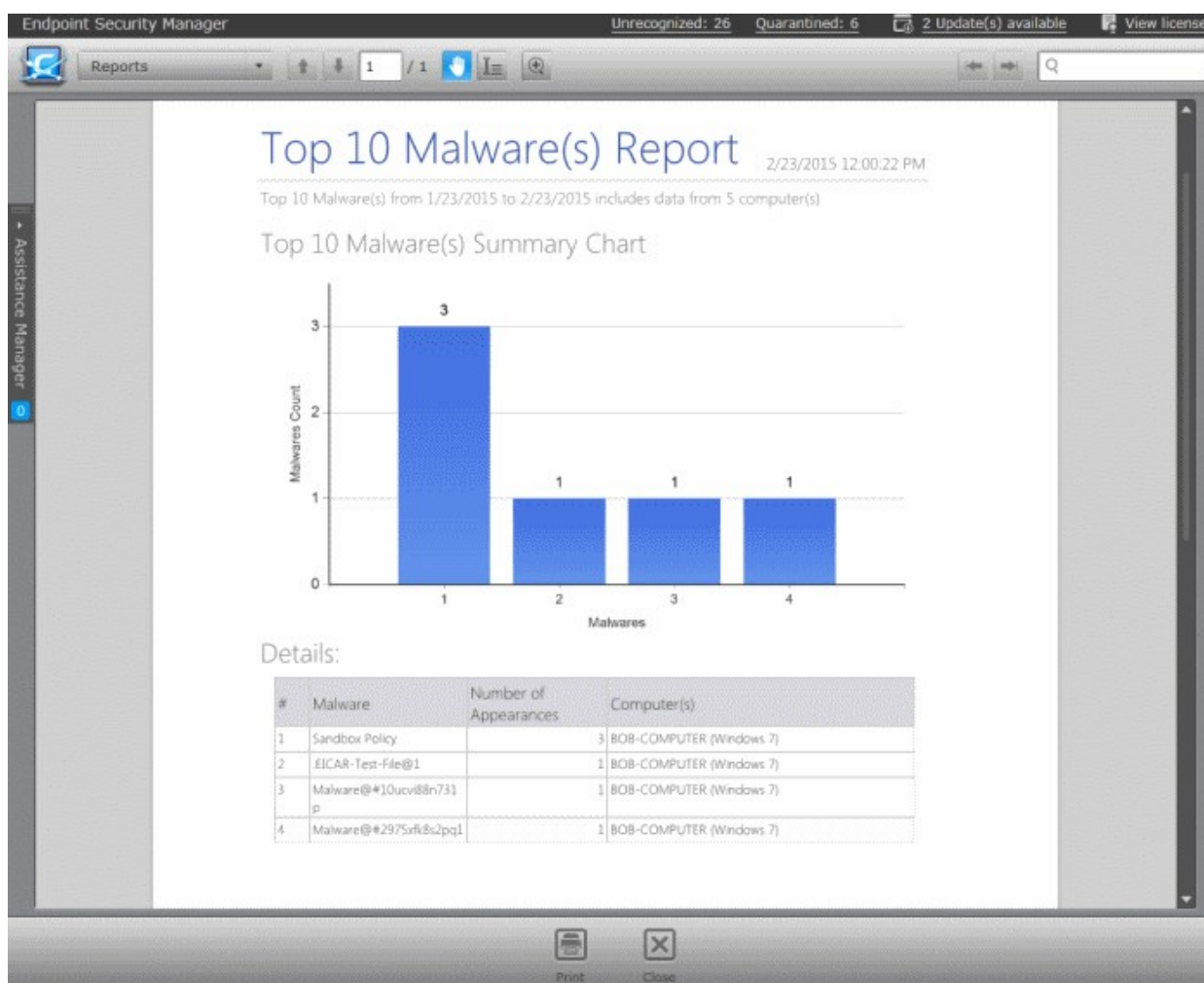
'Reports' area and clicking the download icon at the bottom or clicking the report file icon under the Report File column.

13.   Viewing ESM Information

The 'Help' interface provides administrators with version, license, support and server information. Administrators can use the interface to purchase additional endpoint licenses, to get online help and to get product updates.

The 'Help' interface can be accessed by clicking the CESM icon at the top left or choosing 'Help' from the drop-down in the title bar.

- **Server Information** - Displays details about the server computer on which CESM central console is installed. Refer to **Viewing Server Information** for more details.

- **Support Information** - Displays CESM support contact information and informs admin about different ways to get help on CESM. Refer to **Viewing Support Information** for more.

- **License Information** - Displays license details and allows admins to purchase additional licenses if more computers are to be added to the same CESM console. Refer to **Viewing License Information** for more details.

- **About** - Displays CESM version number, copyright information, End-user license agreement and contains links for getting support. The screen also indicates if any newer version of CESM is available and allows you to download and install the latest version. Refer to **Viewing the About Screen** for more details.
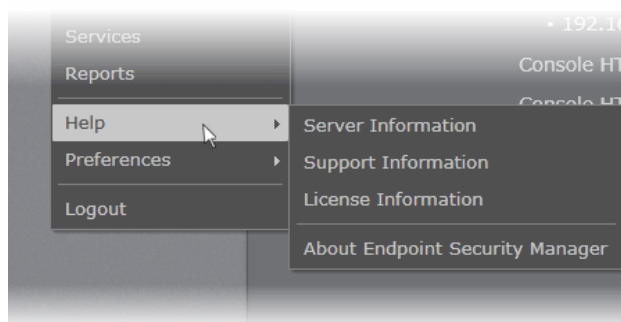
13.1.   Viewing Server Information

The 'Server Information' screen displays details of the server computer(s) on which CESM console is installed.

To access the Server Information screen

- Open the 'Help' area by clicking CESM icon at the top left and click 'Server Information' from the left hand side navigation

    or

- Choose 'Help' > 'Server Information' from the drop-down at the top left

- **Supported Host Names** - Displays the host names and DNS names of the server on which the CESM console is installed.
- **Console HTTP Port** - Displays the port number of the server through which the CESM console can be accessed through a non-secure connection.
- **Console HTTPS Port** - Displays the port number of the server through which the CESM console can be accessed through a secure SSL connection.
- **Agent TCP Port** - Displays the port number of the server through which the agents installed in the endpoints communicate with the server.
- **Remote Session HTTPS Port** - Displays the port number of the CESM server for the target endpoints to connect to the server during their Remote Desktop Connection sessions through a secure SSL connection.

Refer to **Appendix 1** for more information on the configuration of the host names and connection ports of CESM service through the configuration tool.

13.2.   Viewing Support Information

The 'Support Information' screen displays details on getting support in different ways for CESM.

To access the Support Information screen

- Open the 'Help' area by clicking CESM icon at the top left and click 'Support Information' from the left hand side navigation

    or

- Choose 'Help' > 'Support Information' from the drop-down at the top left.
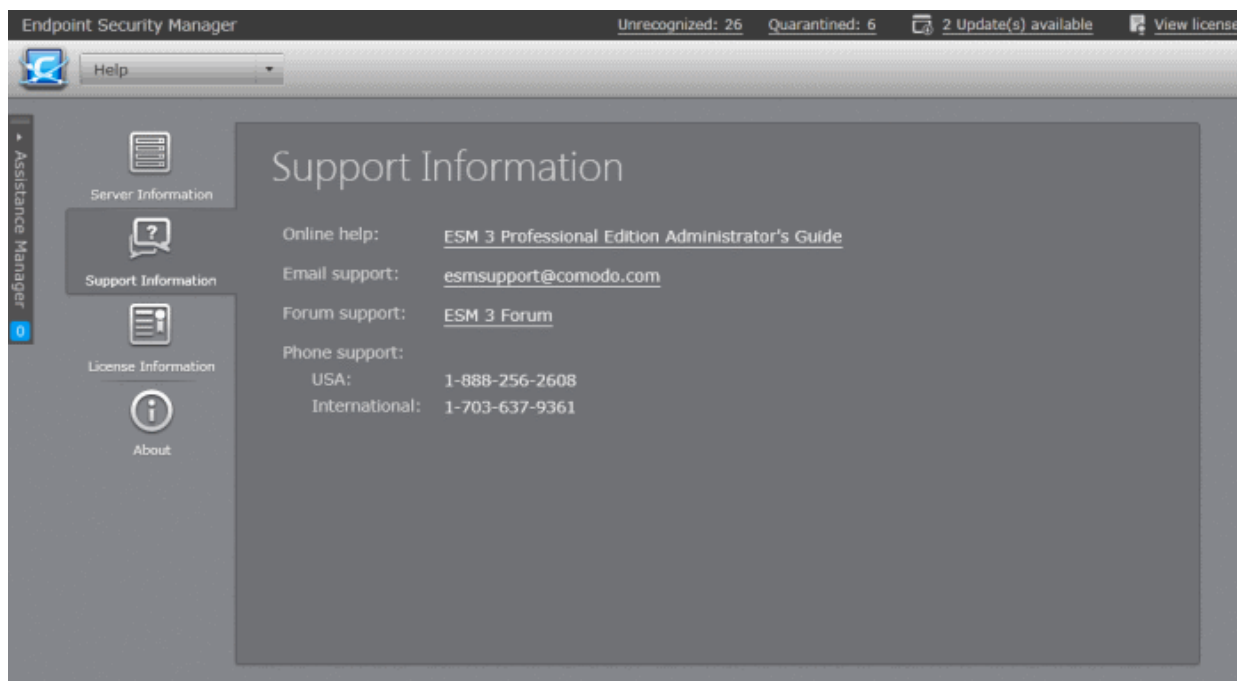
Online help:

If you need assistance on configuring and using CESM, you can refer to its online help guide by clicking the 'ESM 3 Professional Edition Administrator's Guide' link. The Comodo ESM Administrator Guide contains detailed explanations of the functionality, configuration and usage of the application.

Email support:

If you are unable to find a solution for a problem, you can send your query through mail to **ESMsupport@comodo.com**. Your query will be attended as soon as possible. Also You can also send your suggestions for improvements to this mail address.

Comodo Forums:

The fastest way to get further assistance on Comodo Endpoint Security Manager is by posting your question on **Comodo Forums**, a message board exclusively created for our users to discuss anything related to our products. Registration is free and you'll benefit from the expert contributions of developers and fellow users alike.

Phone Support:
You can get phone support for CESM by contacting the following phone numbers:

USA: +1 888 256 2608

International: +1 703 637 9361

Make sure to have your order number or subscription information available.

13.3.   Viewing License Information

The 'License Information' screen displays details on the number of licenses purchased, their type and validity status. The 'License Information' screen also allows the administrator to purchase additional licenses, upgrade licenses, renew licenses and to get live chat support.

To access the License Information screen

- Open the 'Help' area by clicking CESM icon at the top left and click 'License Information' from the left hand side navigation

    or

- Choosing 'Help' > 'License Information' from the drop-down at the top left.
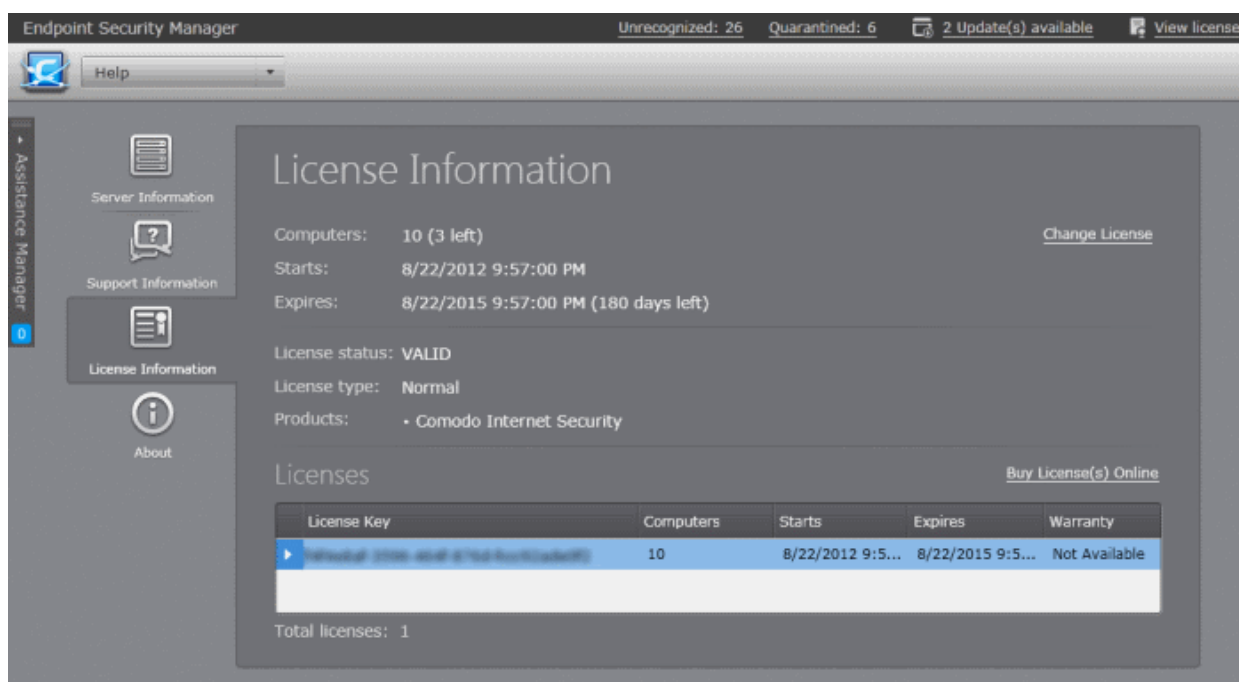
To purchase new licenses

- Click 'Buy License(s) Online':

You will be taken to the Comodo ESM purchase page to purchase the new licenses. After payment is complete, you will receive the license activation key through email.

13.3.1.   Upgrading Your License

If you have purchased new licenses to add more endpoints, you need to upgrade your license by entering the new license key obtained via email. Also you can activate the warranty for the existing license from this screen.

To upgrade your license

- Click the **Change License** link beside 'Computers' from the 'License Information' screen.

The Upgrade License wizard will be started.
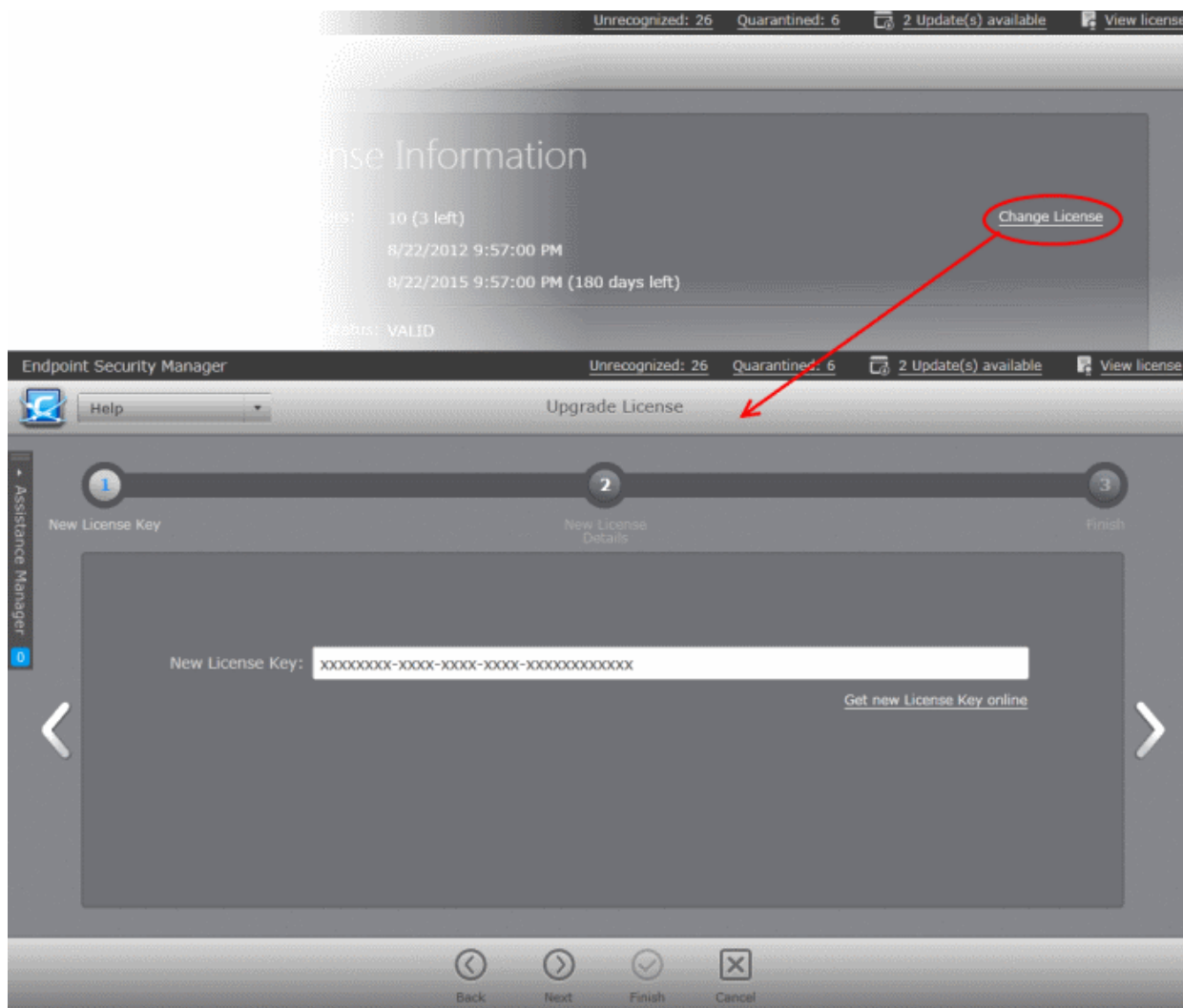
- Enter the new license activation key you received via email.

Note: If you do not have a new license key, click 'Get new License Key online' link to purchase it online from Comodo website.

- Click the right arrow or swipe the screen to the left to move to the next step.

The details of your new license will be displayed.
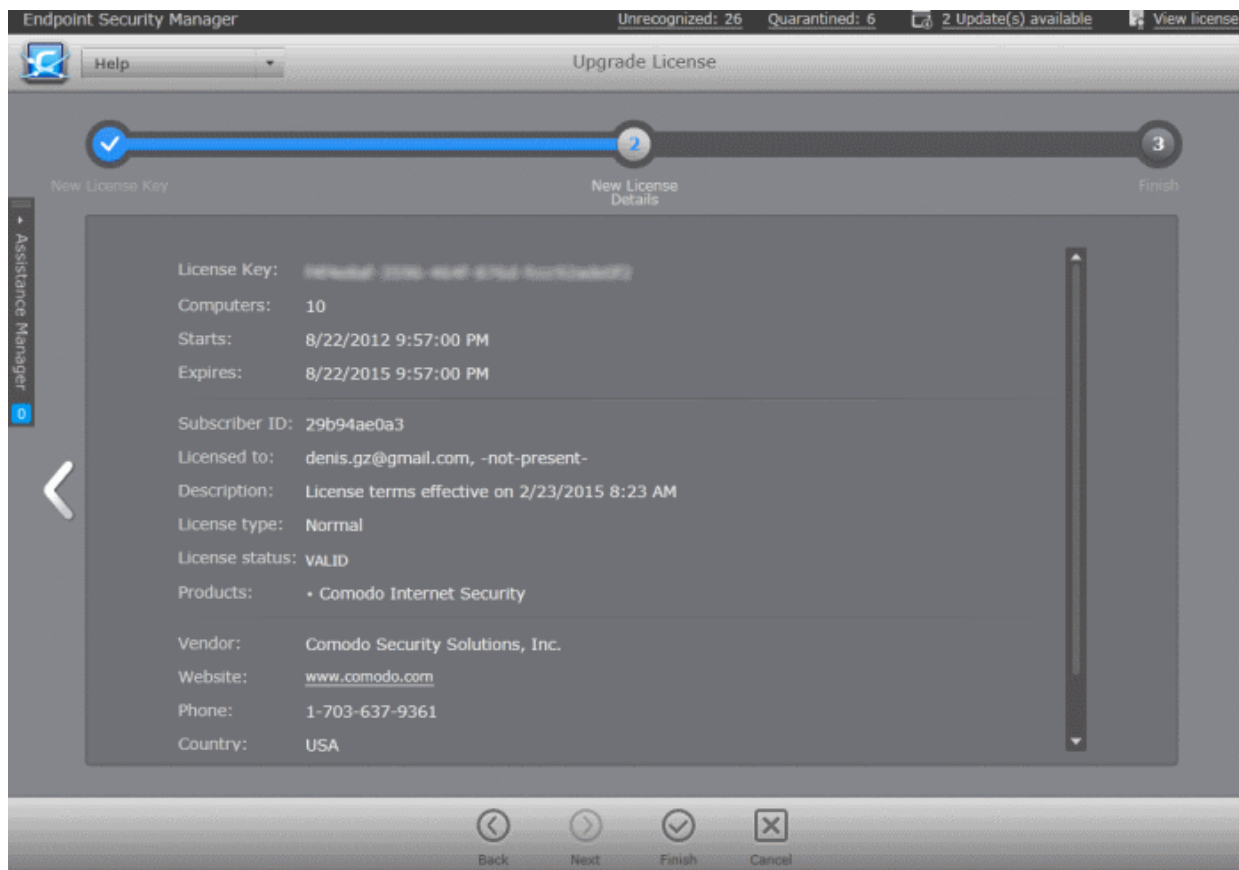
- If you want to activate the warranty for existing license, select the checkbox beside 'Activate' in the Warranty section.

- Click 'Finish' to exit the wizard. Your license will be upgraded/warranty will be activated.

13.4.   Viewing the About Screen

The 'About' screen displays the version information of CESM currently installed on your server, its update status and copyright information. The screen also informs you if an updated version is available and, if so, enables you to download and install it. The screen contains links to get support on CESM from the online help portal and Comodo Forums.

To view the About screen

- Open the 'Help' area by clicking CESM icon at the top left and click 'About' from the left hand side navigation

    or

- Choosing 'Help' > 'About Endpoint Security Manager' from the drop-down at the top left.

- If a newer version of the software is available then a link **Update available. Download version** will be displayed. Clicking this link will start downloading the latest version of CESM Setup <version number>Full.exe.

- Clicking **End-user license agreement** will open the CESM End-user license agreement in a new browser window.

- Clicking **Online help** will take you to online help guide for Comodo Endpoint Security. The CESM help guide contains detailed explanations of the functionality and usage of the application.

- Clicking **Support forums** will take you to Comodo Forums. The fastest way to get assistance on Comodo Endpoint Security Manager is by posting your question on Comodo Forums, a message board exclusively created for our users to discuss anything related to our products. Registration is free and you'll benefit from the expert contributions of developers and fellow users alike.

- Clicking **www.comodo.com** will take you to comodo.com home page.

14.   Viewing and Managing Preferences

The 'Preferences' area allows administrators to configure language settings, report archives, email notifications, dependent CESM servers and auto discovery settings for CESM to identify unmanaged computers in the network. Administrators can also download CESM agents to install on remote endpoints that they wish to manually add to the CESM network.
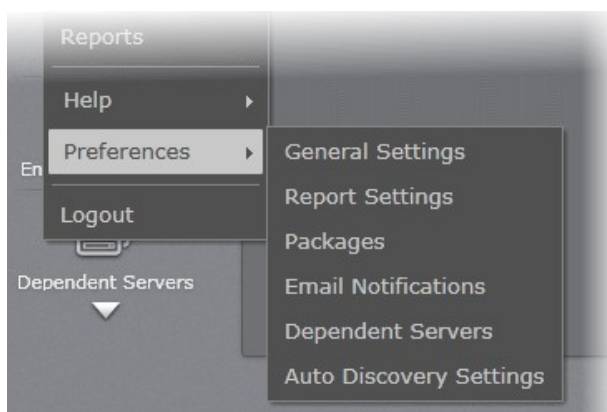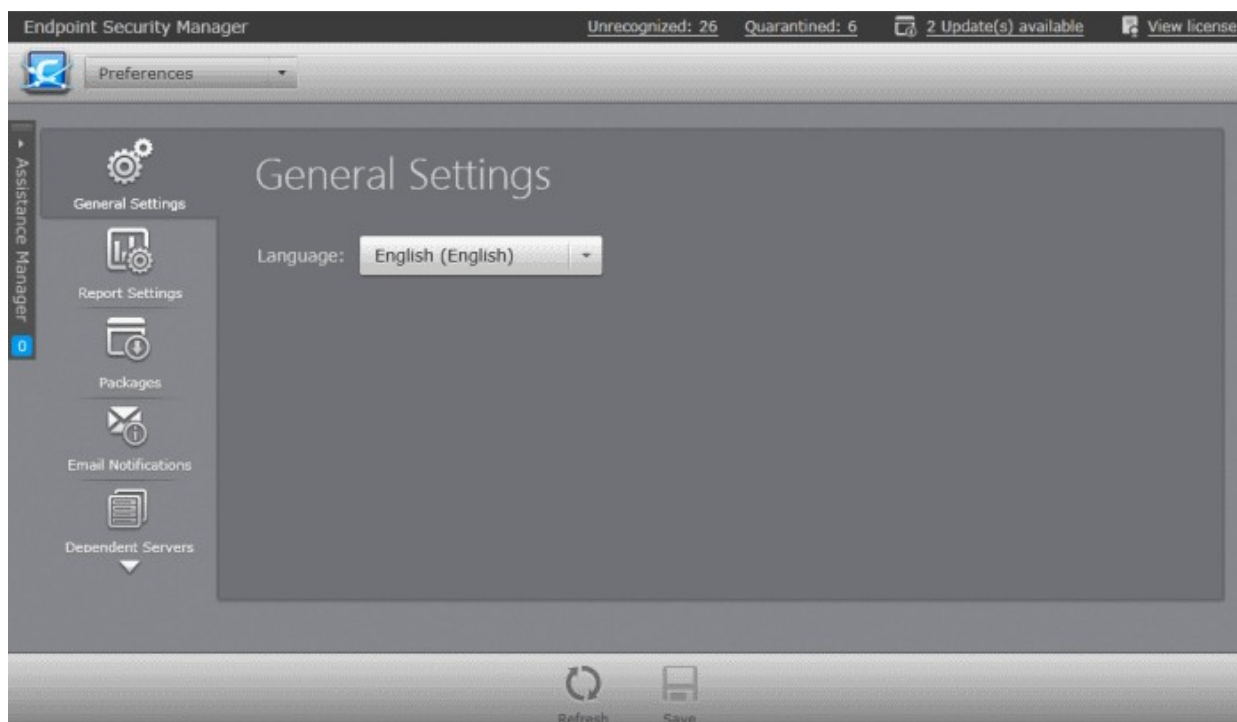
- **General Settings** - Enables administrators to select the language in which CESM interface is to be displayed. Refer to **Configuring General Settings** for more details.

- **Report Settings** - Enables administrators to configure lifetime of archived reports. Refer to **Configuring Report Settings** for more details.

- **Packages** - Enables administrators to download CESM Agent for installation on to remote endpoints, to manually add them to CESM. Refer to **Downloading ESM Agents Packages** for more details.

- **Email Notifications** - Enables administrators to configure for receiving email notifications from CESM. Refer to **Managing Email Notifications** for more details.

- **Dependent Servers** - Enables administrators to add and manage dependent servers for managing computers at remote networks. Refer to **Viewing and Managing Dependent Servers** for more details.

- **Auto Discovery Settings** - Enables administrators to configure the auto discovery feature for identifying unmanaged computers in the network. Refer to **Auto Discovery Settings** for more details.

14.1.   Configuring General Settings

The 'General Settings' screen allows administrators to select the language in which the CESM interface is to be displayed.

To access the General Settings screen

- Click 'Preferences' > 'General Settings' from the drop-down at the top left.
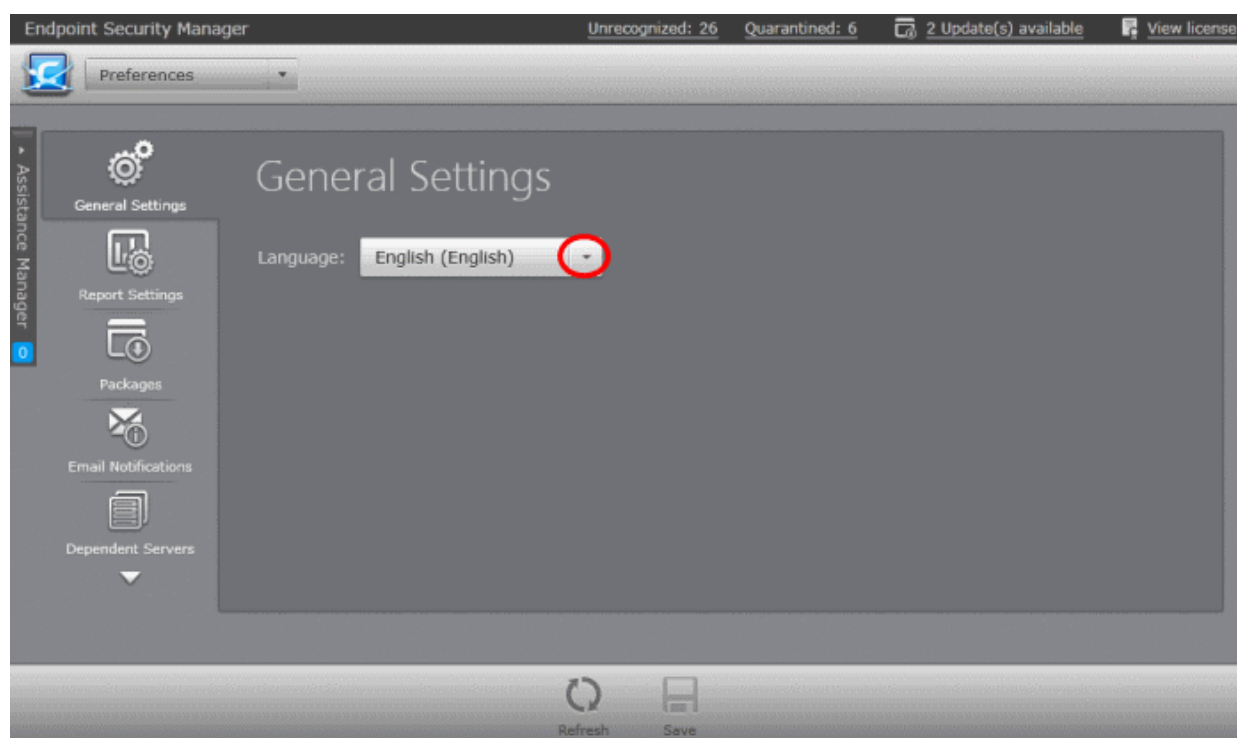
CESM is available in multiple languages.

- Select the language in which the CESM interface is to be displayed from the 'Language' drop-down.
- Click 'Save'.

Your settings will take effect immediately.

14.2. Configuring Report Settings

The 'Report Settings' screen allows administrators to configure the length of time that reports should be stored on the CESM server.

To access the General Settings screen

- Click 'Preferences' > 'Report Settings' from the drop-down at the top left.
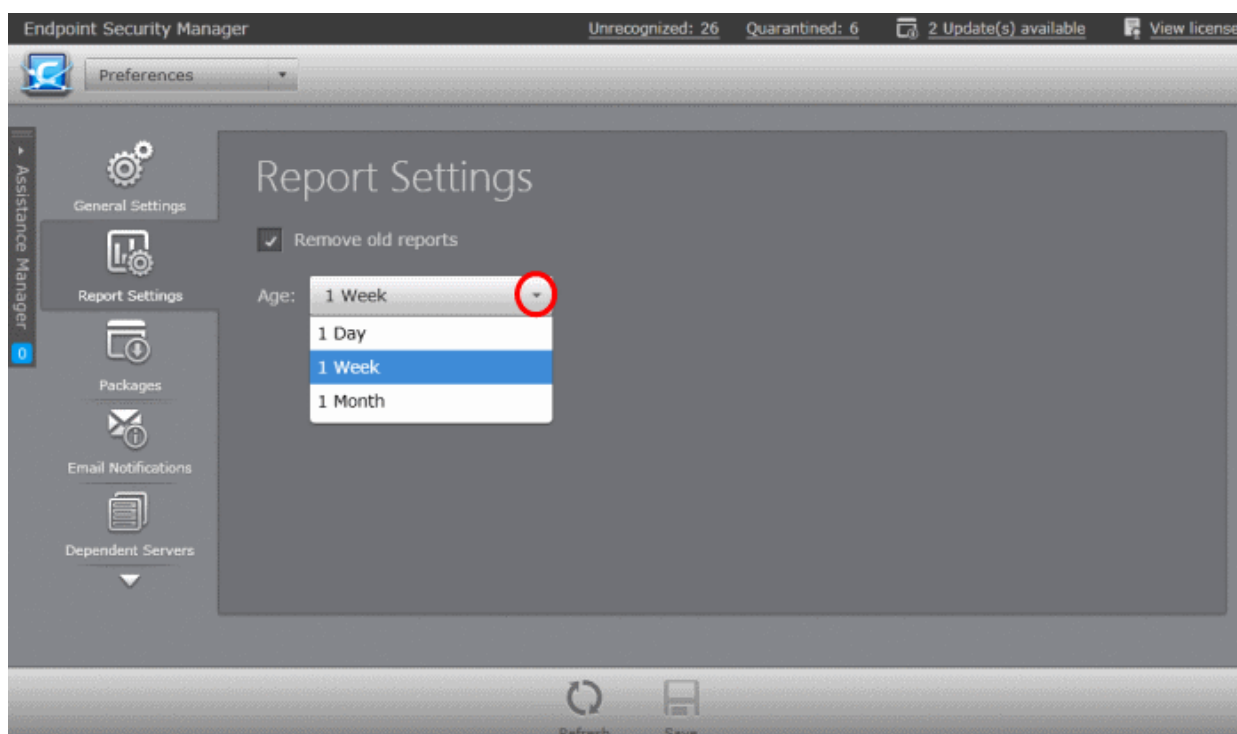
- If you want the older reports to be deleted from the server, select 'Remove old reports' checkbox and select the time period for which the reports can be maintained in the server from the 'Age' drop-down.

- Click 'Save' for your settings to take effect

14.3. Downloading ESM Packages

To connect to the CESM Central Service Server, each endpoint needs a CESM agent installed. For the network endpoint computers that can be reached by the CESM server, the agent will be auto-installed while importing the computer. Refer to **Importing Computers by Automatic Installation of Agent** for more details. But for endpoint computers that are not reachable from the CESM server's network and can be connected through external network like Internet, the agent has to be installed manually in order to establish a connection to the CESM server.

The Agent setup file can be downloaded as an executable file from the admin console. The file can be transferred onto media such as DVD, CD, USB memory for manual installation onto target machines. A single copy of the installation files can be used to install the agent on any number of target machines. Once installed, the agent will establish the connection to the CESM server automatically and enables managing the endpoint from the console. Refer to **Adding Computers by Manual Installation of Agent** for more details.

The Comodo Security Product, Comodo Endpoint Security (CES), Comodo Antivirus for Servers (CAS) and Comodo Antivirus for Mac (CAVM), will be auto-installed while importing the Windows/Mac computers and automatically updated periodically. If needed, the administrator can update the software on-demand, through the Add Computer wizard, accessible from the 'Computers' interface. Refer to **Updating Comodo Software on Managed Computers** for more details. CESM also allows the administrator to manually download the CES/CAS/CAVM package and install it on remote endpoints along with the agent can bring them under centralized management under CESM. Refer to the section **How to Install CES on Endpoints Added by Manually Installing the Agent** for more details on manually installing the CES software.

The Administrator can download CESM Agent setup packages for different Operating Systems and CES/CAS/CAVM installation packages for manual installation from the 'Preferences' > Packages screen.

To access the Agent Packages screen

- Click 'Preferences' > 'Packages' from the drop-down at the top left.

The interface contains two areas:

- The 'Checked In Packages' tab displays the all packages loaded to and registered in the CESM server."
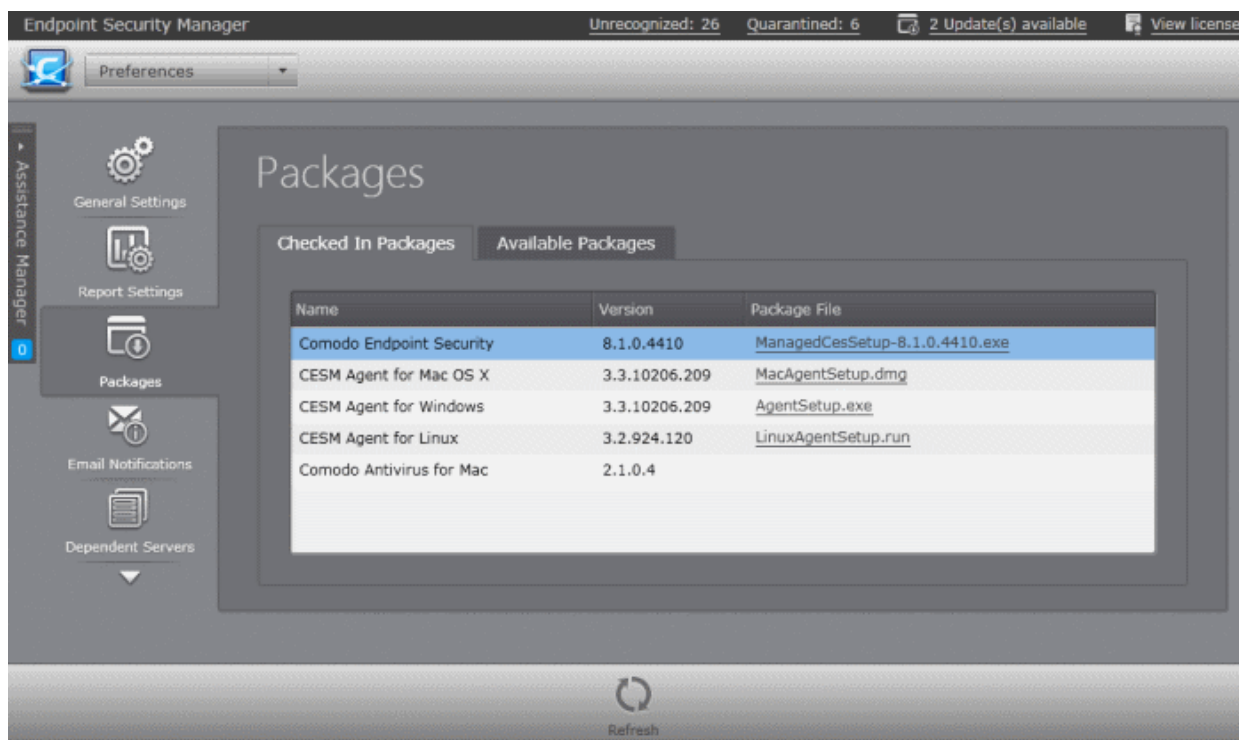
You can download a package in two ways:

- Click on the link in the package file column to directly download the package
- Right click on the link and choose 'Copy link address' to copy download URL to clipboard for downloading the package using a different browser or your favorite download manager
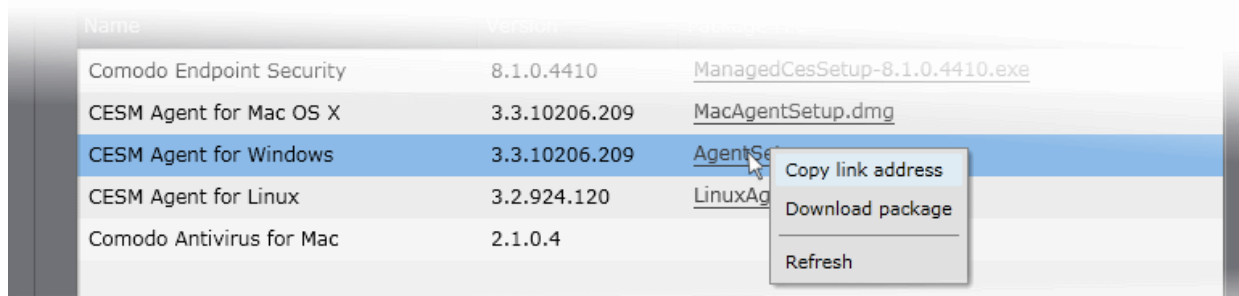
Refer to **Adding Computers by Manual Installation of Agent** for more details on installing the agent on to target endpoints.

- The 'Available Packages' tab displays all packages available for download, allows administrator to check for updates and download them.
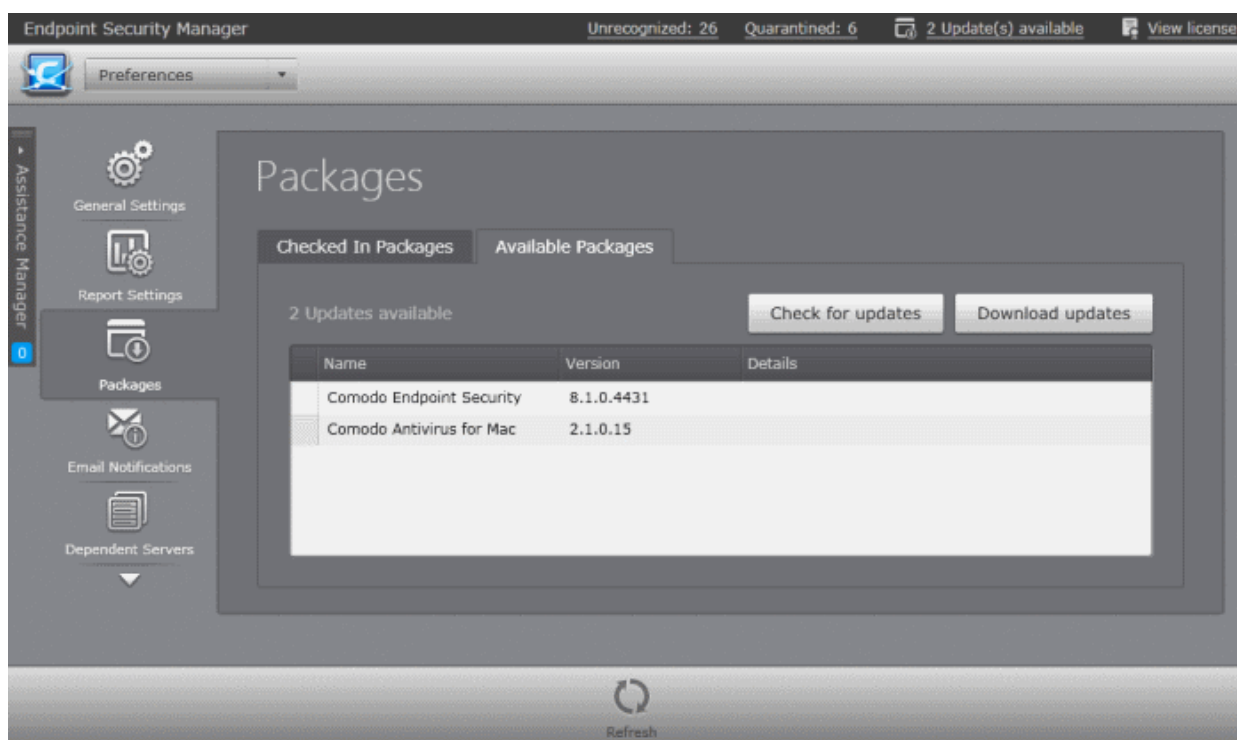
- To check whether any updated versions are available for the CESM agents and managed security software click 'Check for updates'.

- To download the latest updated versions of the CESM agents and managed software into your CESM server, click 'Download updates'.

14.4.   Managing Email Notifications

CESM can send email notifications on the occurrence of virus outbreaks, when malware found on the network exceeds a certain threshold, when the number of non-reporting and outdated endpoints exceeds a certain number, and when your license is nearing expiry. Email notifications are configured from the 'Email Notifications' area.

To access the Email Notifications screen

- Click 'Preferences' > 'Email Notifications' from the drop-down at the top left.
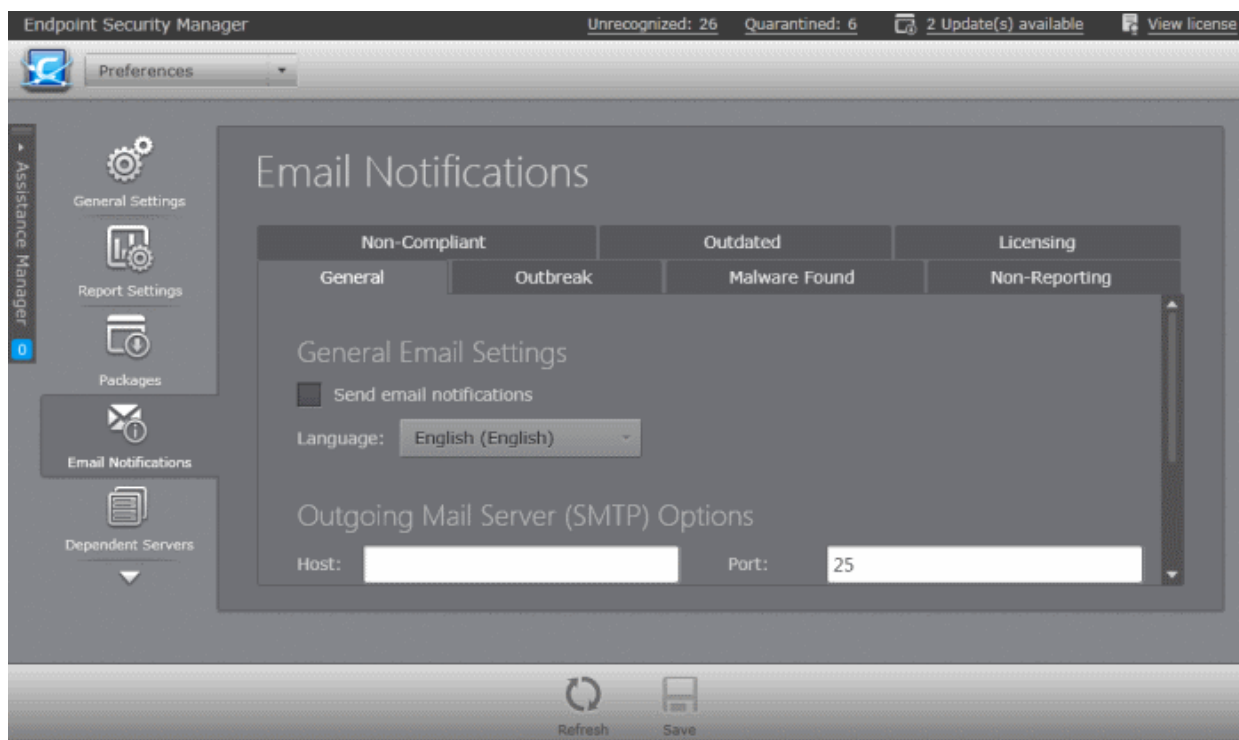
The interface contains seven tabs. The General Tab allows the administrator to enable/disable automated Email Notifications and configure SMTP server settings for sending the notification emails from the CESM server. The other six tabs allow the administrator to configure the events for which the notifications are to be sent.

Refer to the following sections for more details:

- **Configuring General Email Settings and SMTP Server Settings**
- **Configuring Events for Notifications**

Configuring General Email Settings and SMTP Server Settings

The General tab in the Email Notifications interface allows the administrator to enable/disable the notifications and specify the SMTP server for outgoing emails.
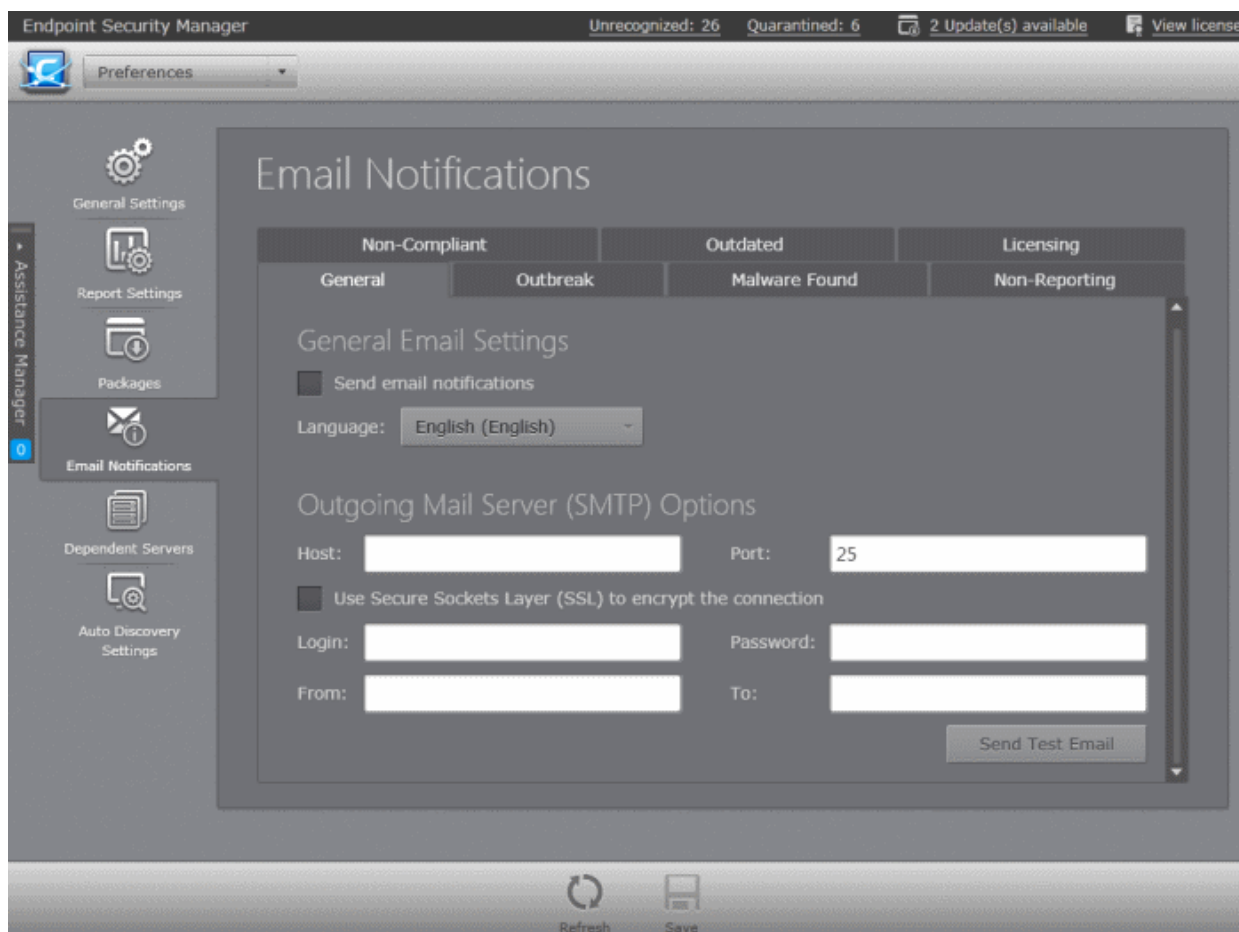
- To enable automated email notifications select the 'Send email Notifications' check box. *(Default=Disabled)*
- Select the language in which the emails are to be sent from the 'Language' drop-down.
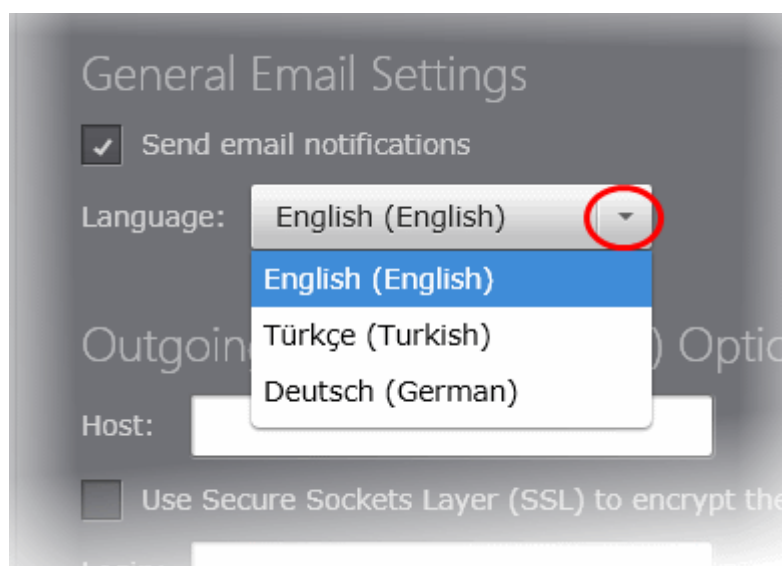
Outgoing Mail Server (SMTP) Options

- Enter the IP address or hostname of your SMTP server and SMTP Port (default = 25) in the Host and Port respective fields
- If the SMTP server uses SSL encryption for outgoing mails, select the Use Secure Sockets Layer (SSL) to encrypt the connection

- Enter your login username and password to the mail server in the Login and Password fields

The email alerts will appear to come from ESM Server by default if the 'From' field contains a simple email address. Your personal mail configuration may be useful in completing the mail server section.

To locate mail settings in:

- Outlook 2003 - Start Outlook 2003 and click Tools > Email Accounts > select the email account for which you want to view the settings and click Change... > More Settings...

- Outlook 2007 - Start Outlook 2007 and click Tools > Account Settings > on the E-mail tab, select the email account for which you want to view the settings and click Change... > More Settings...

- Outlook 2010 - Start Outlook 2010 and click Tools > Account Settings > on the E-mail tab, select the email account for which you want to view the settings and click Change... > More Settings...

- Thunderbird - Start Thunderbird and click Tools > Account Settings...

Configuring Events for Notifications

- Configure the email notification parameters for various events under the respective tabs as shown in the table below:

Event Type	Description	Configurable parameters
Outbreak	Configure automated email notification when number of endpoints infected by virus or other malware reaches a set threshold.	**Number of infected computers** - CESM will send a notification email when the number of endpoints infected by malware equals to or exceeds this value. *Default = 1*. **The computers are infected for the following number of minutes** - Period of time used to define an outbreak. A notification will be sent when the number of infected computers is met or exceeded during the set time period. *Default = 15*.
Malware Found	Configure automated email notification when the number of malware samples identified but not handled by the CES on an endpoint reaches a set threshold.	**Number of Infected Computers** - CESM will send a notification email when the number of endpoints infected by detected malware equals to or exceeds this value. *Default = 1*.
Non-Reporting	Configure automated email notifications when the number of non-reporting computers reaches a certain number.	**Number of non-reporting computers** - CESM will send a notification mail if the number of non-reporting endpoints equals or exceeds this value. *Default = 1*. **The computers do not report for the following number of minutes** - Specify the period of time till which CESM should wait after the endpoint first fails to report before sending the notification, in minutes. *Default = 1020*.
Non-Compliant	Configure a notification mail to be sent when the number of connected computers that are not compliant with the security policy applied to them reaches a set threshold.	**Number of non-compliant endpoints** - CESM will send a notification mail if the number of non-compliant endpoint computers equals or exceeds this value. *Default = 1*
Outdated	Send a notification mail when the number of endpoints using an outdated virus database reaches a set threshold.	**Number of computers with outdated AV bases** - CESM will send an notification email when it detects the number of endpoints with outdated databases equals to or exceeds this value. *Default = 1*
Licensing	Configure automated email notifications when your license is about to expire.	**License expiration days** - Number of days before expiry that CESM will send a reminder mail. *Default = 30*. **Unused endpoints threshold, %** - If the number of unused endpoints equals or falls below this value then CESM will send a notification that your licensing limit is approaching. For example, if you have you 100 total licenses and set this figure to 10%, then a notification

		mail will be sent when you have used 90 licenses. *Default = 10.*

- Click 'Save' at the bottom of the interface to your configuration to take effect.

14.5.   Viewing and Managing Dependent Servers

CESM allows administrators to define and manage 'dependent' CESM servers to manage remote networks of endpoints. A master administrator can log into the admin consoles of dependent CESM servers to directly manage endpoints on the remote network. This login can be done seamlessly through the master admin console. Setting up a dependent CESM server to handle the endpoints of remote networks will render significant speed and resource advantages while allowing a master administrator to maintain full control and visibility over the remote endpoints.

- **Accessing the dependent servers screen**
- **Adding a dependent server**
- **Logging into a Dependent server**
- **Importing endpoints to a dependent server**
- **Managing endpoints controlled by a dependent server**
- **Editing dependent servers**
- **Removing dependent servers**

To access the Dependent Servers screen

- Click 'Preferences' > 'Dependent Servers' from the drop-down at the top-left.
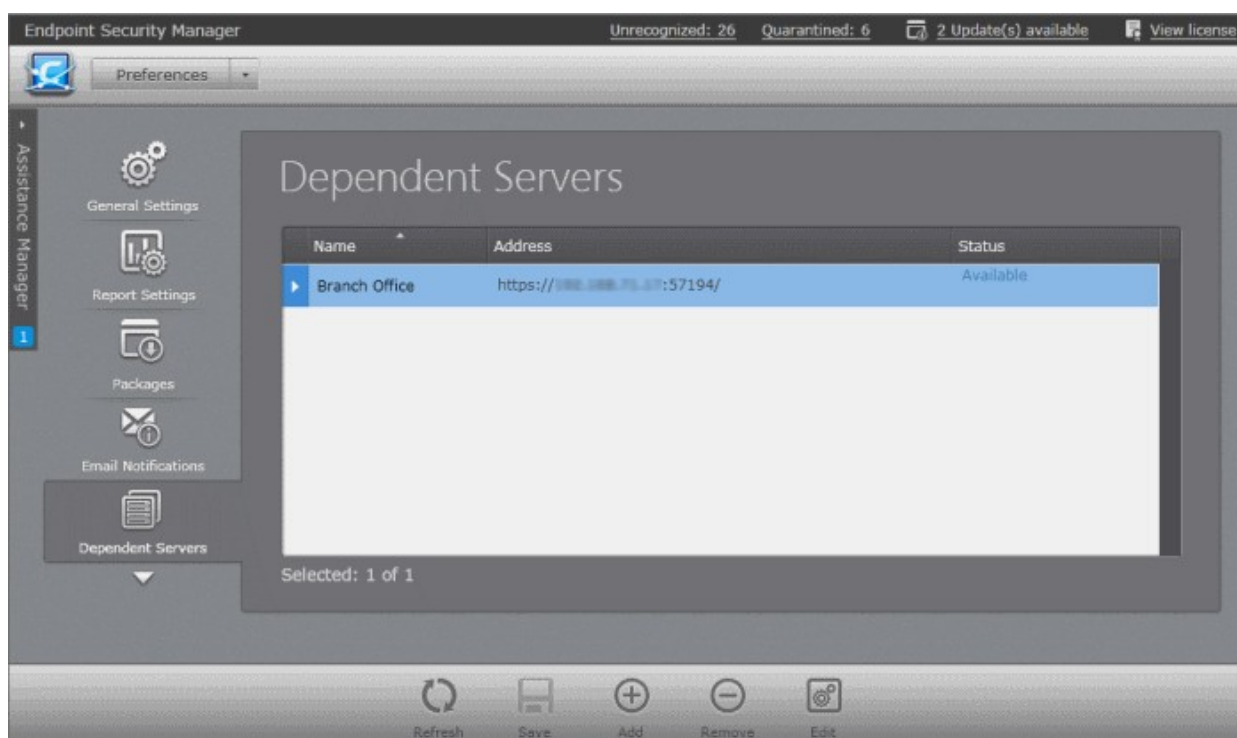
From here, administrators can add, edit and remove dependent servers.

14.5.1.   Adding a Dependent Server

Before adding a remote server as a dependent server, please make sure that the following prerequisites are satisfied:

- The server certificate obtained for the central CESM server contains the DNS name or the IP address of the dependent server in the Subject Alternative Name (SAN) field. You should have entered the SANs in the SAN field when generating the certificate signing request (CSR).

- The same certificate has been installed on the remote CESM server.

- The CESM central service console has been installed on the remote server.

To add a dependent server

- Open the 'Dependent Servers' area by choosing 'Preferences' from the drop-down at the top left and clicking 'Dependent Servers' from the left hand side navigation.

- Click 'Add' from the 'Dependent Servers' screen. The 'Add server' dialog will be displayed.

Add Server - Table of Parameters	
Server address/Port	Enter the DNS name or the IP address of the dependent server and the port through which CESM console can be reached in the Server Address/Port fields (The default port for secure SSL connection to the console is 57194).
Alias	Enter the Alias name of the dependent server.
Use current user credentials	Selecting this option will add the server using the credentials of the current CESM

(Selected by default)	administrator.	
Use custom credentials	Selecting this option will allow you specify an alternative administrative account on the remote server.	
	User Name:	Enter the user-name of the dedicated network administrator of the dependent server.
	Password:	Enter the password of the dedicated network administrator of the dependent server.

- Enter the details and click the 'Add' button,

The remote server will be added to the Dependent Servers list. By accessing this dependent server, administrators will be able to manage endpoints connected to it.

14.5.2.   Logging into a Dependent Server

To log-in to a dependent server, just click on the server address in the 'Dependent Servers area'. The console interface of the remote server will open in a new browser tab or in a new browser window, depending on your browser type and Operating system, with the 'Computers' area displayed. You will not be asked to enter login credentials as those were included when successfully adding the dependent server. You can add new endpoints to the remote server and manage existing endpoints of the remote server from the console.
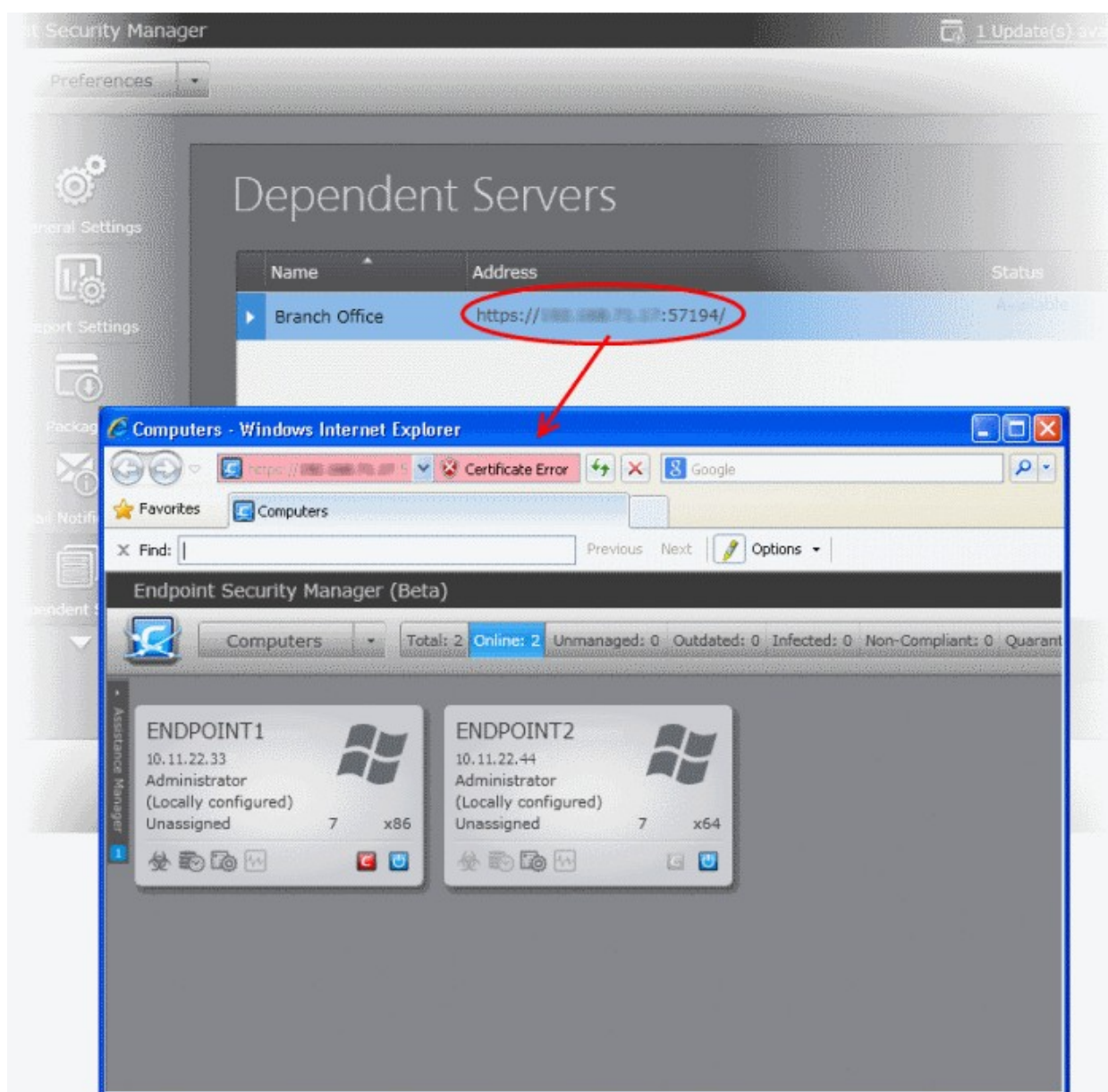
14.5.3.   Importing Endpoints to a Dependent Server

Administrators can import computers connected to the network of the dependent server and manually add endpoints connected through external networks like the Internet.

To import or add endpoints to the dependent server

- On the master console, open the 'Dependent Servers' area by choosing 'Preferences' from the drop-down at the top left and clicking 'Dependent Servers' from the left hand side navigation.

- Log-in to the required dependent server by clicking its address. The CESM console interface of the remote server will open in a new tab within the browser window.

- Start the 'Add Computer' wizard on the remote console by opening the 'Computers' area then clicking 'Add'. Follow the instructions in **Importing Computers by Automatic Installation of Agent** if you need help with the rest of the process.

- To add computers connected to the remote network through an external network like the Internet, download the CESM agent from the CESM console of the remote server and manually install it on the remote computers. For more details on manually adding endpoints, refer to the section **Adding Computers by Manual Installation of Agent**.

14.5.4.   Managing Endpoints Controlled by a Dependent Server

Once you have logged into the console of the dependent server, management of its endpoints is much the same as managing local endpoints with local/master CESM server. The drop-down at the top-left of the CESM console interface of the remote server enables the administrator to navigate to different areas of the interface:

The Computers Area - Enables administrators with the ability to import/add endpoints to the remote server, view and manage networked computers.

- Add/Import computers to the remote CESM console.

- View complete details of the endpoints that are managed by the remote CESM console.

    - Assign and re-assign endpoints to groups.

    - Manage quarantined items, currently running applications, processes and services in remote endpoints.

    - Managing drives and storage at the endpoints.

- Run on-demand antivirus scans on individual or a bunch of selected endpoints.

- Start shared remote desktop session with remote endpoints from the remote server's CESM console.

Refer to **The Computers Area** for more details.

The Groups Area - Allows administrators to create endpoint groups in the remote server's CESM console, as per the organization's structure and apply appropriate security policies.

- Create computer Groups for easy administration.

- Apply security policies to groups.

- Run on-demand antivirus scans on individual or multiple endpoints.

- Generate granular reports for grouped endpoints.

Refer to **The Groups Area** for more details.

The Policies Area - Allows administrators to create, import and manage security policies for remote endpoint machines.

- Create new policies by importing settings from another computer or by modifying an existing policy

- View and modify the configuration of any policy - including name, description, CES components, target computers and whether the policy should allow local configuration

- Apply policies to entire endpoint groups of the remote CESM console

Refer to **The Policies Area** for more details.

Quarantine - Allows you to view all the suspicious programs, executables, applications and files moved to quarantine by CES/CAS installations at the managed endpoints and manage them.

Refer to **Viewing and Managing Quarantine Items** for more details.

Sandbox - Allows you to view all the programs, executables, applications that are currently run inside the sandbox at the managed endpoints and manage them.

See **Viewing and Managing Sandboxed Applications** for more details.

Files Management - Allows you to view all the executable files which are not identified as safe on checking with Comodo certified safe files database and manage them.

See **Files Management** for more details.

The Applications area - Allow you to view all applications installed on endpoints connected to remote CESM sever and uninstall unwanted applications.

Refer to **The Viewing and Managing Installed Applications area** for more details.

The Processes Area - View all processes launched on endpoints connected to remote CESM server and stop the process.

Refer to **Viewing and Managing Currently Running Processes.**

The Reports Area - Enables to generate highly informative, graphical summaries of the security and status of endpoints connected to the remote server. The administrator can view and download the reports from the 'Reports' area of the CESM console of the remote server.

- Drill-down reports can be ordered for anything from a single machine right up to the entire managed network.

- Each report type is highly customizable according to administrator's requirements.

- Reports can be exported to .pdf and .xls formats for printing and/or distribution.

- Available reports include endpoint CES configuration, policy compliance, malware statistics, policy delta, CES logs, quarantined items and more.

Refer to **The Reports Area** for more details.

The Help Area - Allows the administrator to view CESM version and update information of the CESM installation and view and upgrade licenses.

- View the version and update information. View the license information and activate/upgrade licenses.

- View details of the server upon which CESM is installed and download agent setup files for different operating systems for manual installation on endpoints connected through external networks.

- Configure 'dependent' CESM servers. Centrally manage and configure any subordinate CESM server currently managing endpoints on a different network.

Refer to **The Help Area** for more details.

The Preferences Area - Allows the administrator to download the CESM agent for manually adding remote endpoints, configure dependent servers and manage endpoints on remote networks, configure for automated email notifications and configure reports archival.

- Download the Agent setup file to to connect to the CESM Central Service Server.

- Configure the lifetime of the reports generated and retained in CESM server.

- Configure for email notifications when security parameters exceed set thresholds.

- Define and manage 'dependent' CESM servers to manage remote networks of endpoints

Refer to **Viewing and Managing Preferences** for more details.
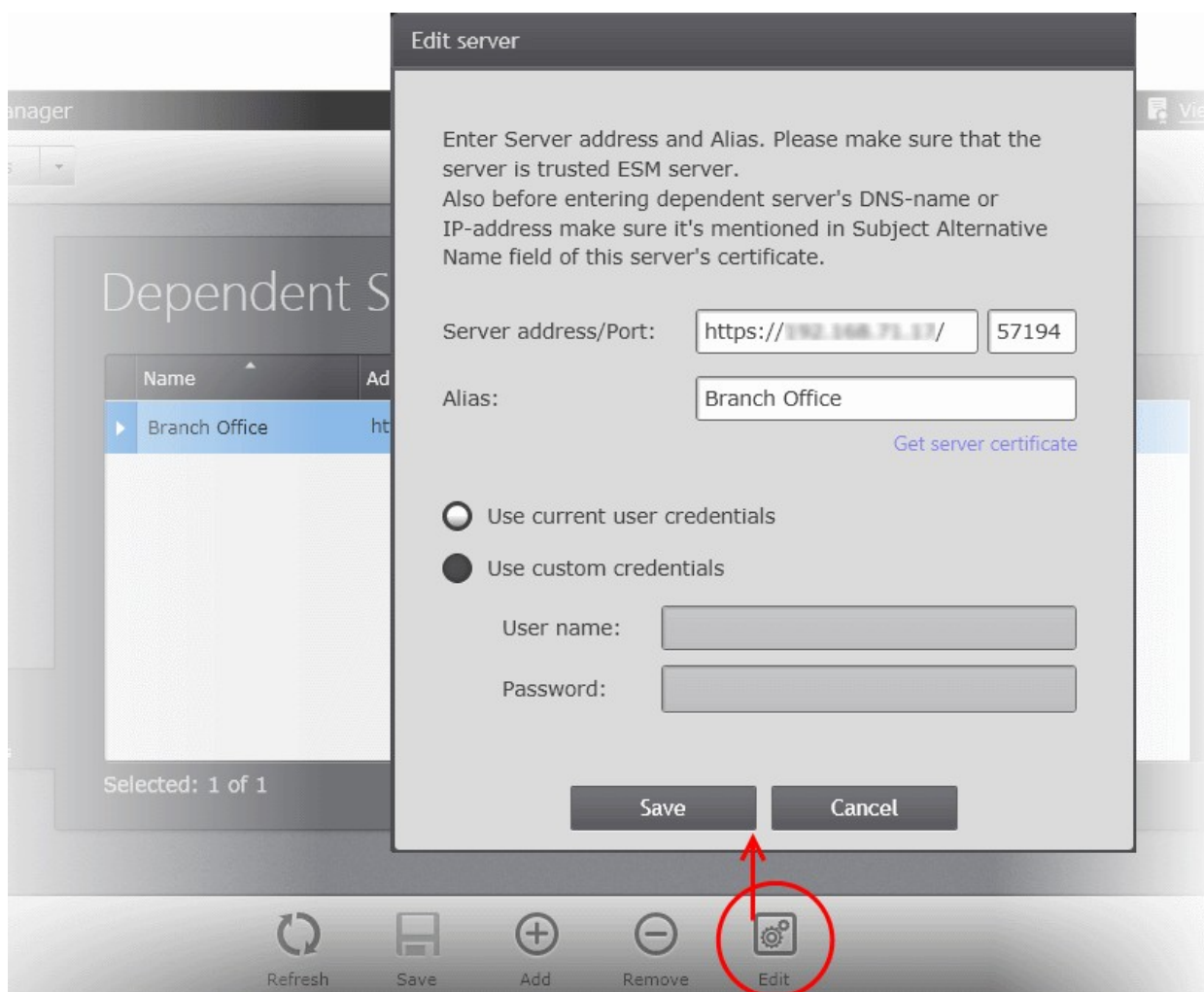
14.5.5.   Editing Dependent Servers

The master CESM console allows the administrator to edit the server/port details and the admin login credentials of existing dependent servers. The administrator can also use the 'Edit' interface to download the remote server certificate so it can be installed onto computers from which the console is to be accessed in future.

To edit a dependent server

- Open the 'Dependent Servers' area by choosing 'Preferences' from the drop-down at the top left and clicking 'Dependent Servers' from the left hand side navigation.

- Select the dependent server to be edited and click the 'Edit' from the bottom of the interface, alternatively double click on the dependent server 'Name' or 'Status'.

The 'Edit Server' dialog will open.

| Edit Server - Table of Parameters	
Server address/Port	Enables to edit the DNS name or the IP address of the dependent server and the port through which CESM console can be reached in the Server Address/Port fields (The default port for secure SSL connection to the console is 57194).
Alias	Enables to edit the Alias name of the dependent server.
Get server certificate	Enables the master CESM administrator to download the server certificate of the remote CESM server. The certificate needs to be installed on the computers from which the master administrator wishes to access the CESM console of the remote server through the master CESM console.
Use current user credentials	Selecting this option enables the master CESM console to log in to the remote server using the credentials of the currently logged in CESM administrator account.
Use custom credentials	Selecting this option enables the administrator to to specify an administrative account of the remote server with the following details:
	User name: Enter the user-name of the remote server.
	Password: Enter the password of the remote server.

- Click 'Save' for your changes to take effect.

14.5.6.   Removing Dependent Servers

The dependent servers can be removed from the master CESM server.

To remove a dependent server

- Open the 'Dependent Servers' area by choosing 'Preferences' from the drop-down at the top left and clicking 'Dependent Servers' from the left hand side navigation.

- Select the dependent server to be removed and click 'Remove'. A confirmation dialog will be displayed.
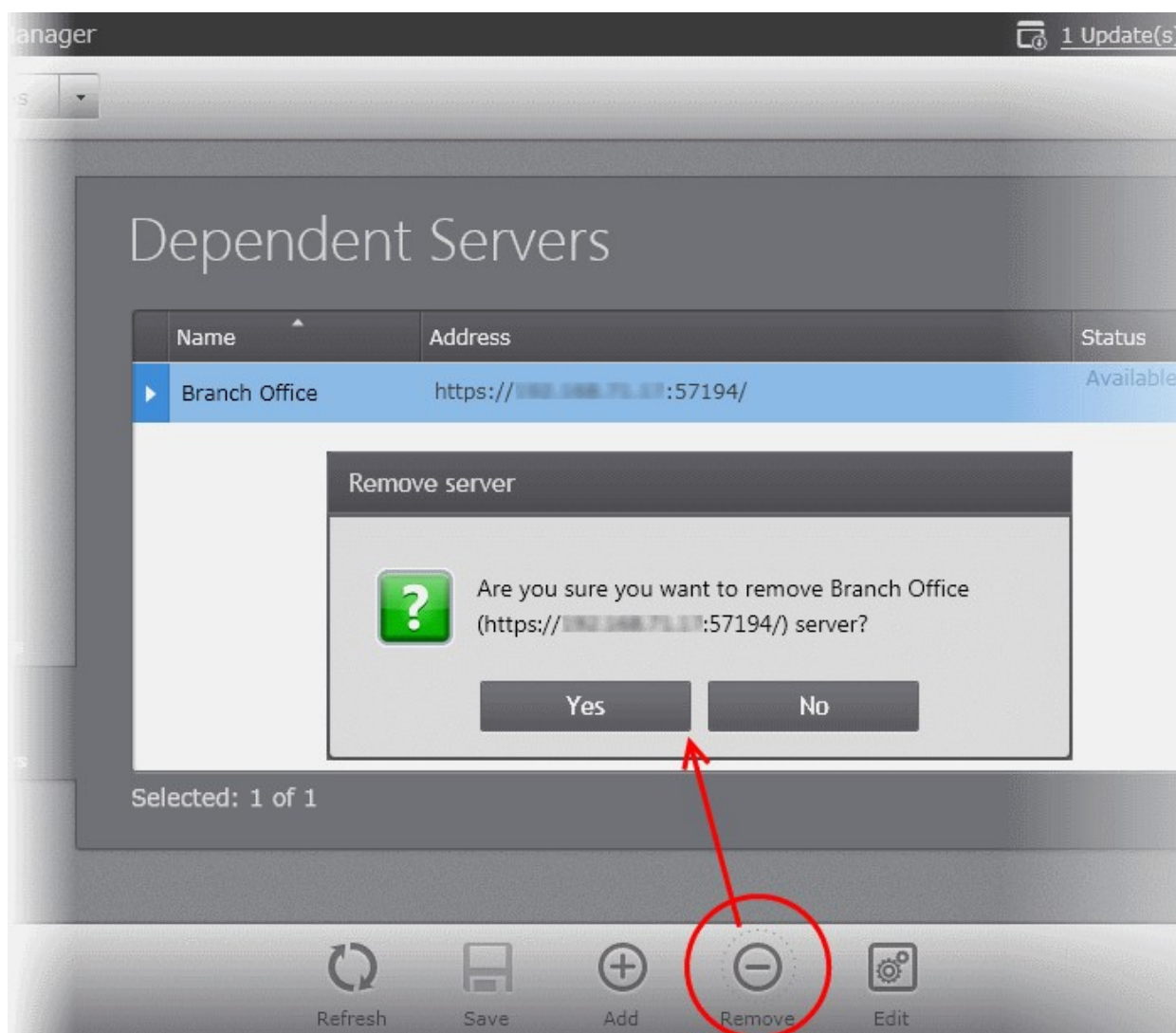
- Click 'Yes'.

14.6.   Auto Discovery Settings

CESM has the ability to discover the endpoint computers in the local network of the CESM server and left unmanaged by it and new computers added to the network but yet to be imported into CESM. The number of unmanaged computers is dynamically displayed on the 'Unmanaged' button at the top of the 'Computers' area.
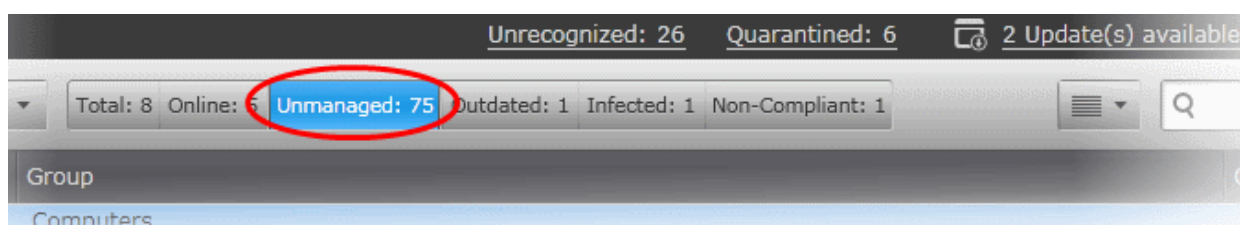

Clicking the 'Unmanaged' button displays the unmanaged computers and enables the administrator to import them into CESM. Refer to the section **Importing Unmanaged Endpoints from Network** for more details.

In order for CESM to scan the network and identify the unmanaged computers, the Auto Discovery feature must have been enabled and configured under Preferences > Auto Discovery pane.

To configure Auto Discovery

- Open the 'Auto Discovery Settings' area by choosing 'Preferences' > 'Auto Discovery Settings' from the drop-down at the top left.
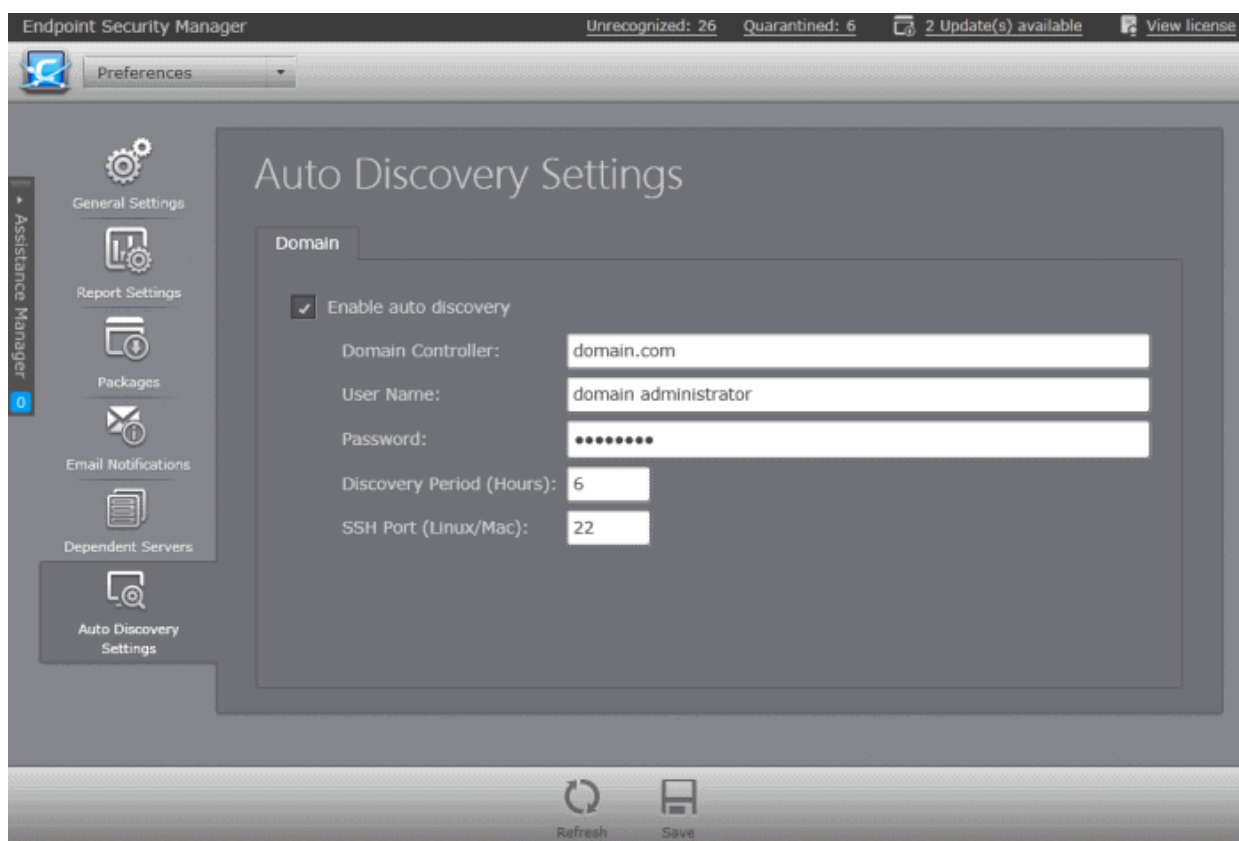
Auto Discovery Settings - Table of Parameters	
Enable auto discovery	Select this check box if auto discovery is to be enabled
Domain Controller	Enter the name of the domain controller of the domain
User Name	Enter the user name of the dedicated administrator account for logging-in to the domain controller
Password	Enter the password of the dedicated administrator account for logging-in to the domain controller
Discovery Period	Specify the interval at which CESM should scan the network for unmanaged computers in hours. (Default = 6)
SSH Port	Specify the Secure Shell (SSH) port of Linux and/or Mac OS computers in the network for CESM to connect to them while scanning. (Default = 22)

• Enter the details and click Save at the bottom of the interface for the configuration to take effect.

Appendix 1 - The Service Configuration Tool

The Service Configuration Tool enables the administrator to start and stop the ESM central service, change server and agent ports settings, change database connection settings and view a log of database events.

The tool is installed as a separate application on the CESM server and can be accessed from the Windows Start Menu.
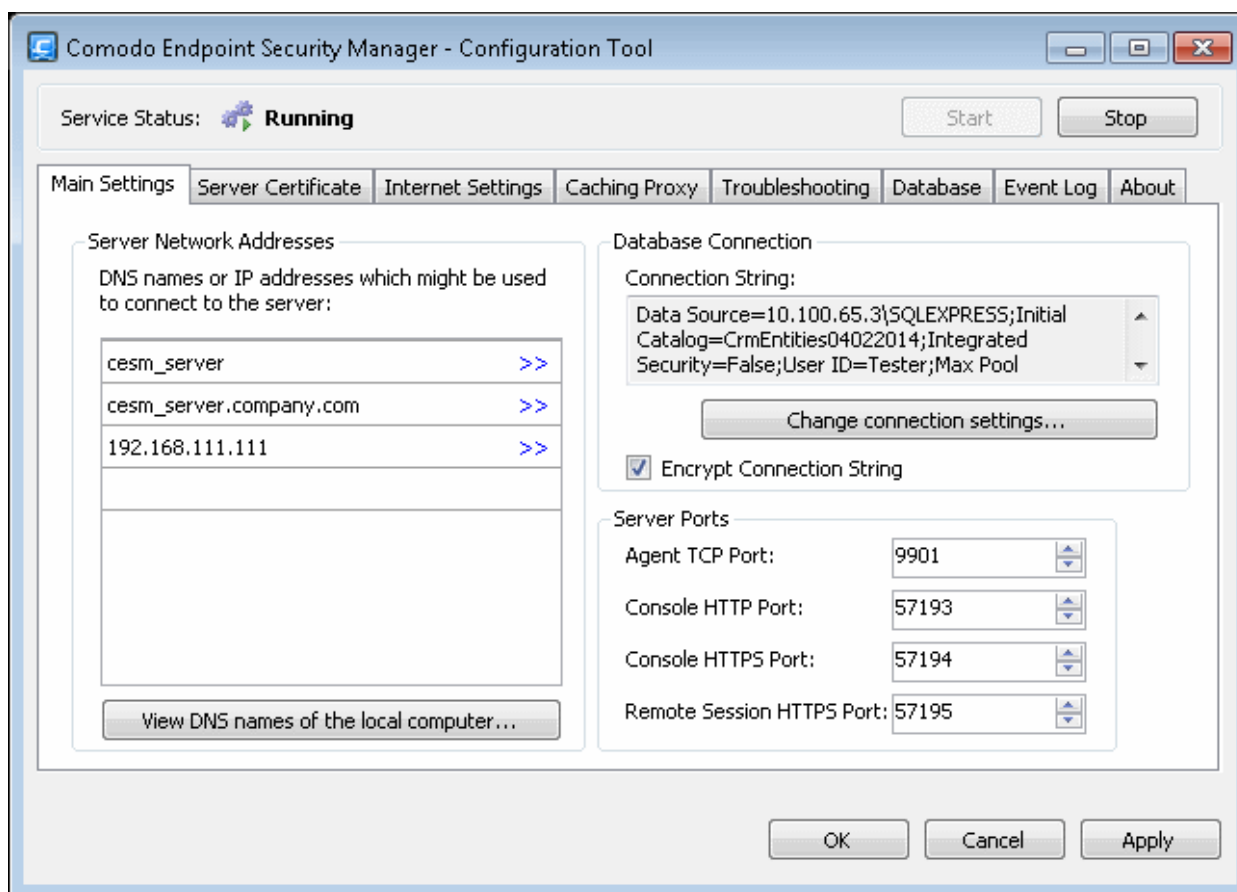
To open the Service Configuration Tool, Click Start > All Programs > COMODO > Endpoint Security Manager > CESM Configuration Tool.
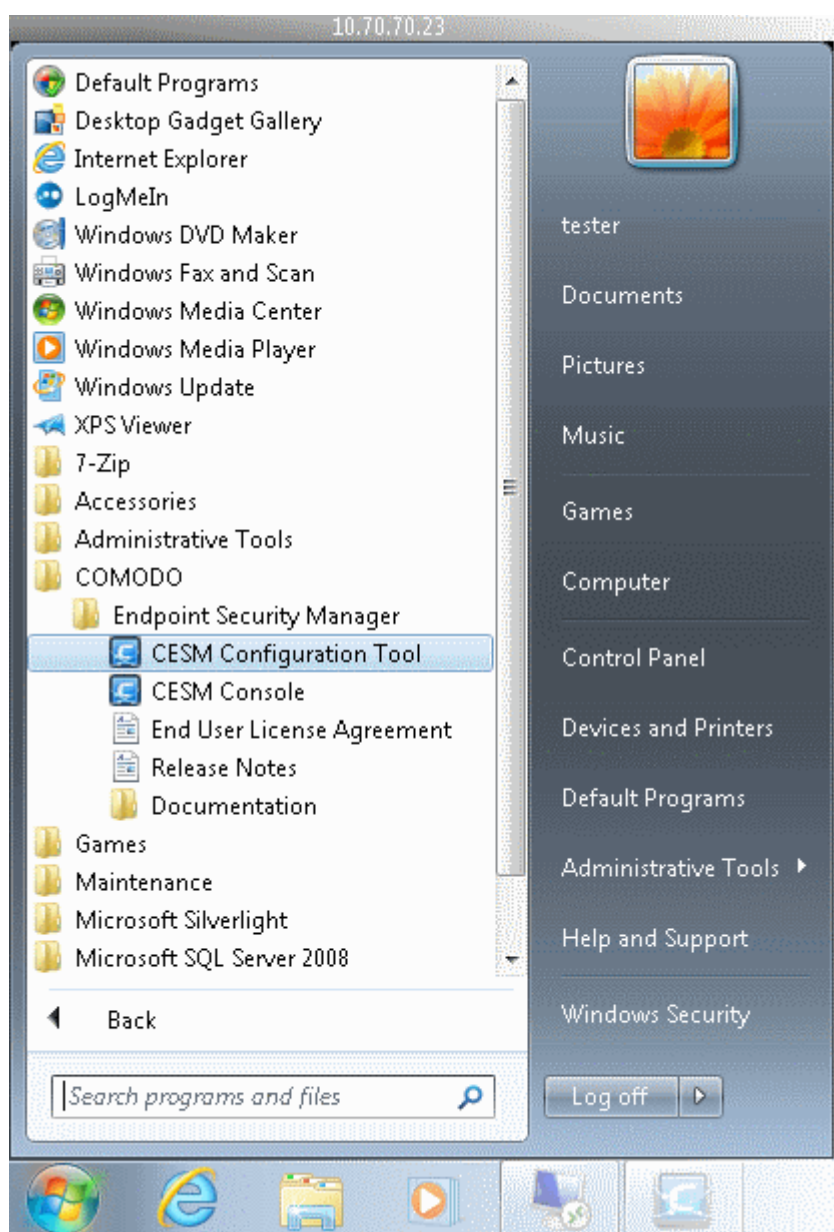
The main interface of the tool will be opened. It contains the following areas:

- **Service Status Area** - Indicates the current service ESM status and allows administrator to start or stop the service.

- **Main Settings** - Enables the administrator to view and modify the connection and port settings.

- **Server Certificate** -Enables the administrators to manage server SSL certificates.

- **Internet Settings** - Enables the administrator to view and modify proxy server settings.

- **Caching Proxy Settings** - Enables administrators to manage access to resources.

- **Troubleshooting** - Enables the administrators to configure debug log storage settings

- **Database** - Enables the administrators to view and manage the CESM database.

- **Event Log** - Enables the administrator to view the log of database events.

- **About** - Indicates the current service ESM version.


Starting and Stopping the CESM Service

The Service Status area at the top of the interface states whether the ESM Service is 'Running' or 'Stopped'.
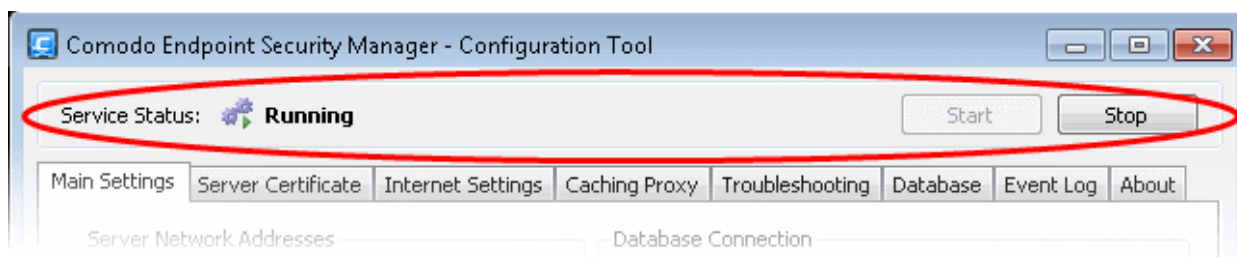
- To stop the running service, click the 'Stop' button.
- To start the service, click the 'Start' button.

Main Settings

The 'Server Network Addresses' area of the 'Main Settings' tab displays ESM server IP addresses and/or hostnames. Database connection settings, Console Port, Secure Console Port and Agent Ports are shown on the right.
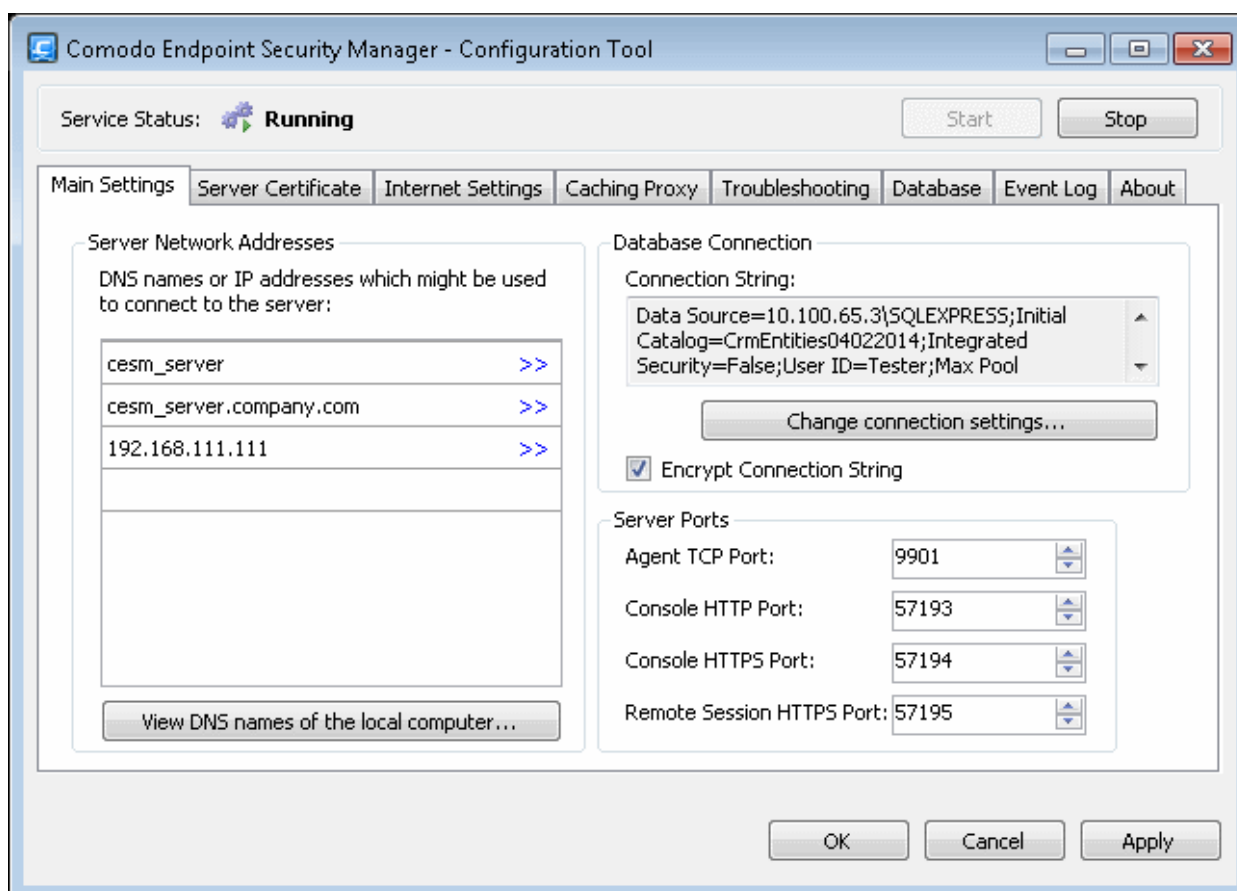

- **Server Network Addresses** - Displays the host names and DNS names of the server on which the CESM console is installed. To add an IP or Hostname, simply begin typing in the blank row beneath those already listed. Click 'OK' to confirm.
- **Server Ports:**

- **Agent TCP Port** - Displays the port number of the server through which the agents installed in the endpoints communicate with the server.

- **Console HTTP Port** - Displays the port number of the server through which the CESM console can be accessed through a non-secure connection.

- **Console HTTPS Port** - Displays the port number of the server through which the CESM console can be accessed through a secure SSL connection.

- **Remote Session HTTPS Port** - Displays the port number of the CESM server for the target endpoints to connect to the server during their Remote Desktop Connection sessions through a secure SSL connection.

- To change port numbers, simply type the new port number in the appropriate field.

- **Database Connection Settings -** Displays the connection string currently in action to connect to the SQL Server. To change the database connection settings, directly edit the parameters at the 'Connection String' click 'Change connection settings'.

The SQL Server Connection Properties dialog will open.
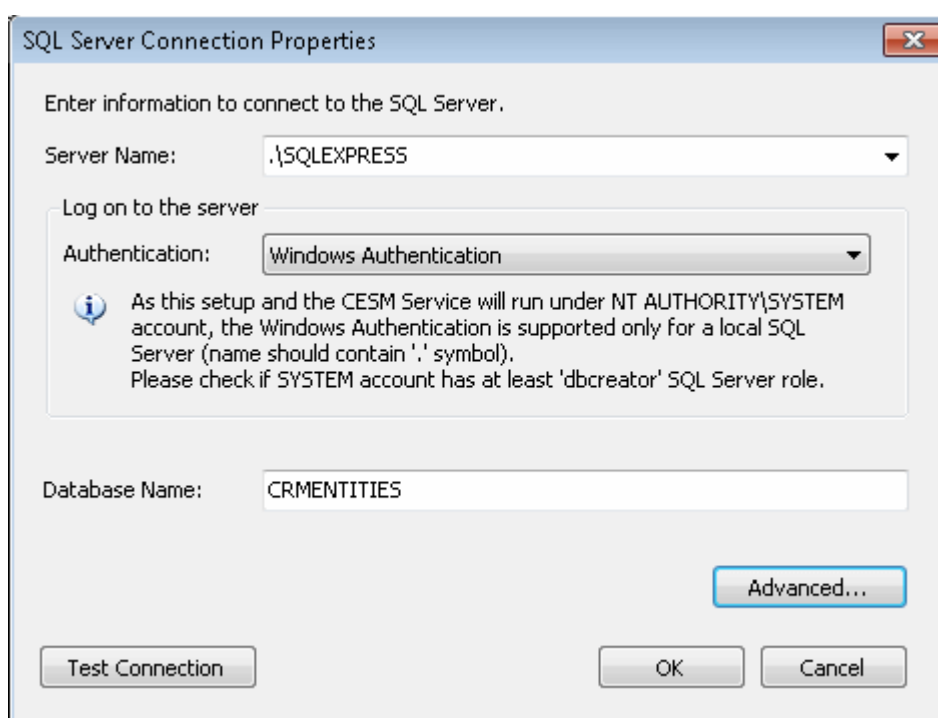
- You can configure the Windows or SQL server connection settings from this dialog. For configuring advanced connection properties, click the 'Advanced' button.
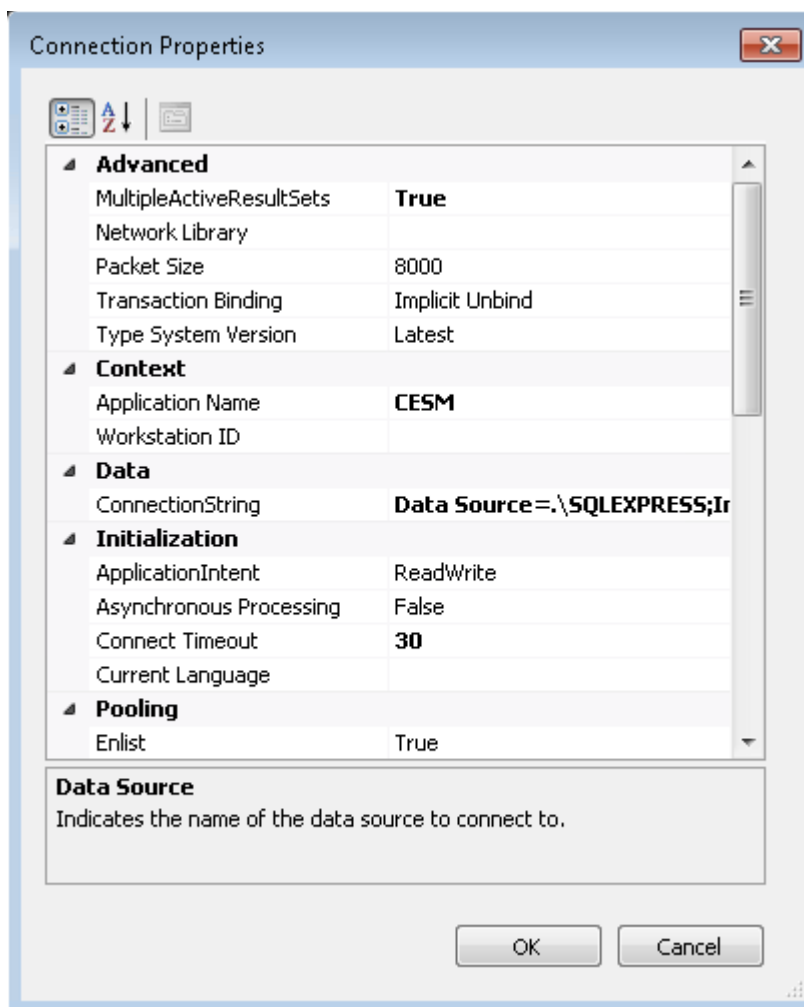
- Edit the parameters directly in the 'Connection Properties' dialog and click OK.

- To test whether the connections settings are appropriate, click 'Test Connection' in the 'SQL server connection Properties' dialog.

- Click OK in the 'SQL server connection Properties' dialog for your changes to take effect.

- You will need to enter the hostname/IP and console port in the address bar of your browser to connect to the ESM server. For example, https://192.168.111.111:57194 will open the ESM console hosted at that IP address using the secure console port.

- To facilitate external connections, you may have to open the listed port numbers on your corporate firewall.

Server Certificate

The Server Certificate tab allows administrators to view SSL certificate details, import a new certificate, create a certificate signing request (CSR) and to install a new certificate.
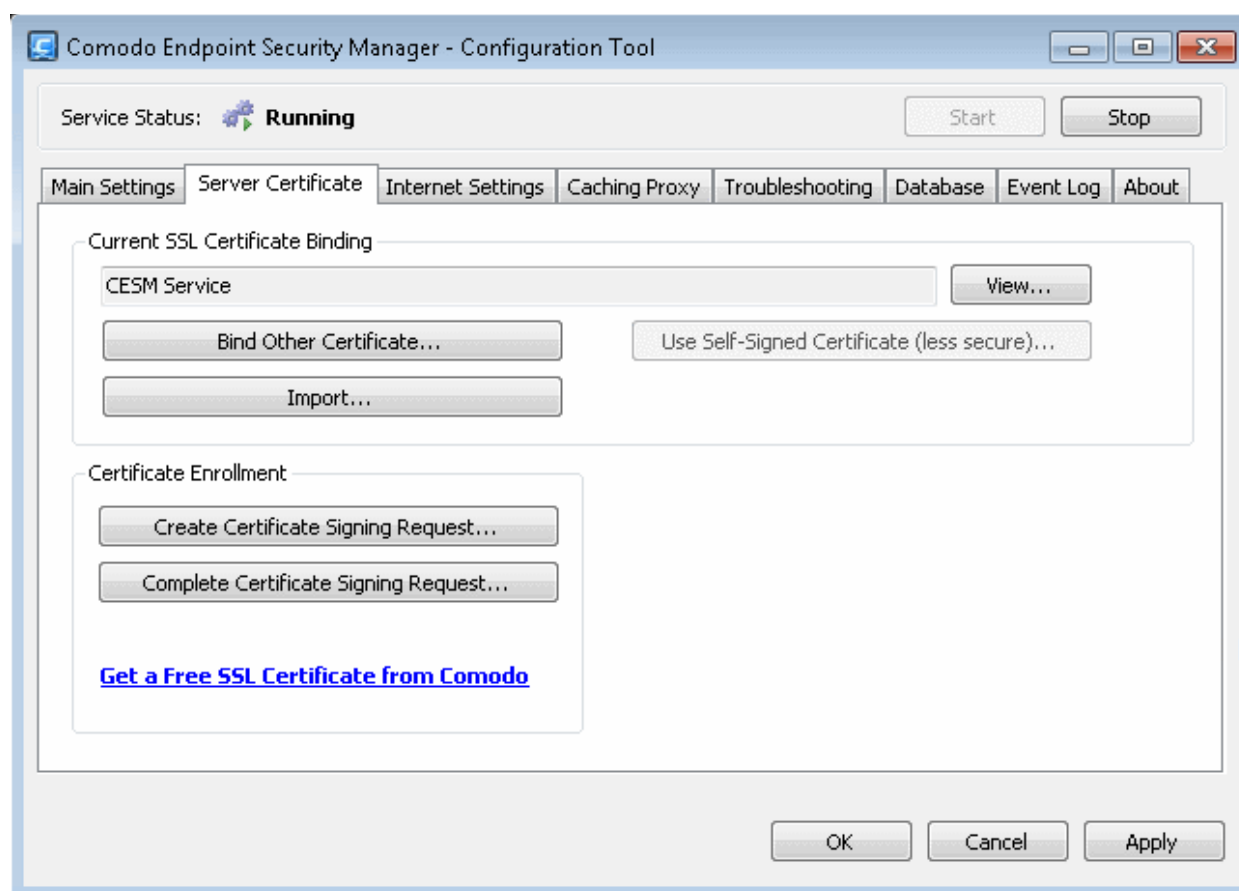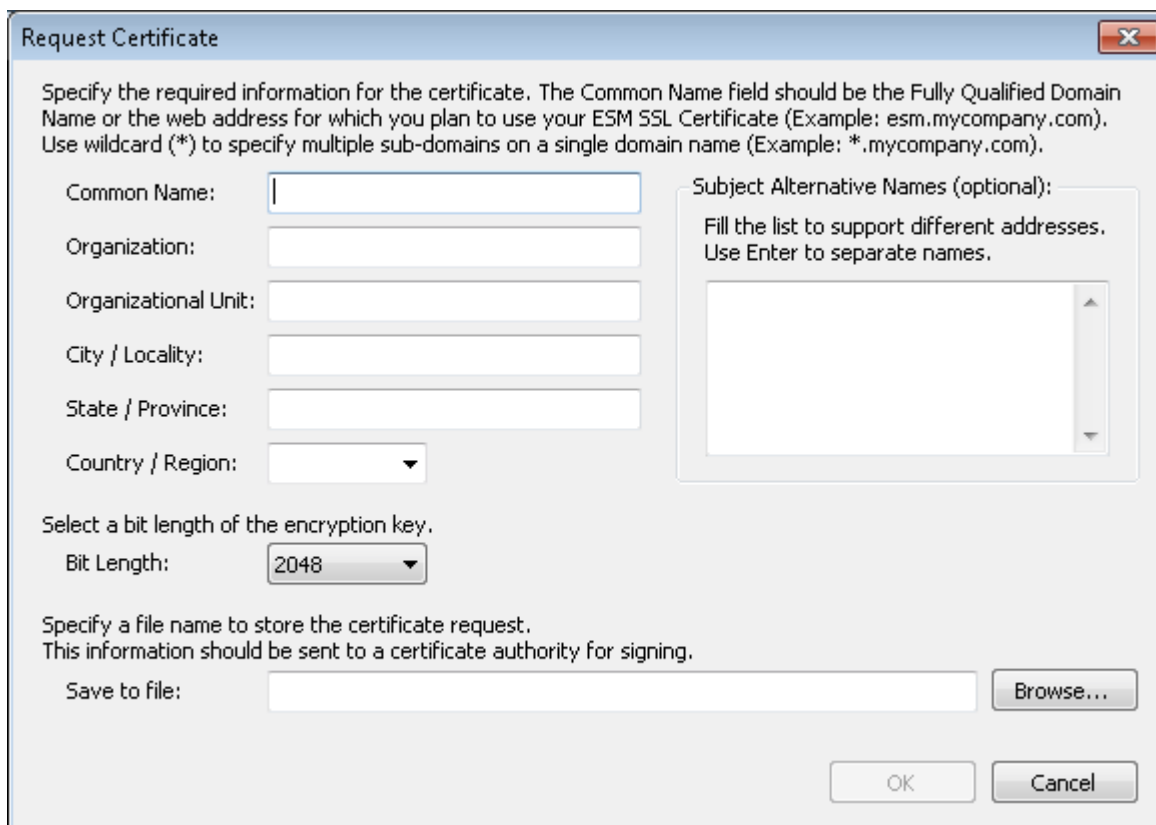
- To view the details of the currently installed server certificate, click the 'View' button.

- If multiple SSL certificates are used in the server, a certificate name error may occur when a HTTPS connection is established. To avoid this, you can bind the CESM to the required certificate using the 'Bind Other Certificate' option.

- To import certificates from other locations, click the 'Import' button.

Certificate Enrollment

The options in the Certificate Enrollment area allows you to enroll for a new server certificate.

- To create a Certificate Signing Request (CSR) for your server, click the 'Create Certificate Signing Request' button and fill in the required details in the 'Request Certificate' dialog.

- The generated CSR can be used for applying for a certificate.

- Click the 'Install SSL Certificate' button to install new SSL certificate in the server.

- Click the 'Get a Free SSL Certificate from Comodo' link to obtain a free SSL certificate from Comodo, using the CSR generated.

Internet Connection Settings

The Internet Settings tab allows administrators to specify proxy settings for Internet connection, if your network uses a proxy server.
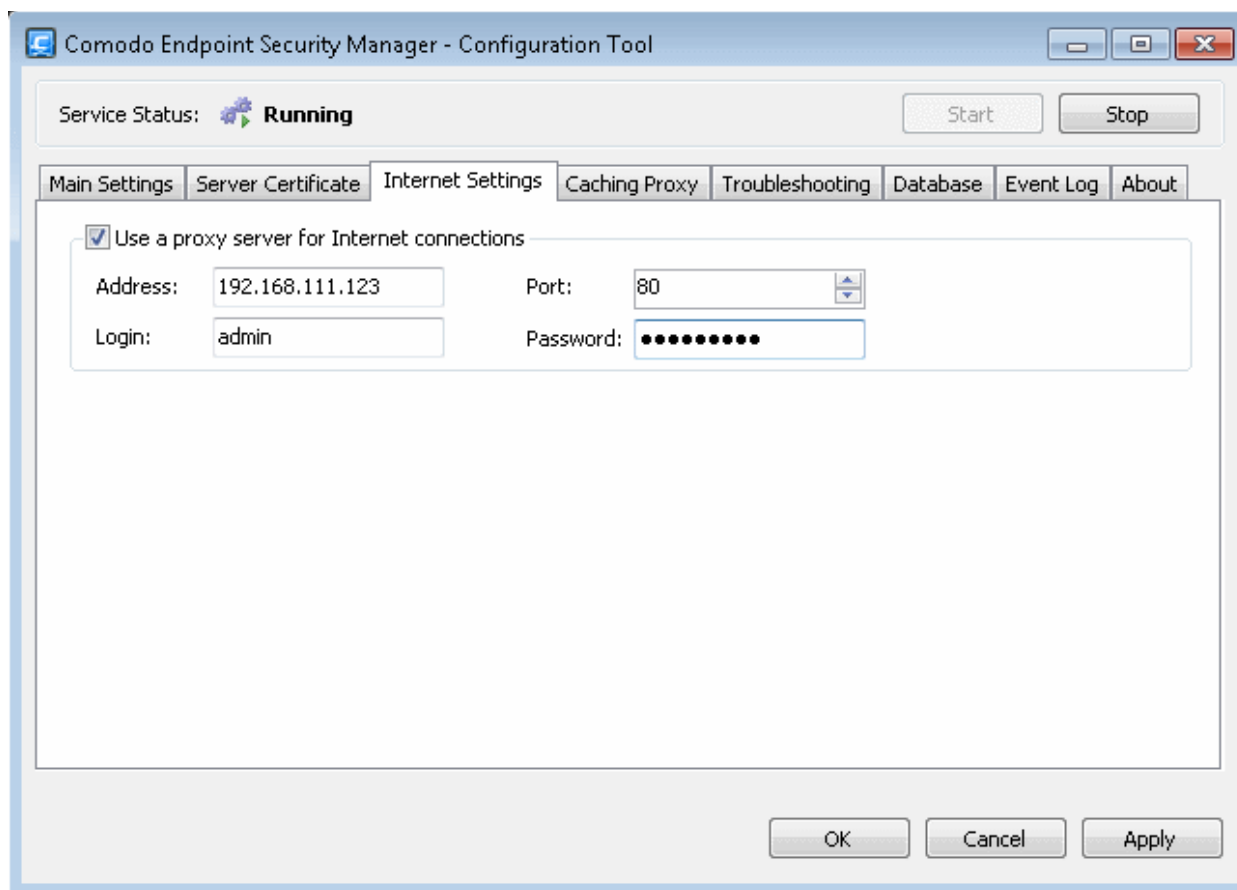
The administrator can select whether or not the CESM server should connect to Internet through a proxy server and specify the hostname/IP address and login credentials of the proxy server to be used.

Caching Proxy Settings

The Caching Proxy tab allows administrators to specify the proxy server settings for storing cache content. The proxy server will store antivirus updates. CES on endpoints that are configured to connect to this proxy server will receive the latest updates, which will be considerably reduce Internet traffic.
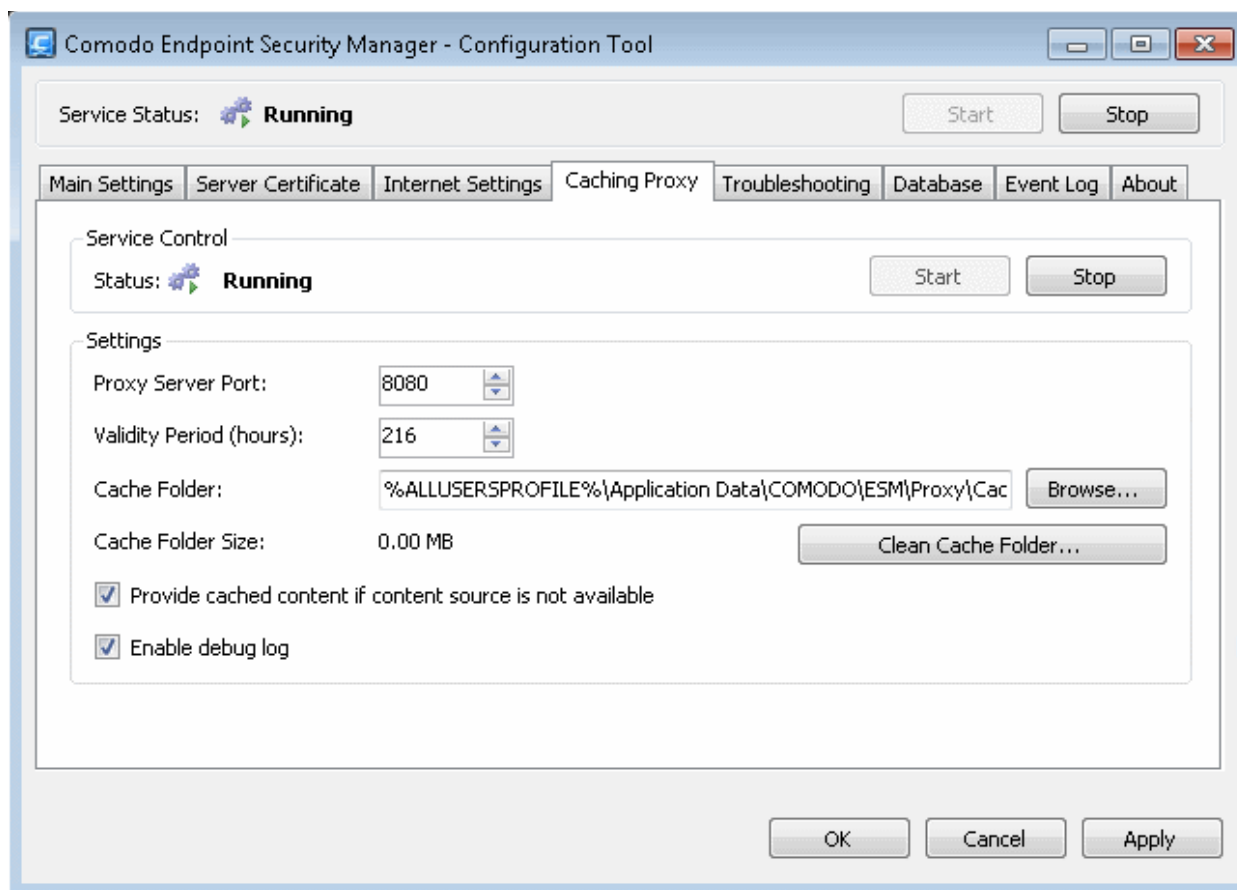
- Click the 'Start' or Stop' button to enable or disable the proxy server.

- The settings panel allows the administrator to configure the proxy server port, validity period of the cache content in hours and to define a path for the cache folder.

- Click the 'Clean Cache Folder...' button to remove the content in the cache folder.

- Select the check box 'Provide cached content if content source is not available' for the endpoints to update from the proxy server if the content source is not available via Internet.

Troubleshooting

The 'Troubleshooting' tab allows administrators to specify storage settings for debug logs, which are useful for identifying issues.
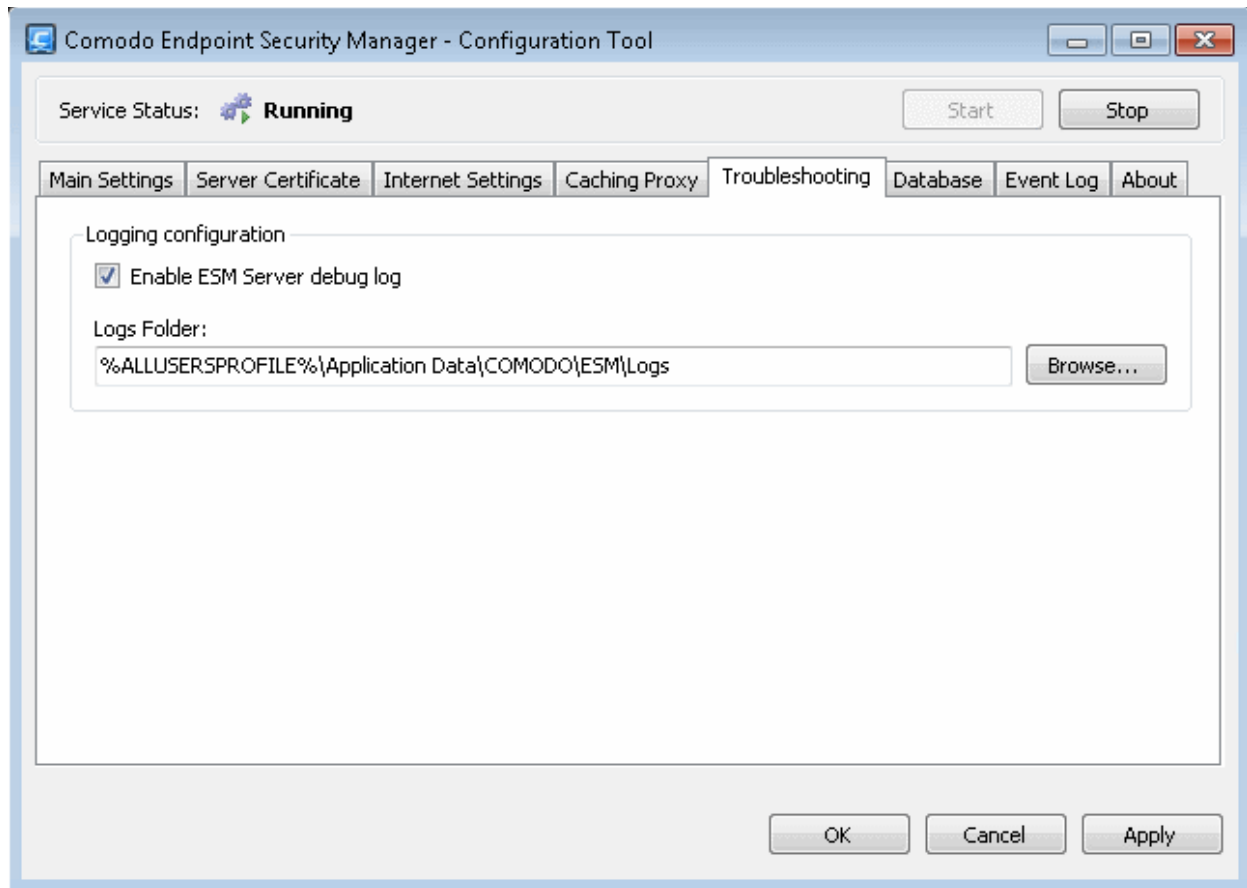
The administrator can choose whether or not the CESM debug logs are to be saved and specify the location in the server for storing the log files.

Viewing and Managing CESM Database Files

The Database tab allows administrators to view and clean the database files of CESM stored in server. Please note the tab displays the CESM database in the server that was configured in the Main Settings tab > Database Connection.
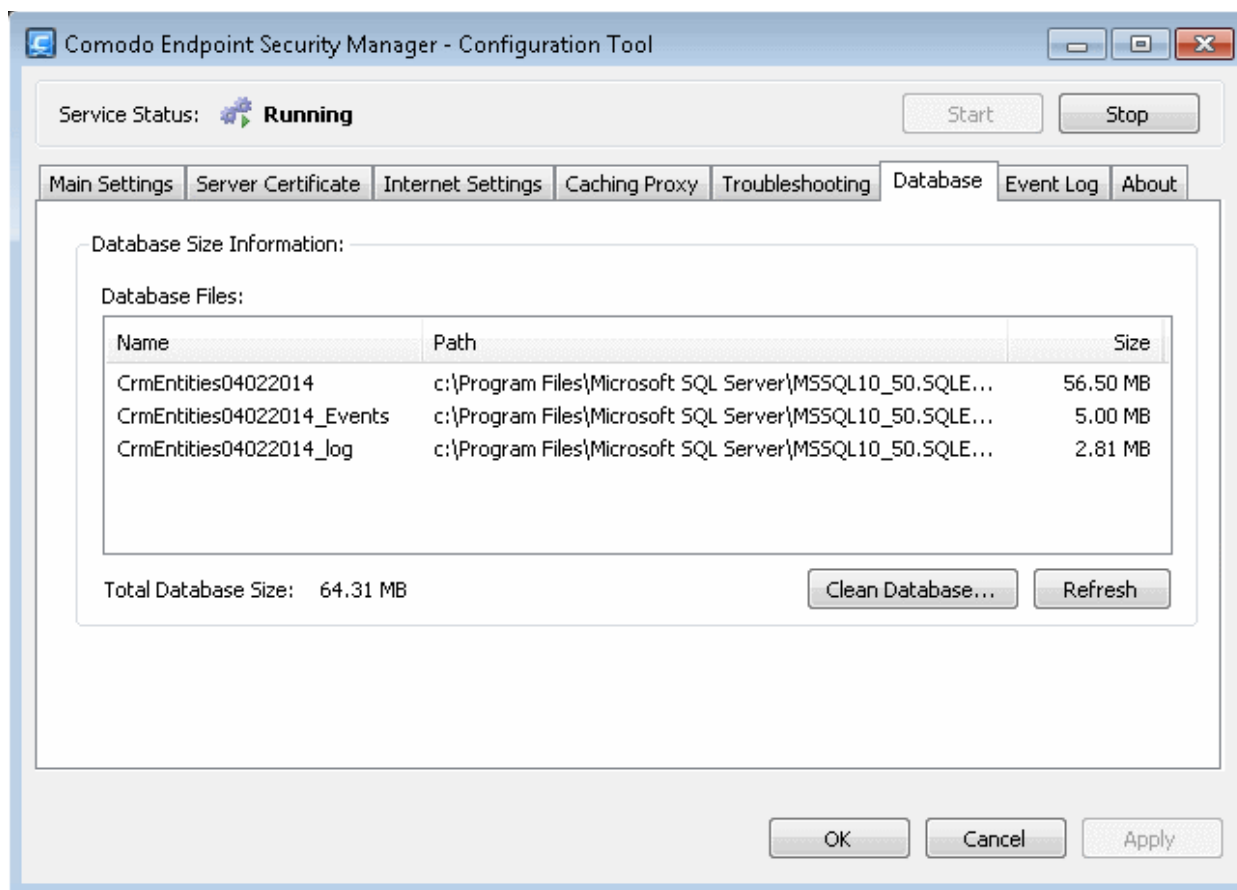
Admins that use a local database or SQL Express may not require this feature since they have database size limitation built into them. However, this can useful for other versions of SQL server to clean up tables and make ESM server more efficient.

- Click the 'Refresh' button to load the latest entries

- Click the 'Clean Database...' button to clear the database

Viewing Event Log

The 'Event Log' contains a list of notifications from ESM central service that may assist administrators to troubleshoot problems.
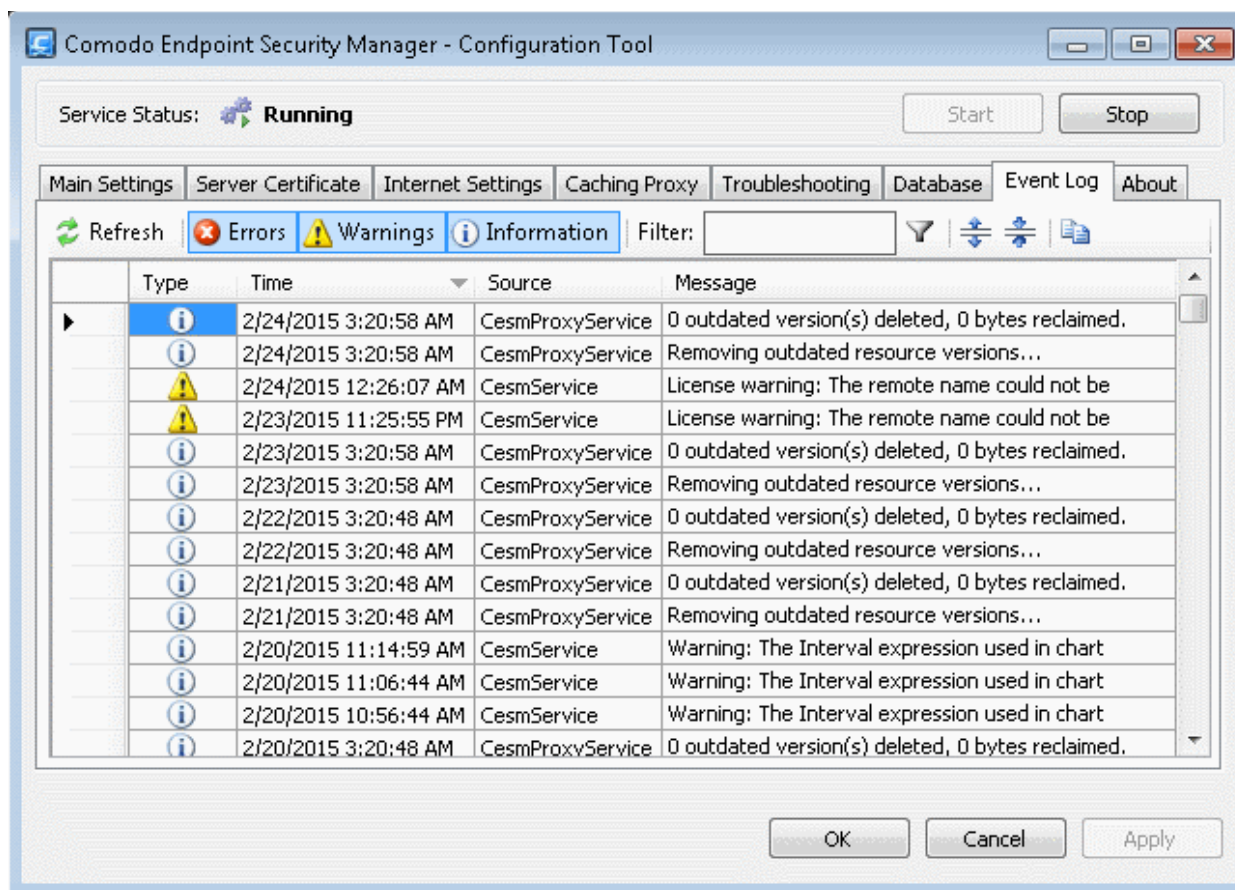
- The type of alerts that are displayed can be filtered by clicking the 'Errors', 'Warnings' and 'Information' buttons
- Alternatively, type a specific search term into the text field then click the 'Apply Filter' button.
- Each cell can be individually selected by clicking it.
- Multiple cells can be selected whilst holding down the 'Shift' or 'CTRL' keys and left-clicking on target cells.
- Cells can be copied to the clipboard by clicking the 'Copy' button.

Column	Types/Format	Definition / Description
Type (of event)		Error - 'Errors' are those events whereby the ESM Central Service failed to execute a command.
		Warning - High severity errors that may (or already have) prevented the ESM service from connecting to the data source. For example, a critical application crash.
		Information - 'Information' events typically inform the administrator of the successful completion of task by the ESM service.
Time	*MM/DD/YYY HH:MM:SS*	Displays the precise time that the event was generated on the endpoint machine.
Message	*Text*	Contains a description of the event. • Use the control to view the full message.

Column	Types/Format	Definition / Description
		• Use the [icon] control to view a condensed version of the message (this is the default view). • Use the [icon] control to copy the contents of the message to the clipboard.

Control	Control Type	Description
Errors	Filter by event	Click this button to add or remove events of type 'Error' from the displayed list.
Warnings	Filter by event	Click this button to add or remove events of type 'Warning' from the displayed list.
Information	Filter by event	Click this button to add or remove events of type 'Information' from the displayed list.
Refresh	Remove filters and refresh list	Clears any active filters so all event types are displayed. Also loads the latest event entries.
Filter:	Filter by string	Allows the administrator to filter events by typing a specific text string. Administrator should then click the 'Apply Filter' button.
[icon]	Apply Filter	Implements the filter typed into the text field.
[icon]	Select Event	Selects a particular event row. Once selected, clicking the 'Expand Rows' control will highlight the information pertaining to this event.
[icon]	Expand Rows	Displays the complete 'Message' for all event rows. The event row that is selected using the 'Select Event' control will be highlighted. Information of this detail level may be required for troubleshooting purposes.
[icon]	Contract Rows	Displays the condensed 'Message' (all events). This is the default view.
[icon]	Copy	Copies the contents of the selected cells to the clipboard.

About

The 'About' tab displays copyright information, the current ESM version number and allows administrators to select available languages. You can switch between installed languages by selecting from the 'Language' drop-down menu (English (United States), by default).
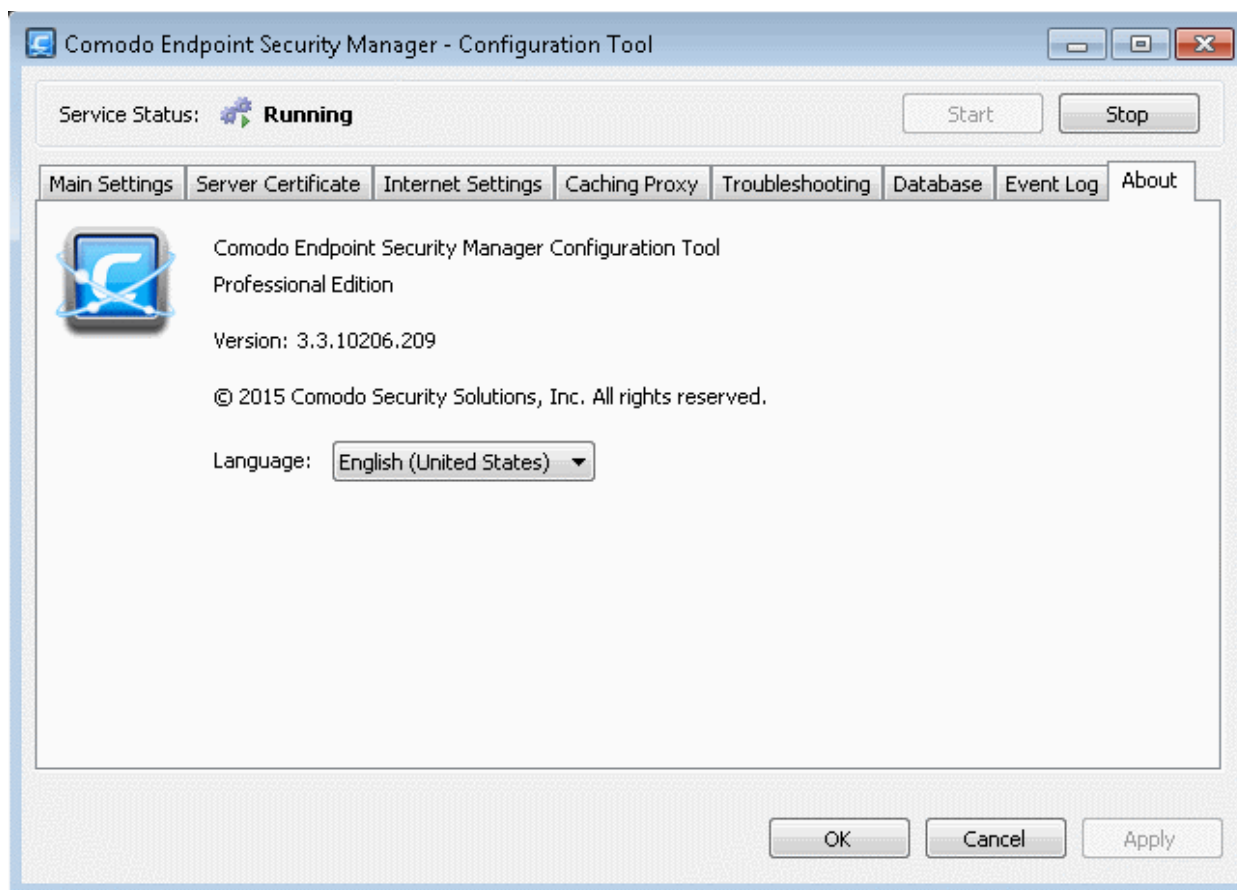
Appendix 2 - How to... Tutorials

The 'How To...' section of the guide contains guidance on using CESM PE effectively. Click on the links below to go the respective tutorial page for guidance of the respective feature.

- **How to configure CESM policies - an introduction**
- **How to Setup External Access from Internet**
- **How to Install CES/CAS on Windows Endpoints Which Were Added by Manually Installing the Agent**
- **How to Install CAVM on Mac Endpoints Which Were Added by Manually Installing the Agent**

How to Configure CESM policies - An Introduction

A CESM policy is the security configuration of Comodo Endpoint Security (CES) or Comodo Antivirus for Servers (CAS) deployed on an endpoint or a group of endpoints. Each policy determines the antivirus settings, Internet access rights, firewall traffic filtering rules and Defense+ application control settings for an endpoint.

The CESM Policy can be derived from the configuration of Antivirus, Firewall, Defense+ and File rating components of CES or Antivirus, Defense+ and File rating components of CAS on an endpoint and can be rolled out to any number of endpoints or endpoint groups.

In order to configure Antivirus, Firewall, Defense+, File Rating settings in CES or Antivirus, Defense+ and File rating components in CAS on an endpoint computer, the administrator has to ensure that the endpoint computer is 'Locally Configured' (or CESM will remotely re-apply the endpoint's security policy and override any changes made by the administrator).

To change the policy applied to an endpoint to 'Locally Configured'

1. Open the Computers interface by choosing 'Computers' from the drop-down at the top left

2. Select the endpoint and open the 'Endpoint Properties' interface by clicking the 'Properties' or double clicking on the selected endpoint

---

3. Click 'Advanced' from the left hand side navigation

4. Select the 'Use individual policy for this computer' radio button.

5. Choose 'Locally Configured' from both Local Policy and Internet Policy drop-downs.
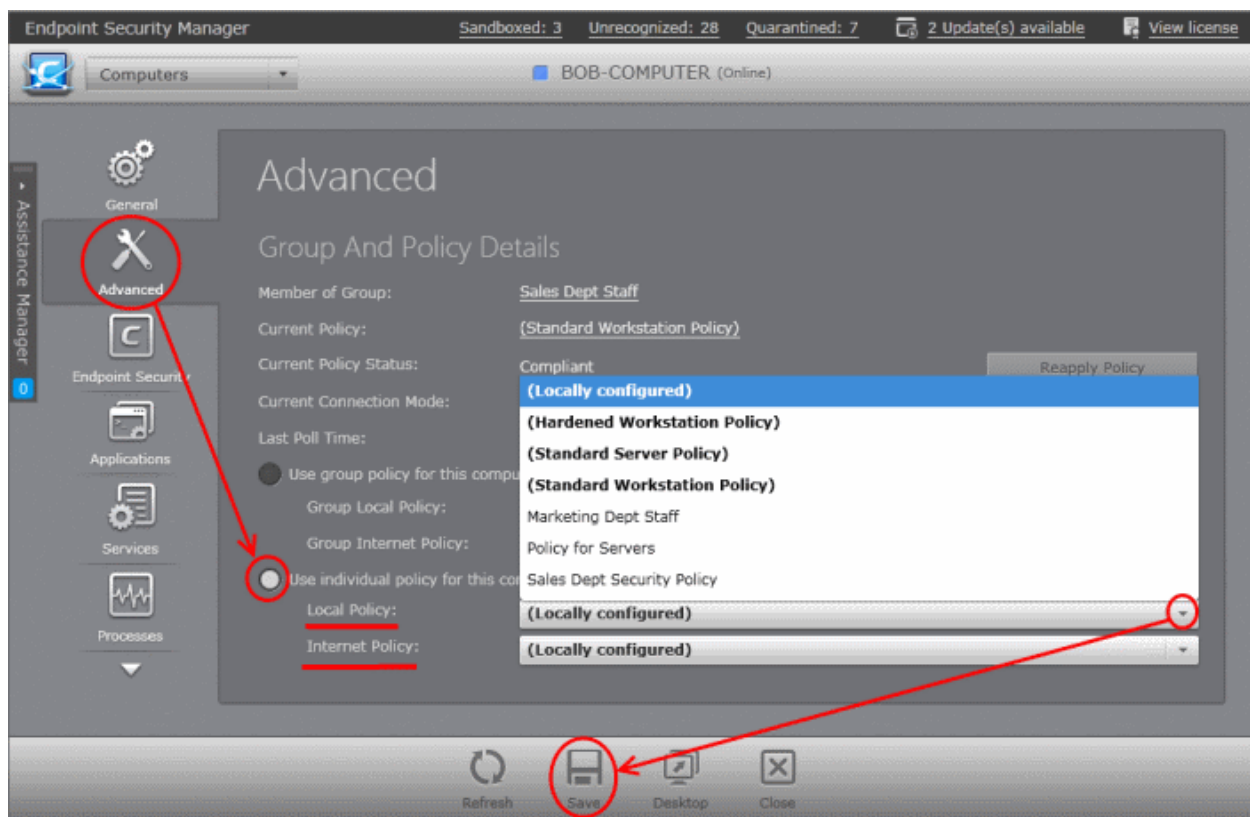
6. Click 'Save' at the bottom of the interface

The administrator can now configure the settings for Antivirus, Firewall and Defense+ components and file rating settings of CES or Antivirus, Defense+ and components and file rating settings of CAS at the endpoint, for importing into the policy created.

Once the administrator has created the policy on the new machine, it can be imported in CESM from this machine then applied to target computers as required (including the one from which the settings are imported). See '**Creating a New Security Policy**' for more details.

The remainder of this page is a quick primer to key areas within CES for modifying Antivirus, Firewall and Defense+ settings along with links to the appropriate section in the dedicated CES user-guide should further help be required.

Antivirus Settings (for CES and CAS)
Comodo Antivirus leverages multiple technologies, including Real-time/On-Access Scanning, On Demand Scanning and a fully featured Scan Scheduler to immediately start cleaning or quarantining suspicious files from your hard drives, shared disks, emails, downloads and system memory.

To configure Antivirus Behavior Settings

• Click the 'Tasks' arrow from the CES / CAS home screen to switch to 'Tasks' pane.
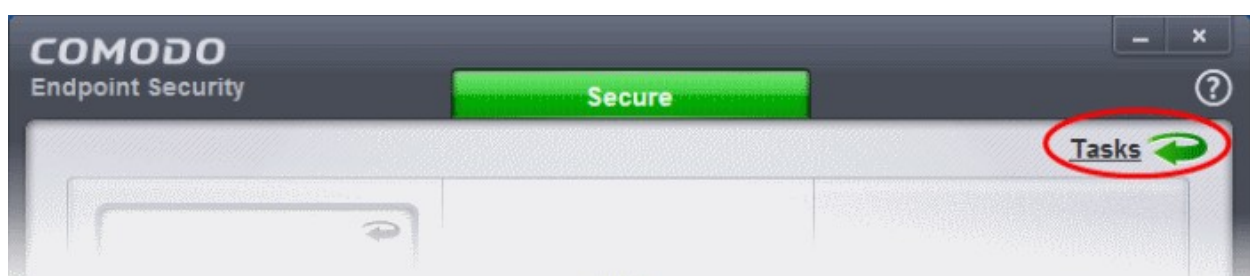
• Click 'Advanced Tasks' then 'Open Advanced settings'

- Click 'Security Settings' > 'Antivirus' from the left hand side navigation of Advanced Settings interface.

  - Click 'Realtime Scan' from the LHS navigation to configure real time or on access scanner settings.

  - Click 'Scans' from the LHS navigation to create or edit custom scan profiles, that allow you to define areas to be scanned, schedule scans and to specify the behavior of the scan engine for each profile.

  - Click 'Exclusions' from the LHS navigation to add files folders and programs that are to be excluded from scanning.
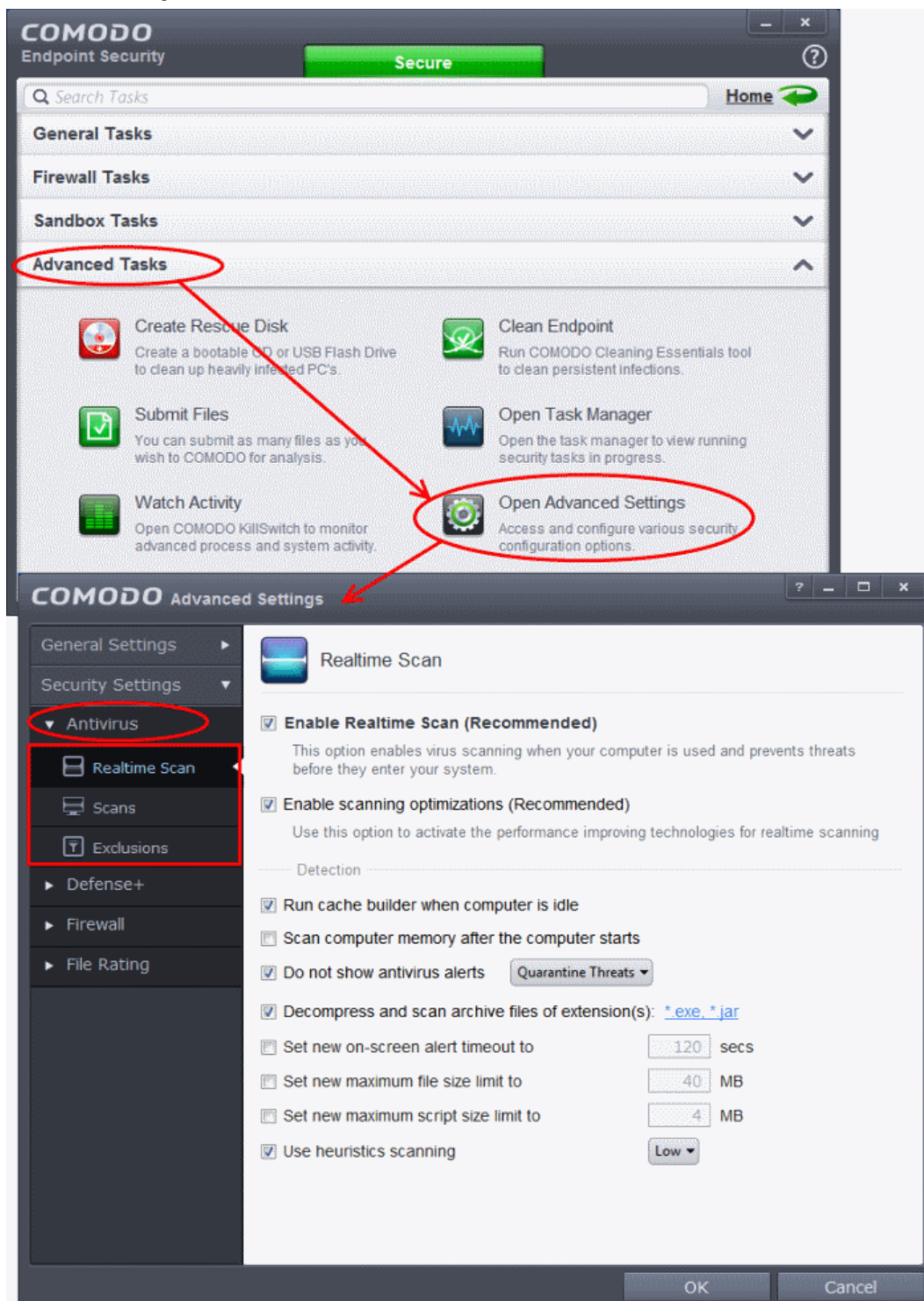

If more details are required for these settings, see Antivirus Settings help pages of CES online help guide at **http://help.comodo.com/topic-84-1-499-5553-Antivirus-Settings.html**. Each configuration area has its own dedicated page containing detailed descriptions of the options and settings configurable through it.

Firewall Settings (for CES only)

The firewall component of Comodo Endpoint Security offers the highest levels of security against inbound and outbound threats, can stealth endpoint ports against hackers and can prevent malicious software from transmitting confidential data over the Internet.

To configure Firewall Behavior Settings

- Click the 'Tasks' arrow from the CES home screen to switch to 'Tasks' pane.

- Click 'Advanced Tasks' then 'Open Advanced settings'.

- Click 'Security Settings' > 'Firewall' from the left hand side navigation of 'Advanced Settings' interface.
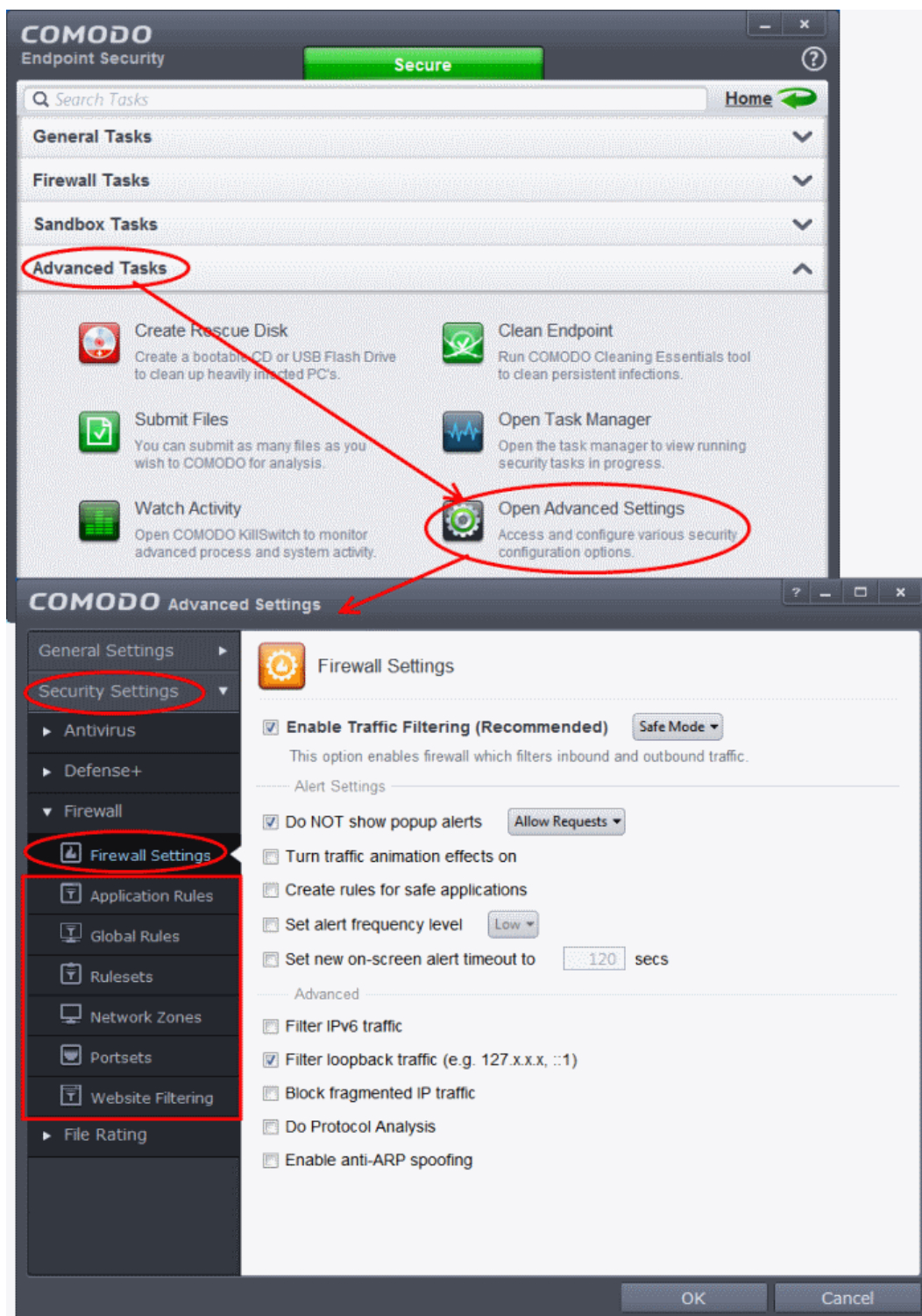
- Click 'Firewall Settings' from the LHS navigation to configure overall Firewall behavior settings.

- Click 'Application Rules' from the LHS navigation to configure individual firewall rules for specific applications containing instructions that determine whether the application should be allowed or blocked;

which protocols it is allowed to use; which ports it is allowed to use and so forth. The individual Application Rules can be used to constitute a Firewall Rule set.

- Click 'Global Rules' from the LHS navigation to configure rules to be applied to all traffic traveling in and out of your computer. Individual Global Rules can be used to constitute a Firewall Rule set.

- Click 'Rulesets' from the LHS navigation to configure rulesets, containing a set of one or more individual network control rules that have been saved and which can be re-deployed on multiple applications. Comodo Firewall allows or denies network access requests from an application based upon the Firewall Ruleset that has been specified for that application.

- Click 'Network Zones' from the LHS navigation to define trusted network zones to allow access and untrusted network zones to be blocked access to them.

- Click 'Portsets' from the LHS navigation to define handy, predefined groupings of one or more ports that can be re-used and deployed across multiple Application Rules and Global Rules.

- Click 'Website Filtering' from the LHS navigation to set up rules to allow or block access to specific websites.

If more details are required for these settings, see Firewall Settings help pages of CES online help guide at **http://help.comodo.com/topic-84-1-499-6043-Firewall-Settings.html**. Each configuration area has its own dedicated page containing detailed descriptions of the options and settings configurable through it.

Defense+ Settings (for CES and CAS)

The Defense+ component of CES / CAS is a collection of prevention based security technologies designed to preserve the integrity, security and privacy of your operating system and user data.

- **Sandbox** - Authenticates every executable and process running on your computer and prevents them from taking actions that could harm your computer. Unrecognized processes and applications will be auto-sandboxed and run under a set of restrictions so they cannot harm your computer. This gives untrusted (but harmless) applications the freedom to operate whilst untrusted (and potentially malicious) applications are prevented from damaging your PC or data. You can define rules how these identified applications can be run in the Sandbox, that is,

- run with restricted access to operating system resources
- run completely isolated from your operating system and files on the rest of your computer
- completely block from running
- or allow it to run outside the sandbox environment without any restriction.
- **Host Intrusion Protection (HIPS)** - A rules-based intrusion prevention system that monitors the activities of all applications and processes on your computer. HIPS blocks the activities of malicious programs by halting any action that could cause damage to your operating system, system-memory, registry keys or personal data.

- **Viruscope** - It monitors the activities of processes running on your computer and alerts you if they take actions that could potentially threaten your privacy and/or security. Apart from forming yet another layer of malware detection and prevention, the sub-system represents a valuable addition to the core process-monitoring functionality of the Defense+ by introducing the ability to reverse potentially undesirable actions of software without necessarily blocking the software entirely.

To configure Defense+ Settings

- Click the 'Tasks' arrow from the CES / CAS home screen to switch to 'Tasks' pane.

- Click 'Advanced Tasks' then 'Open Advanced settings'.

- Click 'Security Settings' > 'Defense+' from the left hand side navigation of 'Advanced Settings' interface.
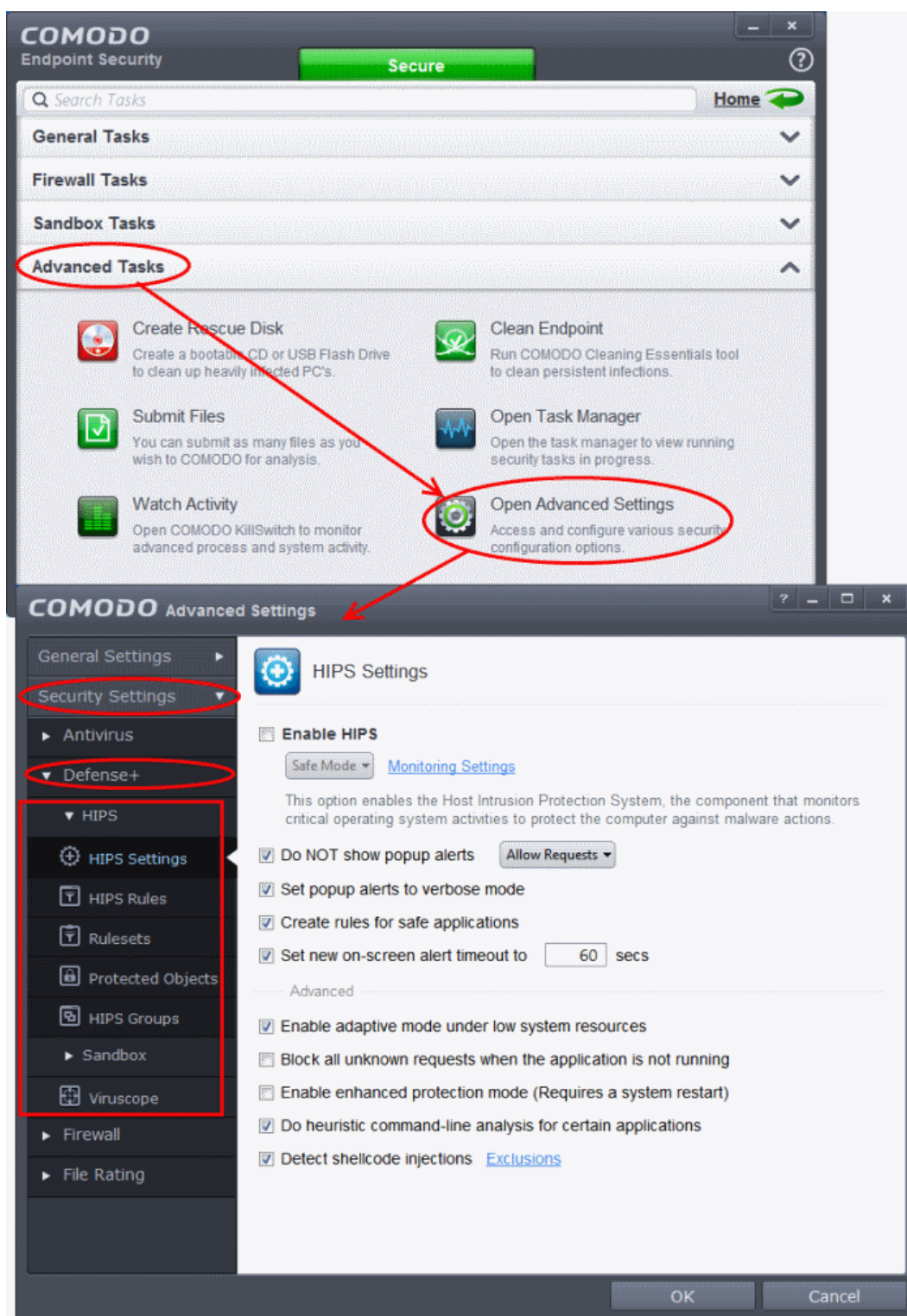
- Click 'Hips' and then the options below it from the LHS navigation to configure the overall behavior of host intrusion prevention system.

- Click 'Sandbox' and then the options below it from the LHS navigation to create auto-sandbox rules and to configure the sandbox settings.

- Click 'Viruscope' to configure its settings for monitoring activities of all the running processes.

If more details are required for these settings, see Defense+ Settings help pages of CES online help guide at **http://help.comodo.com/topic-84-1-499-5554-Defense+-Settings.html**. Each configuration area has its own dedicated page containing detailed descriptions of the options and settings configurable through it.

File Rating Settings (for CES and CAS)

CES/CAS allows the administrators to add trusted files that should be excluded from monitoring by HIPS, Unrecognized files

that should be blocked and add trusted software vendors to Trusted Vendors list so that the applications from trusted vendors will not be monitored by HIPS.

To configure File Rating Settings

- Click the 'Tasks' arrow from the CES/CAS home screen to switch to 'Tasks' pane.

- Click 'Advanced Tasks' then 'Open Advanced settings'.

- Click 'Security Settings' > 'File Rating' from the left hand side navigation of 'Advanced Settings' interface.
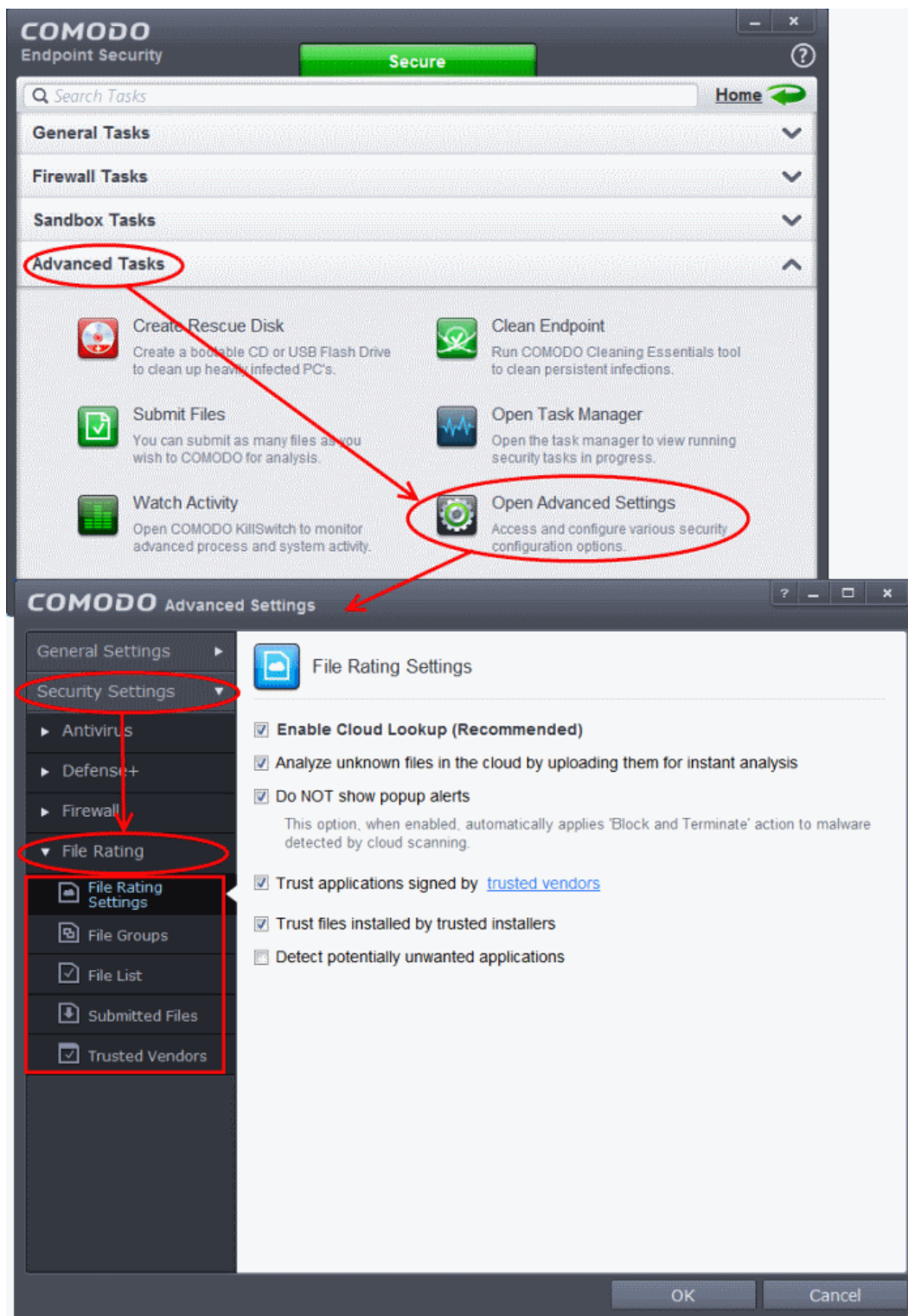
- Click 'File Rating Settings' from the LHS navigation to configure settings that govern the overall behavior of file rating.

- Click 'File Groups' from the LHS navigation to create predefined groups of one or more file types.

- Click 'Files List' from the LHS navigation to view and manage list of programs. applications and executable files discovered from your computer with their file rating and manually add files to it.

- Click 'Submitted Files' from the LHS navigation to view the list of files submitted for analysis to Comodo.

- Click 'Trusted Vendors' from the LHS navigation to view the list of trusted software vendors and manually add vendors.

If more details are required for these settings, see File Rating Settings help pages of CES online help guide at **http://help.comodo.com/topic-84-1-499-5556-Manage-File-Rating.html**. Each configuration area has its own dedicated page containing detailed descriptions of the options and settings configurable through it.

How to Setup External Access from Internet

The following guide explains how to configure CESM so that it can remotely manage endpoints that are connected via the Internet:

- Make sure that the CESM server has an externally accessible IP address.

- Open the CESM configuration tool - click 'Start > All Programs > COMODO > Endpoint Security Manager > CESM Configuration Tool'.
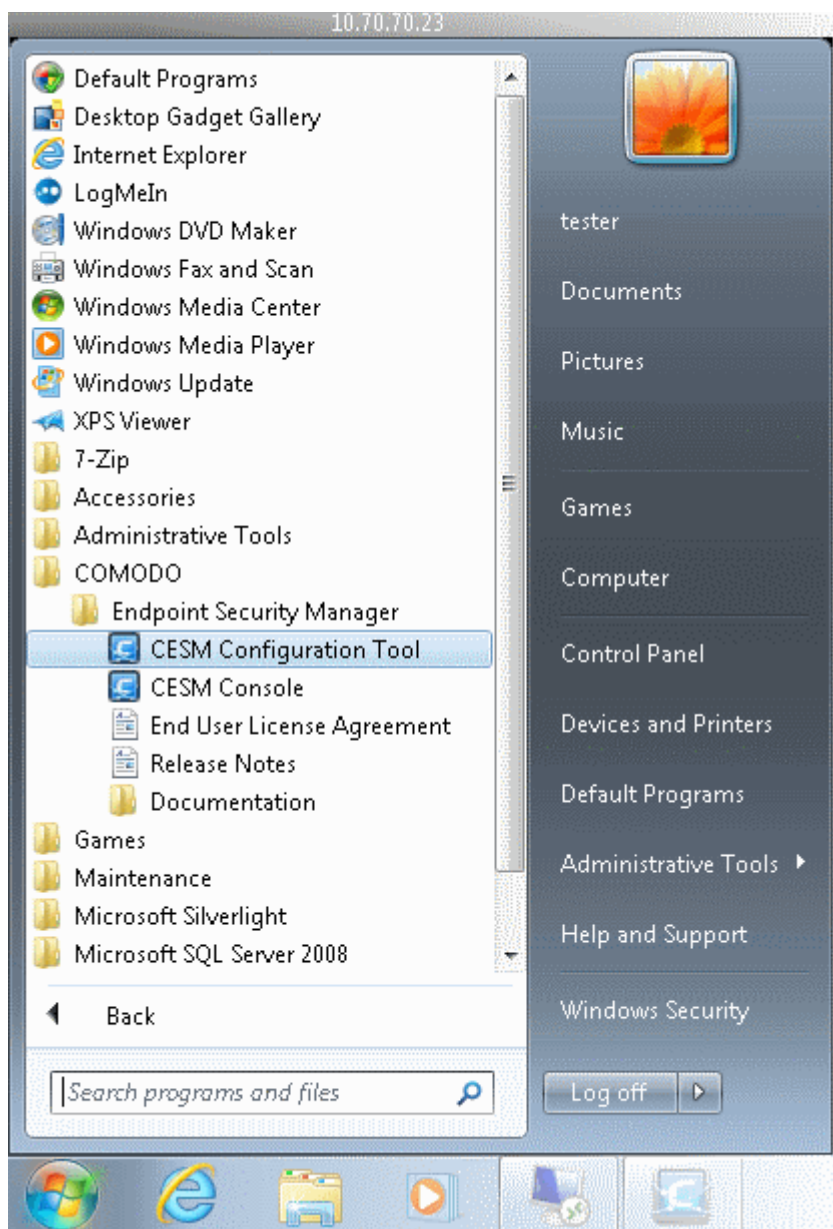
- Add the Internet reachable server IP address (alternatively hostname or FQDN) to the 'Server network addresses' list (just begin typing in the first blank row).
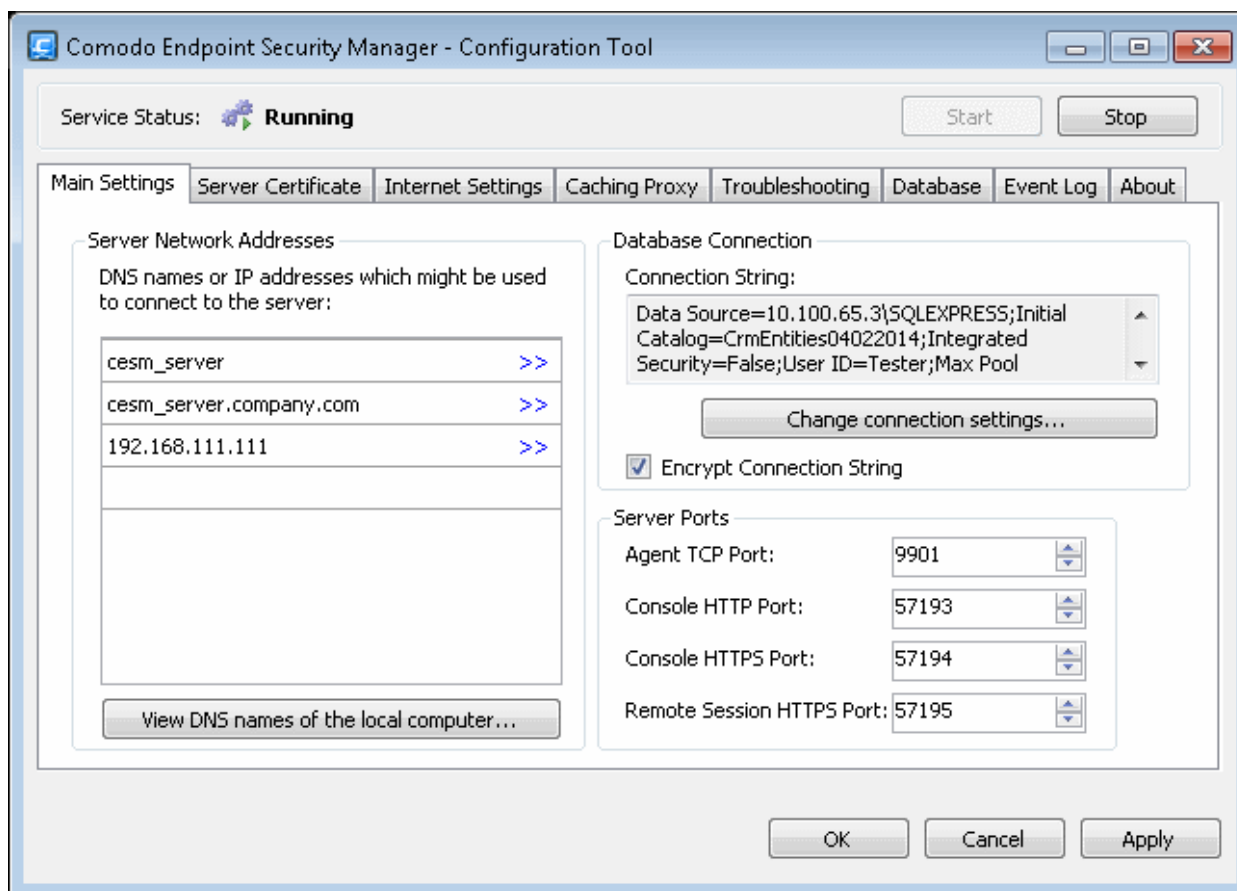
- Restart CESM service. See the 'Service Status' at the top of this interface, and after you click Apply, accept the prompt to restart the service:

- **If your network is equipped with a router or other similar device, it should be configured with CESM ports forwarding** (list of ports to be forwarded are listed in the 'Server Ports' on the right. Default ports are 57193, 57194 (console), 57195 (remote desktop session) and 9901 (agent).

To install agents on endpoints that are not on the local network

- Open 'Packages' screen by choosing 'Preferences' > 'Packages' from the drop-down at the top left.
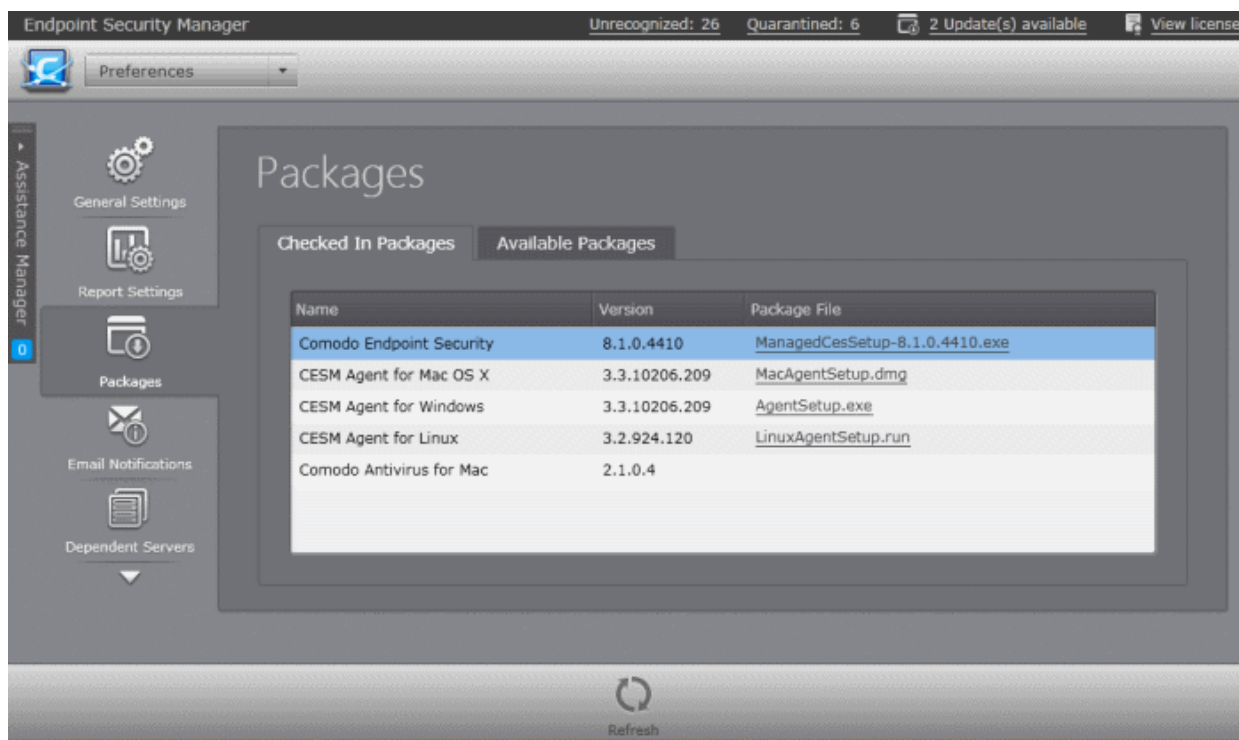
You can download a package in two ways:

- Click on the link in the package file column to directly download the package

- Right click on the link and choose 'Copy link address' to copy download URL to clipboard for downloading the package using a different browser or your favorite download manager
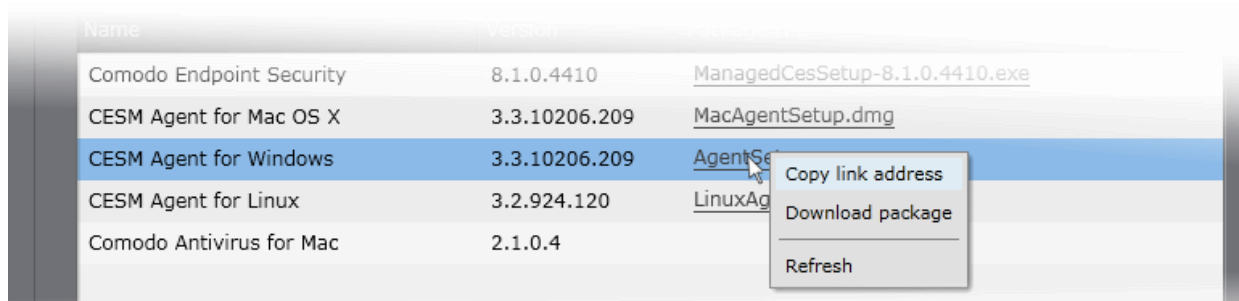
- The Agent Setup file enables the agent to be installed on any computers or laptops that will be used outside the network. The agent setup file can be copied to the target endpoint computer from DVD, CD, USB memory or by any other means and saved in a desired location. The agent can also be deployed using a third-party software distribution package.

- Double clicking on the setup file will start the installation wizard. For more details, please see **Adding Computers by Manual Installation of Agent and CES**.

Applying Policy for Endpoints Connected in Local Network and for Endpoints Connected via Internet

An administrator can create two policies for applying to a group of endpoints, where some endpoints are connected in local network and some are connected via the Internet. For example, the group may be named as 'HR Department' and the administrator can create two policies named as 'Policy for HR department - High Security' and 'Policy for HR department - Medium Security'. Now the administrator can select 'Policy for HR department - Medium Security' as Local Policy and 'Policy for HR department - High Security' as Internet Policy for this group.

The endpoints in the 'HR Department' group that connect to CESM through local network will be applied 'Policy for HR department - Medium Security' and for endpoints that connect via Internet will be applied 'Policy for HR department - High Security'.

- See section **Creating New Endpoint Groups and importing Existing Endpoints** for more details on creating endpoint groups.

- See section **Creating a New Security Policy** for more details on creating a new policy.

- See section **Key Concepts** to know about CESM Key Concepts.

- See section '**Best Practices**' to know how to use CESM effectively.

How to Install CES/CAS on Windows Endpoints Which Were Added by Manually Installing the Agent

CES/CAS can be remotely installed on Windows endpoints that were added to CESM by manually installing the agent. This situation frequently applies to endpoints which are connecting from an external network.
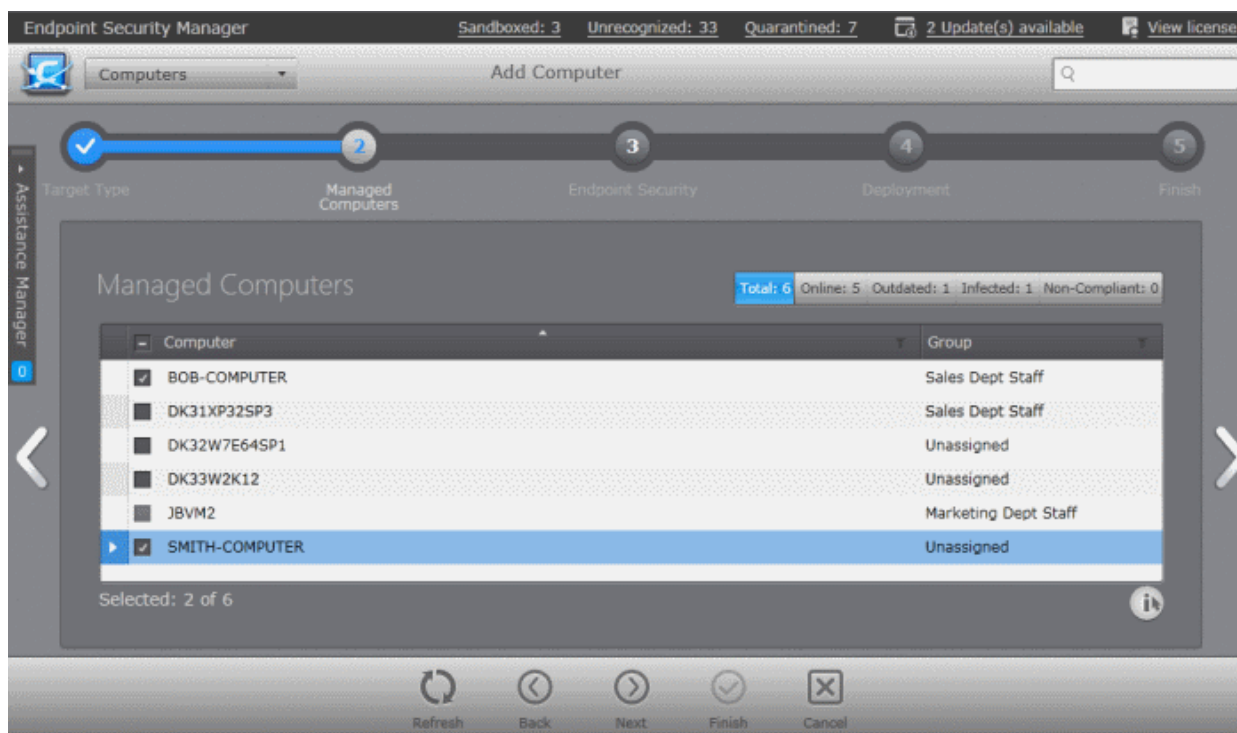
To install CES/CAS

1. Open the 'Computers' area by selecting Computers from the drop-down at the top left.

2. Click 'Add' from the 'Computers' area to start the wizard.
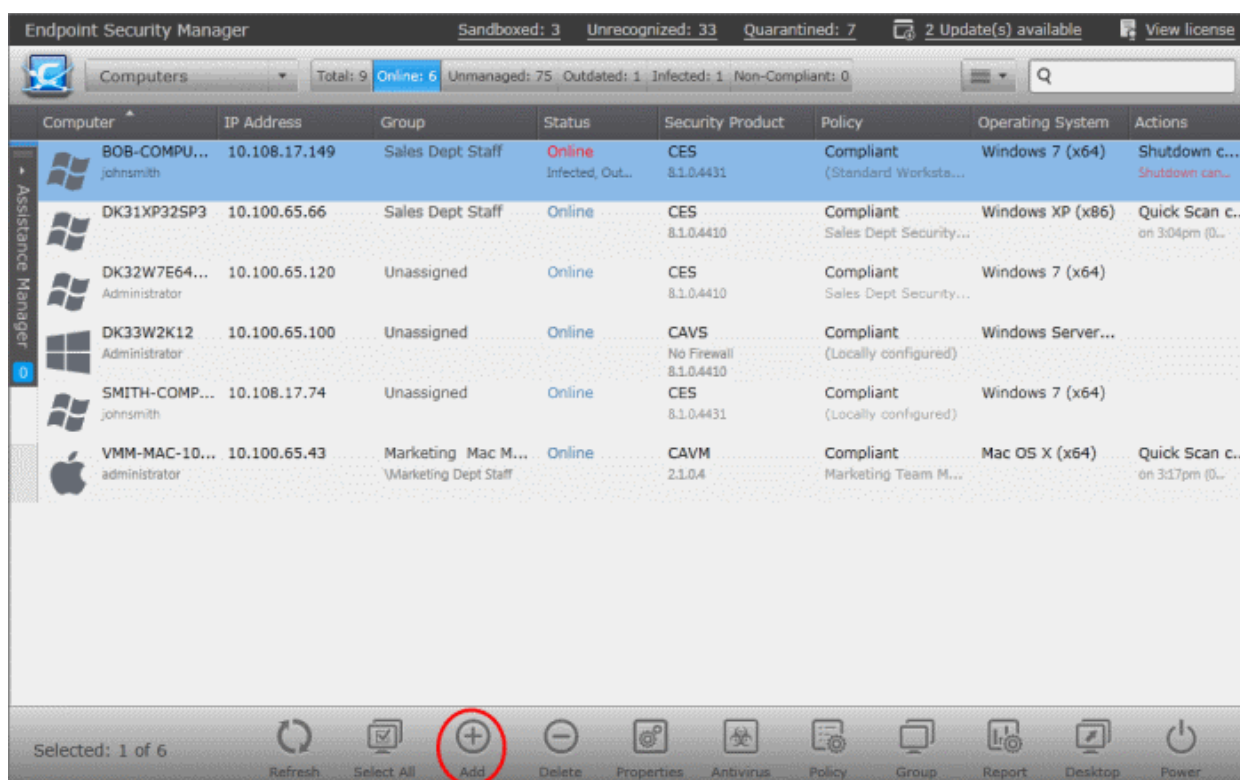
3. Select 'Managed Computers' and click the right arrow button to proceed to the next step.
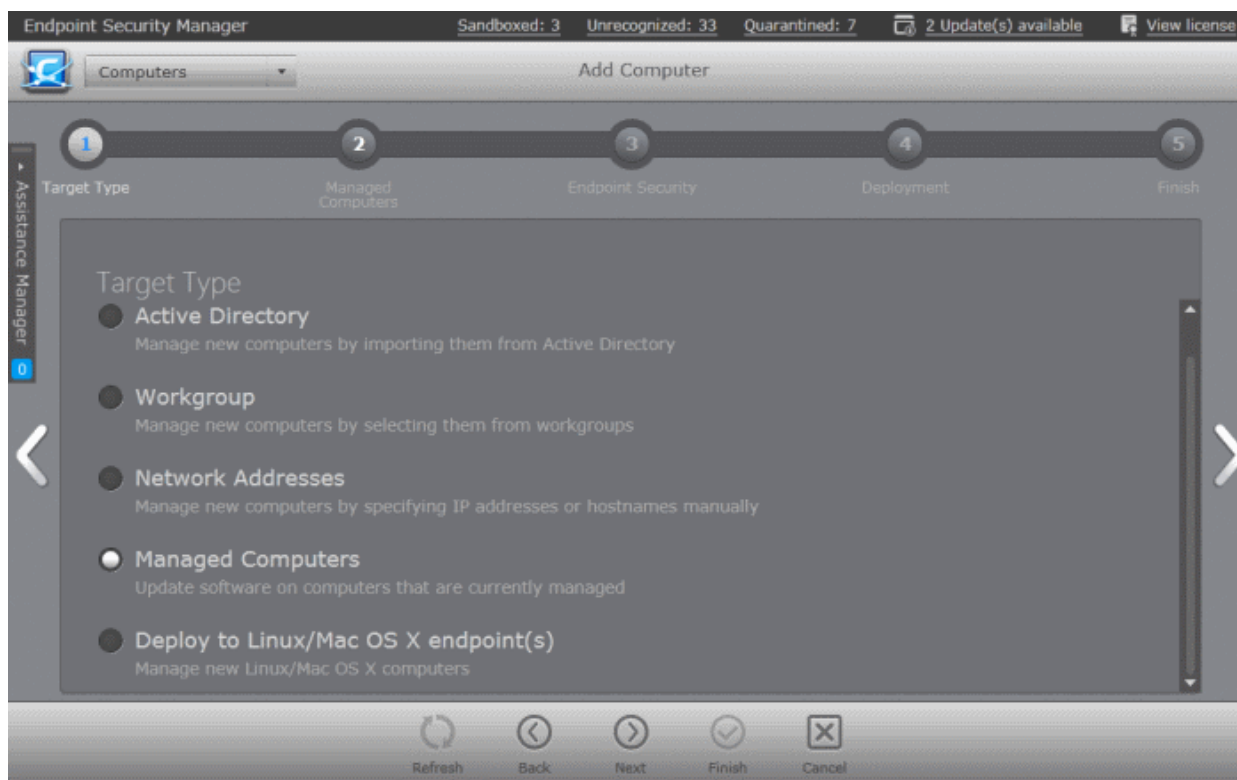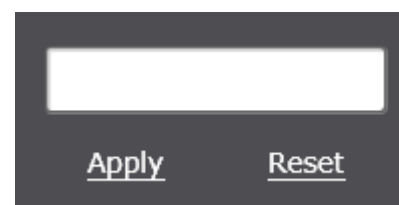
All the managed computers will be listed.

4.   Select the Windows endpoints on which you want to install CES/CAS application from the list.

- Click the filter icon ▼ in the 'Computer' column header to search for a particular endpoint, enter the endpoint name and click 'Apply'.
- After selecting the endpoints, click the right arrow or swipe left to
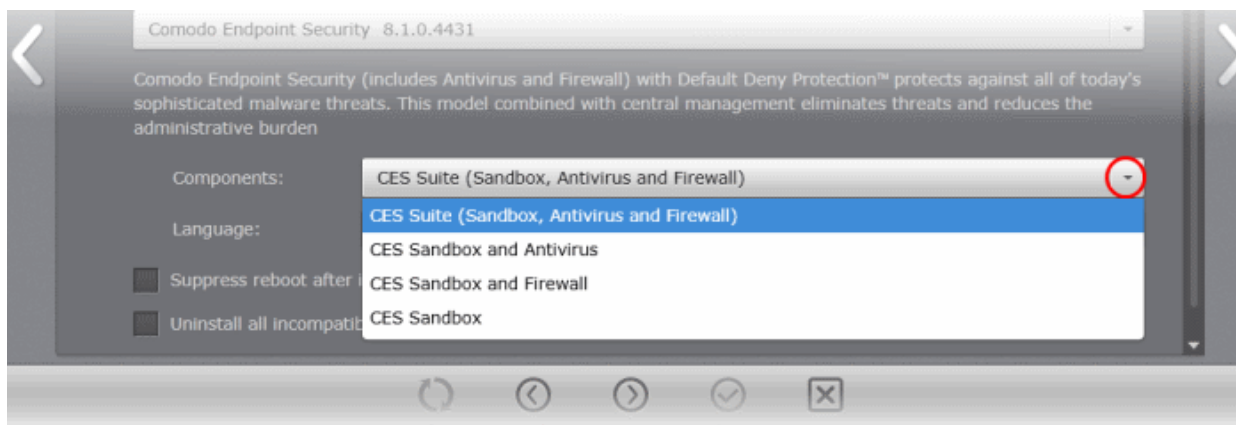
proceed to the next step.

The next step is to choose installation options for Comodo Endpoint Security (CES/CAS):
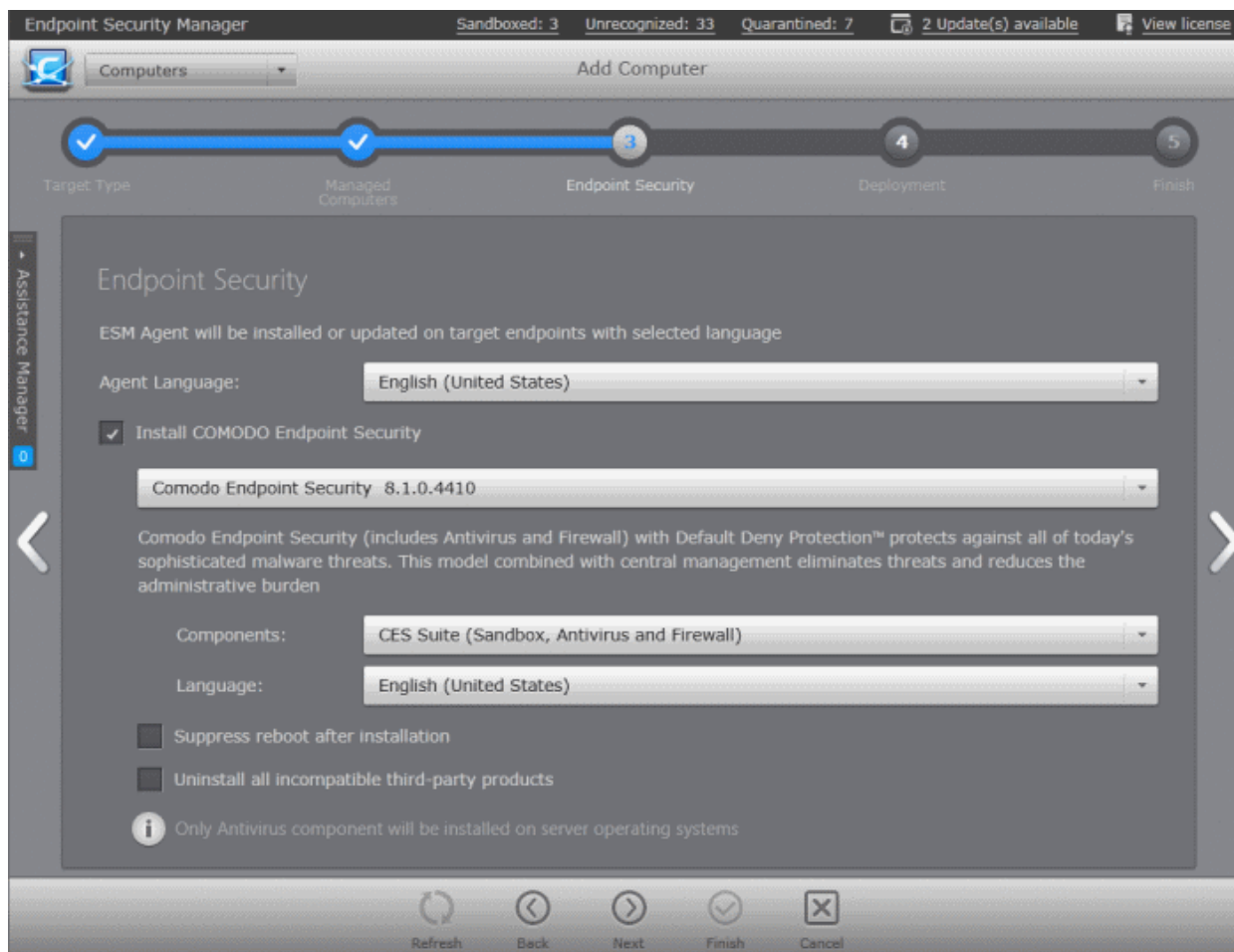
5.   Select 'Install Comodo Endpoint Security' check box.

6.   Select the version of CES/CAS you wish to install on the selected endpoints from the drop-down. The base package is same for both CES and CAS. CESM will automatically install CES or CAS depending on whether the endpoint is a Windows Client computer or a Windows Server.
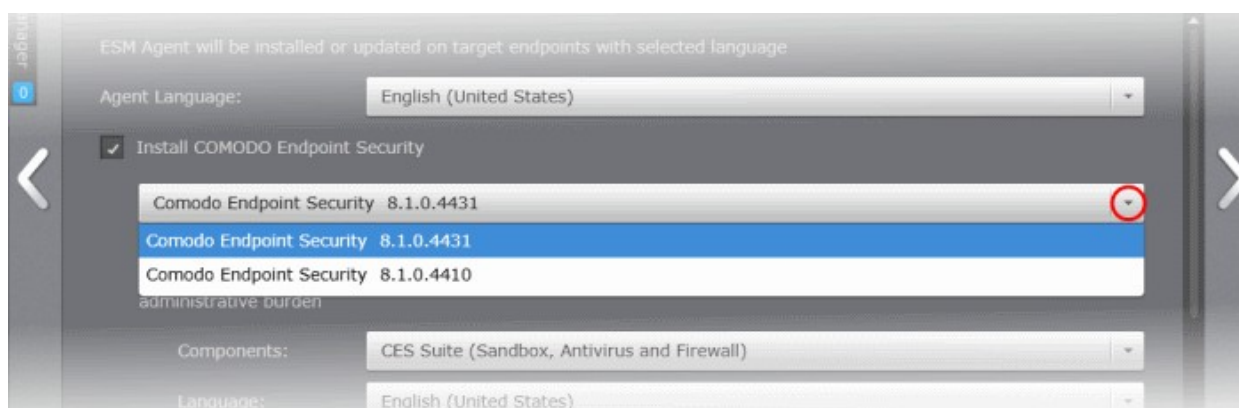

•   Select the components that you want to include from the Components drop-down:

   •   CES Suite, which contains all the components (Sandbox, Antivirus and Firewall)

   •   CES Sandbox and Antivirus

   •   CES Sandbox and Firewall

   •   CES Sandbox only

- **Suppress reboot after installation** - CES installation will restart of the endpoints for the installation to take effect. If you do not want the endpoints to be restarted on completion of installation, select this check box. CES installation will complete but will take effect only on the next restart of the endpoint.

- **Uninstall all incompatible products** - Selecting this option uninstalls select third party antivirus, firewall and other desktop security software from the endpoints, prior to the installation of CES. Performing this step will remove potentially incompatible products and thus enable CES to operate correctly. Some incompatible products can be detected, but not automatically uninstalled and must be removed manually. If your product is detected but not uninstalled, please consult your vendor's documentation for precise uninstallation guidelines.

- **Click here** to see the full list of incompatible products.

7. Click the right arrow to move to the next step.

The next step is the deployment process.
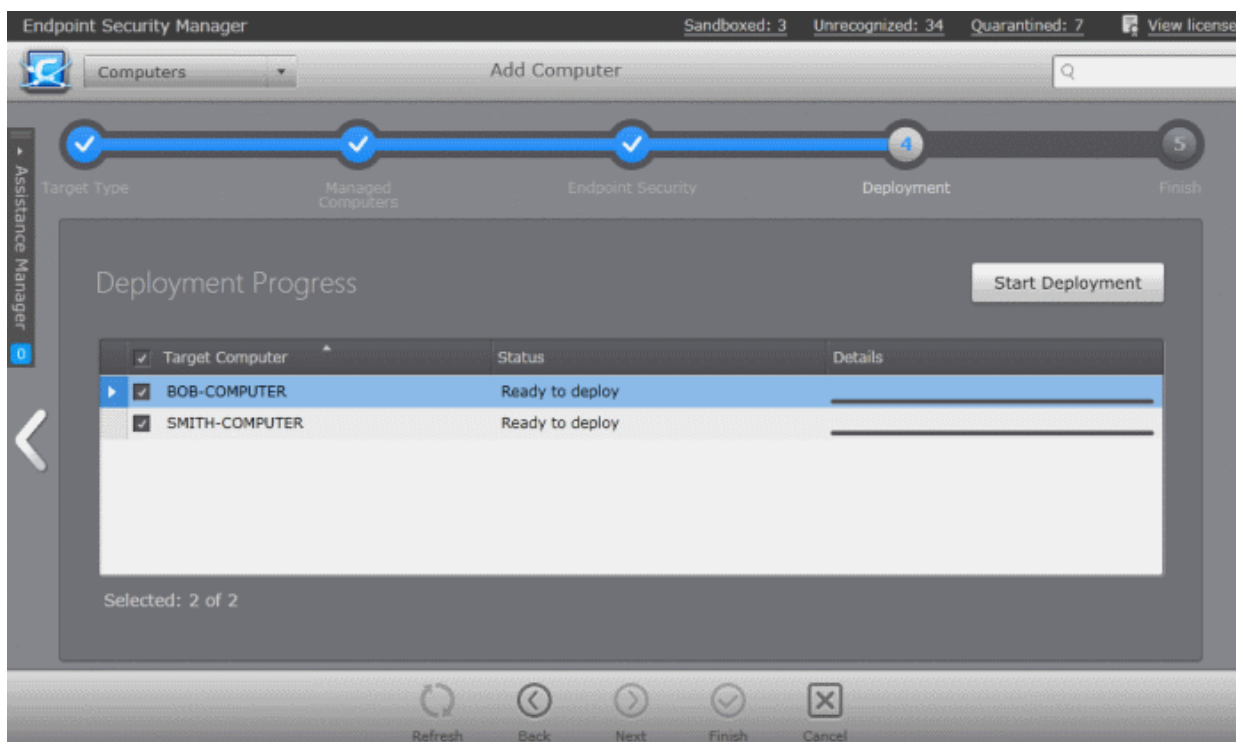
8. Click 'Start Deployment'.

The deployment progress will be displayed.
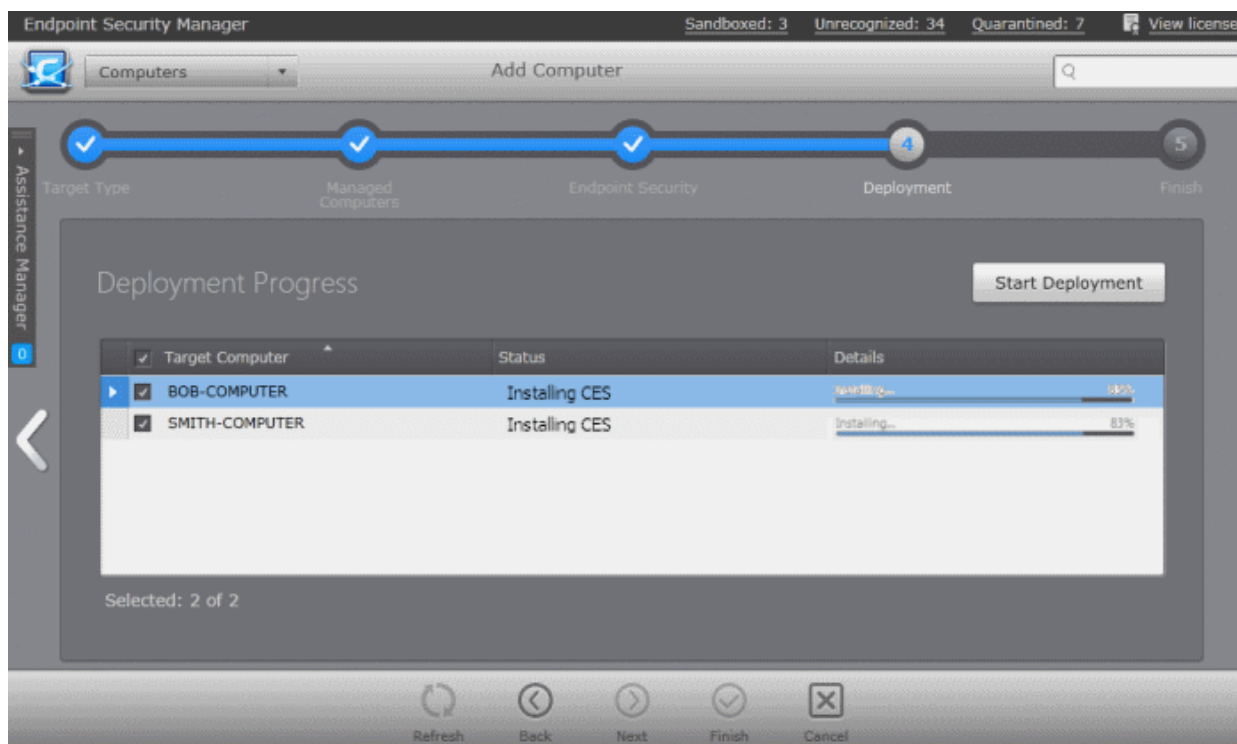
On completion of installation, the results screen will appear.

    9.   Click the 'Finish' icon or swipe the screen to the left to exit the wizard.

> **Note**: If you have selected 'Suppress reboot after installation' checkbox, the endpoints that were updated have to be restarted for the update to take effect.

# How to Install CAVM on Mac Endpoints Which Were Added by Manually Installing the Agent

Comodo Antivirus for MAC (CAVM) can be remotely installed on Mac endpoints that were added to CESM by manually installing the agent. This situation frequently applies to endpoints which are connecting from an external network.
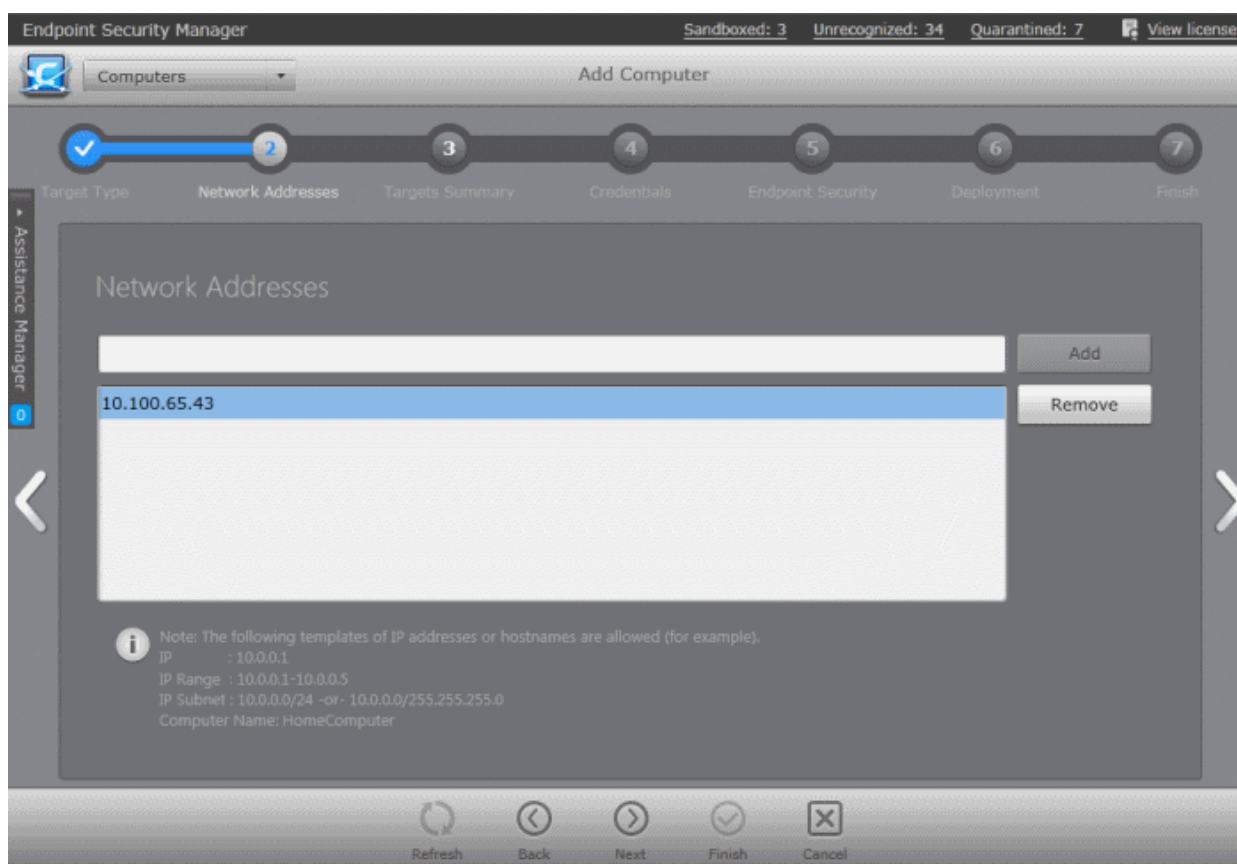
To install CAVM

    1.   Open the 'Computers' area by selecting Computers from the drop-down at the top left.

    2.   Click 'Add' from the 'Computers' area to start the wizard.
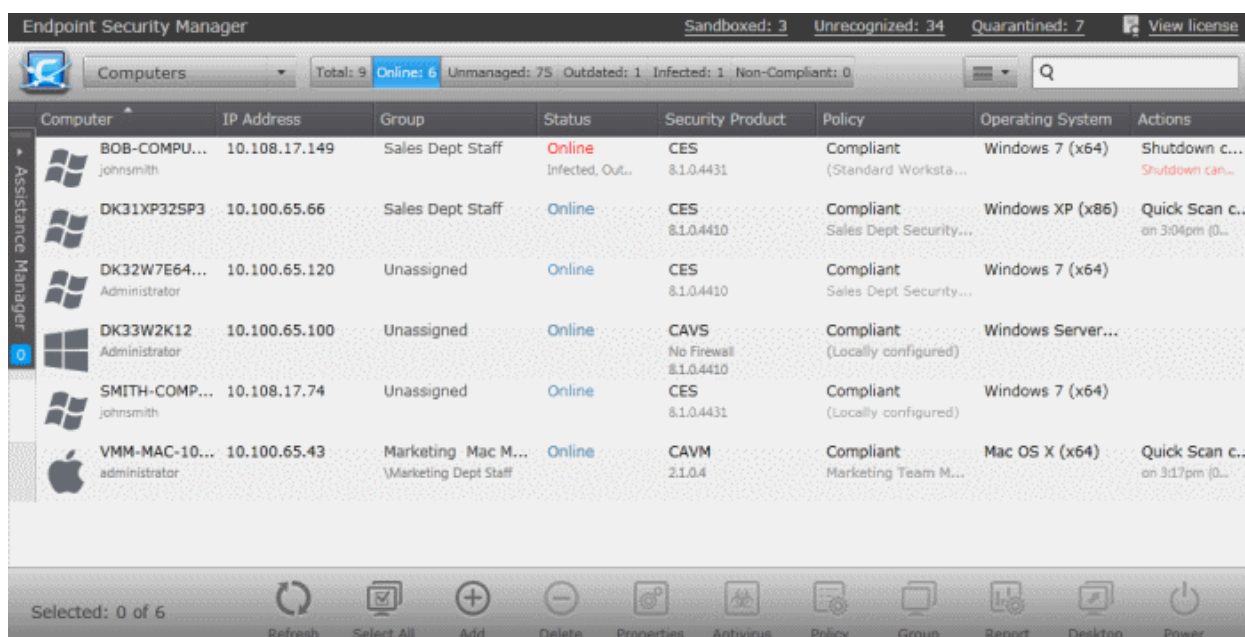
3. Select 'Deploy to Linux/Mac OS X endpoint(s)' and click the right arrow button to proceed to the next step.
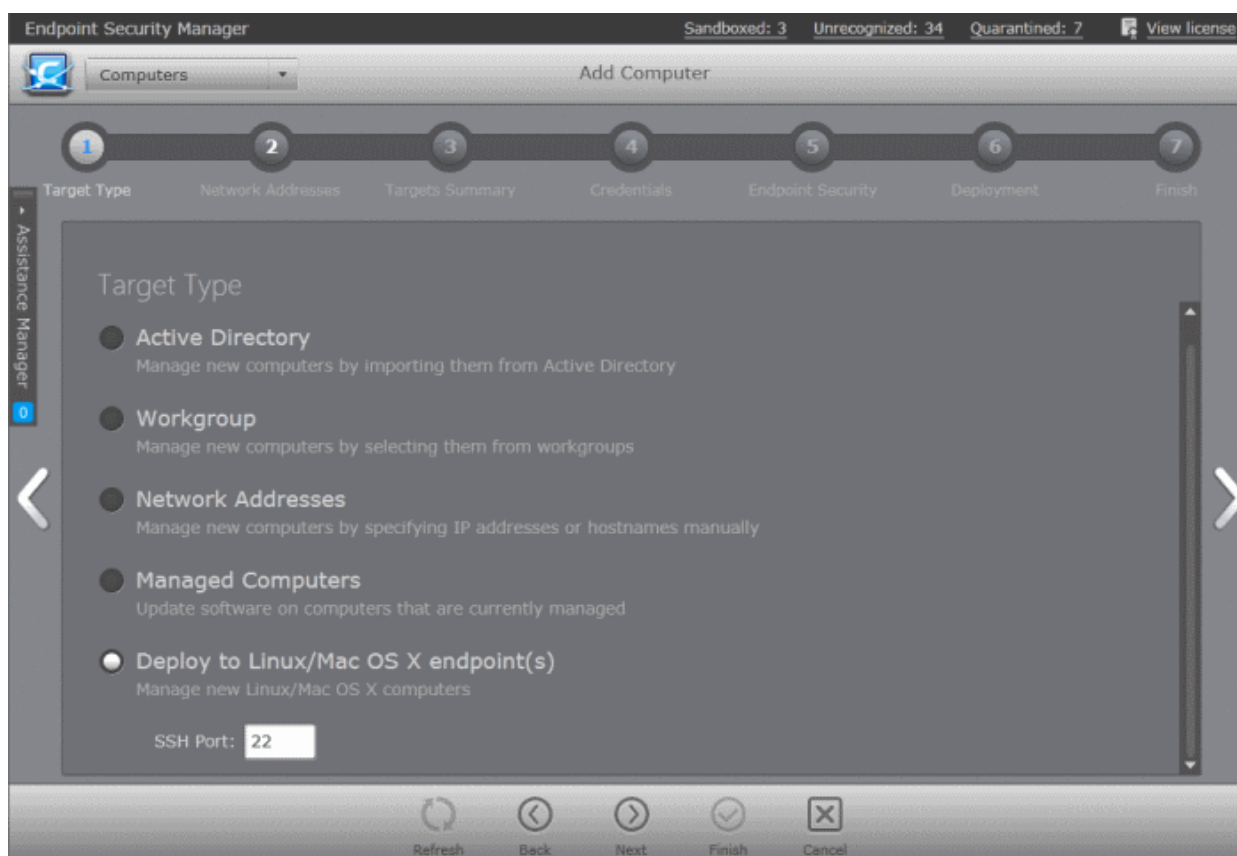

4. SSH Port - The port at the endpoint through which the CESM server can connect using secure shell access. The default port number is 22. Change the port if required.

5. The next step is to add the target Mac computers by specifying their IP address(es).

Computers can be added in four ways:

- **Import individual computers by specifying their IP addresses one-by-one** - Enter the IP address of the computer and click the 'Add' button. The IP address will be added and displayed below the text box. To add more computers, repeat the process.

- **Import individual computers by specifying their names one-by-one** - Enter the name of the target computer as identified in the network and click the 'Add' button. The computer name will be added and displayed below the text box. To add more computers, repeat the process.

- **Import a group of computers by specifying their IP Address range** - Enter the IP Address range of the target computers with the Start address and End address separated by a hyphen (e.g. 192.168.111.111-192.168.111.150) and click the 'Add' button. The entered IP address range will be added and displayed below the text box. To add more IP address ranges, repeat the process.

- **Import a group of computers by specifying IP Addresses and Subnet mask** - Enter the IP Address and Subnet mask (e.g. 192.168.111.111/24 or 192.168.111.111/255.255.255.0) in the text field and click the 'Add' button. The entered IP address/subnet mask will be added and displayed below the text box. To add more IP address/subnet mask, repeat the process.

6. Click the right arrow to move to the next step.

All the endpoints included in the previous step will be displayed.
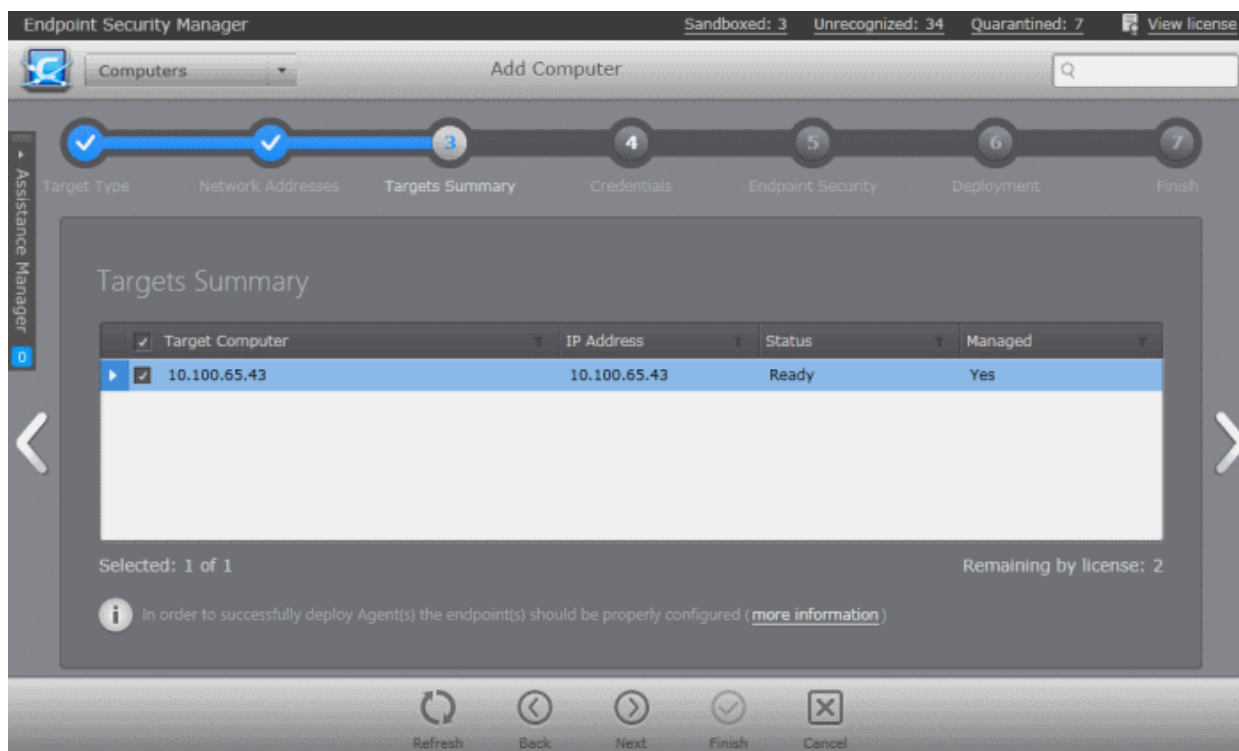
7. Select the Mac endpoint(s) that you want to deploy the CAVM to. You can use the filter option to select the endpoints from the list displayed.

    •   Click the filter icon ⊤ in the 'Target Computer' column header to search for a particular endpoint and click 'Apply'.
    •   Click the filter icon in the 'IP' column header to search for endpoints with particular IP(s) and click 'Apply'.
    •   Click the filter icon in the 'Status' column header to search for endpoints that are 'Ready' or 'Unavailable' and click 'Apply'.
    •   Click the filter icon in the 'Managed' column header to search for endpoints that are 'Managed' or 'No' and click 'Apply'.

8. Click the right arrow or swipe left to move to the next step.

The next step is to select the administrative account (login) credentials that will be used to remotely upload the installation package using the administrative share on all target computer(s).
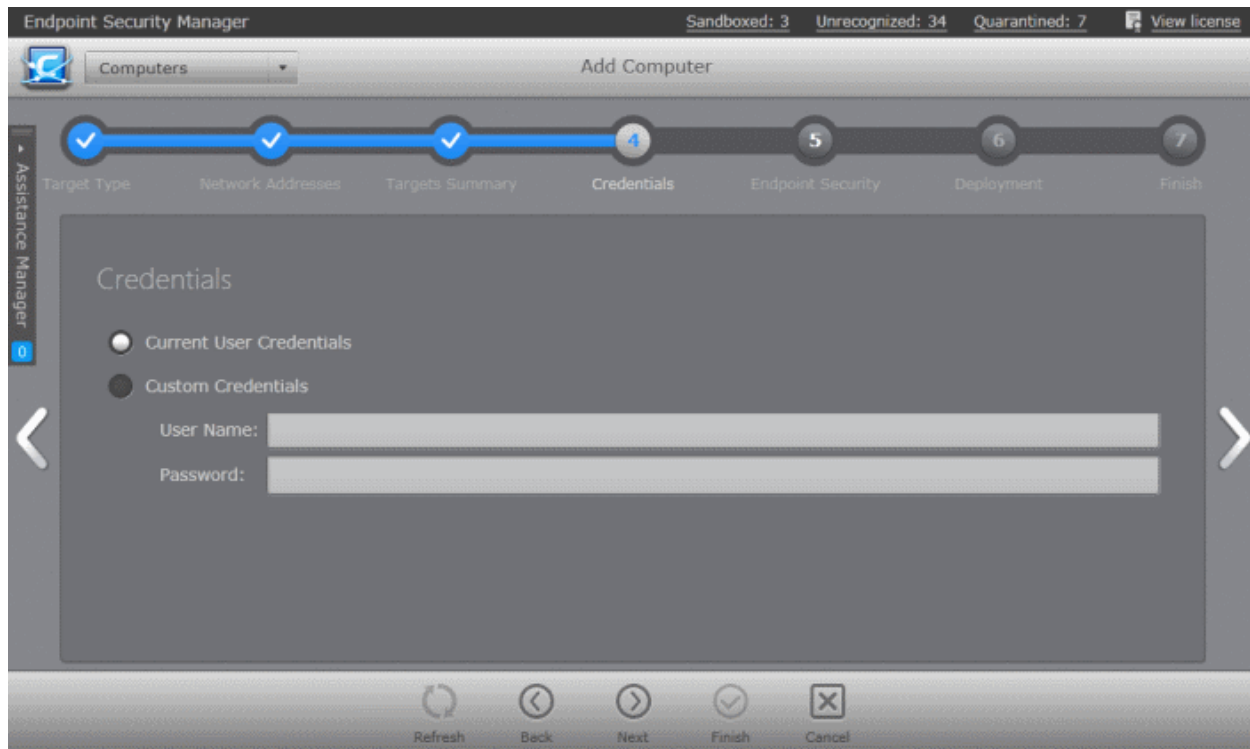
| Credentials - Table of Parameters	
Current User Credentials (Selected by default)	Selecting this option will install CAVM using the credentials of the currently logged -in CESM administrator account in each endpoint.
Custom Credentials	Selecting this option allows the administrator to specify an administrative account for installation of CAVM.
User Name:	Enter the user-name of the dedicated network administrator.
Password:	Enter the password of the dedicated network administrator.

9. Click the right arrow after entering the credentials to move to the next step.

The next step is to choose installation options for CAVM.
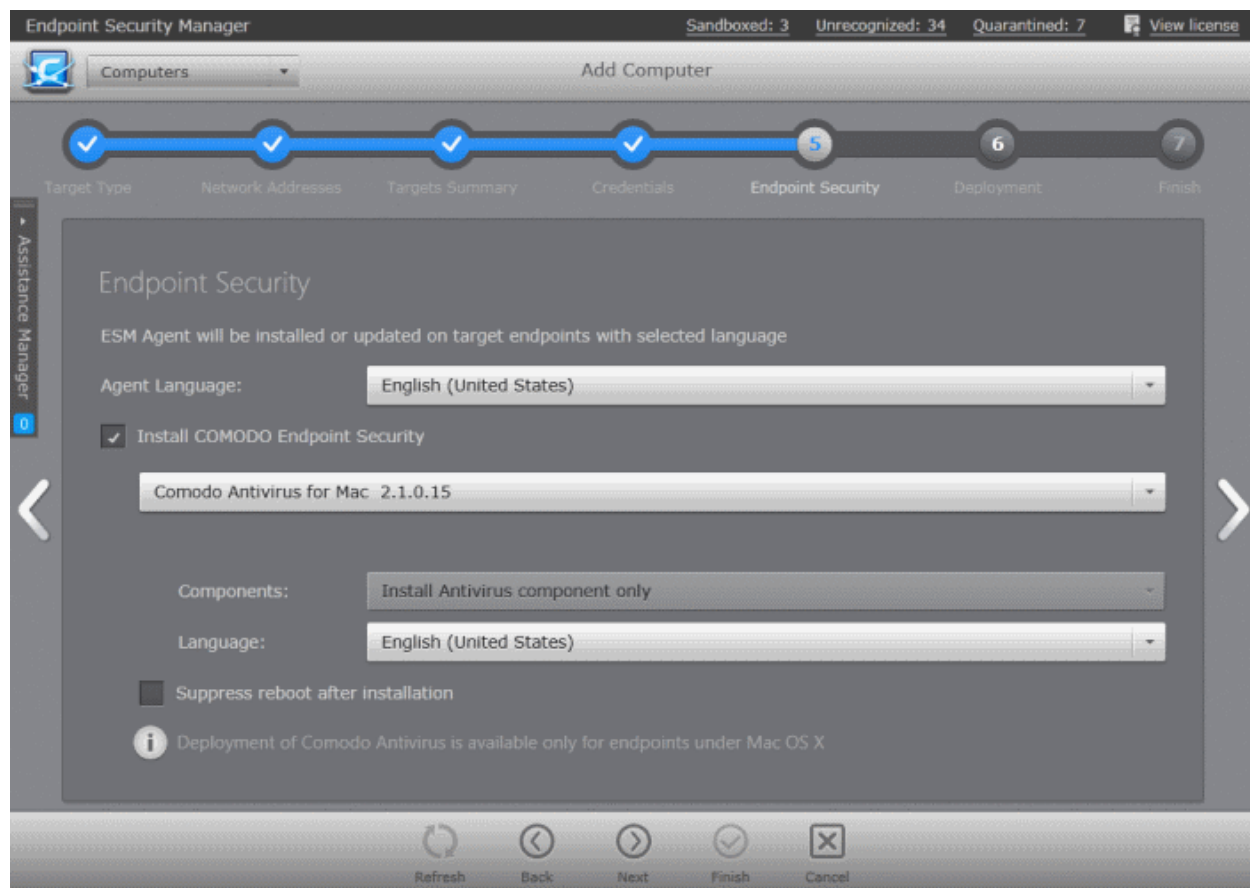
10. Select 'Install Comodo Endpoint Security' check box.

11. Select the version of CAVM you wish to install on the selected endpoints from the drop-down.

12. Select the language in which the CAVM is to be installed from the Language drop-down.
    - **Suppress reboot after installation** - CAVM installation requires restart of the endpoints for the installation to take effect. If you do not want the endpoints to be restarted on completion of installation, select this check box. CAVM installation will complete but will take effect only on the next restart of the endpoint.

13. Click the right arrow to move to the next step.

The next step is the deployment process.
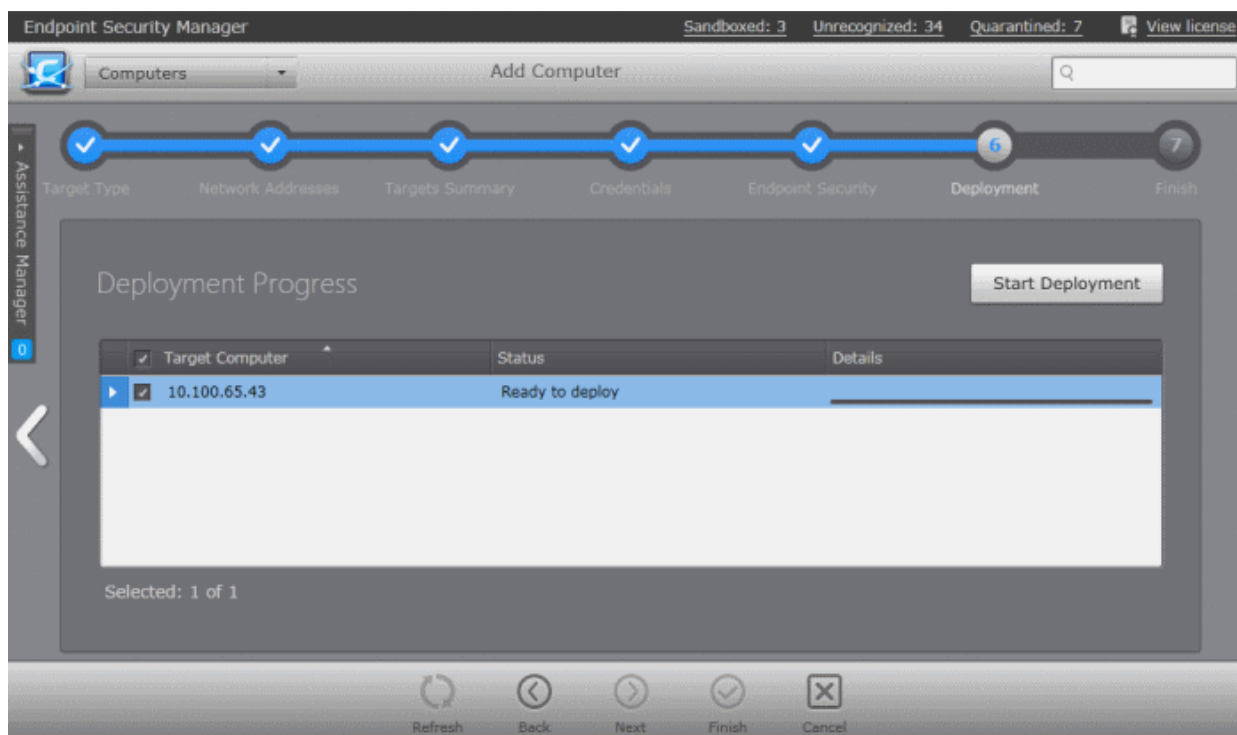
14. Click 'Start Deployment'.

The deployment progress will be displayed and on completion of installation, the results screen will appear.
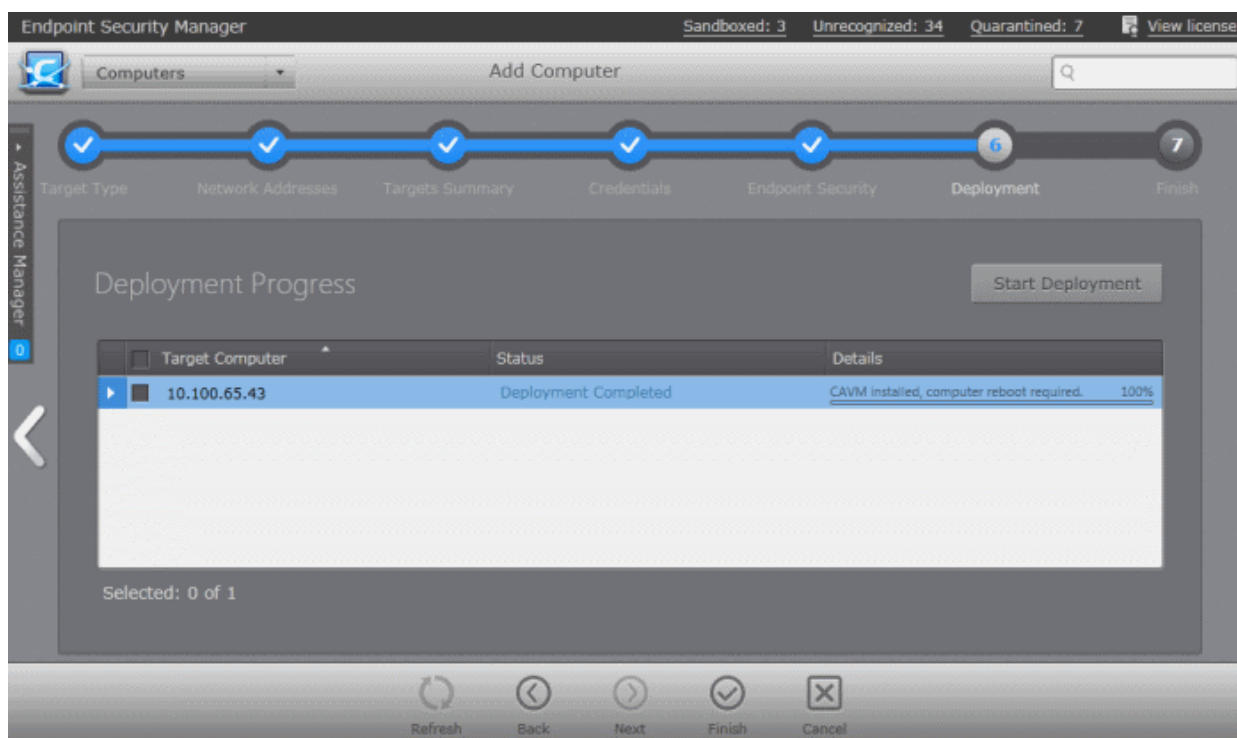
15. Click the 'Finish' icon or swipe the screen to the left to exit the wizard.

Note: If you have selected 'Suppress reboot after installation' checkbox, the endpoints that were updated have to be restarted for the update to take effect.

About Comodo

The Comodo companies are leading global providers of Security, Identity and Trust Assurance services on the Internet. Comodo CA offers a comprehensive array of PKI Digital Certificates and Management Services, Identity and Content Authentication (Two-Factor - Multi-Factor) software, and Network Vulnerability Scanning and PCI compliance solutions. In addition, with over 10,000,000 installations of its threat prevention products, Comodo Security Solutions maintains an extensive suite of endpoint security software and services for businesses and consumers.

Continual innovation, a core competence in PKI and a commitment to reversing the growth of Internet-crime distinguish the Comodo companies as vital players in the Internet's ongoing development. Comodo, with offices in the US, UK, China, India, Romania and the Ukraine, secures and authenticates the online transactions and communications for over 200,000 business customers and millions of consumers, providing the intelligent security, authentication and assurance services necessary for trust in on-line transactions.

Comodo Security Solutions, Inc.

1255 Broad Street

Clifton, NJ 07013

United States

Tel : +1.877.712.1309

Email: **EnterpriseSolutions@Comodo.com**

For additional information on Comodo - visit **http://www.comodo.com**.