COMODO
Creating Trust Online®

Comodo
Endpoint Security Manager Professional Edition

Software Version 3.0

Administrator Guide

Guide Version 3.0.052313

Comodo Security Solutions
1255 Broad Street
STE 100
Clifton, NJ 07013

Table of Contents

1. Introduction to Comodo Endpoint Security Manager - Professional Edition

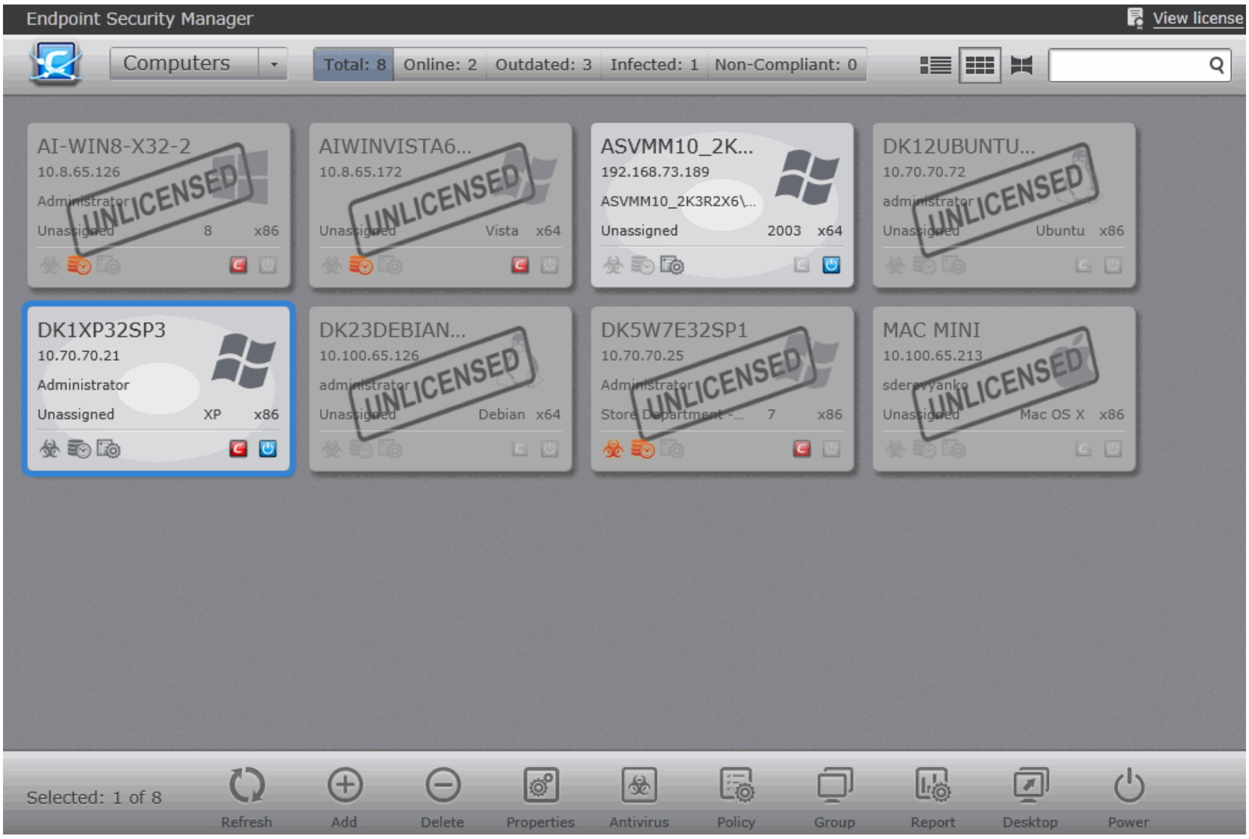
Comodo Endpoint Security Manager (CESM) Professional Edition is designed to help administrators of corporate networks deploy, manage and monitor Comodo Endpoint Security software on networked computers.

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, 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.
- Supports Linux and MacOS based computers (device management only).
- New reports with built in drill down to computers and in-report remediation.

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, CES 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 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 CES configuration, policy compliance, malware statistics, policy delta, CES 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 and download agent setup files for different operating systems for manual installation on endpoints connected through external networks.
- View support contact information and different ways to get help on CESM.

The Preferences Area - Allows the administrators to configure 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.
- 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.

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.

Central Service

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

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 agent.
- **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	1 GHz 32 bit processor	1 GHz 64 bit processor
Memory	1 GB RAM minimum (2-4 GB recommended)	2 GB RAM minimum (4 GB recommended)
Hard Disk	16 GB	20 GB
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 Server 2003 SP2 or higher Windows Server 2003 Small Business Server Windows Server 2003 R2 Windows Server 2008 SP2 or higher Windows Server 2008 Small Business Server Windows Server 2012 **Microsoft Windows Client Family:** Windows XP SP3 or higher Windows Vista Windows 7 Windows 8	The following operating systems are supported: **Microsoft Windows Server Family:** Windows Server 2003 SP2 or higher Windows Server 2003 Small Business Server Windows Server 2003 R2 Windows Server 2008 SP2 or higher Windows Server 2008 Small Business Server Windows Server 2008 R2 Windows Server 2012 **Microsoft Windows Client Family:** Windows Vista Windows 7 Windows 8
Software Environment	Microsoft .NET Framework 4.5 Microsoft ReportViewer 2010 SP1 (**Note** - The above components will be installed automatically if not present)	Microsoft .NET Framework 4.5 Microsoft ReportViewer 2010 SP1 (**Note** - The above components will be installed automatically if not present)
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)

CENTRAL SERVICE COMPUTER - SYSTEM REQUIREMENTS	
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 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 Server 2003 SP2 or higher Windows Server 2003 Small Business Server Windows Server 2003 R2 Windows Server 2008 SP2 or higher Windows Server 2008 Small Business Server Windows Server 2012 **Microsoft Windows Client Family:** Windows XP SP3 or higher Windows Vista Windows 7 Windows 8	The following operating systems are supported: **Microsoft Windows Server Family:** Windows Server 2003 SP2 or higher Windows Server 2003 Small Business Server Windows Server 2003 R2 Windows Server 2008 SP2 or higher Windows Server 2008 Small Business Server Windows Server 2008 R2 Windows Server 2012 **Microsoft Windows Client Family:** Windows Vista Windows 7 Windows 8
Browsers and software	Microsoft Silverlight 5.1 Microsoft Internet Explorer 7.0 or higher Mozilla Firefox 3.0 or higher Google Chrome 4.0 or higher Comodo Dragon 15.0 or higher	Microsoft Silverlight 5.1 Microsoft Internet Explorer 7.0 or higher Mozilla Firefox 3.0 or higher Google Chrome 4.0 or higher
Other		

ADMINISTRATIVE CONSOLE COMPUTER - SYSTEM REQUIREMENTS	
Requirements	• TCP Ports 57193,57194 will be used for http: and https: connections

Endpoint Computer - (a managed PC that will run Comodo Endpoint Security and the Agent)

ENDPOINT COMPUTER - SYSTEM REQUIREMENTS		
Hardware		
Component	**32 bit**	**64-Bit**
Processor *recommended*	1 GHz 32 bit processor	1 GHz 64 bit processor
Memory *recommended*	1 GB RAM	2 GB RAM
Software		
Operating System	The following operating systems are supported: **Microsoft Windows Server Family:** Windows Server 2003 SP2 or higher Windows Server 2003 Small Business Server Windows Server 2003 R2 Windows Server 2008 SP2 or higher Windows Server 2008 Small Business Server Windows Server 2012 **Microsoft Windows Client Family:** Windows XP SP3 or higher Windows Vista Windows 7 Windows 8	The following operating systems are supported: **Microsoft Windows Server Family:** Windows Server 2003 SP2 or higher Windows Server 2003 Small Business Server Windows Server 2003 R2 Windows Server 2008 SP2 or higher Windows Server 2008 Small Business Server Windows Server 2008 R2 Windows Server 2012 **Microsoft Windows Client Family:** Windows Vista Windows 7 Windows 8
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».	

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	Components
Agnitum	Outpost Security Suite Pro 7.1	Detect only	Outpost Security Suite Pro 7.1
AVAST Software	avast! Free Antivirus	Detect only	avast! Free Antivirus
AVG Technologies	AVG Internet Security	Detect only	AVG 2011
Avira GmbH	Avira AntiVir Premium	Detect only	Avira AntiVir Desktop
Comodo Group	Comodo Internet Security 4.1, 5.8	Automatic	Comodo Internet Security
Doctor Web, Ltd.	Dr.Web anti-virus for Windows 6.0 (x86/x64)	Detect only	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	ESET Smart Security	Automatic	ESET Smart Security
Kaspersky Lab.	Kaspersky Antivirus	Detect only	Kaspersky Antivirus
McAfee, Inc.	McAfee Total Protection	Detect only	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	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	Sophos AutoUpdate Sophos Anti-Virus Sophos Client Firewall
Symantec Corporation	Symantec Endpoint Protection	Automatic	Symantec Endpoint Protection

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.

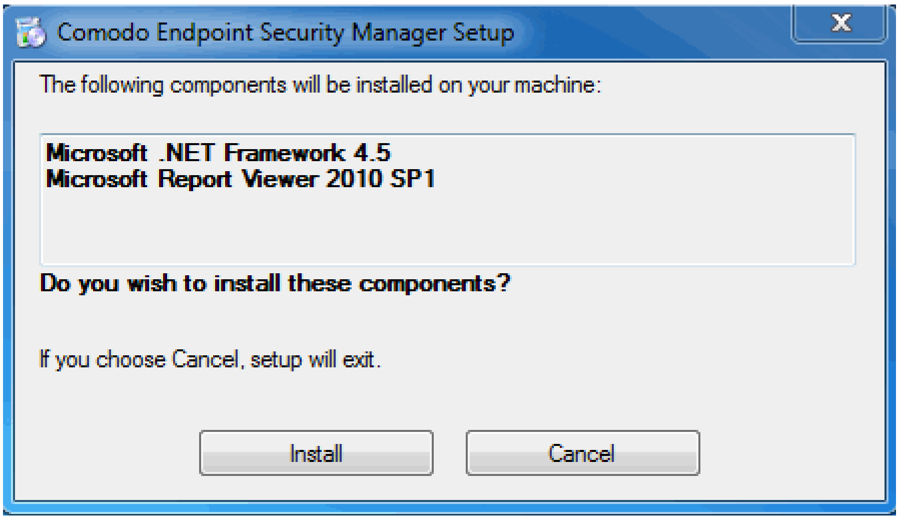
You have a choice of two installation files, 'CESM_Setup_3.0.<version>.exe' or 'CESM_Setup_3.0.<version>_Full.exe'.

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 installer welcome screen will be displayed.

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.



Comodo Endpoint Security Manager Setup

The following components will be installed on your machine:

Microsoft .NET Framework 4.5
Microsoft Report Viewer 2010 SP1

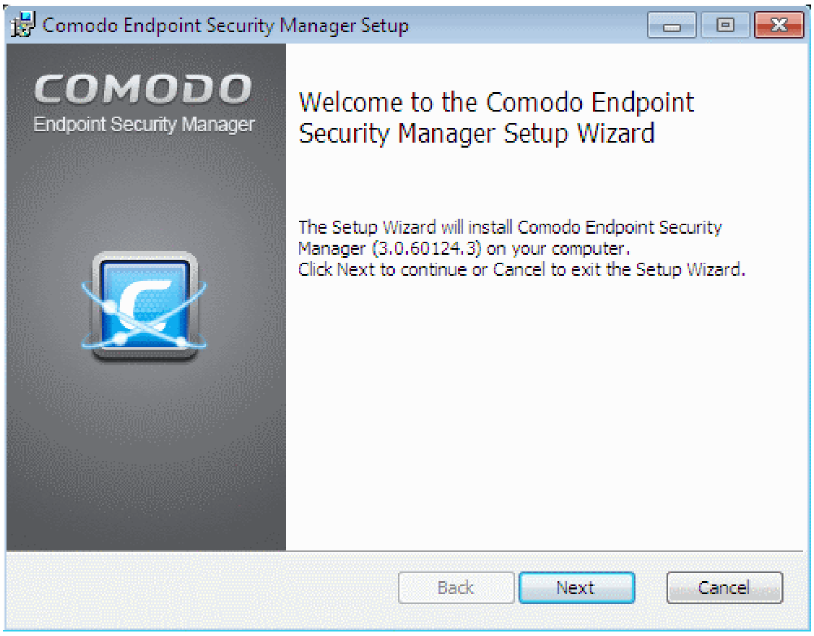
Do you wish to install these components?

If you choose Cancel, setup will exit.

If the additional software are already available, the installation of CESM will start.

2. Welcome Screen

The welcome screen will be displayed.



Comodo Endpoint Security Manager Setup
COMODO
Endpoint Security Manager

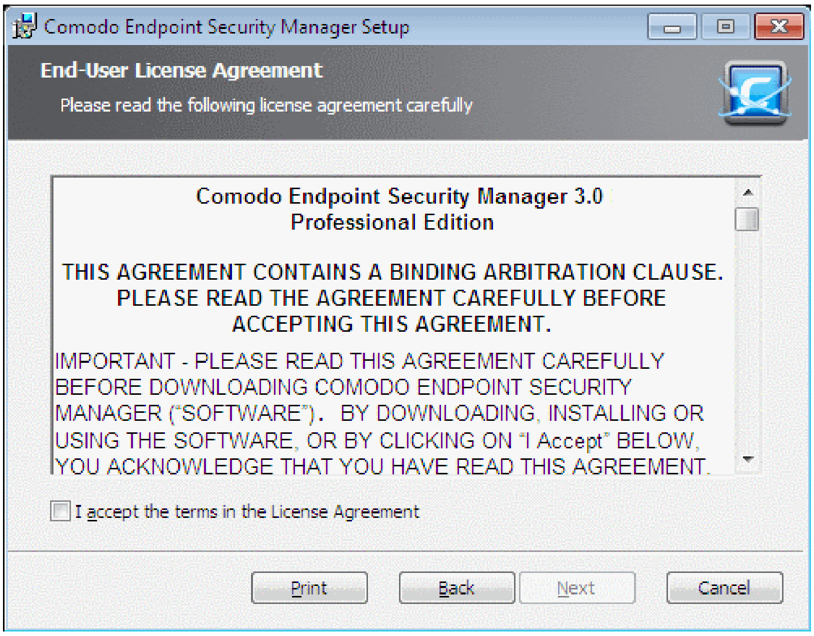
Welcome to the Comodo Endpoint Security Manager Setup Wizard

The Setup Wizard will install Comodo Endpoint Security Manager (3.0.60124.3) on your computer.
Click Next to continue or Cancel to exit the Setup Wizard.

- Click 'Next'.

3. License Agreement

The End-User License Agreement will be displayed:



End-User License Agreement

Please read the following license agreement carefully

Comodo Endpoint Security Manager 3.0
Professional Edition

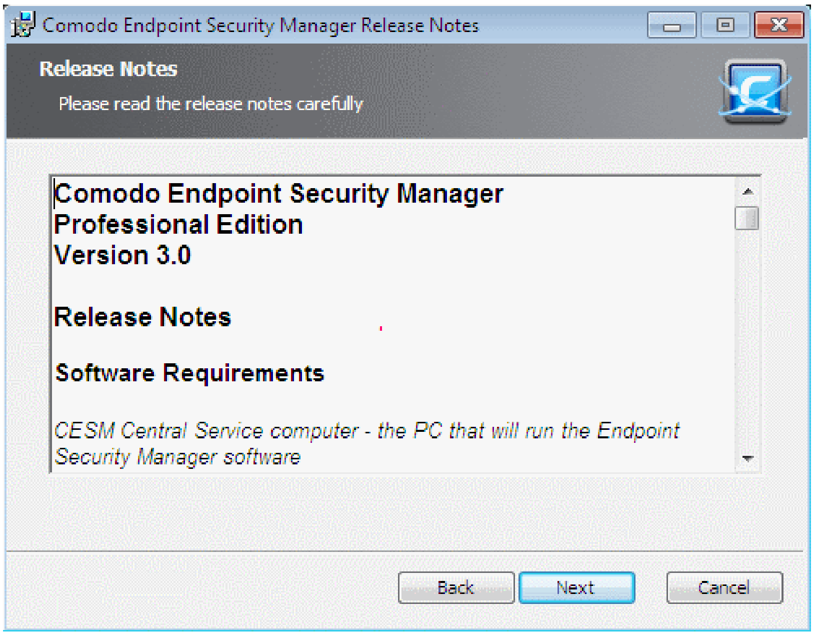
THIS AGREEMENT CONTAINS A BINDING ARBITRATION CLAUSE. PLEASE READ THE AGREEMENT CAREFULLY BEFORE ACCEPTING THIS AGREEMENT.

IMPORTANT - PLEASE READ THIS AGREEMENT CAREFULLY BEFORE DOWNLOADING COMODO ENDPOINT SECURITY MANAGER ("SOFTWARE"). BY DOWNLOADING, INSTALLING OR USING THE SOFTWARE, OR BY CLICKING ON "I Accept" BELOW, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT.

□ I accept the terms in the License Agreement

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.



Release Notes

Please read the release notes carefully

Comodo Endpoint Security Manager
Professional Edition
Version 3.0

Release Notes

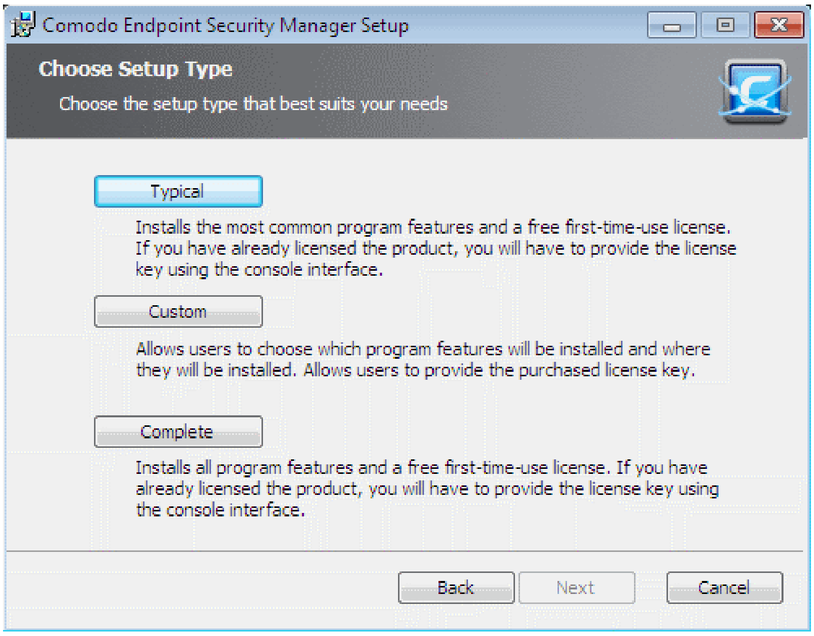
Software Requirements

CESM Central Service computer - the PC that will run the Endpoint Security Manager software

- Read the notes and click 'Next'.

4. Choosing Installation Preferences

The next stage is to choose the setup type:



Choose Setup Type

Choose the setup type that best suits your needs

Typical

Installs the most common program features and a free first-time-use license. If you have already licensed the product, you will have to provide the license key using the console interface.

Custom

Allows users to choose which program features will be installed and where they will be installed. Allows users to provide the purchased license key.

Complete

Installs all program features and a free first-time-use license. If you have already licensed the product, you will have to provide the license key using the console interface.

- **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', 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:

Note: If you choose to install CESM PE in Custom mode, you will be prompted to provide a valid license key during setup. The installation will continue only if you enter the license key and register the product.

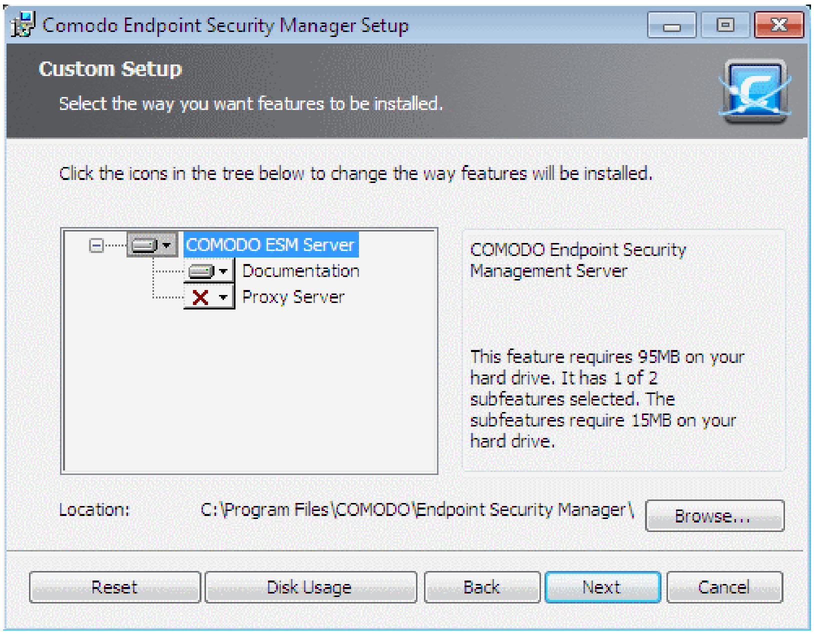
On selecting 'Custom' and clicking 'Next', the setup progress will move to **Selecting Components**

- **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.



Comodo Endpoint Security Manager Setup

Custom Setup

Select the way you want features to be installed.

Click the icons in the tree below to change the way features will be installed.

- COMODO ESM Server
  - Documentation
  - ✕ Proxy Server

COMODO Endpoint Security Management Server

This feature requires 95MB on your hard drive. It has 1 of 2 subfeatures selected. The subfeatures require 15MB on your hard drive.

Location: C:\Program Files\COMODO\Endpoint Security Manager\

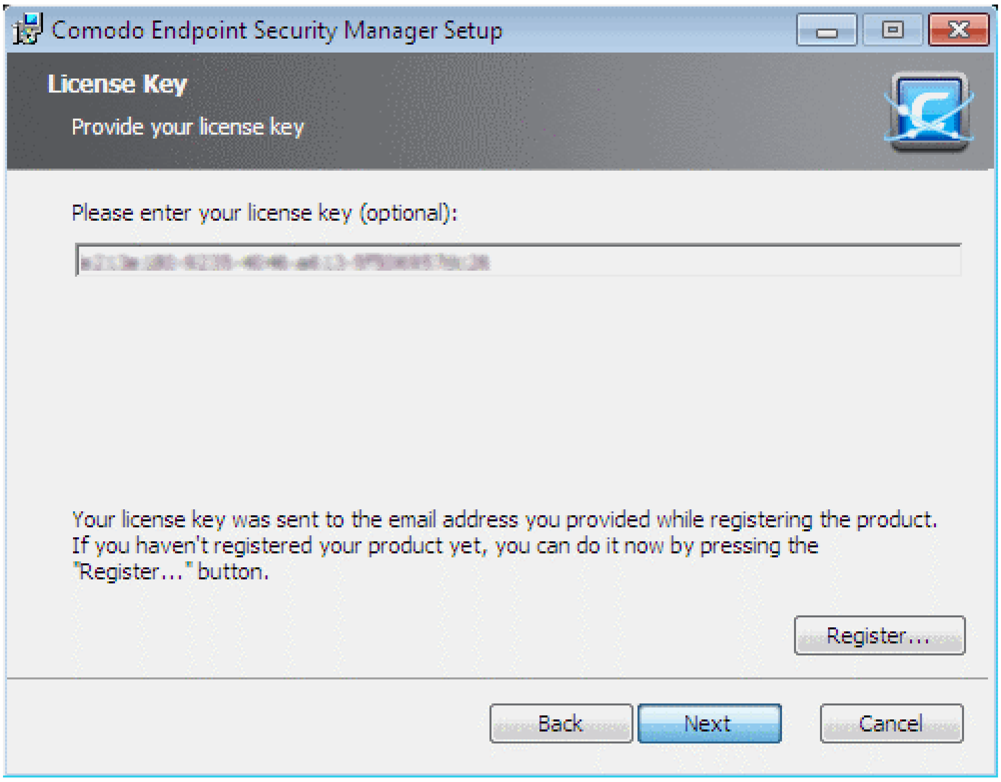
Custom Setup - Key	
Control	**Description**
▭ ▾	Icons with the ▼ symbol to the right are the currently selected installation option. Clicking this icon will open a menu allowing the user to select alternative installation options. These alternative installation options are explained in the next four 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.
1▭	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.

Custom Setup - Key	
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.



Comodo Endpoint Security Manager Setup

License Key

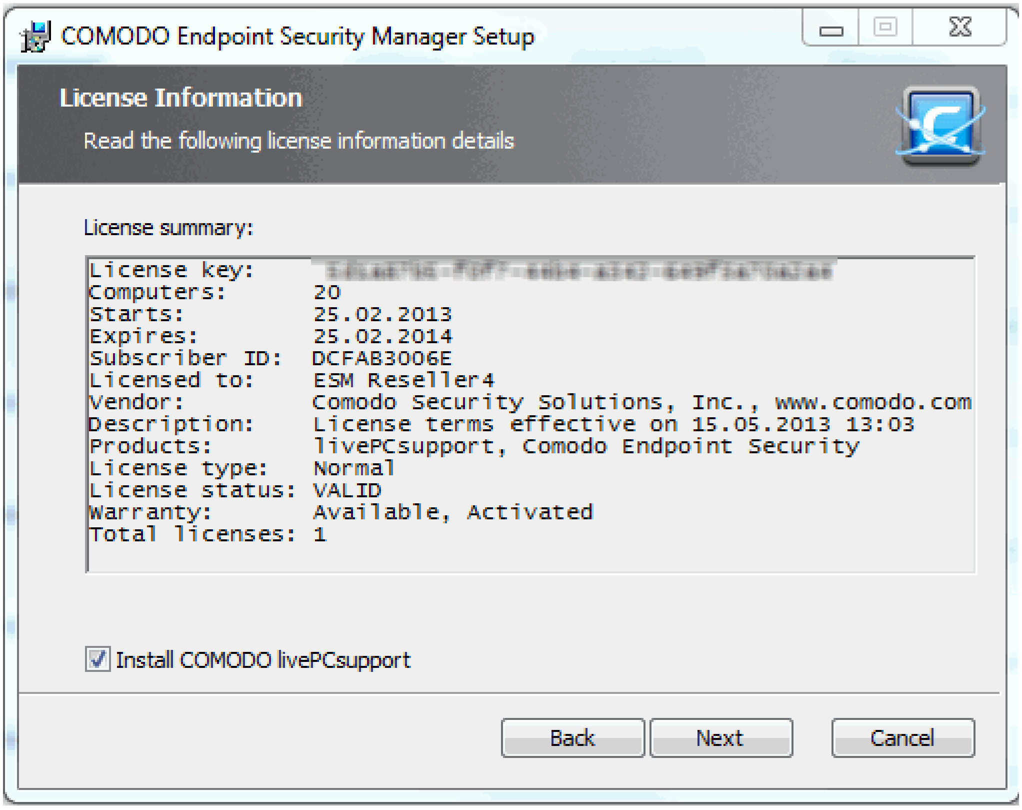
Provide your license key

Please enter your license key (optional):

[redacted]

Your license key was sent to the email address you provided while registering the product. If you haven't registered your product yet, you can do it now by pressing the "Register..." button.

The setup will communicate with Comodo in order to register your product. Once the registration process is complete, the license summary will be displayed.



License Information

Read the following license information details

License summary:

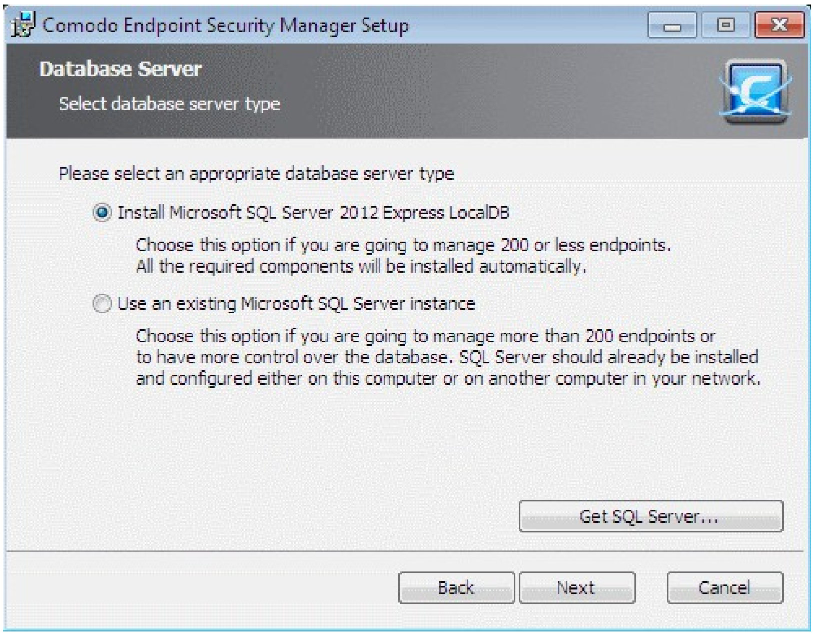
```
License key:      [redacted]
Computers:        20
Starts:           25.02.2013
Expires:          25.02.2014
Subscriber ID:    DCFAB3006E
Licensed to:      ESM Reseller4
Vendor:           Comodo Security Solutions, Inc., www.comodo.com
Description:      License terms effective on 15.05.2013 13:03
Products:         livePCsupport, Comodo Endpoint Security
License type:     Normal
License status:   VALID
Warranty:         Available, Activated
Total licenses:   1
```

☑ Install COMODO livePCsupport

- Click 'Next' to continue the installation.

7. Selecting Database Server

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



Database Server

Select database server type

Please select an appropriate database server type

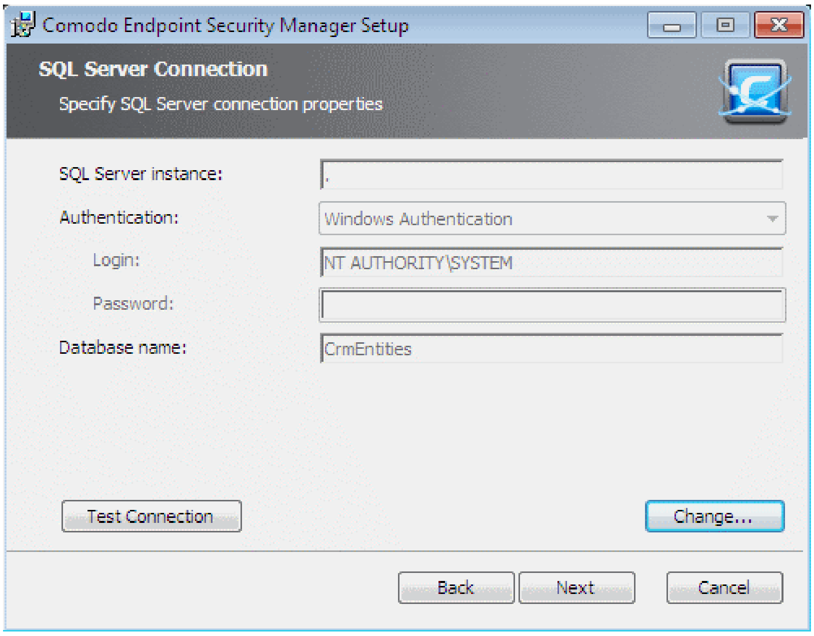
● Install Microsoft SQL Server 2012 Express LocalDB

Choose this option if you are going to manage 200 or less endpoints.
All the required components will be installed automatically.

○ Use an existing Microsoft SQL Server instance

Choose this option if you are going to manage more than 200 endpoints or to have more control over the database. SQL Server should already be installed and configured either on this computer or on another computer in your network.

- 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'.


Comodo Endpoint Security Manager Setup

SQL Server Connection

Specify SQL Server connection properties

SQL Server instance: .

Authentication: Windows Authentication

Login: NT AUTHORITY\SYSTEM

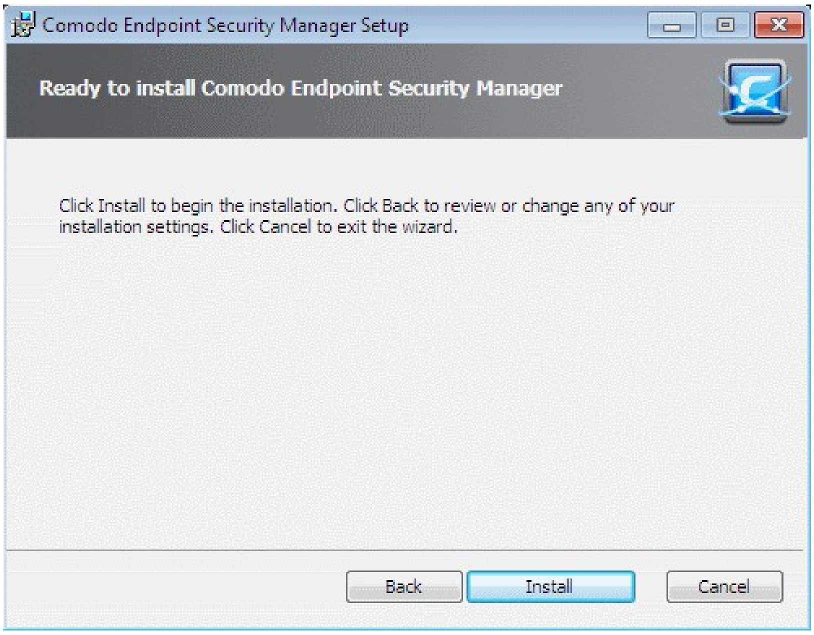
Password:

Database name: CrmEntities

- 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

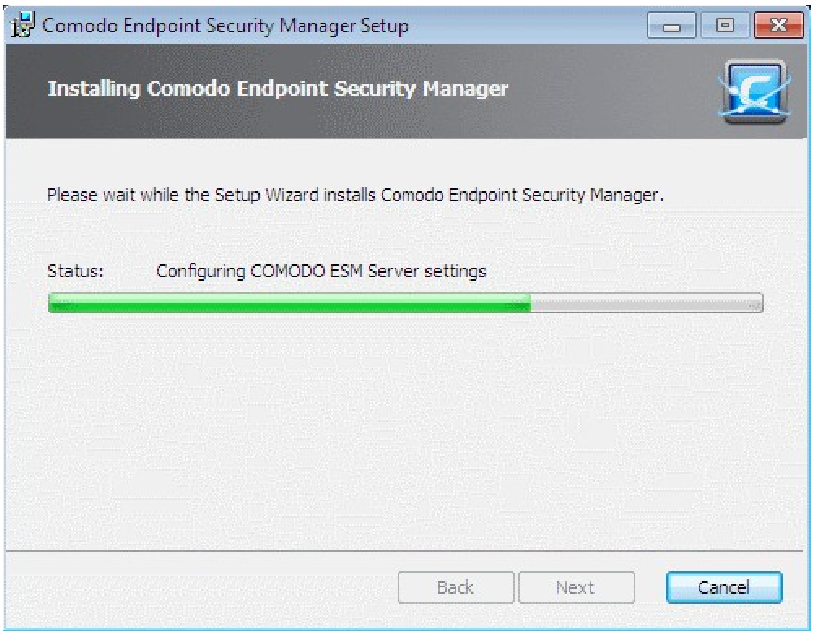
On completion of the configuration, the 'Ready to Install' screen will be displayed.


Comodo Endpoint Security Manager Setup

Ready to install Comodo Endpoint Security Manager

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

- Click 'Install'. The installation will be started and the progress will be displayed.



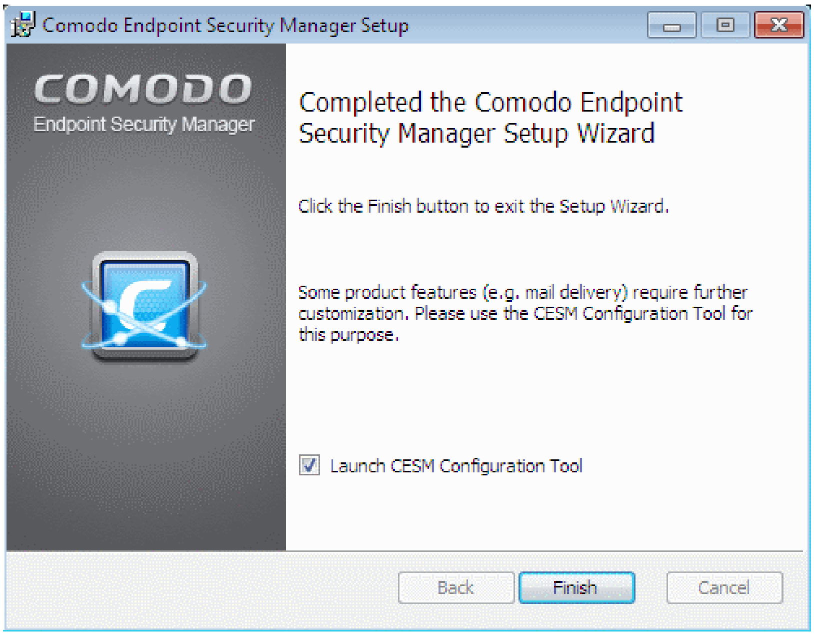
Comodo Endpoint Security Manager Setup

Installing Comodo Endpoint Security Manager

Please wait while the Setup Wizard installs Comodo Endpoint Security Manager.

Status: Configuring COMODO ESM Server settings

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**.



Comodo Endpoint Security Manager Setup

Completed the Comodo Endpoint Security Manager Setup Wizard

Click the Finish button to exit the Setup Wizard.

Some product features (e.g. mail delivery) require further customization. Please use the CESM Configuration Tool for this purpose.

☑ Launch CESM 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 - Endpoint refers to any desktop, laptop or any other computing device that is connected to a corporate network. CESM allows network and system administrators to install, manage and monitor the security software Comodo Endpoint Security (CES) at each endpoint, remotely, from a central location.

Managed Endpoint - Refers to any desktop, laptop or any other computing device that is running the Agent and CES, managed by the CESM central service.

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 client program to be installed on each and every managed endpoint for connection to and communication with the CESM server. The agent is responsible for receiving tasks like applying security policy to CES at the managed computer, running AV scans etc. from the central Service and executing them on the managed computer. The agent is also responsible for gathering reports as requested by the central service and to pass them to the central service. The endpoints imported into a CESM service by installing the agent can be managed only by the same CESM service - meaning the agent cannot be reconfigured to connect to any other CESM service, increasing the security.

Groups - CESM allows computer groups to be created as required by the structure of the corporate organization. Once groups have been created sorting the computers in the network, admins can run tasks (such as applying security policy, running AV scans and deploying agents) as required for specific groups.

Remote Mode - CESM can apply a security policy and can run tasks like AV scans and database updates only if CES in an endpoint is maintained in Remote Management Mode (i.e., it is being remotely administered through CESM).

Unassigned Group - The 'Unassigned' group is the default computer group in CESM. Any target computer, imported into CESM by installing the agent automatically through the CESM admin console or manually, will be first placed in the 'Unassigned' group and will be assigned the 'Locally Configured' Policy. The administrator can create new groups as required and import computers into those groups from the 'Unassigned' group.

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

Reports - CESM allows the administrators to generate highly informative, real-time and active graphical summaries of the security and 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.

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 are installed automatically from the administrative console or manually at the endpoints using the 'Manage this Endpoint' feature of CES 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) 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)

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.

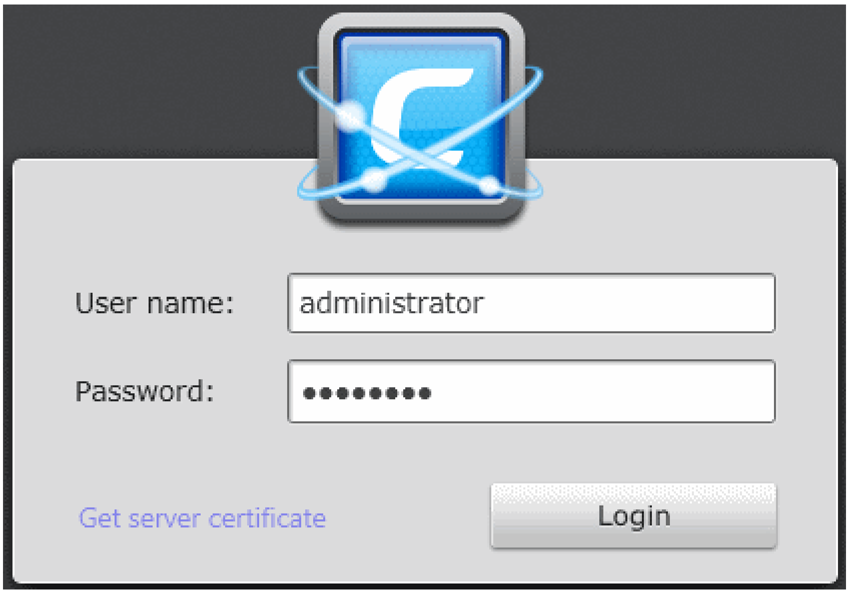
Step 2 - Login to the Admin Console *(see* **logging into the console** *if you need more help with this)*

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.



User name: administrator

Password: ●●●●●●●●

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)

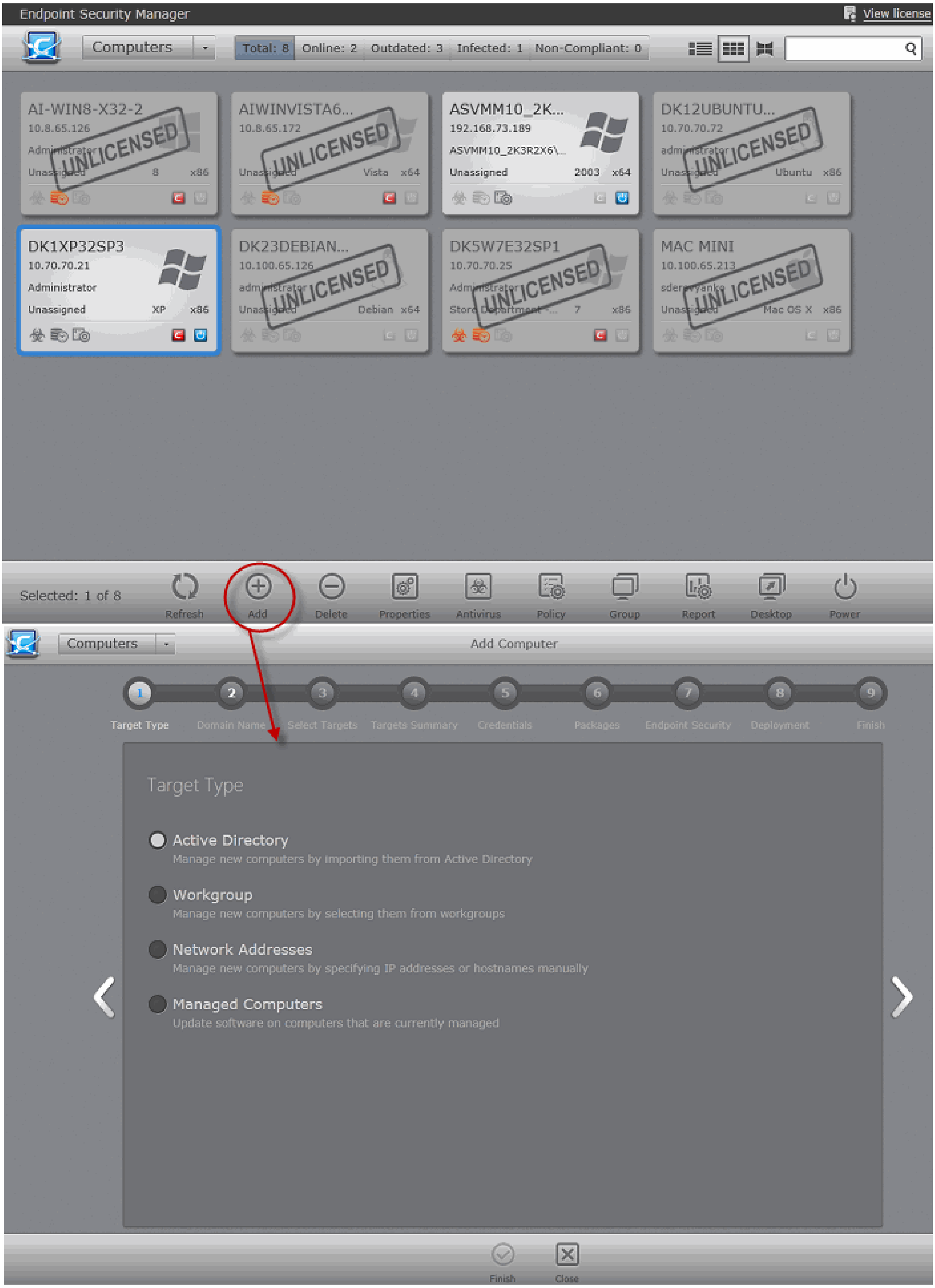
Next, we need to import endpoints and install the agent and Comodo Endpoint Security on them. The agent is a small piece of software that facilitates communication between the endpoint and the CESM server.

There are two ways to accomplish this:

- Remotely, using a console wizard to automatically push the agent and (optionally) CES 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 and CES**.

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.



Target Type

○ Active Directory
Manage new computers by importing them from Active Directory

● Workgroup
Manage new computers by selecting them from workgroups

● Network Addresses
Manage new computers by specifying IP addresses or hostnames manually

● Managed Computers
Update software on computers that are currently managed

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. 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.

    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 Comodo Endpoint Security. 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 CES. 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 next stage 'Packages' displays the version details of ESM Agent and CES. You can also check for updates of these applications and download it in your server for deployment on to the end-points. Swipe left (or click the right arrow button) to move onto the next step.

9. The final step prior to deployment is to decide whether you want to install Comodo Endpoint Security (CES) *also* at this time.

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

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

      (2) Choose components to install - Firewall, Antivirus or All Components.

      (3) 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.

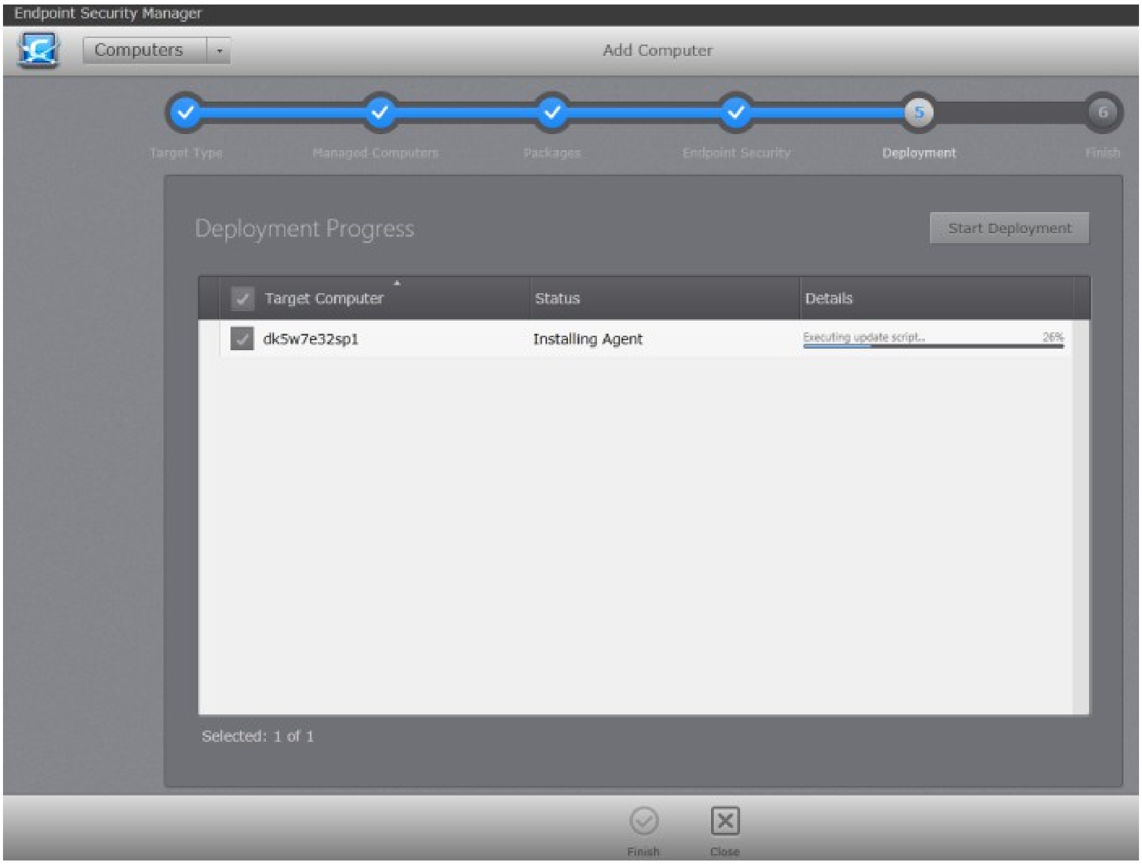
      (4) 'Uninstall all incompatible products' - Check this option to uninstall select third party antivirus, firewall and other desktop security software from the endpoints, prior to the installation of CES. Performing this step will remove potentially incompatible products and thus enable CES to operate 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 button to continue to move onto the next step to move to deployment step.

10. Deployment.

    - Click 'Start Deployment'. You will see installation progress per-endpoint. Once installation is complete, you should see a results screen similar to the following screenshot.

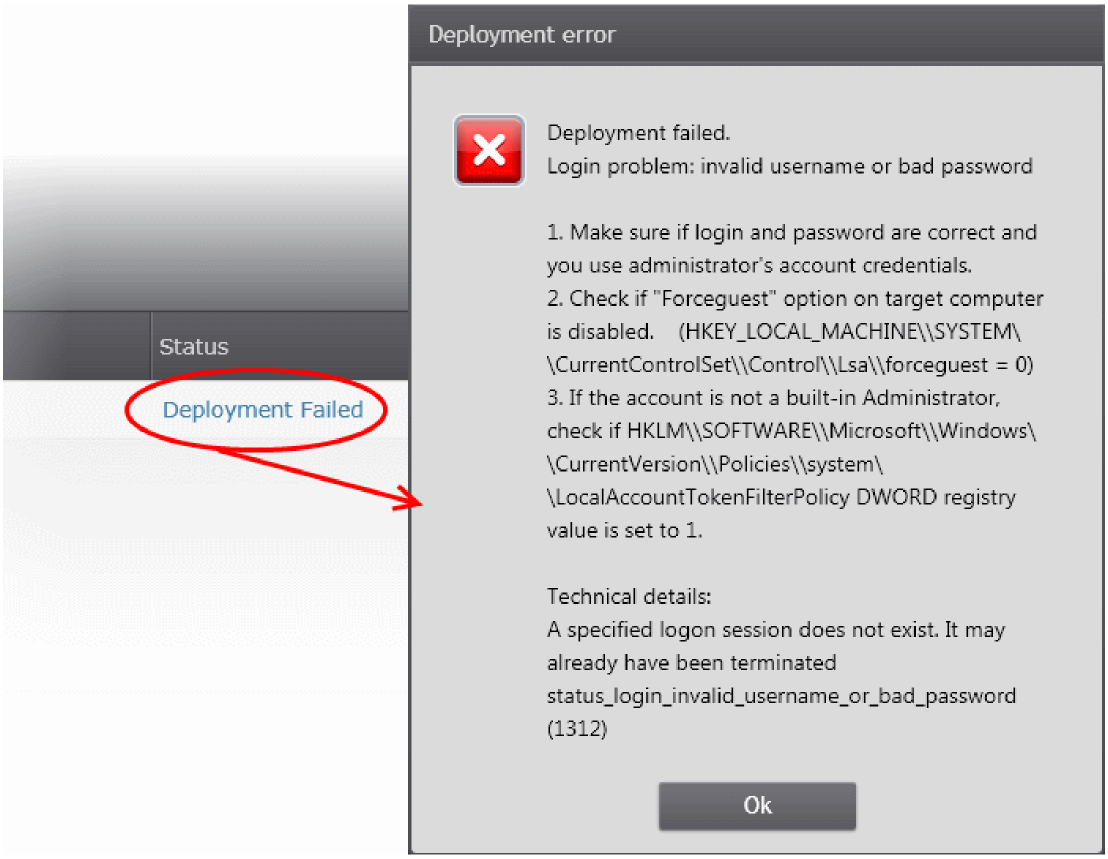


Deployment Progress

Target Computer	Status	Details
dk5w7e32sp1	Installing Agent	Executing update script... 26%

Selected: 1 of 1

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



Deployment error

Deployment failed.
Login problem: invalid username or bad password

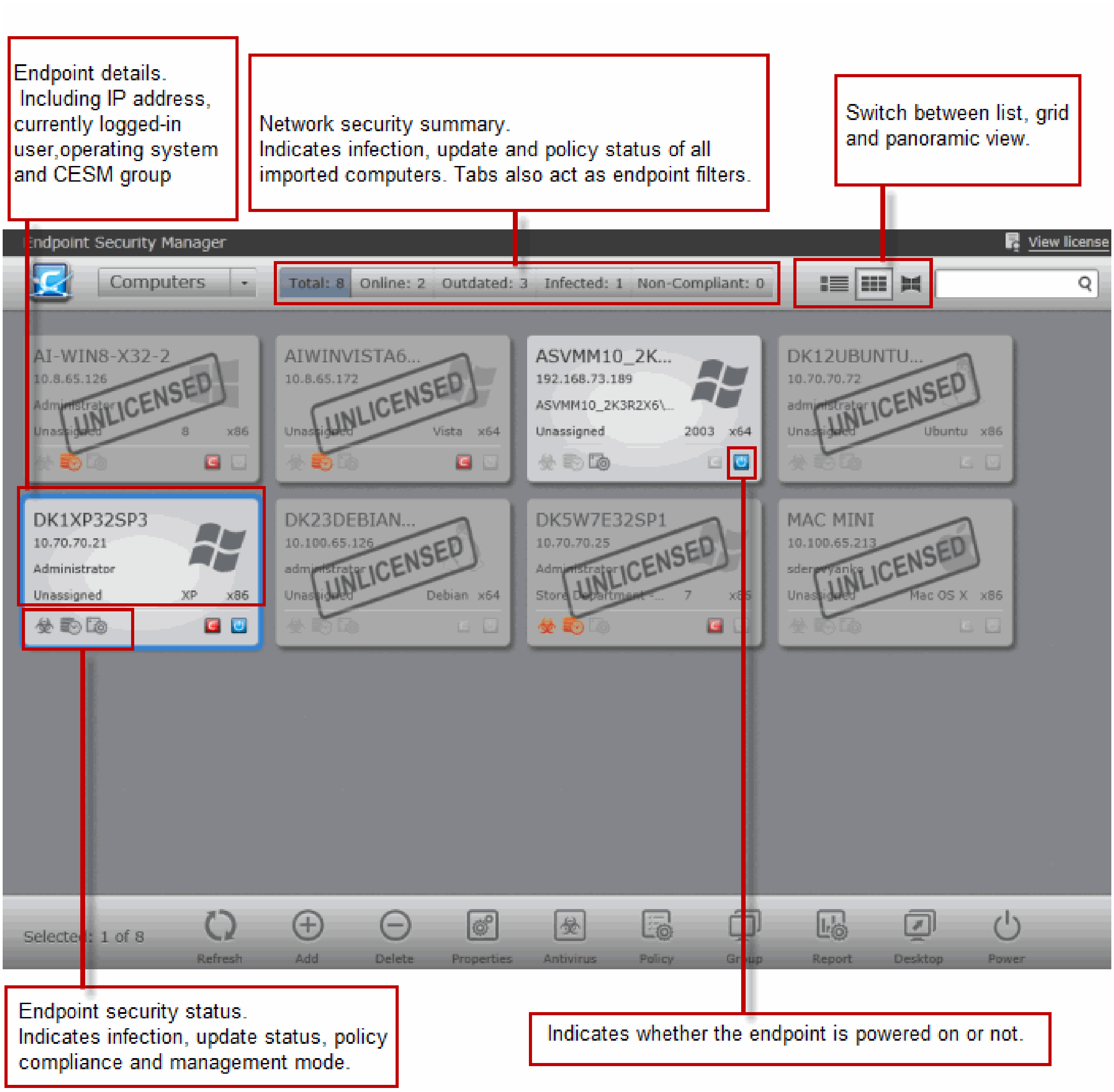
1. Make sure if login and password are correct and you use administrator's account credentials.
2. Check if "Forceguest" option on target computer is disabled. (HKEY_LOCAL_MACHINE\\SYSTEM\\CurrentControlSet\\Control\\Lsa\\forceguest = 0)
3. If the account is not a built-in Administrator, check if HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Policies\\system\\LocalAccountTokenFilterPolicy DWORD registry value is set to 1.

Technical details:
A specified logon session does not exist. It may already have been terminated
status_login_invalid_username_or_bad_password (1312)

- Once deployment is successful, click the 'Finish' icon at the base of the interface to exit the wizard. If you have chosen to install both the agent & CES then those endpoints should now be reporting to CESM.

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.



Endpoint details. Including IP address, currently logged-in user,operating system and CESM group

Network security summary. Indicates infection, update and policy status of all imported computers. Tabs also act as endpoint filters.

Switch between list, grid and panoramic view.

Endpoint security status. Indicates infection, update status, policy compliance and management mode.

Indicates whether the endpoint is powered on or not.

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 databases are 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 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) 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 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 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.
- Selecting 'Force target computers to be managed remotely upon policy assignment' means CESM will engage 'Remote Mode' and thus enforce policy compliance on the selected endpoint. if the policy becomes altered, CESM will automatically re-apply it. If not selected, the endpoints will remain in locally managed mode (although your policy will still be applied, it could become changed over time at the local level).
- Finally, give the policy a name and description and select 'Apply policy after finish' to immediately implement. Do not select this if you wish to deploy later.

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

Step 7 – Viewing Reports

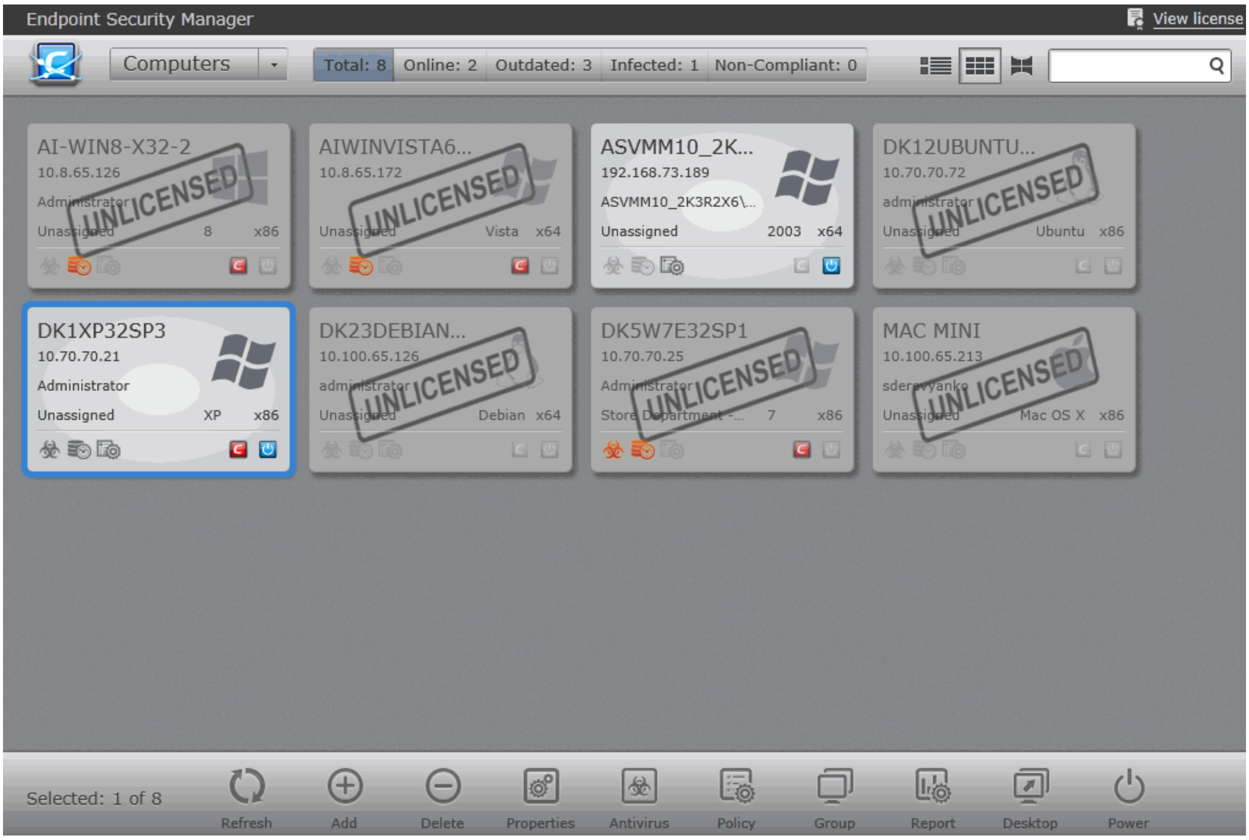
The reports area contains a wealth of valuable information for administrators. Admins can also drill-down to individual endpoints from any report. Reports can be exported, printed and cover the following categories:

- Antivirus Updates
- CES Configuration
- CES Logs
  - Antivirus Logs
  - Firewall Logs
  - Defense+ Logs
- Computer Details
- Computer Infections
- Malware Statistics
- Policy Compliance
- Policy Delta
- Quarantined Items
- Top 10 Malwares

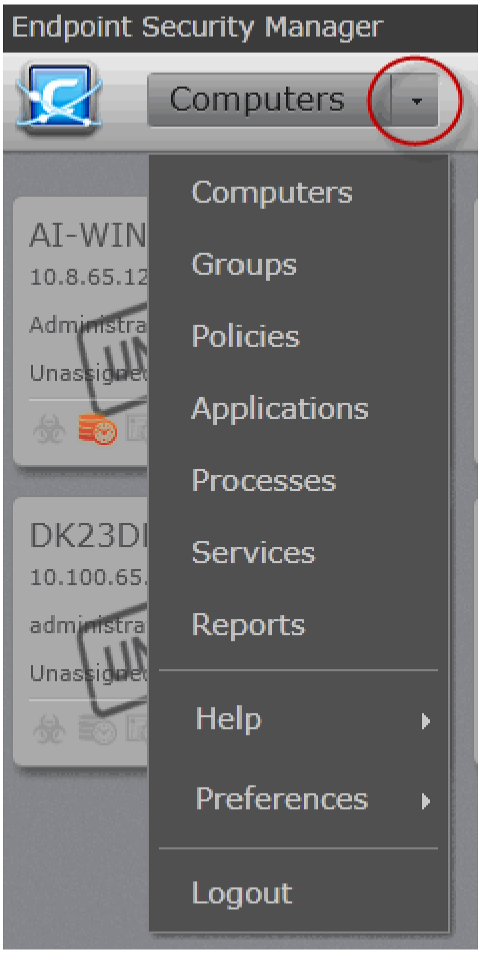
Click here to read more about reports.

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 seven main areas that can be selected from the drop-down menu near the top left - 'Computers', 'Groups' 'Policies', 'Applications', 'Processes', 'Services', 'Reports', 'Help', 'Preferences' and 'Logout':



Main Functional Areas

- **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.
- **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.
- **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.
- **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.
- **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

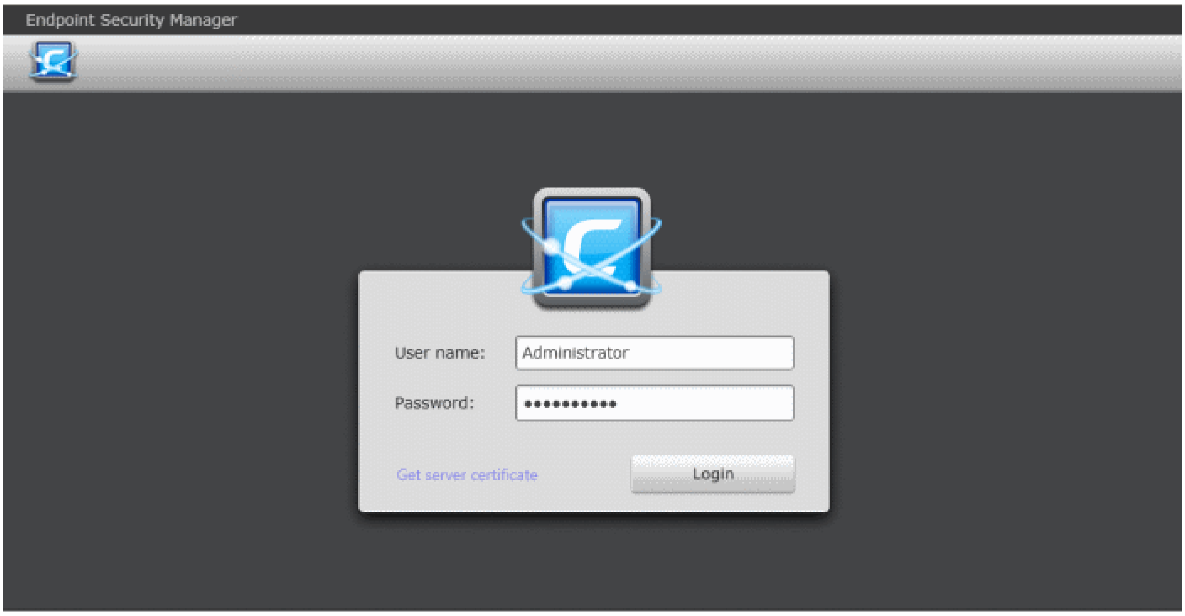
  https://<server hostname or IP address>:57194

  - 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).



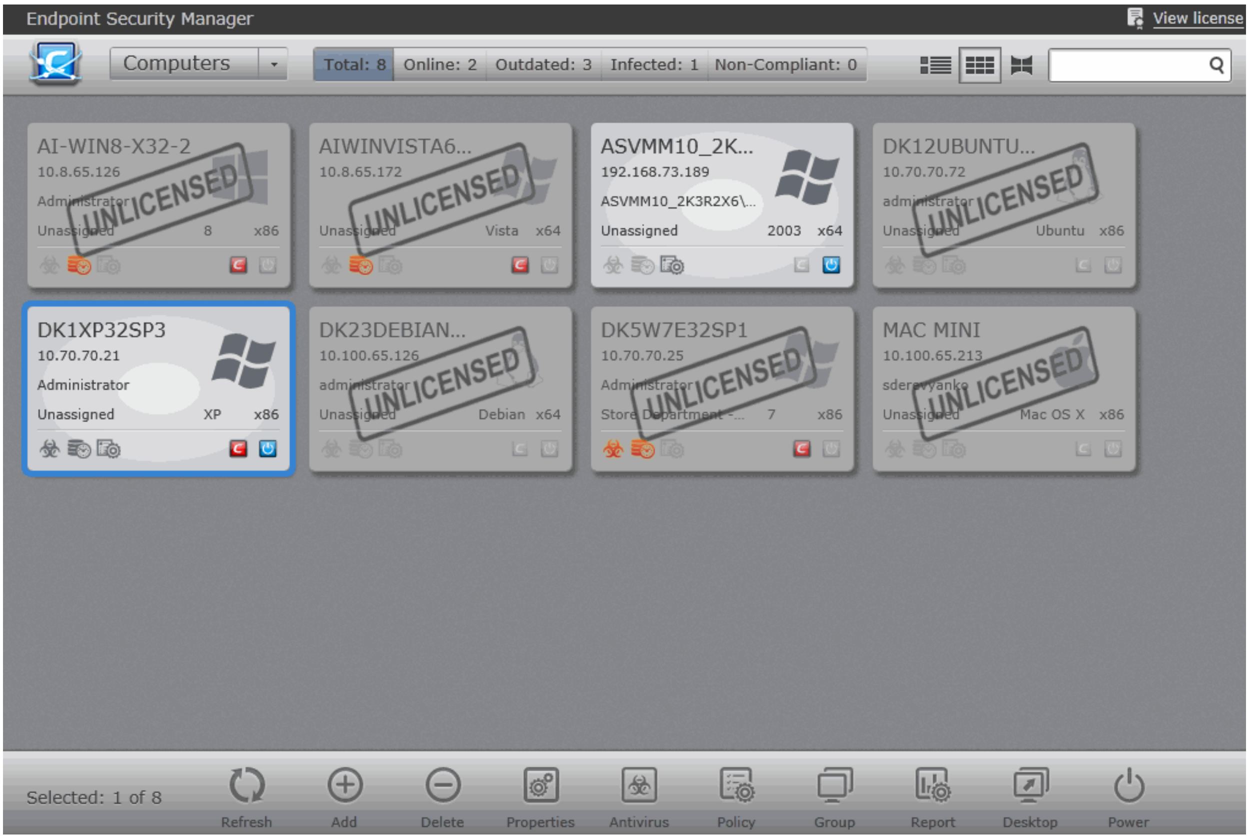
User name: Administrator

Password: ●●●●●●●●●●●

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. Endpoints can be filtered according to status using the buttons above the main display. You can add endpoints or perform actions on selected endpoints using the options along the bottom of the interface.



AI-WIN8-X32-2 10.8.65.126 Administrator Unassigned 8 x86

AIWINVISTA6... 10.8.65.172 Unassigned Vista x64

ASVMM10_2K... 192.168.73.189 ASVMM10_2K3R2X6\... Unassigned 2003 x64

DK12UBUNTU... 10.70.70.72 administrator Unassigned Ubuntu x86

DK1XP32SP3 10.70.70.21 Administrator Unassigned XP x86

DK23DEBIAN... 10.100.65.126 administrator Unassigned Debian x64

DK5W7E32SP1 10.70.70.25 Administrator Store Department -... 7 x86

MAC MINI 10.100.65.213 sderevyanko Unassigned Mac OS X x86

The 'Computers' area allows administrators to:

- View the list of endpoints that are managed by CESM.
- Add/Import computers to CESM for centralized management.
- 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.
- 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 Reports for a target endpoint.
- Reboot endpoints where required,

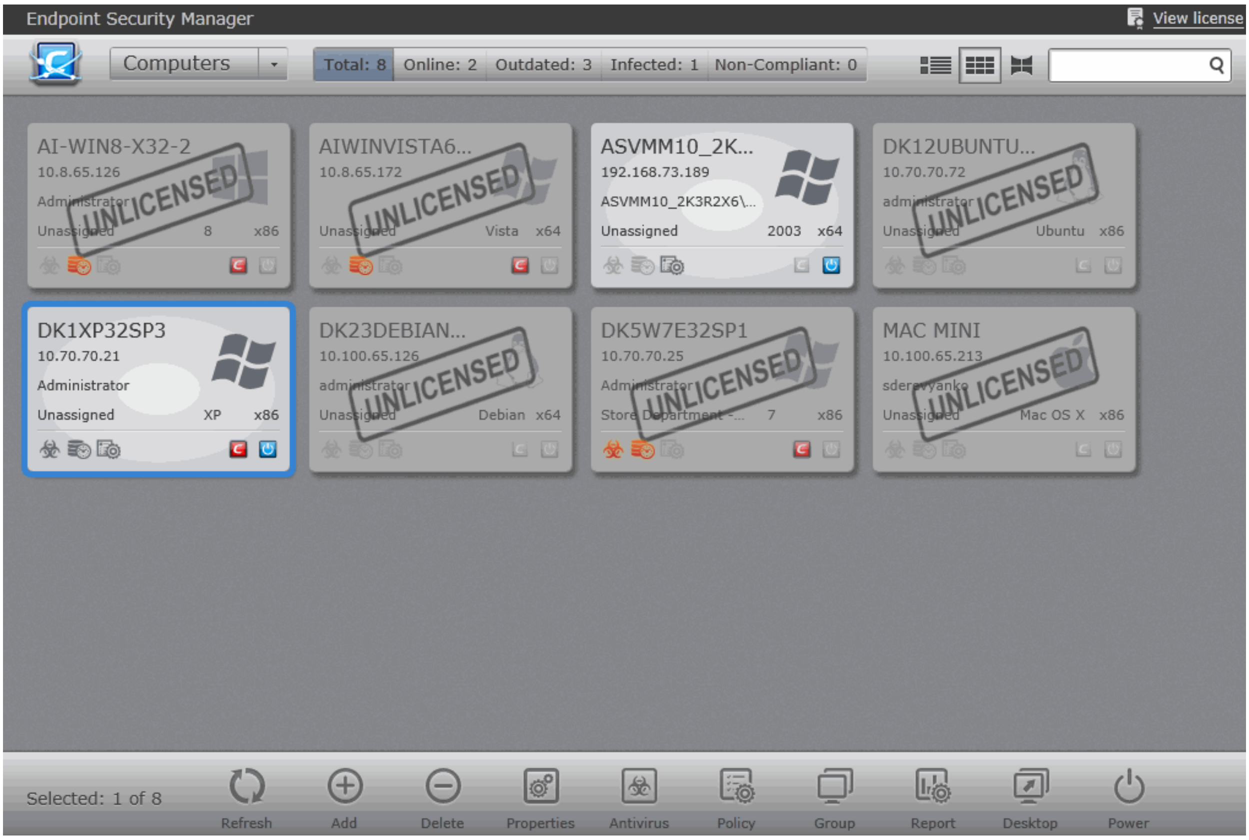
Once the agent is installed, the endpoint computer is added into CESM and is ready to be managed through CESM. See the section '**Adding Endpoint Computers to CESM**' for complete instructions.

View and Filter Options

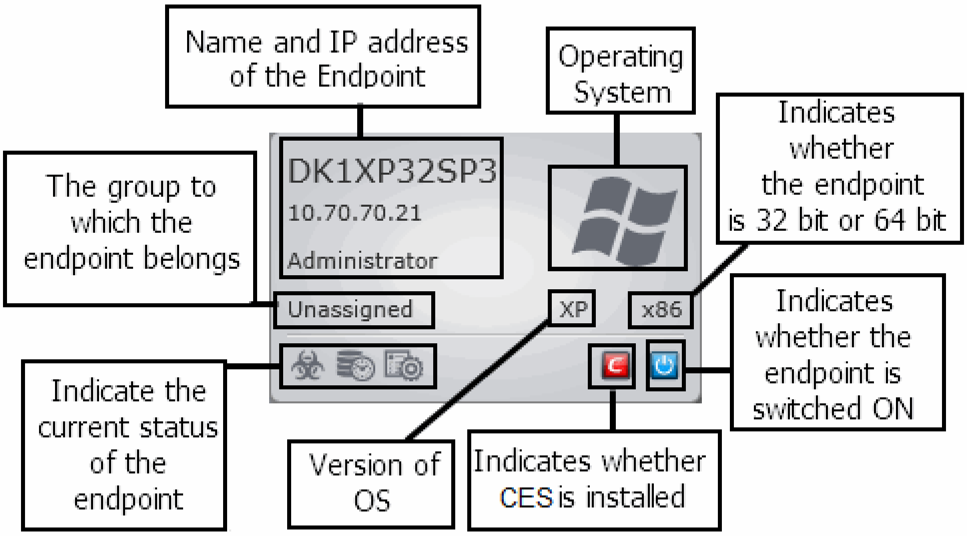
The Computers area can display the computers connected to CESM in **tile view** or **list view** or **3D Panoramic view**.

Tile View

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



Each computer is represented by a tile with its status details:


Name and IP address of the Endpoint
Operating System
Indicates whether the endpoint is 32 bit or 64 bit
The group to which the endpoint belongs
DK1XP32SP3
10.70.70.21
Administrator
Unassigned
XP
x86
Indicates whether the endpoint is switched ON
Indicate the current status of the endpoint
Version of OS
Indicates whether CES is installed

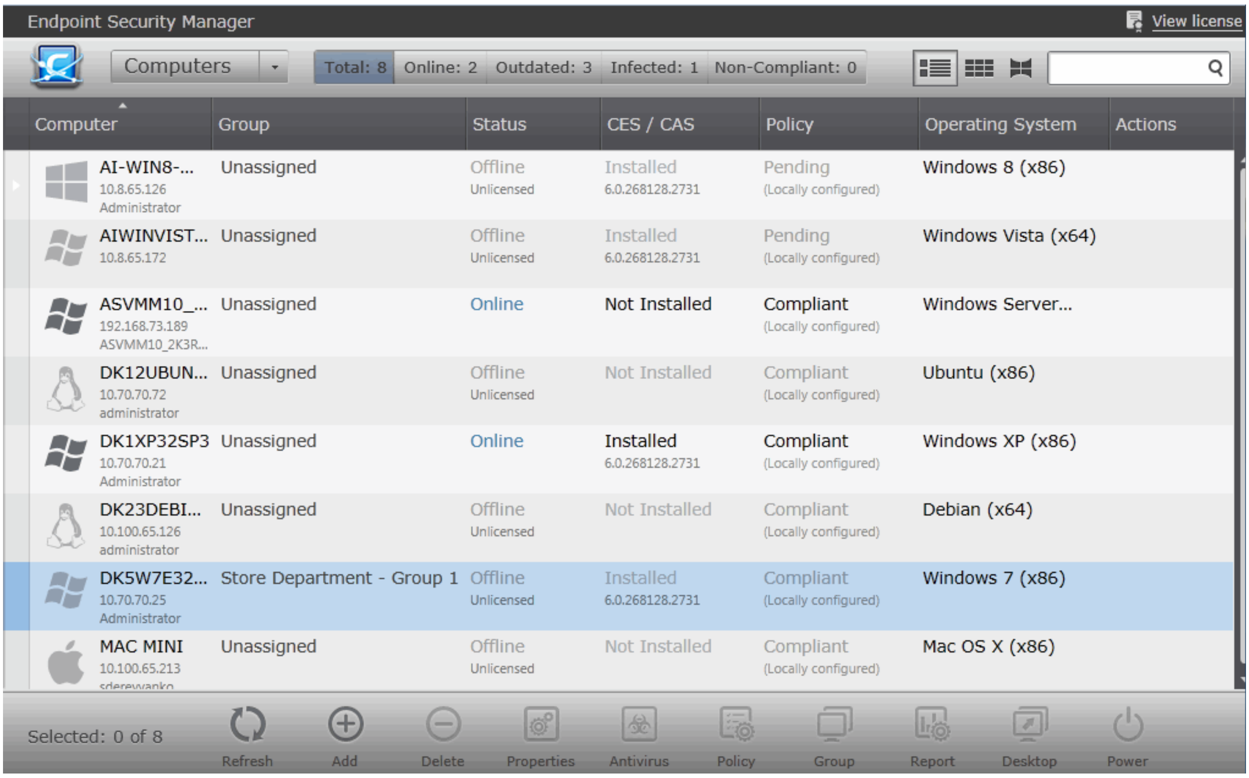
The icons at the bottom indicate the current status of the endpoint.

Status	Icon	Indication

Power	⏻	The endpoint is powered ON
	⏻	The endpoint is powered OFF
Comodo Endpoint Security	C	CES is installed
	C	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

List View

- To switch the Computers area to List View, click the List View button ☰ from the gray stripe.



Endpoint Security Manager

View license

Computers

Total: 8 Online: 2 Outdated: 3 Infected: 1 Non-Compliant: 0

Computer	Group	Status	CES / CAS	Policy	Operating System	Actions
AI-WIN8-... 10.8.65.126 Administrator	Unassigned	Offline Unlicensed	Installed 6.0.268128.2731	Pending (Locally configured)	Windows 8 (x86)	
AIWINVIST... 10.8.65.172	Unassigned	Offline Unlicensed	Installed 6.0.268128.2731	Pending (Locally configured)	Windows Vista (x64)	
ASVMM10_... 192.168.73.189 ASVMM10_2K3R...	Unassigned	Online	Not Installed	Compliant (Locally configured)	Windows Server...	
DK12UBUN... 10.70.70.72 administrator	Unassigned	Offline Unlicensed	Not Installed	Compliant (Locally configured)	Ubuntu (x86)	
DK1XP32SP3 10.70.70.21 Administrator	Unassigned	Online	Installed 6.0.268128.2731	Compliant (Locally configured)	Windows XP (x86)	
DK23DEBI... 10.100.65.126 administrator	Unassigned	Offline Unlicensed	Not Installed	Compliant (Locally configured)	Debian (x64)	
DK5W7E32... 10.70.70.25 Administrator	Store Department - Group 1	Offline Unlicensed	Installed 6.0.268128.2731	Compliant (Locally configured)	Windows 7 (x86)	
MAC MINI 10.100.65.213 sderevyanko	Unassigned	Offline Unlicensed	Not Installed	Compliant (Locally configured)	Mac OS X (x86)	

Selected: 0 of 8

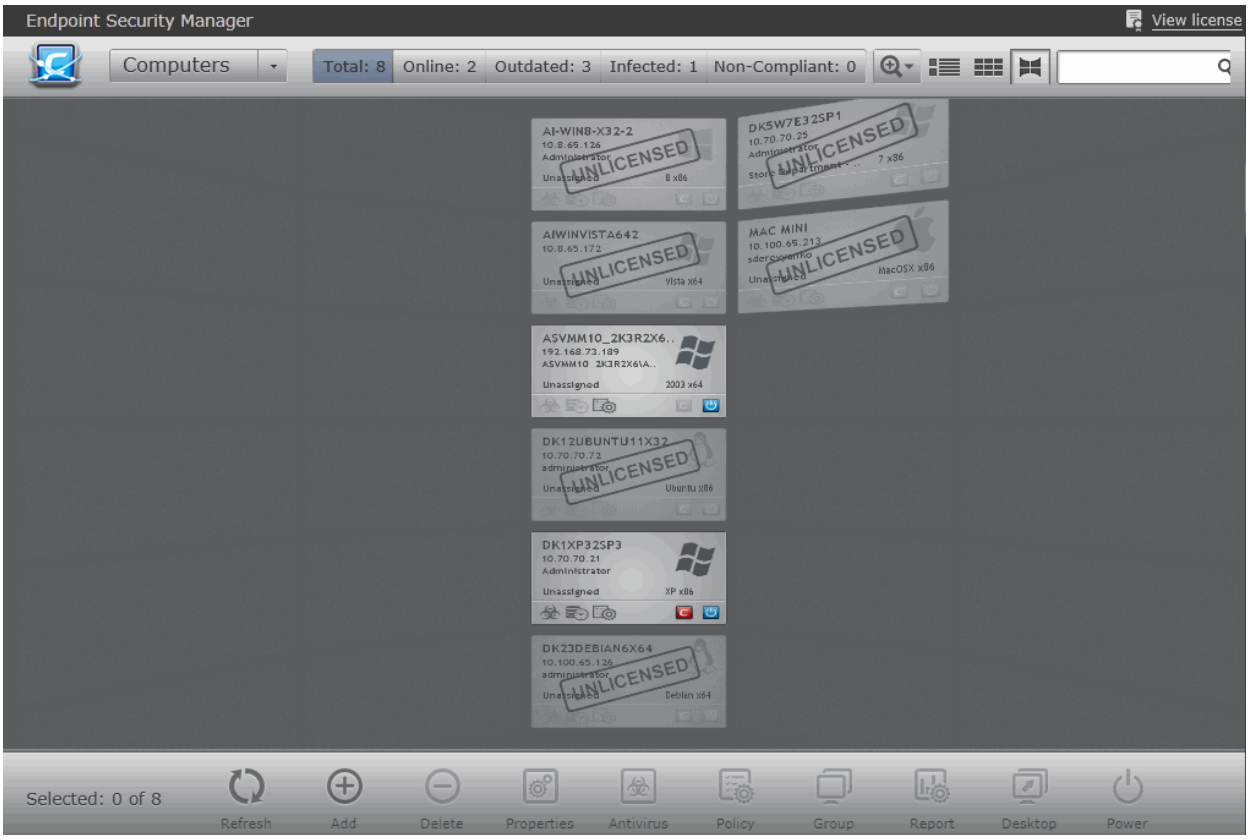
Column Heading	Description
Computer	Displays the name of the Endpoint computer.
Group	Displays the Group to which the endpoint belongs.
Status	Indicates whether the endpoint is online or offline. The connection state can be one of the following: • **Online** - The endpoint agent is connected to CESM. • **Offline** - The endpoint agent is not connected to CESM at this moment.

CES/CAS	Indicates whether the CES/CAS is installed to the endpoint or not and if it's version is supported by CESM or too old to manage. • **Local** - The CES installation at the endpoint is being managed locally. • **Remote** - The CES installation at the endpoint is being managed remotely. • **Unknown** - The management mode of CES at the endpoint cannot be established. This may be because CES is not installed; is not active or because of network problems.
Policy	Displays the compliance status of the CES installation on the endpoint with the applied security policy. The local connection and Internet connection security policies applied for the endpoint are displayed beneath the compliance status. The compliance status can be one of the following: • **Non-Compliant** - The CES installation at the endpoint is not compliant to the applied security policy. • **Pending** - The compliance status of the CES installation at the endpoint is yet to be assessed. For further reading on 'Policies', please see '**The Policies Area**'.
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.

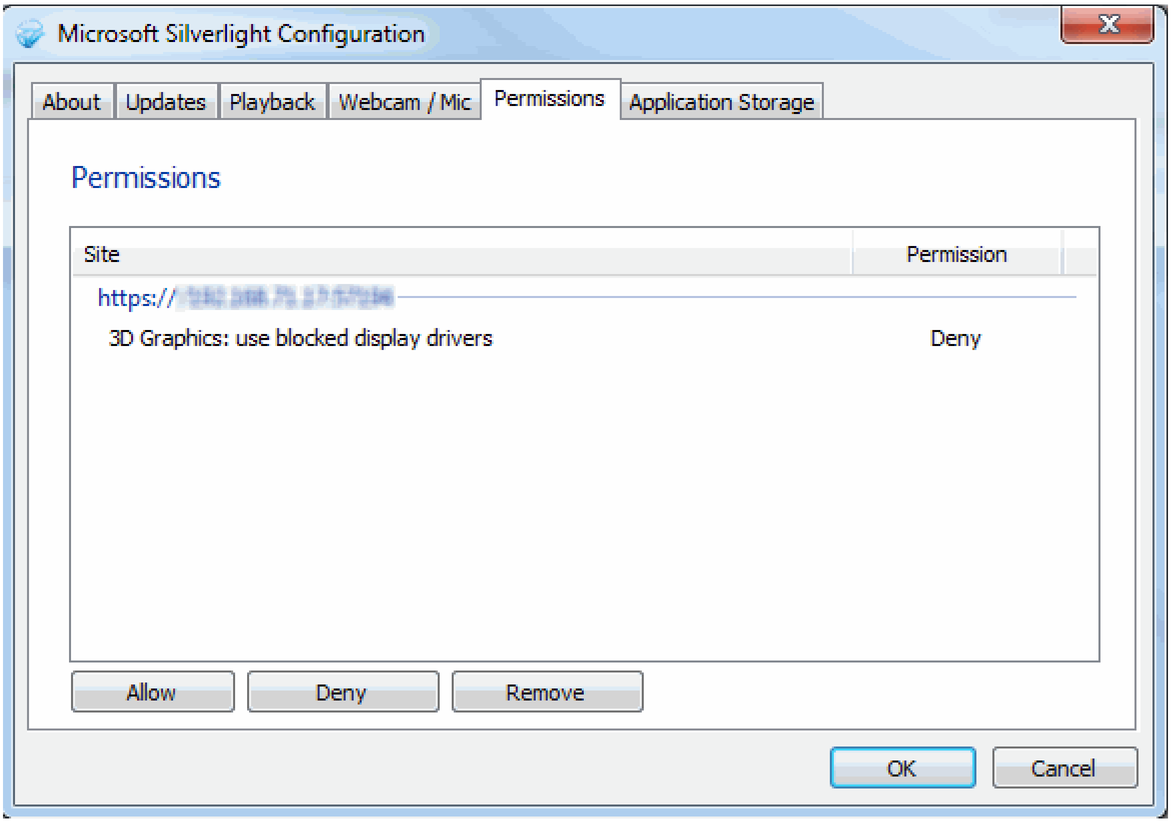
- To switch to 3D Panoramic view, click the 3D View button from the gray stripe.



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.



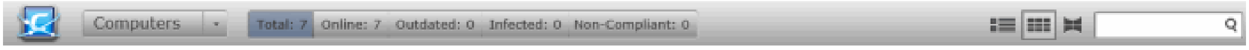
Site	Permission
https://[redacted]	
3D Graphics: use blocked display drivers	Deny

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

The filter options in the gray stripe, gives at-a-glance statistics of the computers in the network 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 computer by entering its name or IP address, partially or fully.



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

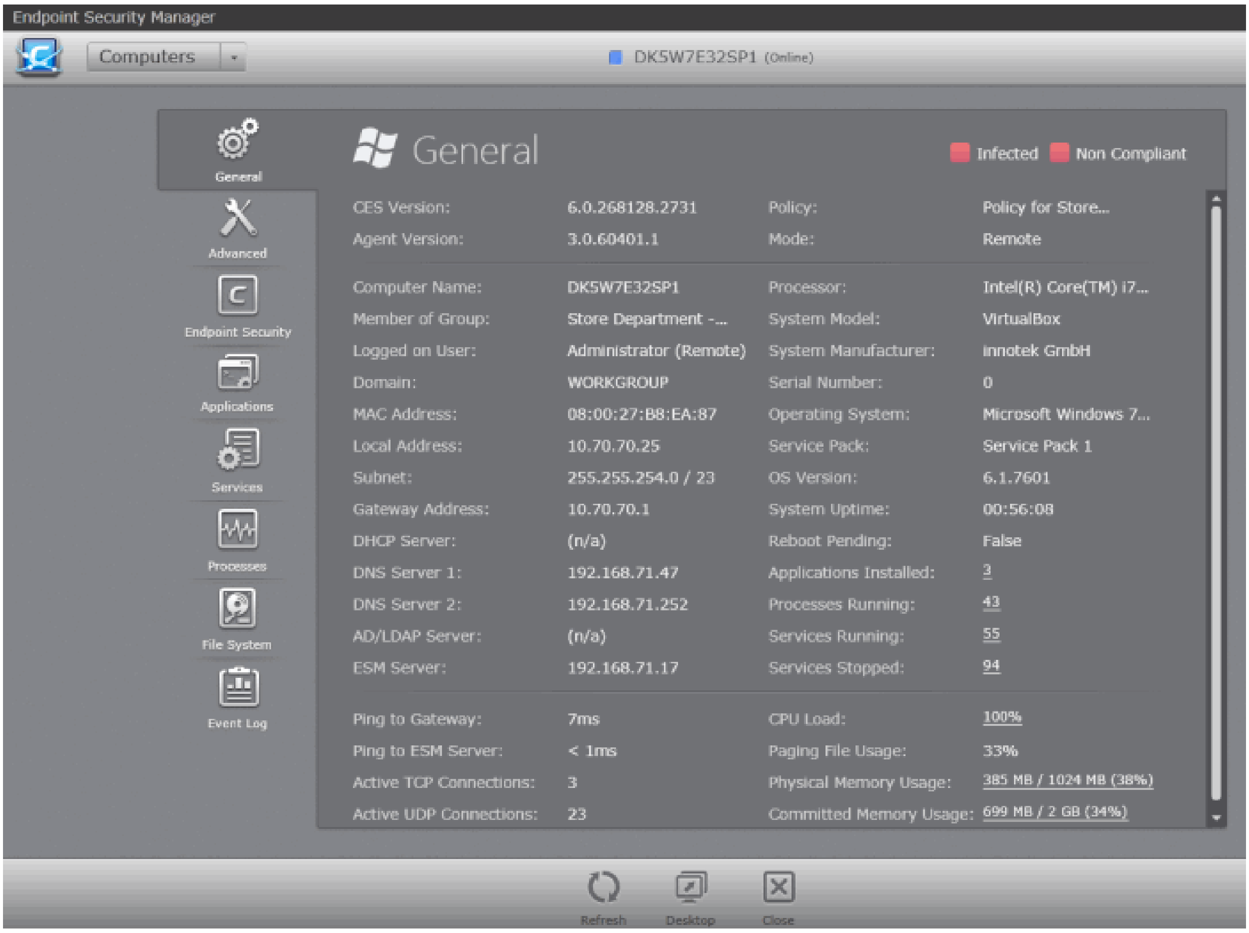
From the 'Computer Properties' screen, the administrator view a detailed breakdown of information about the endpoint and perform various management tasks on the endpoint. These include applying/re-applying security policies, managing CES configuration, assigning the endpoint to groups, running a virus 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.



CES Version:	6.0.268128.2731	Policy:	Policy for Store...
Agent Version:	3.0.60401.1	Mode:	Remote
Computer Name:	DK5W7E32SP1	Processor:	Intel(R) Core(TM) i7...
Member of Group:	Store Department -...	System Model:	VirtualBox
Logged on User:	Administrator (Remote)	System Manufacturer:	innotek GmbH
Domain:	WORKGROUP	Serial Number:	0
MAC Address:	08:00:27:B8:EA:87	Operating System:	Microsoft Windows 7...
Local Address:	10.70.70.25	Service Pack:	Service Pack 1
Subnet:	255.255.254.0 / 23	OS Version:	6.1.7601
Gateway Address:	10.70.70.1	System Uptime:	00:56:08
DHCP Server:	(n/a)	Reboot Pending:	False
DNS Server 1:	192.168.71.47	Applications Installed:	3
DNS Server 2:	192.168.71.252	Processes Running:	43
AD/LDAP Server:	(n/a)	Services Running:	55
ESM Server:	192.168.71.17	Services Stopped:	94
Ping to Gateway:	7ms	CPU Load:	100%
Ping to ESM Server:	< 1ms	Paging File Usage:	33%
Active TCP Connections:	3	Physical Memory Usage:	385 MB / 1024 MB (38%)
Active UDP Connections:	23	Committed Memory Usage:	699 MB / 2 GB (34%)

The Computer Properties screen allows the administrator to:

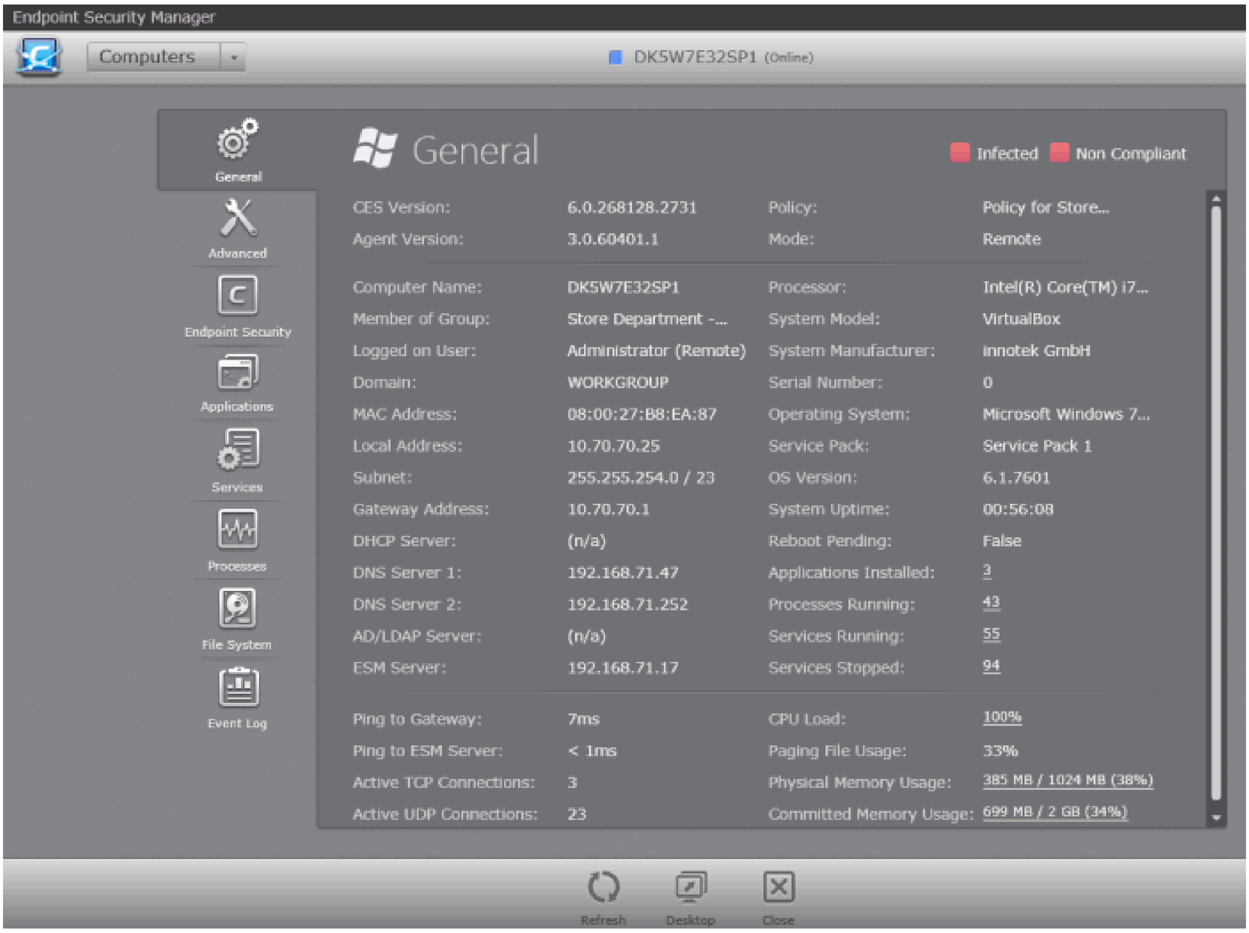
- **View General Properties**
- **View and Manage Group and Security Policy Details**
- **View and Manage Internet Security Software**
- **View and Manage installed applications**
- **View and Manage currently running services**
- **View and Manage currently running processes**
- **View and Manage Drives 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, agent 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.



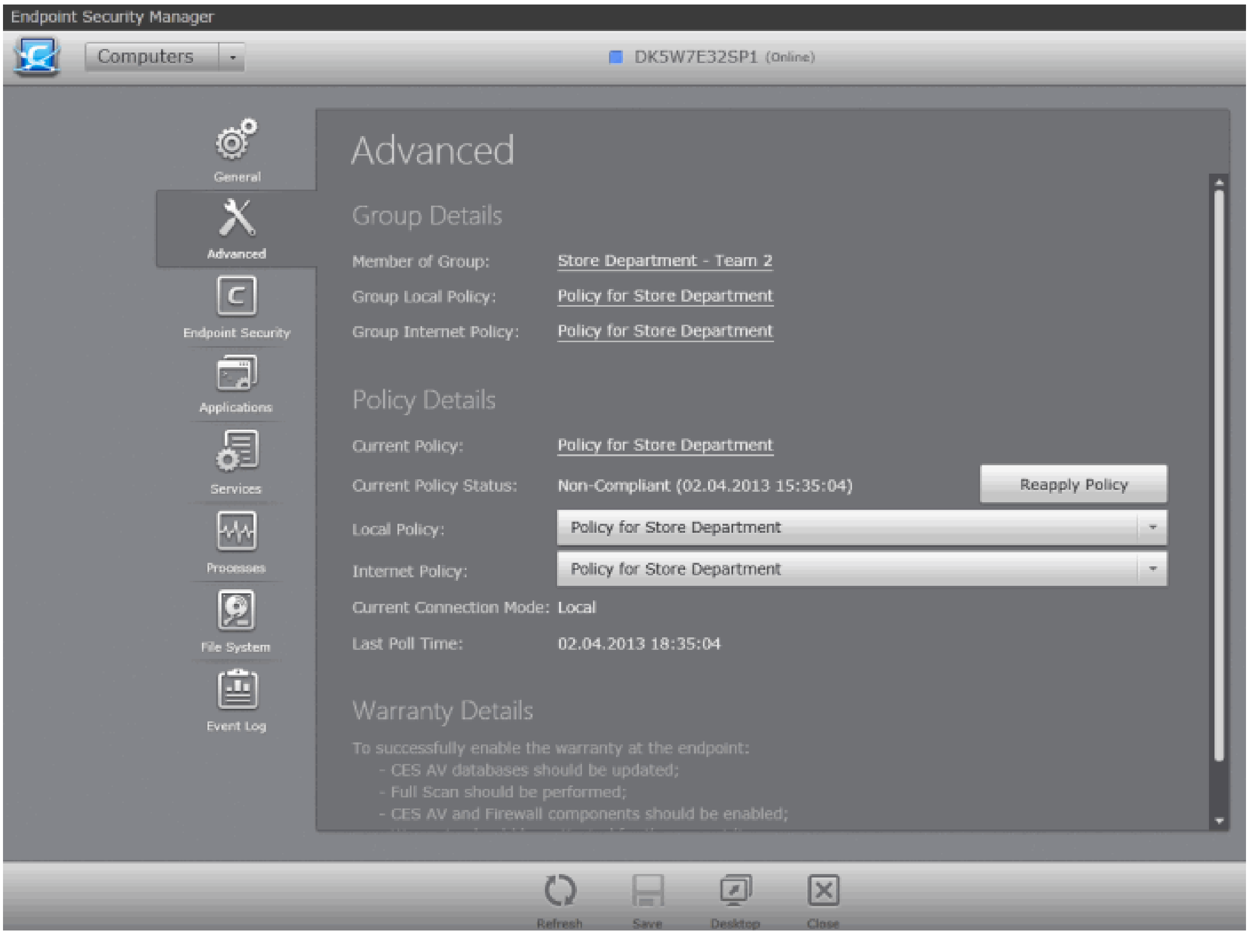
CES Version:	6.0.268128.2731	Policy:	Policy for Store...
Agent Version:	3.0.60401.1	Mode:	Remote
Computer Name:	DK5W7E32SP1	Processor:	Intel(R) Core(TM) i7...
Member of Group:	Store Department -...	System Model:	VirtualBox
Logged on User:	Administrator (Remote)	System Manufacturer:	innotek GmbH
Domain:	WORKGROUP	Serial Number:	0
MAC Address:	08:00:27:B8:EA:87	Operating System:	Microsoft Windows 7...
Local Address:	10.70.70.25	Service Pack:	Service Pack 1
Subnet:	255.255.254.0 / 23	OS Version:	6.1.7601
Gateway Address:	10.70.70.1	System Uptime:	00:56:08
DHCP Server:	(n/a)	Reboot Pending:	False
DNS Server 1:	192.168.71.47	Applications Installed:	3
DNS Server 2:	192.168.71.252	Processes Running:	43
AD/LDAP Server:	(n/a)	Services Running:	55
ESM Server:	192.168.71.17	Services Stopped:	94
Ping to Gateway:	7ms	CPU Load:	100%
Ping to ESM Server:	< 1ms	Paging File Usage:	33%
Active TCP Connections:	3	Physical Memory Usage:	385 MB / 1024 MB (38%)
Active UDP Connections:	23	Committed Memory Usage:	699 MB / 2 GB (34%)

- 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' and 'Services Stopped' opens the 'System Services' pane that allows you to view the currently running Windows services at the endpoint and to terminate unnecessarily running services in order to optimize the system's performance. Refer to **Viewing and Managing Currently Running Services** for more details.

3.1.2. Viewing and Managing Group and Security Policy 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. 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.



Advanced

Group Details

Member of Group: Store Department - Team 2

Group Local Policy: Policy for Store Department

Group Internet Policy: Policy for Store Department

Policy Details

Current Policy: Policy for Store Department

Current Policy Status: Non-Compliant (02.04.2013 15:35:04)

Local Policy: Policy for Store Department

Internet Policy: Policy for Store Department

Current Connection Mode: Local

Last Poll Time: 02.04.2013 18:35:04

Warranty Details

To successfully enable the warranty at the endpoint:
- CES AV databases should be updated;
- Full Scan should be performed;
- CES AV and Firewall components should be enabled;

Group Details

The 'Group Details' area displays the details of the group to which the endpoint belongs and the security policy applied to the group.

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

Policy Details

The 'Policy Details' area displays the security policy applied to the endpoint individually. It also allows the administrator to change the security policy applied to the endpoint, if required.

- **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.
- **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.
- **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.

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.

- Click 'Refresh' to renew the currently viewed screen.
- To close the currently open detailed summary of information about the selected endpoint click 'Close'.
- To start the a currently running process remotely, select it and click 'Desktop'.

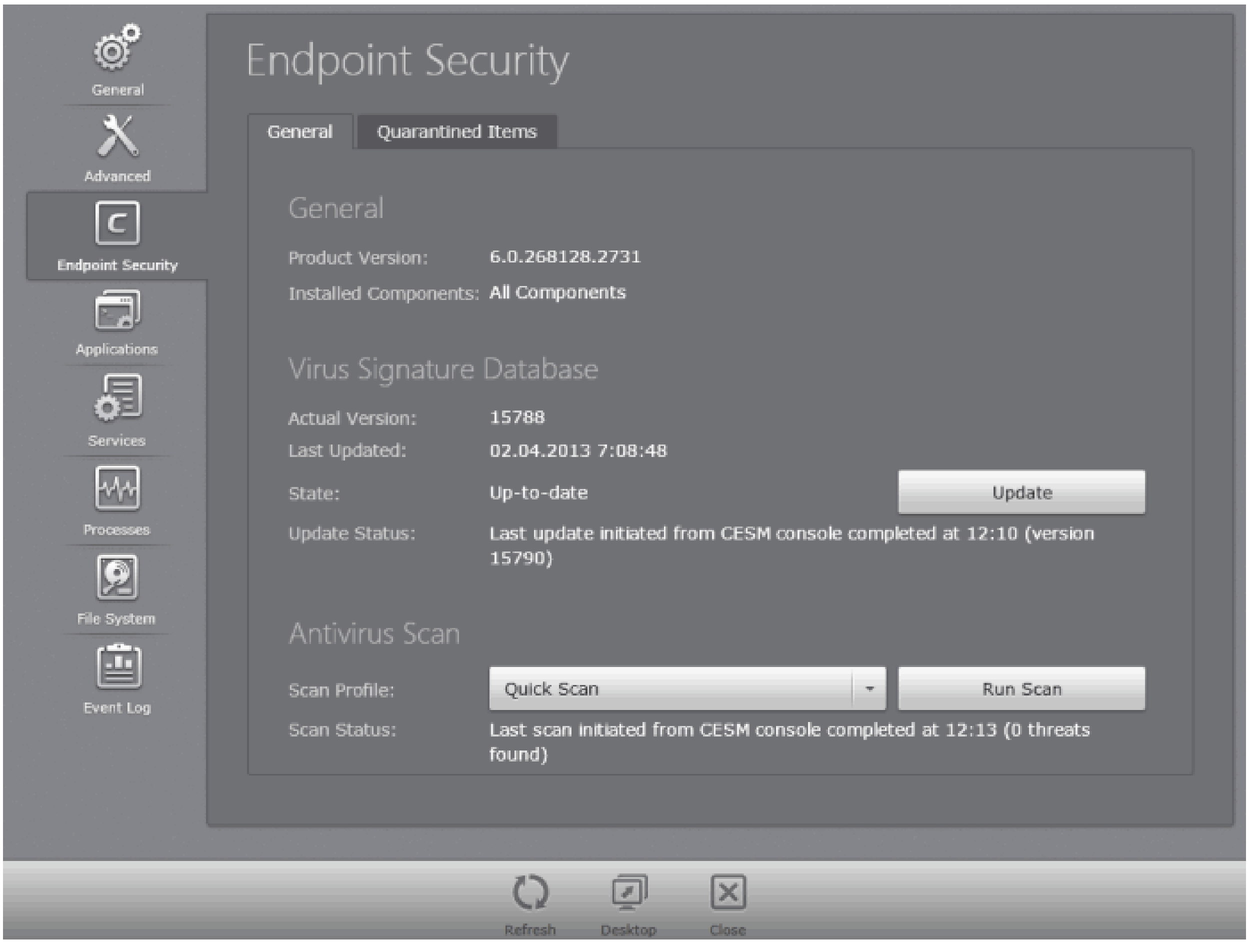
3.1.3. Viewing and Managing Endpoint Security Software

The 'Endpoint Security' pane displays the details of the CES installation on the endpoint. The administrator can run scans on-demand antivirus scans on the endpoint and manage items quarantined by the CES at the 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 two tabs:
    - **General**
    - **Quarantined Items**

General

The general tab displays the version, virus database update status of the CES installation. The administrator can run antivirus scans from this area.



Endpoint Security

General | Quarantined Items

General

Product Version: 6.0.268128.2731

Installed Components: All Components

Virus Signature Database

Actual Version: 15788

Last Updated: 02.04.2013 7:08:48

State: Up-to-date

Update Status: Last update initiated from CESM console completed at 12:10 (version 15790)

Antivirus Scan

Scan Profile: Quick Scan

Scan Status: Last scan initiated from CESM console completed at 12:13 (0 threats found)

General

- **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

- **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 Antivirus 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-72-1-451-4757-Custom-Scan-Settings.html**
- Click 'Scan'.

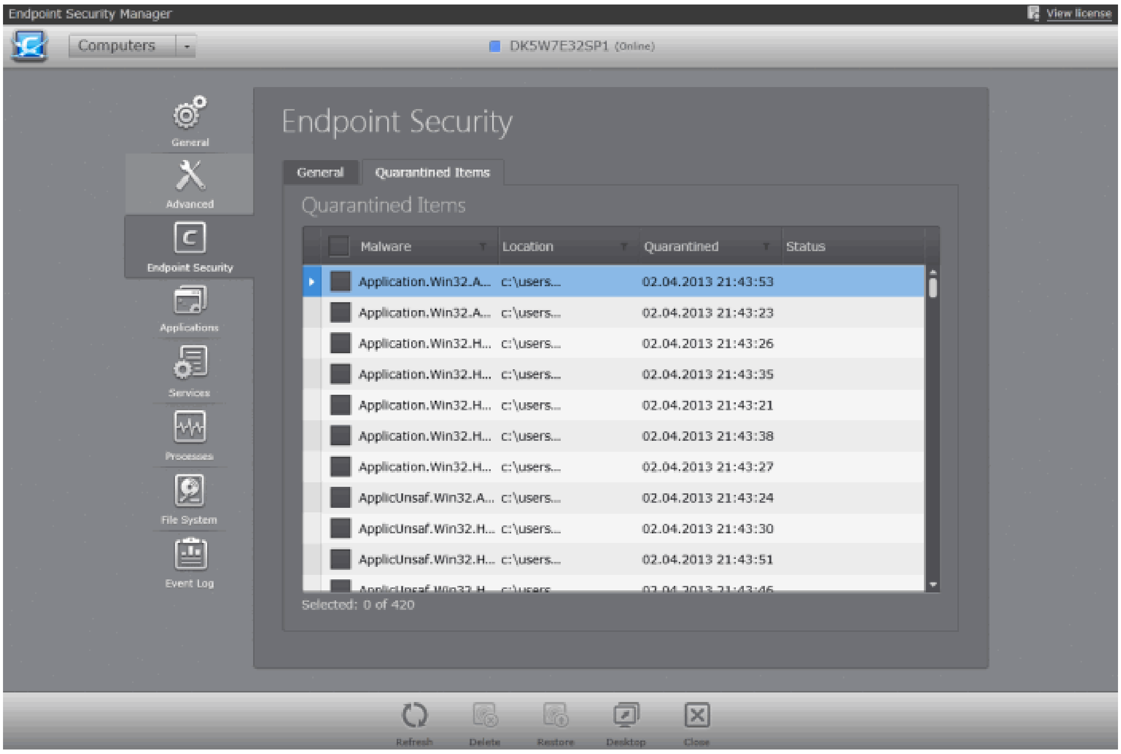
Tip: Alternatively, you can run a scan on an individual endpoint by right-clicking on the endpoint and selecting 'Scan' from the context sensitive menu or selecting an endpoint and clicking 'Run a Scan' or clicking 'Antivirus' > 'Scan' > 'Full Scan from the 'Computers' area.

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.

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

	Malware	Location	Quarantined	Status
□	Application.Win32.A...	c:\users...	02.04.2013 21:43:53	
□	Application.Win32.A...	c:\users...	02.04.2013 21:43:23	
□	Application.Win32.H...	c:\users...	02.04.2013 21:43:26	
□	Application.Win32.H...	c:\users...	02.04.2013 21:43:35	
□	Application.Win32.H...	c:\users...	02.04.2013 21:43:21	
□	Application.Win32.H...	c:\users...	02.04.2013 21:43:38	
□	Application.Win32.H...	c:\users...	02.04.2013 21:43:27	
□	ApplicUnsaf.Win32.A...	c:\users...	02.04.2013 21:43:24	
□	ApplicUnsaf.Win32.H...	c:\users...	02.04.2013 21:43:30	
□	ApplicUnsaf.Win32.H...	c:\users...	02.04.2013 21:43:51	
□	ApplicUnsaf.Win32.H...	c:\users...	02.04.2013 21:43:46	

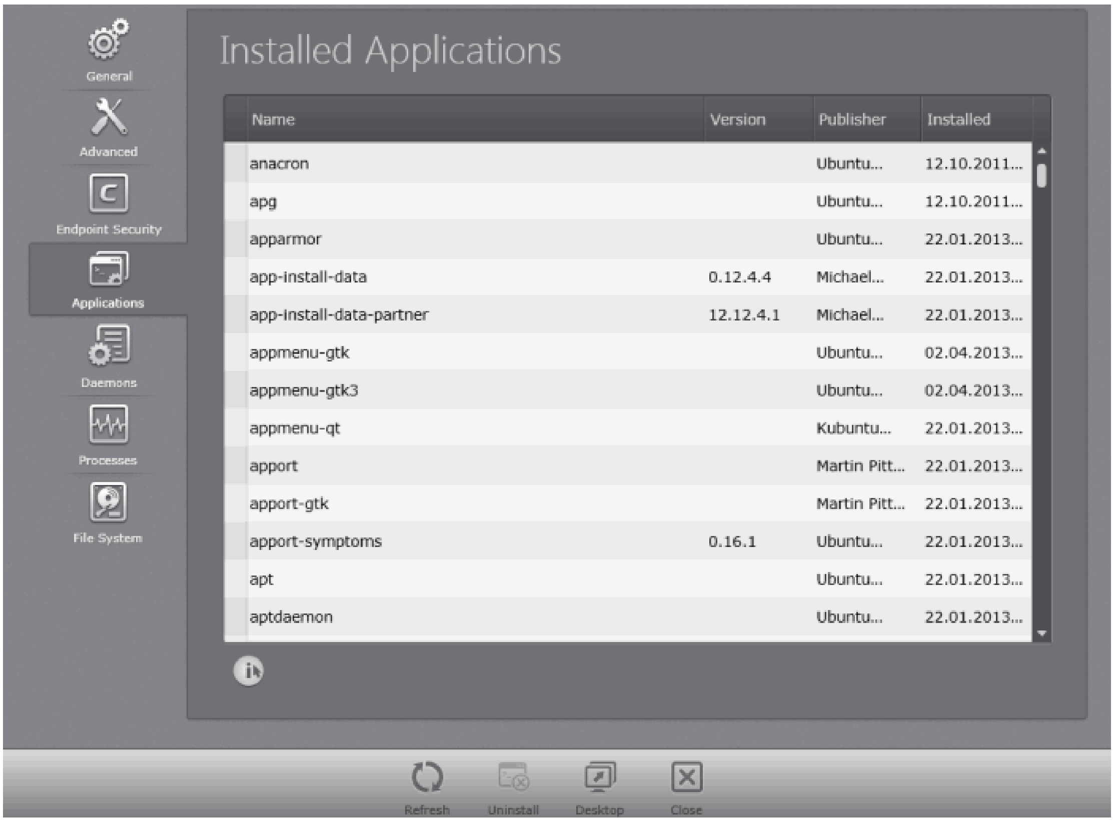
Selected: 0 of 420

- 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.
- To close the currently open detailed summary of information about the selected endpoint click 'Close'.
- Click 'Refresh' to renew the currently viewed screen.
- To start the a currently running process remotely, select it and click 'Desktop'.

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.



Installed Applications

Name	Version	Publisher	Installed
anacron		Ubuntu...	12.10.2011...
apg		Ubuntu...	12.10.2011...
apparmor		Ubuntu...	22.01.2013...
app-install-data	0.12.4.4	Michael...	22.01.2013...
app-install-data-partner	12.12.4.1	Michael...	22.01.2013...
appmenu-gtk		Ubuntu...	02.04.2013...
appmenu-gtk3		Ubuntu...	02.04.2013...
appmenu-qt		Kubuntu...	22.01.2013...
apport		Martin Pitt...	22.01.2013...
apport-gtk		Martin Pitt...	22.01.2013...
apport-symptoms	0.16.1	Ubuntu...	22.01.2013...
apt		Ubuntu...	22.01.2013...
aptdaemon		Ubuntu...	22.01.2013...

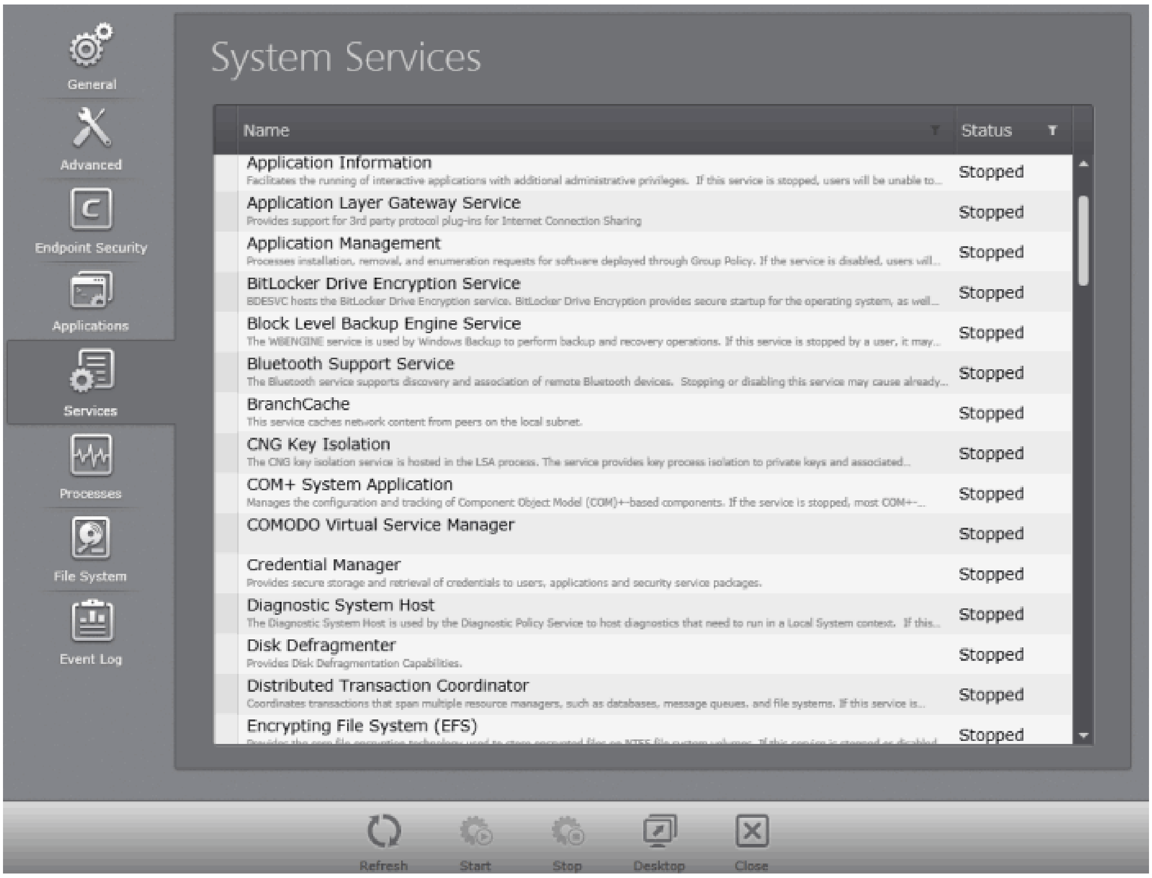
- To uninstall an application, select it and click 'Uninstall'. The application will be uninstalled form the endpoint.
- Click 'Refresh' to renew the currently viewed screen.
- To start the a currently running process remotely, select it and click 'Desktop'.
- To close the currently open detailed summary of information about the selected endpoint click 'Close'.

Note: You can uninstall only MSI based applications from this interface.

3.1.5. Viewing and Managing Currently Running Services

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

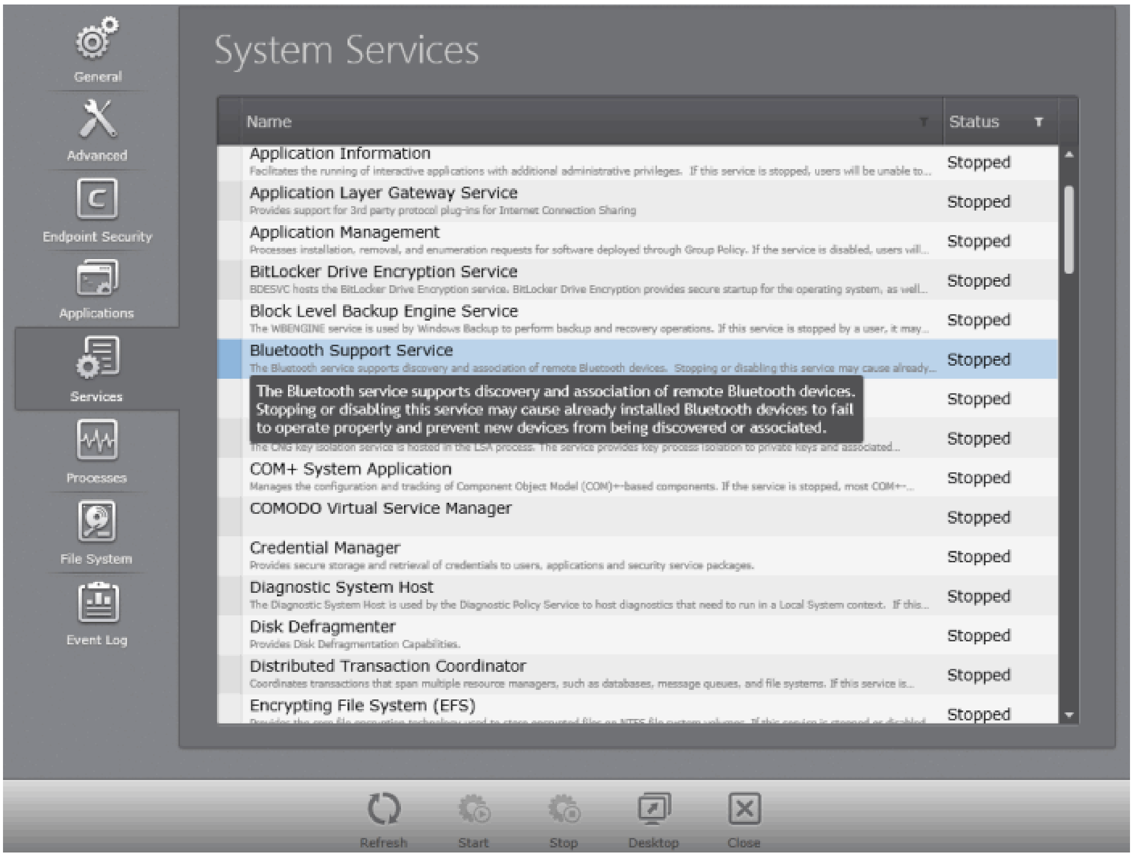
- To open the 'System Services' pane, click the 'Services' tab or 'Daemons' tab from the left hand side navigation of the Computer Properties screen.



System Services

Name	Status
Application Information Facilitates the running of interactive applications with additional administrative privileges. If this service is stopped, users will be unable to...	Stopped
Application Layer Gateway Service Provides support for 3rd party protocol plug-ins for Internet Connection Sharing	Stopped
Application Management Processes installation, removal, and enumeration requests for software deployed through Group Policy. If the service is disabled, users will...	Stopped
BitLocker Drive Encryption Service BDESVC hosts the BitLocker Drive Encryption service. BitLocker Drive Encryption provides secure startup for the operating system, as well...	Stopped
Block Level Backup Engine Service The WBENGINE service is used by Windows Backup to perform backup and recovery operations. If this service is stopped by a user, it may...	Stopped
Bluetooth Support Service The Bluetooth service supports discovery and association of remote Bluetooth devices. Stopping or disabling this service may cause already...	Stopped
BranchCache This service caches network content from peers on the local subnet.	Stopped
CNG Key Isolation The CNG key isolation service is hosted in the LSA process. The service provides key process isolation to private keys and associated...	Stopped
COM+ System Application Manages the configuration and tracking of Component Object Model (COM)+-based components. If the service is stopped, most COM+-...	Stopped
COMODO Virtual Service Manager	Stopped
Credential Manager Provides secure storage and retrieval of credentials to users, applications and security service packages.	Stopped
Diagnostic System Host The Diagnostic System Host is used by the Diagnostic Policy Service to host diagnostics that need to run in a Local System context. If this...	Stopped
Disk Defragmenter Provides Disk Defragmentation Capabilities.	Stopped
Distributed Transaction Coordinator Coordinates transactions that span multiple resource managers, such as databases, message queues, and file systems. If this service is...	Stopped
Encrypting File System (EFS)	Stopped

To view a short description of a service, hover the mouse cursor over the service.



System Services

Name	Status
Application Information Facilitates the running of interactive applications with additional administrative privileges. If this service is stopped, users will be unable to...	Stopped
Application Layer Gateway Service Provides support for 3rd party protocol plug-ins for Internet Connection Sharing	Stopped
Application Management Processes installation, removal, and enumeration requests for software deployed through Group Policy. If the service is disabled, users will...	Stopped
BitLocker Drive Encryption Service BDESVC hosts the BitLocker Drive Encryption service. BitLocker Drive Encryption provides secure startup for the operating system, as well...	Stopped
Block Level Backup Engine Service The WBENGINE service is used by Windows Backup to perform backup and recovery operations. If this service is stopped by a user, it may...	Stopped
Bluetooth Support Service The Bluetooth service supports discovery and association of remote Bluetooth devices. Stopping or disabling this service may cause already...	Stopped
	Stopped
The CNG key isolation service is hosted in the LSA process. The service provides key process isolation to private keys and associated...	Stopped
COM+ System Application Manages the configuration and tracking of Component Object Model (COM)+-based components. If the service is stopped, most COM+-...	Stopped
COMODO Virtual Service Manager	Stopped
Credential Manager Provides secure storage and retrieval of credentials to users, applications and security service packages.	Stopped
Diagnostic System Host The Diagnostic System Host is used by the Diagnostic Policy Service to host diagnostics that need to run in a Local System context. If this...	Stopped
Disk Defragmenter Provides Disk Defragmentation Capabilities.	Stopped
Distributed Transaction Coordinator Coordinates transactions that span multiple resource managers, such as databases, message queues, and file systems. If this service is...	Stopped
Encrypting File System (EFS)	Stopped

The Bluetooth service supports discovery and association of remote Bluetooth devices. Stopping or disabling this service may cause already installed Bluetooth devices to fail to operate properly and prevent new devices from being discovered or associated.

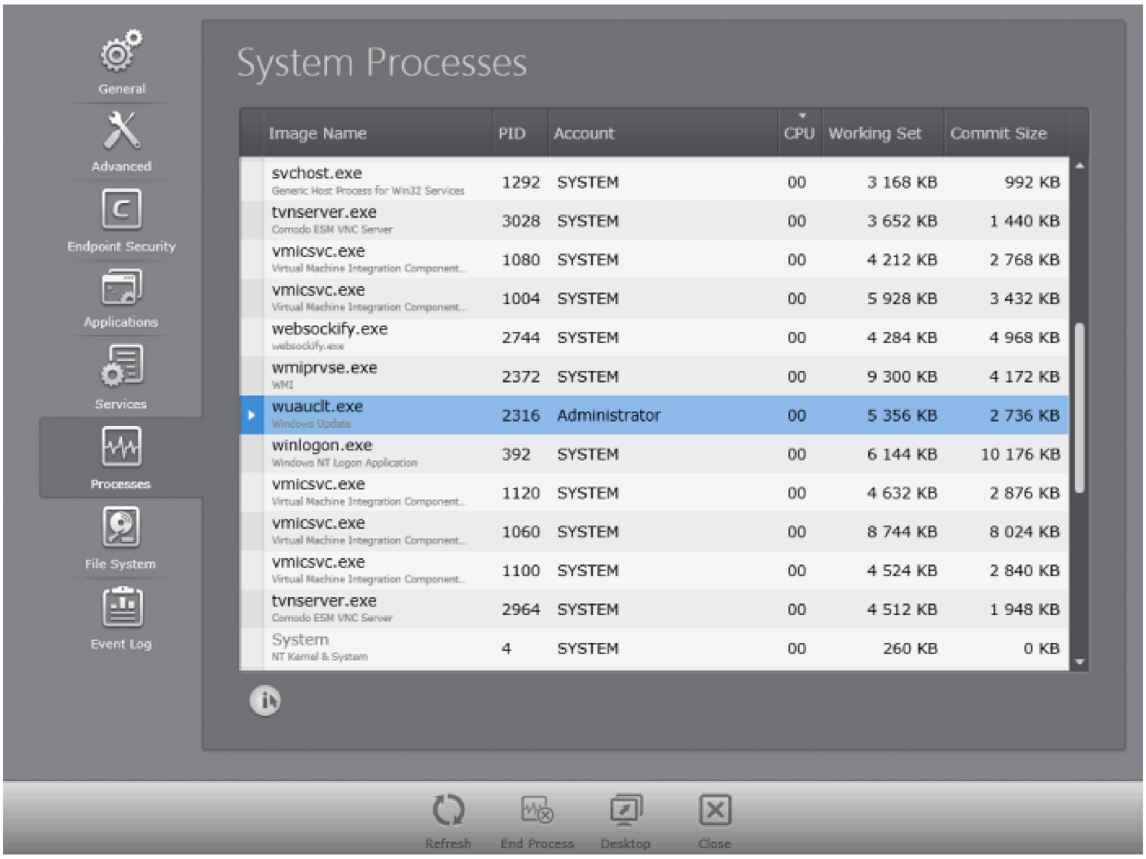
- Click 'Refresh' to renew the currently viewed screen.
- To stop a running service, select it and click 'Stop'.

- To start a stopped service, select it and click 'Start'.
- To start the a currently running process remotely, select it and click 'Desktop'.
- To close the currently open detailed summary of information about the selected endpoint click 'Close'.

3.1.6. Viewing and Managing Currently Running Processes

The 'System Processes' pane displays the list of Processes that are currently running in 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.



System Processes

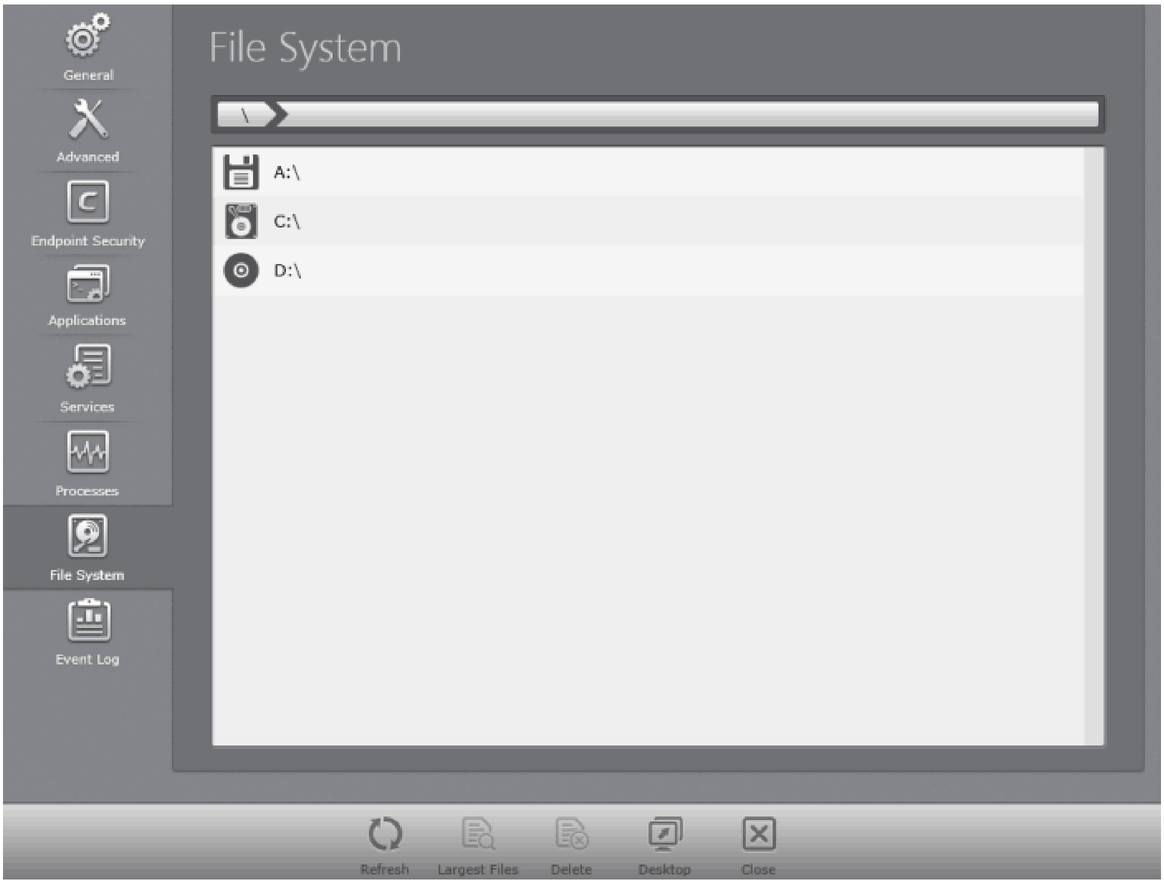
Image Name	PID	Account	CPU	Working Set	Commit Size
svchost.exe Generic Host Process for Win32 Services	1292	SYSTEM	00	3 168 KB	992 KB
tvnserver.exe Comodo ESM VNC Server	3028	SYSTEM	00	3 652 KB	1 440 KB
vmicsvc.exe Virtual Machine Integration Component...	1080	SYSTEM	00	4 212 KB	2 768 KB
vmicsvc.exe Virtual Machine Integration Component...	1004	SYSTEM	00	5 928 KB	3 432 KB
websockify.exe websockify.exe	2744	SYSTEM	00	4 284 KB	4 968 KB
wmiprvse.exe WMI	2372	SYSTEM	00	9 300 KB	4 172 KB
wuauclt.exe Windows Update	2316	Administrator	00	5 356 KB	2 736 KB
winlogon.exe Windows NT Logon Application	392	SYSTEM	00	6 144 KB	10 176 KB
vmicsvc.exe Virtual Machine Integration Component...	1120	SYSTEM	00	4 632 KB	2 876 KB
vmicsvc.exe Virtual Machine Integration Component...	1060	SYSTEM	00	8 744 KB	8 024 KB
vmicsvc.exe Virtual Machine Integration Component...	1100	SYSTEM	00	4 524 KB	2 840 KB
tvnserver.exe Comodo ESM VNC Server	2964	SYSTEM	00	4 512 KB	1 948 KB
System NT Kernel & System	4	SYSTEM	00	260 KB	0 KB

- To stop a currently running process, select it and click 'End Process'.
- To start the a currently running process remotely, select it and click 'Desktop'.
- Click 'Refresh' to renew the currently viewed screen.
- To close the currently open detailed summary of information about the selected endpoint, click 'Close'.

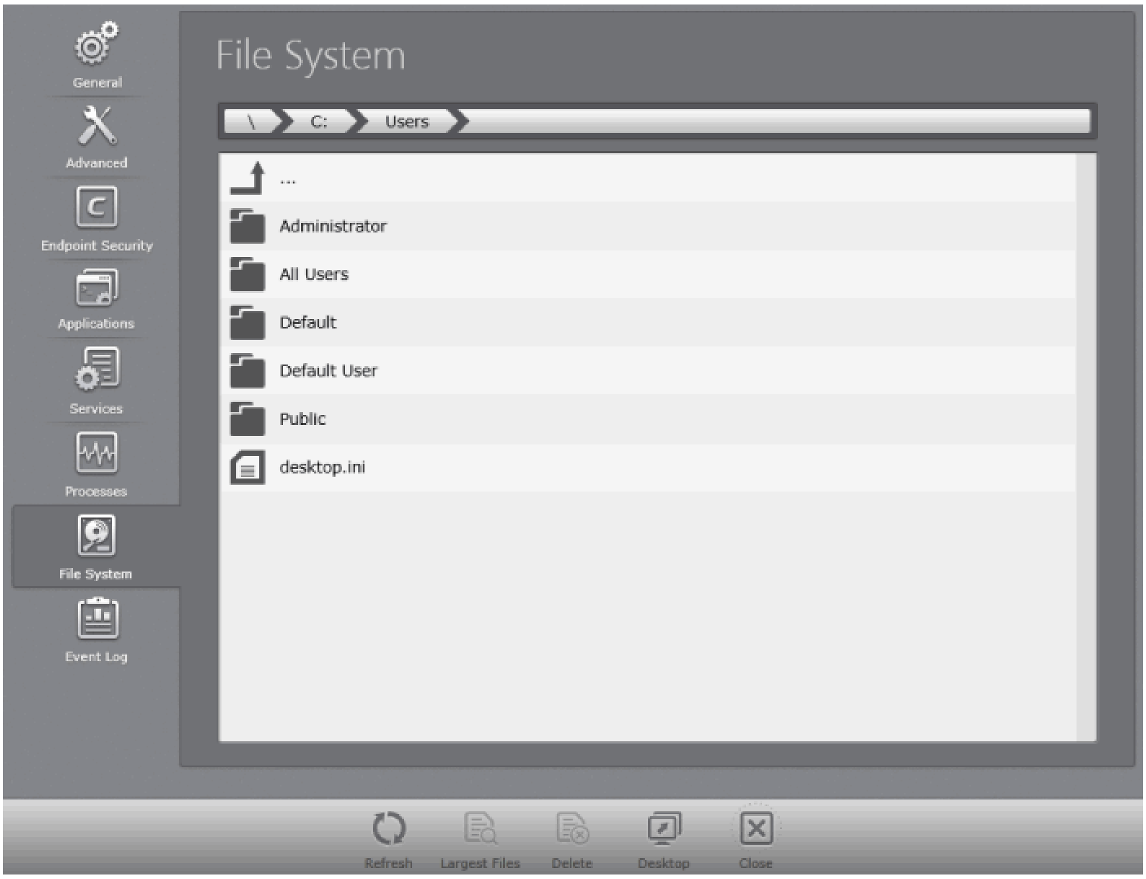
3.1.7. Viewing and Managing Drives and Storage

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 'Get Largest Files' feature allows admins to identify the top 10 largest files in a drive and to delete them if required.

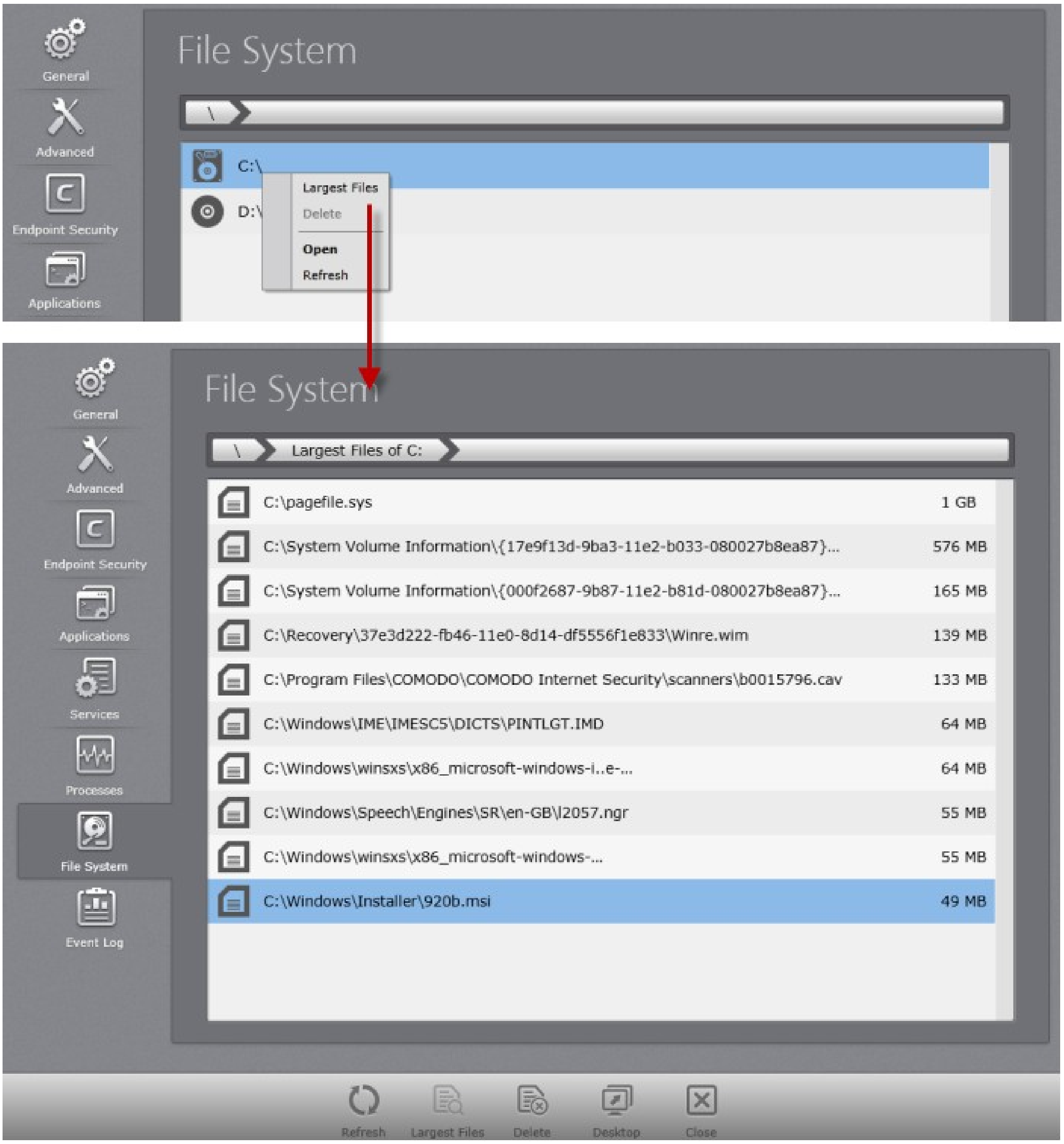
- To open the 'File System' pane, click the 'File System' tab from the left hand side navigation of the Computer Properties screen.



- 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' or right click on a drive and choose 'Largest Files' from the context sensitive menu.



C:\pagefile.sys	1 GB
C:\System Volume Information\{17e9f13d-9ba3-11e2-b033-080027b8ea87}...	576 MB
C:\System Volume Information\{000f2687-9b87-11e2-b81d-080027b8ea87}...	165 MB
C:\Recovery\37e3d222-fb46-11e0-8d14-df5556f1e833\Winre.wim	139 MB
C:\Program Files\COMODO\COMODO Internet Security\scanners\b0015796.cav	133 MB
C:\Windows\IME\IMESC5\DICTS\PINTLGT.IMD	64 MB
C:\Windows\winsxs\x86_microsoft-windows-i..e-...	64 MB
C:\Windows\Speech\Engines\SR\en-GB\l2057.ngr	55 MB
C:\Windows\winsxs\x86_microsoft-windows-...	55 MB
C:\Windows\Installer\920b.msi	49 MB

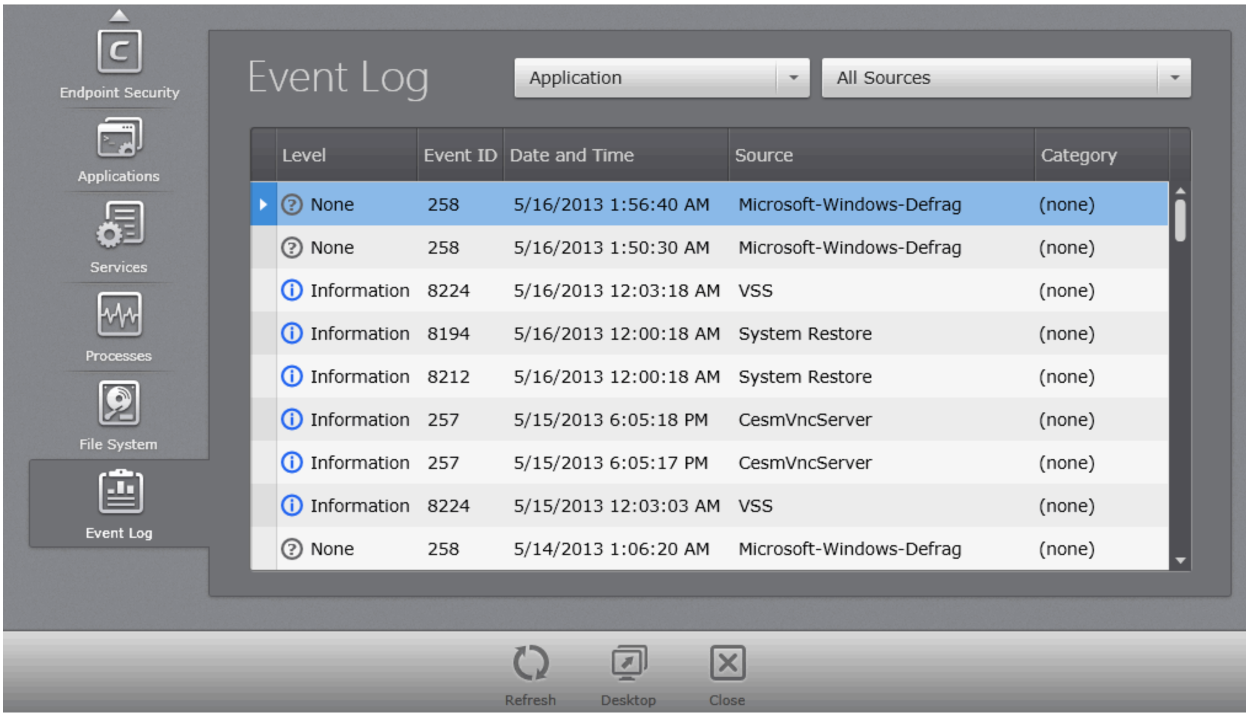
The administrator can delete unwanted files from the large files list, to conserve disk space and improve system performance.

To open a remote session above the current file system, select it and click 'Desktop'.

3.1.8. Viewing Event Log

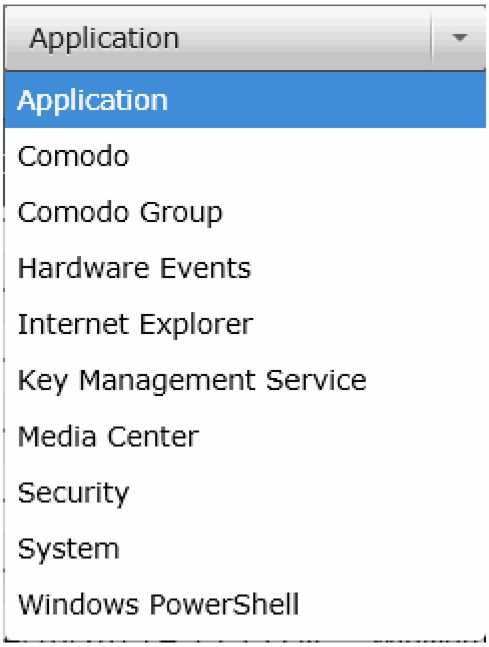
The 'Event Log' pane allows administrators to browse endpoint events, such as a failure to start a component or complete an action at the selected endpoint.

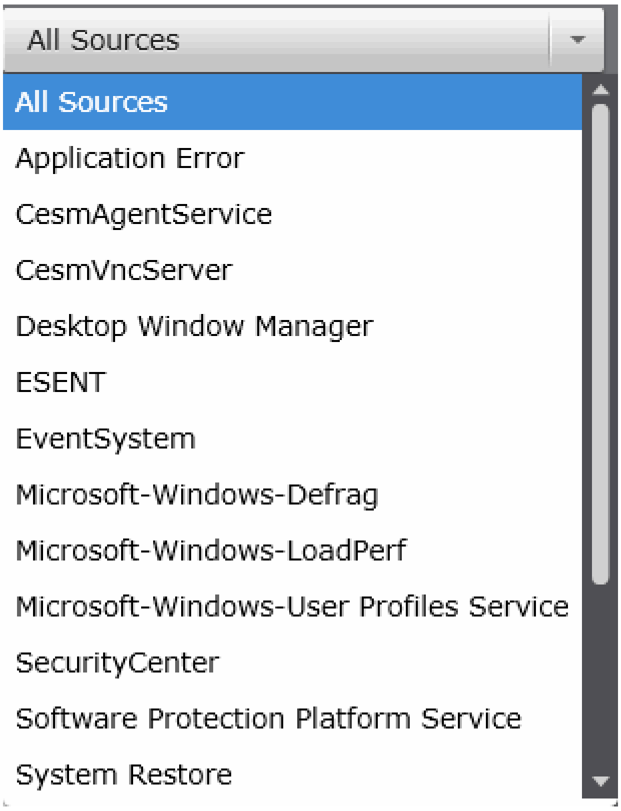
To open the 'Event Log' pane, click the 'Event Log' tab from the left hand side navigation of the 'Computer Properties' screen.



Level	Event ID	Date and Time	Source	Category
None	258	5/16/2013 1:56:40 AM	Microsoft-Windows-Defrag	(none)
None	258	5/16/2013 1:50:30 AM	Microsoft-Windows-Defrag	(none)
Information	8224	5/16/2013 12:03:18 AM	VSS	(none)
Information	8194	5/16/2013 12:00:18 AM	System Restore	(none)
Information	8212	5/16/2013 12:00:18 AM	System Restore	(none)
Information	257	5/15/2013 6:05:18 PM	CesmVncServer	(none)
Information	257	5/15/2013 6:05:17 PM	CesmVncServer	(none)
Information	8224	5/15/2013 12:03:03 AM	VSS	(none)
None	258	5/14/2013 1:06:20 AM	Microsoft-Windows-Defrag	(none)

- You can filter the results based on the kinds 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.





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 and 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.

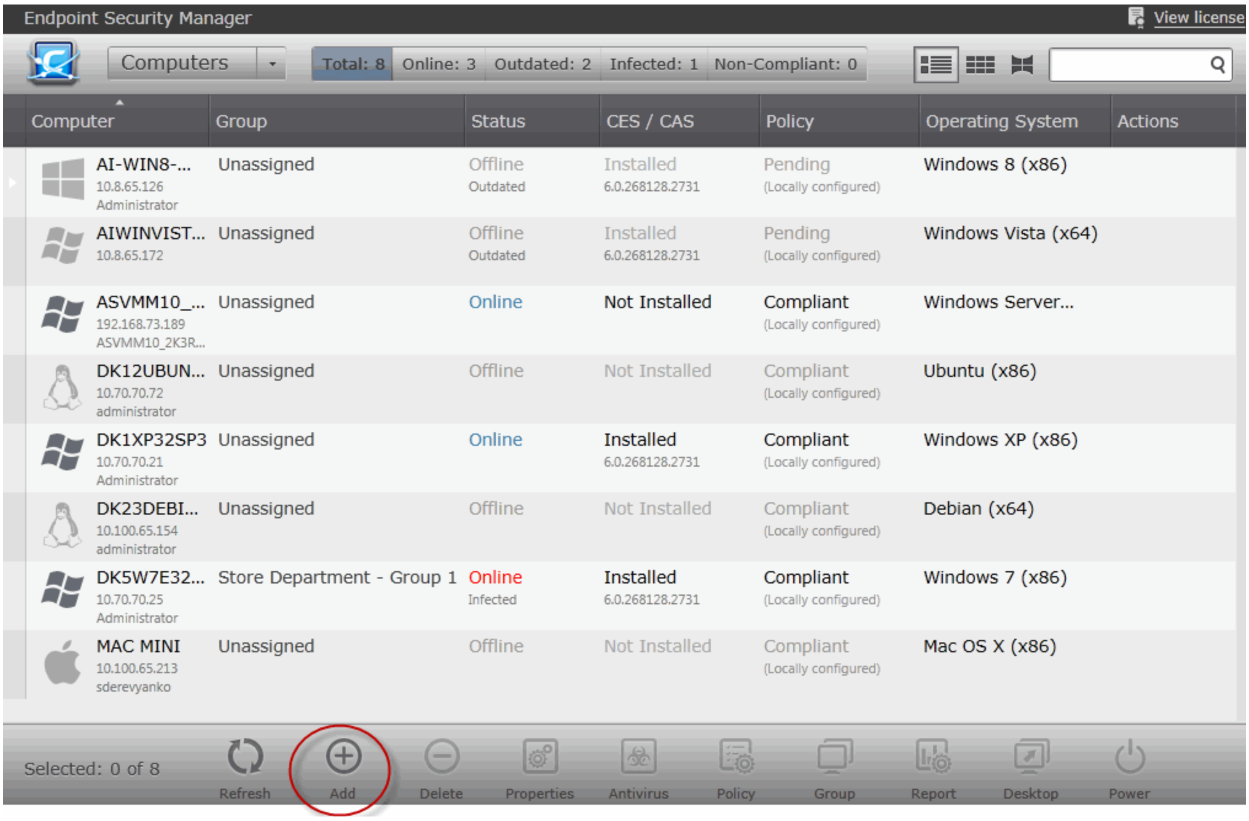
The 'Computers' area also allows the administrators to arrange the added computers into 'Groups' as per the structure of the organization for easy administration. Once created administrators can run tasks on entire groups of computers (such as applying security policy for CES, running AV scans, deploying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

3.2.1. Importing Computers by Automatic Installation of Agent

The 'Add Computer' wizard will install the CESM agent software and CES software on 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. The wizard also allows to 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:



Computer	Group	Status	CES / CAS	Policy	Operating System	Actions
AI-WIN8-... 10.8.65.126 Administrator	Unassigned	Offline Outdated	Installed 6.0.268128.2731	Pending (Locally configured)	Windows 8 (x86)	
AIWINVIST... 10.8.65.172	Unassigned	Offline Outdated	Installed 6.0.268128.2731	Pending (Locally configured)	Windows Vista (x64)	
ASVMM10_... 192.168.73.189 ASVMM10_2K3R...	Unassigned	Online	Not Installed	Compliant (Locally configured)	Windows Server...	
DK12UBUN... 10.70.70.72 administrator	Unassigned	Offline	Not Installed	Compliant (Locally configured)	Ubuntu (x86)	
DK1XP32SP3 10.70.70.21 Administrator	Unassigned	Online	Installed 6.0.268128.2731	Compliant (Locally configured)	Windows XP (x86)	
DK23DEBI... 10.100.65.154 administrator	Unassigned	Offline	Not Installed	Compliant (Locally configured)	Debian (x64)	
DK5W7E32... 10.70.70.25 Administrator	Store Department - Group 1	Online Infected	Installed 6.0.268128.2731	Compliant (Locally configured)	Windows 7 (x86)	
MAC MINI 10.100.65.213 sderevyanko	Unassigned	Offline	Not Installed	Compliant (Locally configured)	Mac OS X (x86)	

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 individual computers specified by their IP Addresses.

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

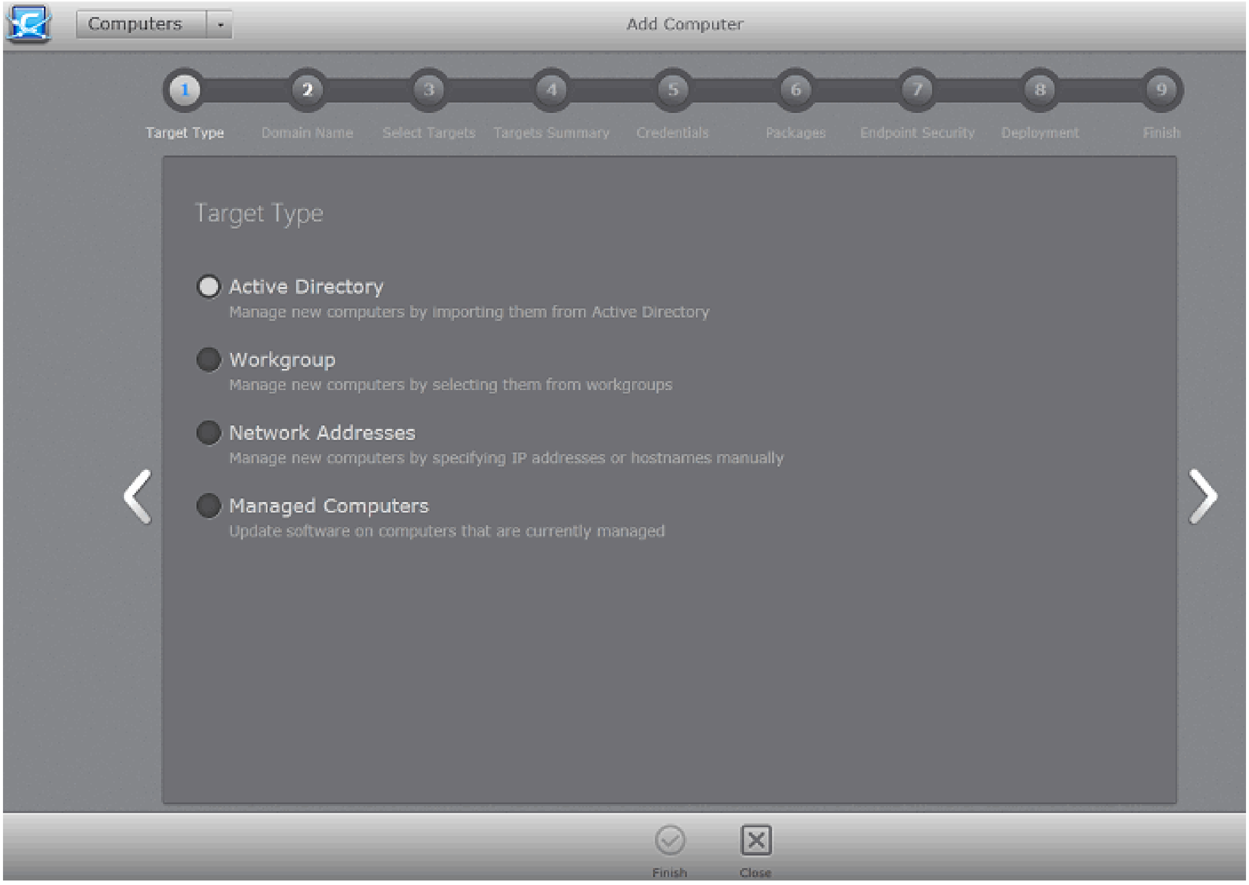
> **Note:** Targets are contacted by the CESM service computer and its network connection, not the computer running the management console.

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** and **Import Computers by IP Address**.

- Select the appropriate method to import the computers from Active Directory or Workgroup or select Network Addresses if you want to import computers by specifying their IP addresses or DNS names.



Target Type

○ Active Directory
Manage new computers by importing them from Active Directory

● Workgroup
Manage new computers by selecting them from workgroups

● Network Addresses
Manage new computers by specifying IP addresses or hostnames manually

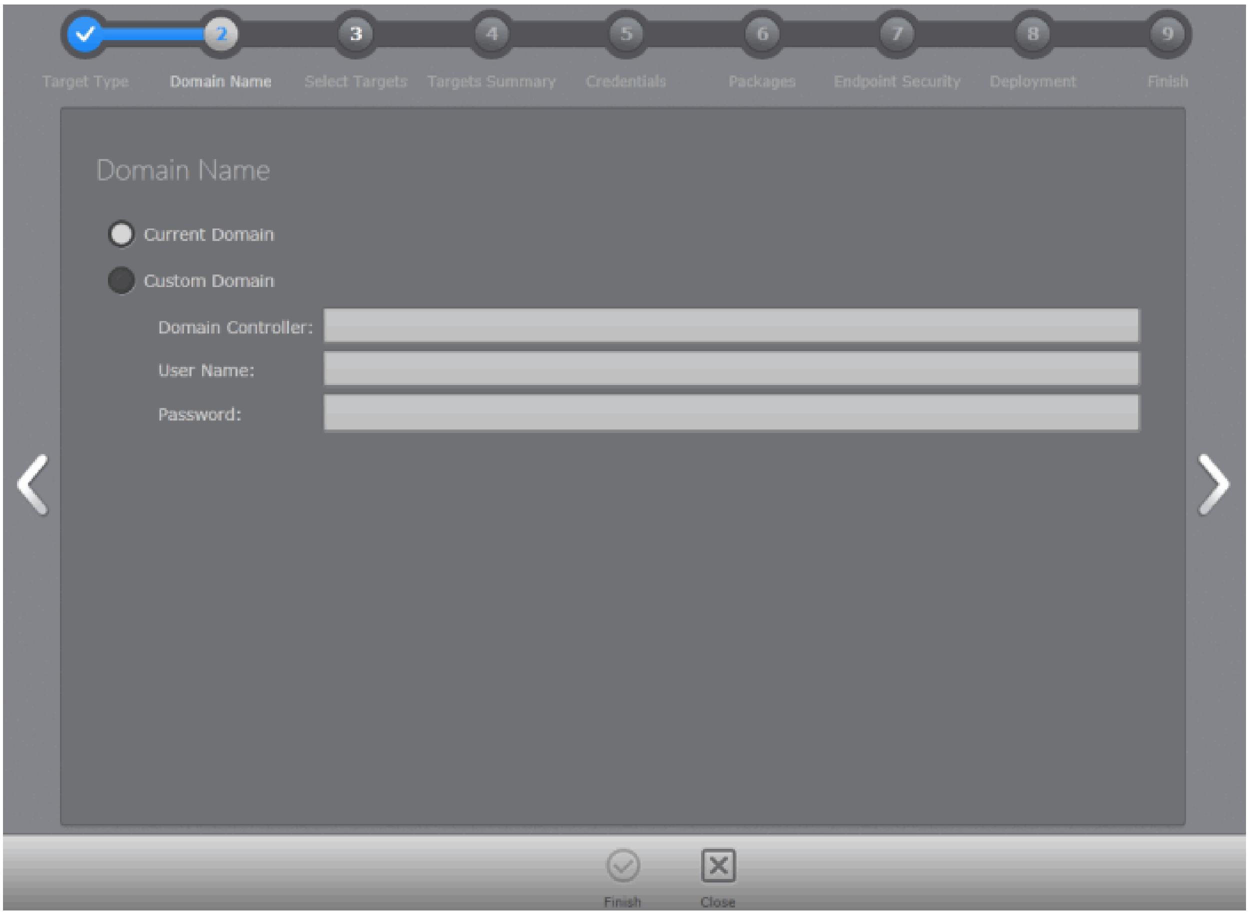
● Managed Computers
Update software on computers that are currently managed

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 Name

○ Current Domain

● Custom Domain

Domain Controller:

User Name:

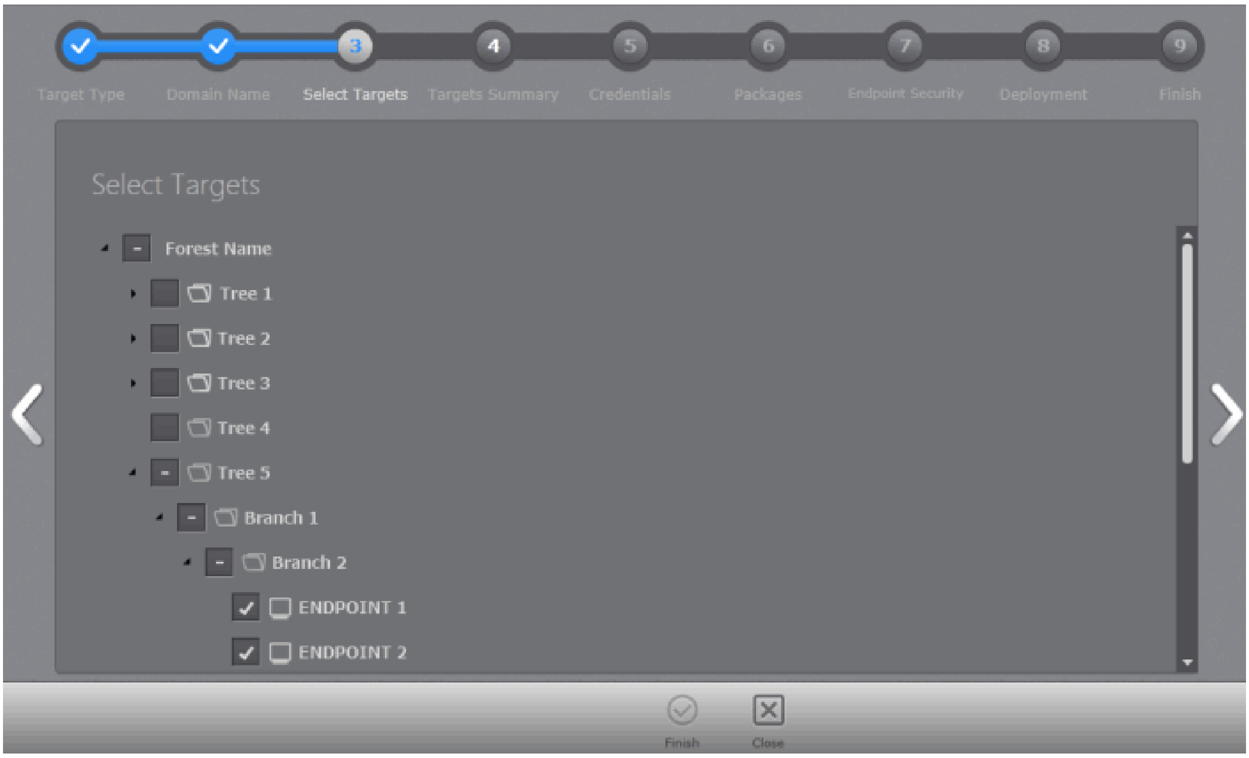
Password:

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.



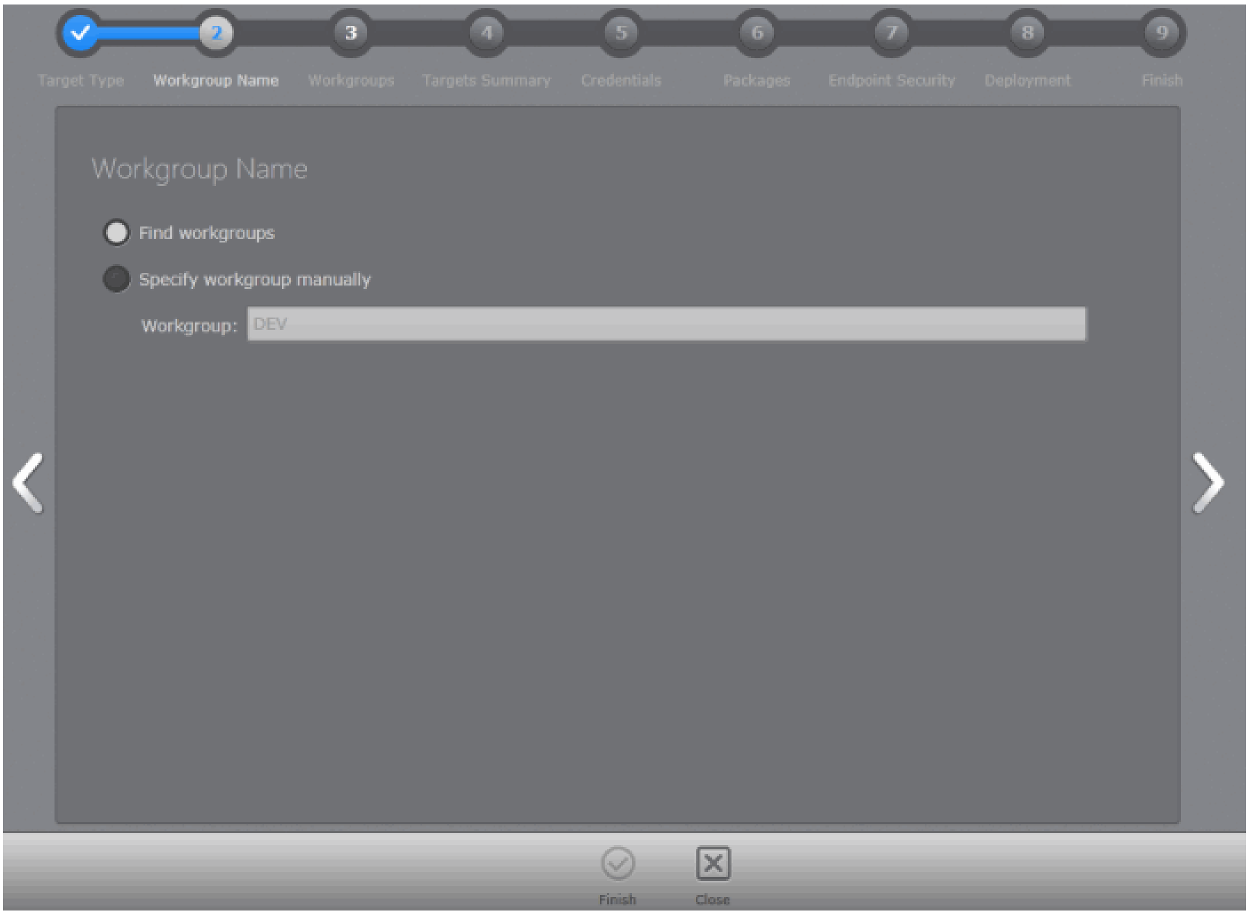
- Click the ‣ icon to expand or collapse the tree structure.
- Select the target endpoints onto which you wish to install the agent and import into CESM.
- Click the right arrow or swipe left to move to **step 3** to select the endpoints.

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.



Workgroup Name

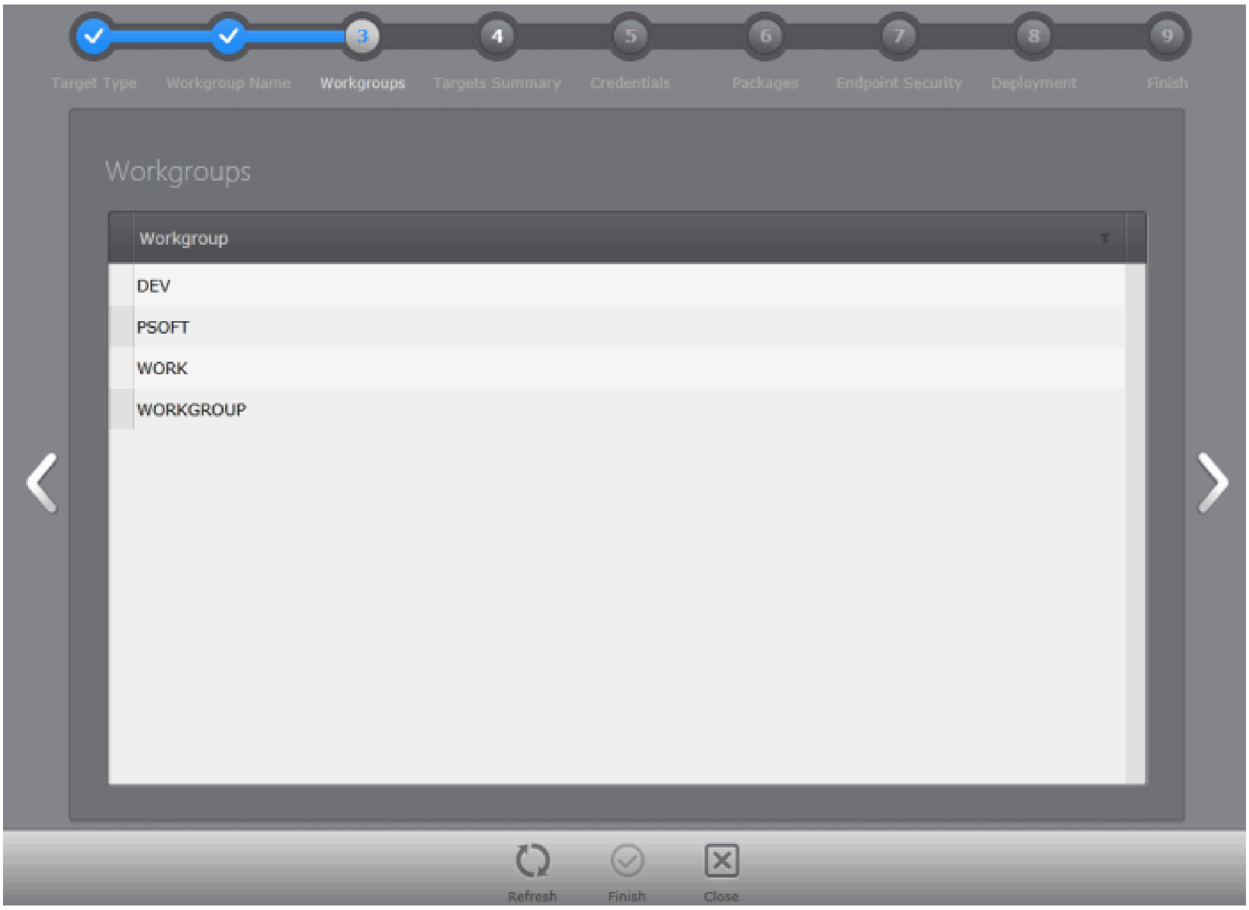
○ Find workgroups

● Specify workgroup manually

Workgroup: DEV

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.



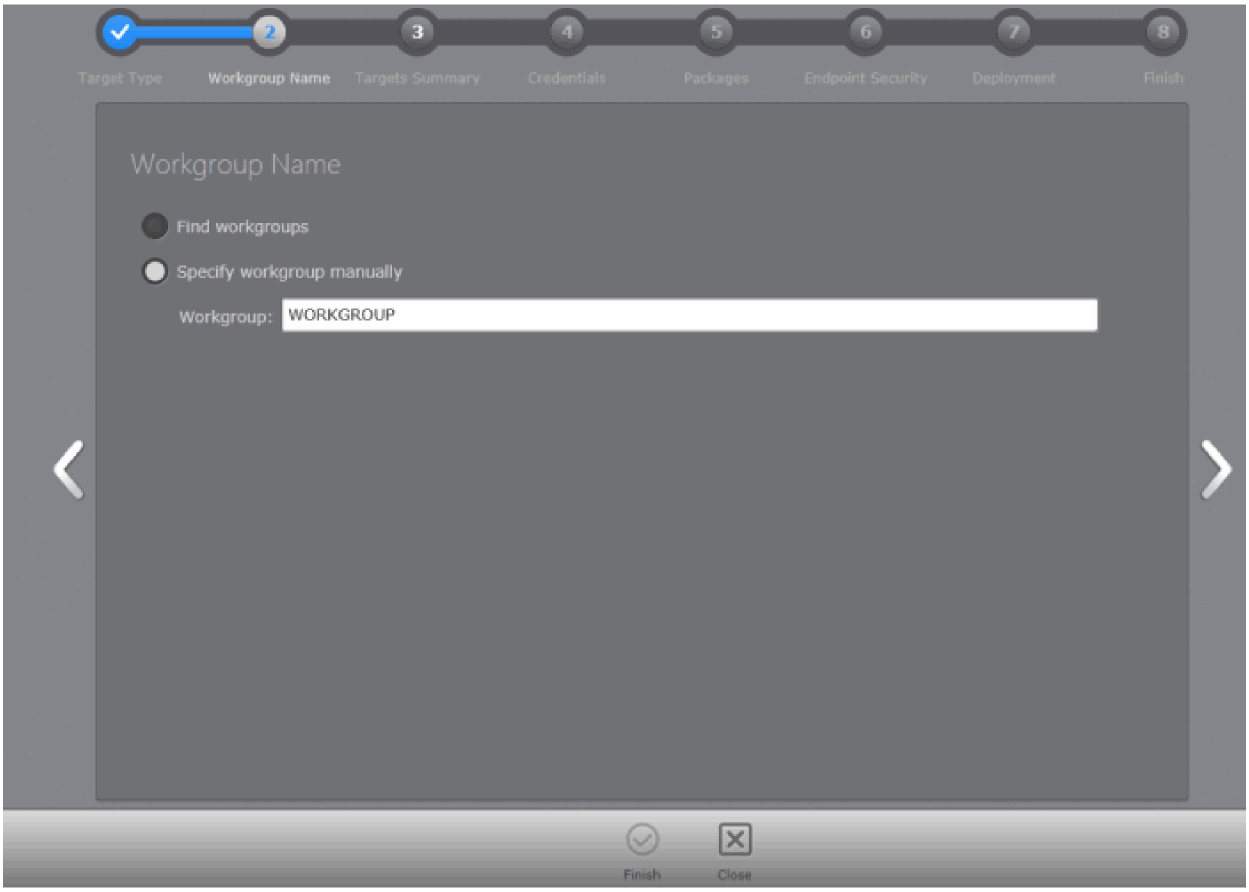
Workgroups

Workgroup
DEV
PSOFT
WORK
WORKGROUP

- 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.



Workgroup Name

○ Find workgroups

● Specify workgroup manually

Workgroup: WORKGROUP

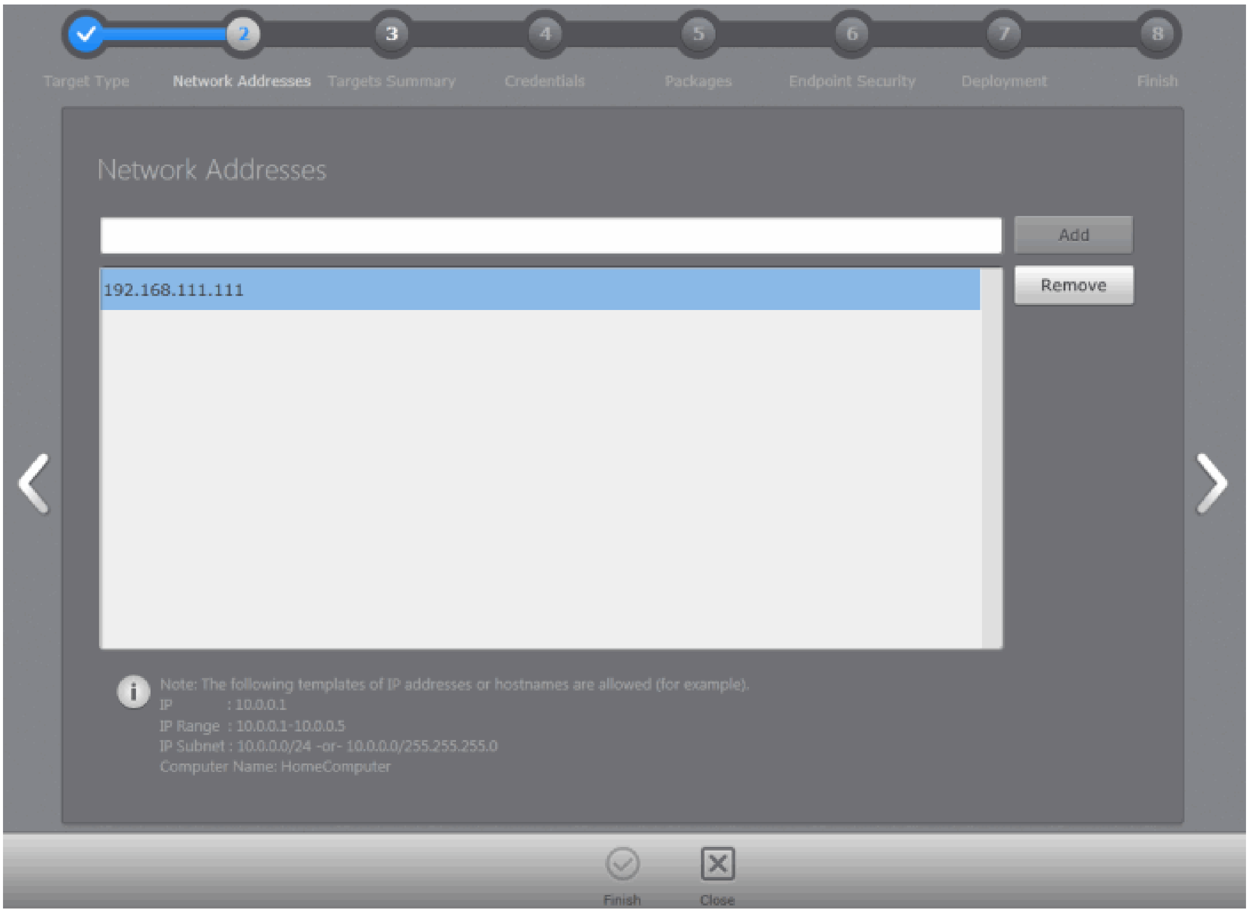
- Enter the name of a network Workgroup and click the right arrow to move to **step 3** to select the endpoints.

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).



Network Addresses

192.168.111.111

Note: The following templates of IP addresses or hostnames are allowed (for example).
IP : 10.0.0.1
IP Range : 10.0.0.1-10.0.0.5
IP Subnet : 10.0.0.0/24 -or- 10.0.0.0/255.255.255.0
Computer Name: HomeComputer

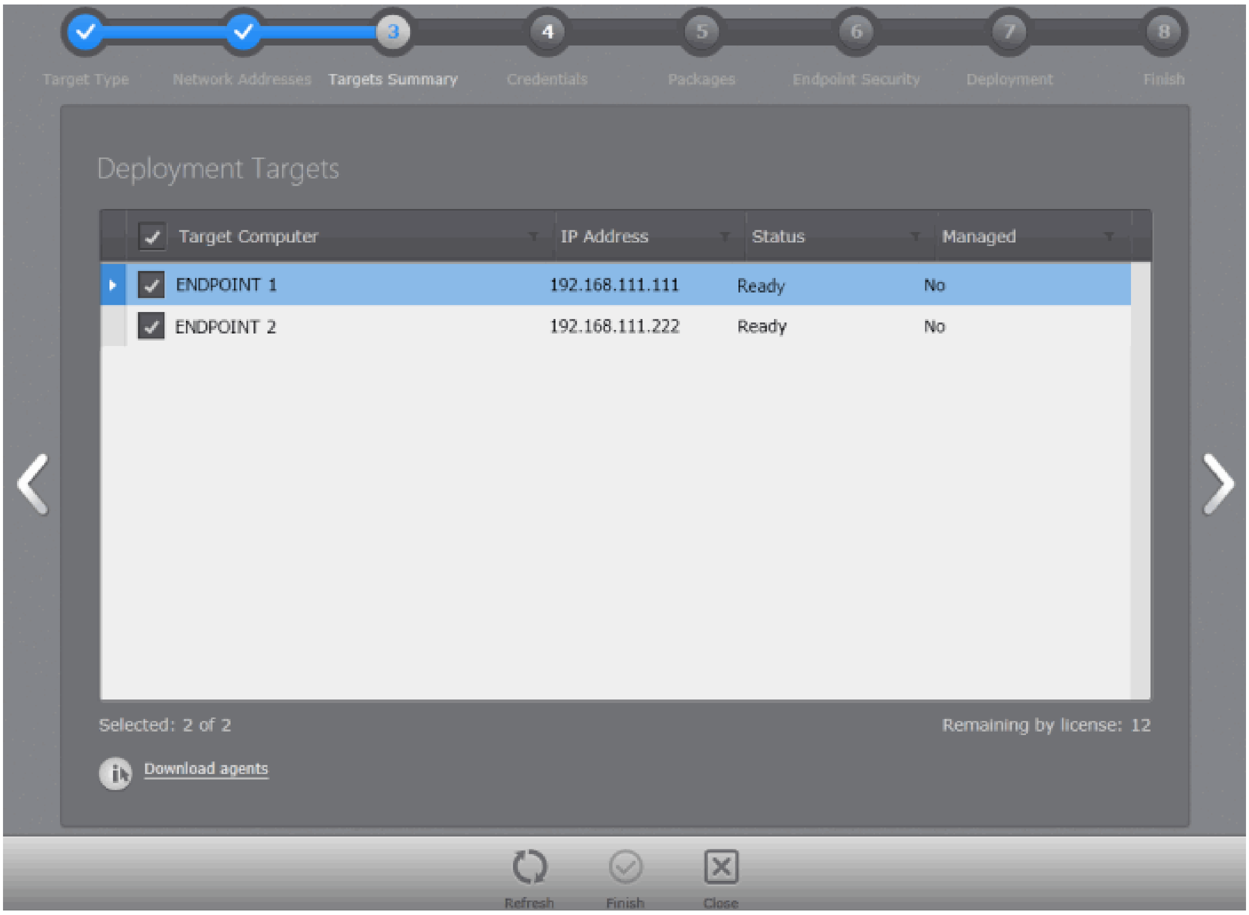
Computers can be added in four ways:

- **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.



Deployment Targets

☑ Target Computer	IP Address	Status	Managed
☑ ENDPOINT 1	192.168.111.111	Ready	No
☑ ENDPOINT 2	192.168.111.222	Ready	No

Selected: 2 of 2

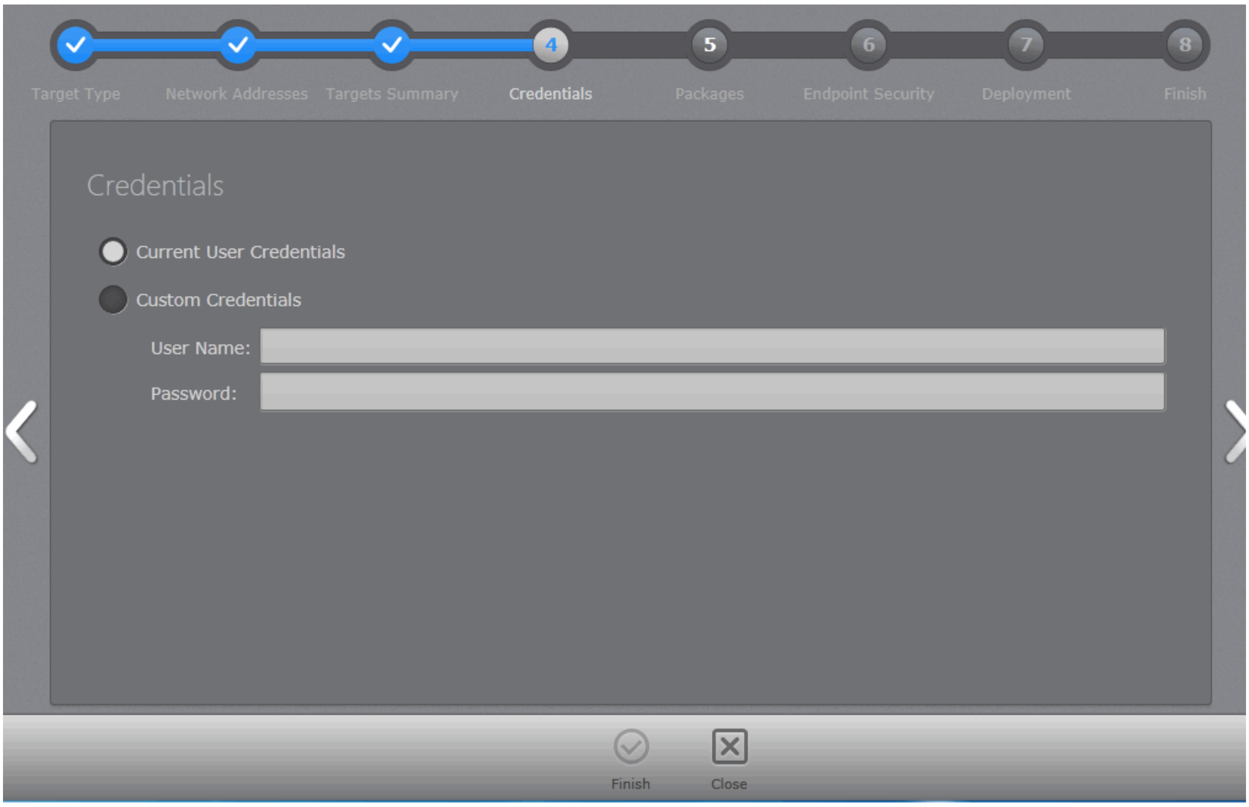
Remaining by license: 12

Download agents

- 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).

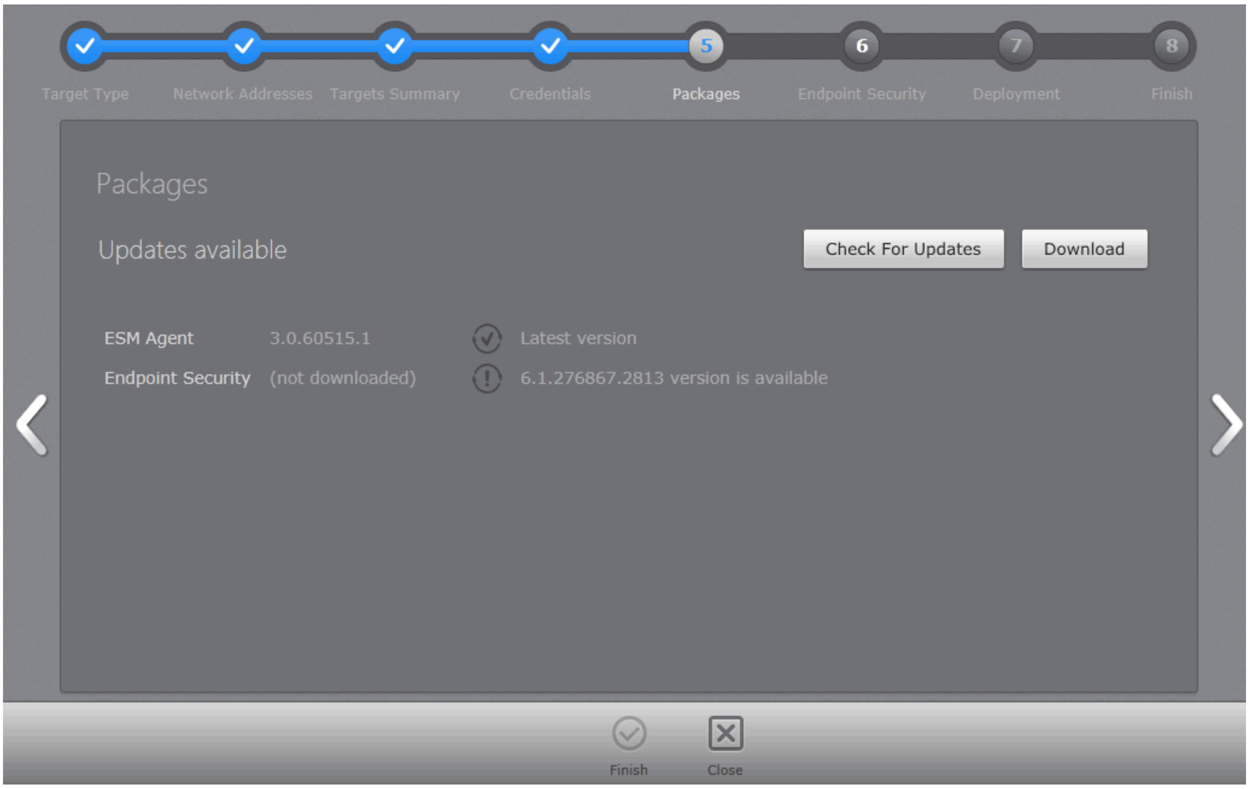


Credentials - Table of Parameters	
Current User Credentials (Selected by default)	Selecting this option will install the agent using the credentials of the currently logged -in CESM administrator account in each endpoint.
Custom Credentials	Selecting this option allows the administrator to specify an administrative account for installation of the agent. Choosing this option requires administrators to specify the following details:
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 - Checking for Updated Software

The next stage 'Packages' displays the version details of ESM Agent and CES. You can also check for updates of these applications and download it in your server for deployment on to the end-points.



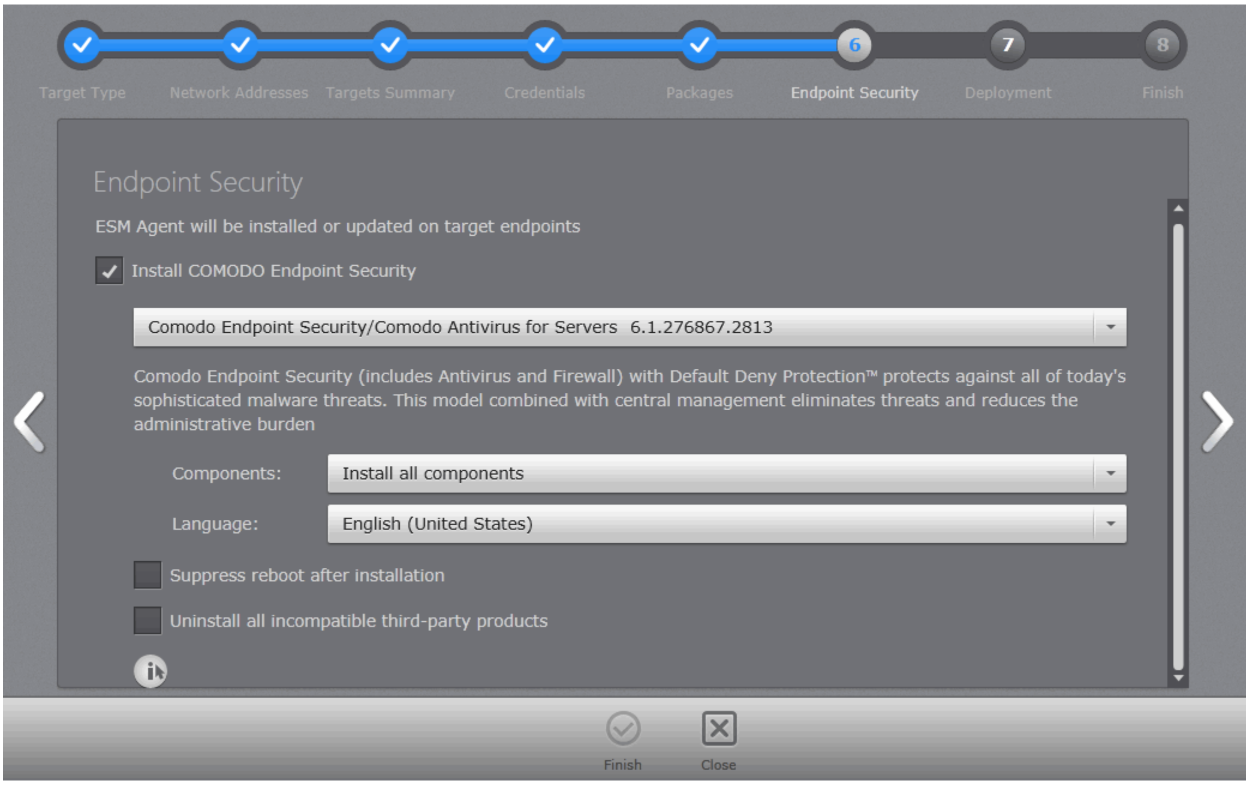
Packages

Updates available

ESM Agent	3.0.60515.1	Latest version
Endpoint Security	(not downloaded)	6.1.276867.2813 version is available

- Click 'Check for Updates' to find out if any newer version of ESM Agent and CES are available.
- If any newer versions are available, you can choose to download them to the CESM server by clicking 'Download'.
- Click the right arrow to move to the next step.

Step 6 – Endpoint Security



Endpoint Security

ESM Agent will be installed or updated on target endpoints

☑ Install COMODO Endpoint Security

Comodo Endpoint Security/Comodo Antivirus for Servers 6.1.276867.2813

Comodo Endpoint Security (includes Antivirus and Firewall) with Default Deny Protection™ protects against all of today's sophisticated malware threats. This model combined with central management eliminates threats and reduces the administrative burden

Components: Install all components

Language: English (United States)

□ Suppress reboot after installation

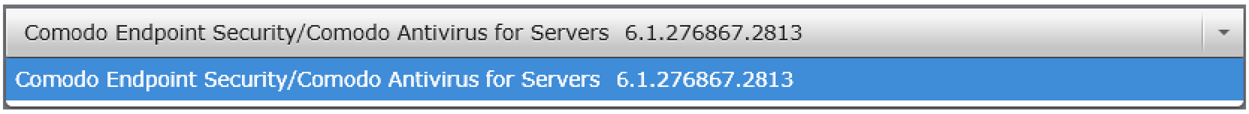
□ Uninstall all incompatible third-party products

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 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.



Comodo Endpoint Security/Comodo Antivirus for Servers 6.1.276867.2813

Comodo Endpoint Security/Comodo Antivirus for Servers 6.1.276867.2813

- Select whether you want to include all the components (Firewall and Antivirus), Antivirus only or Firewall only from the Components 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 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.

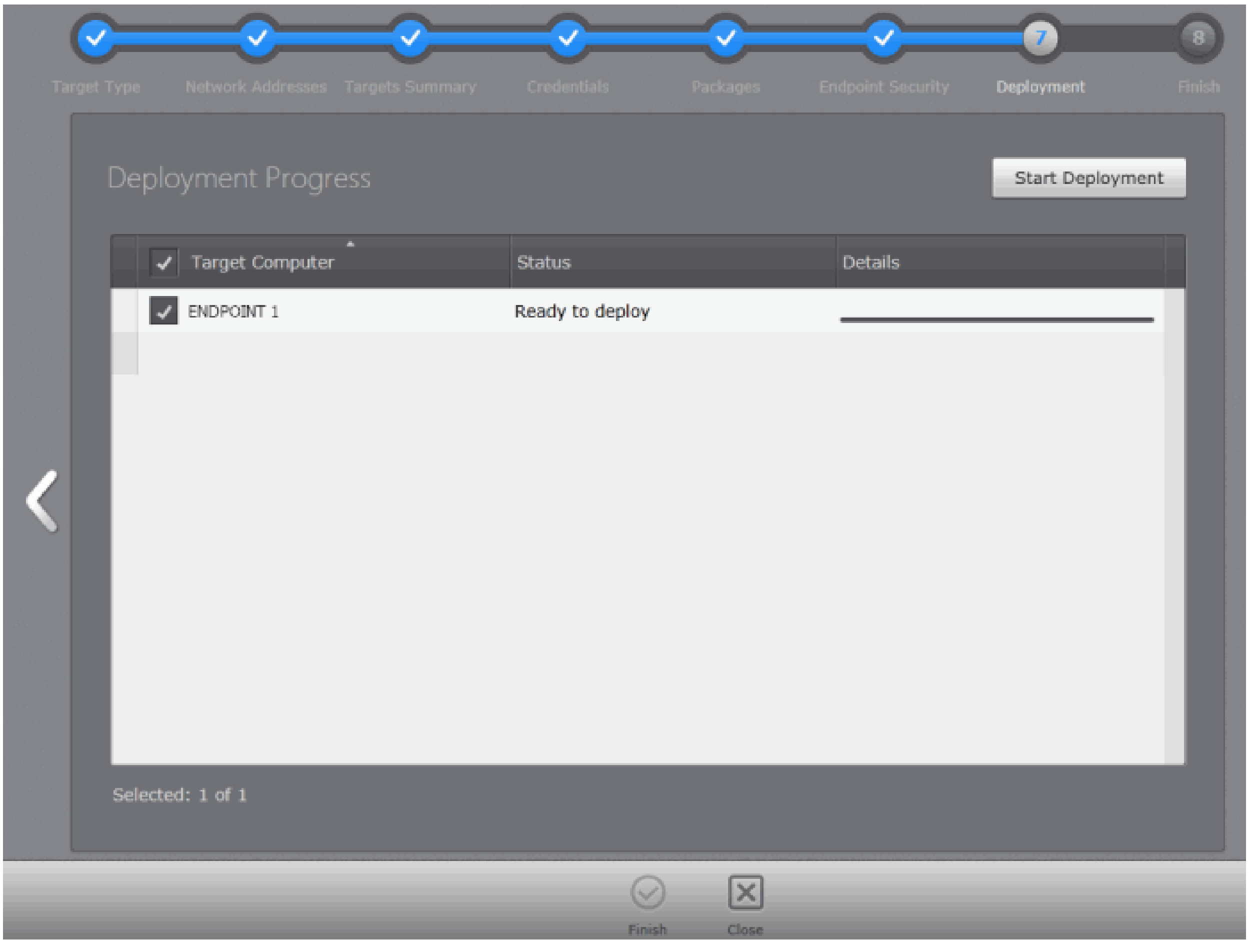
Tip:

You can also:

- Install CES manually onto endpoint computers. Refer to **How to Install CES**; and
- Import stand-alone CES application pre-installed at the endpoints under the management of CESM.

Step 7 - Deployment Progress

- Click 'Start Deployment'.

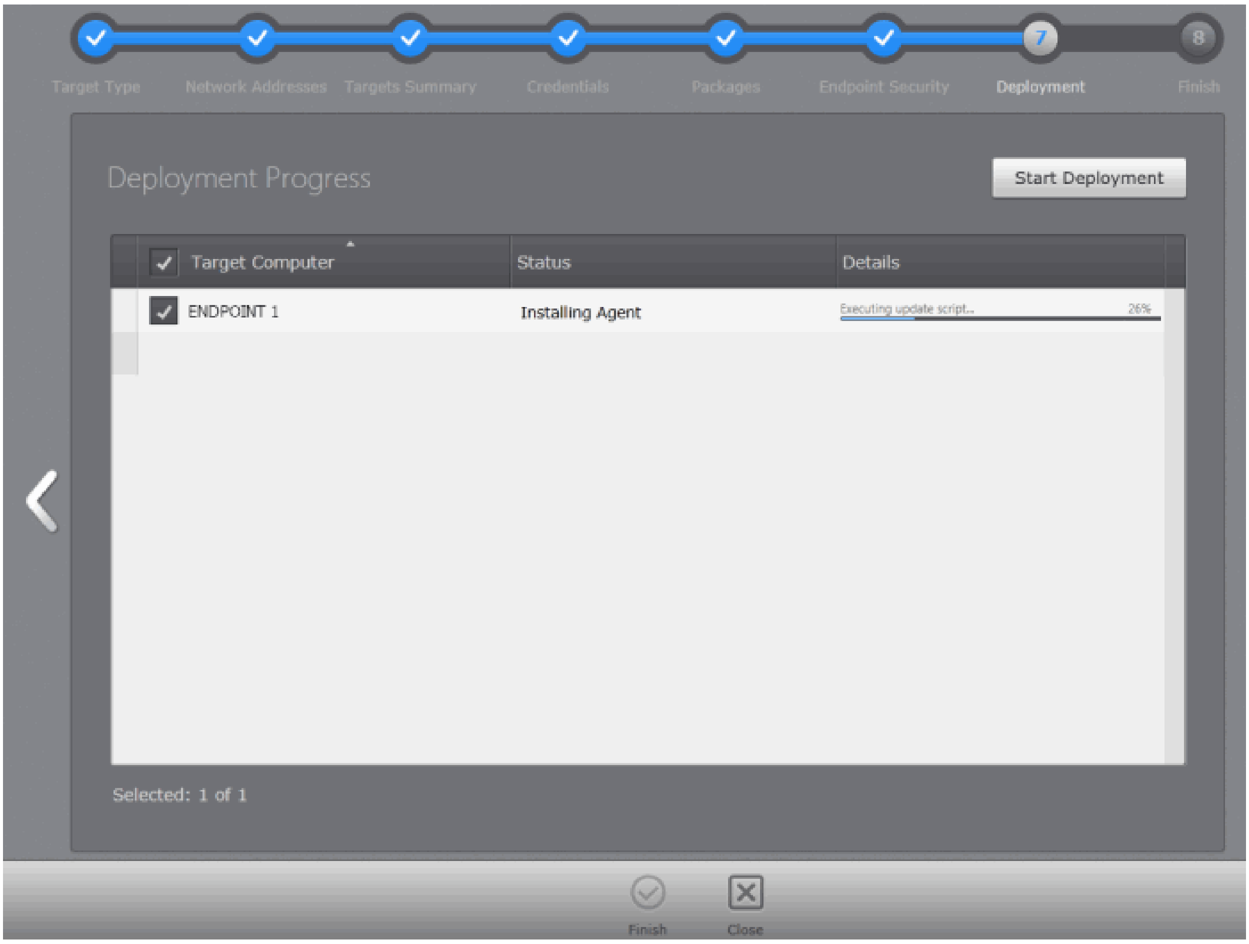


Deployment Progress

☑ Target Computer	Status	Details
☑ ENDPOINT 1	Ready to deploy	

Selected: 1 of 1

CESM will start installing the agent/CES on to the selected endpoints and the progress per endpoint will be displayed.



Deployment Progress

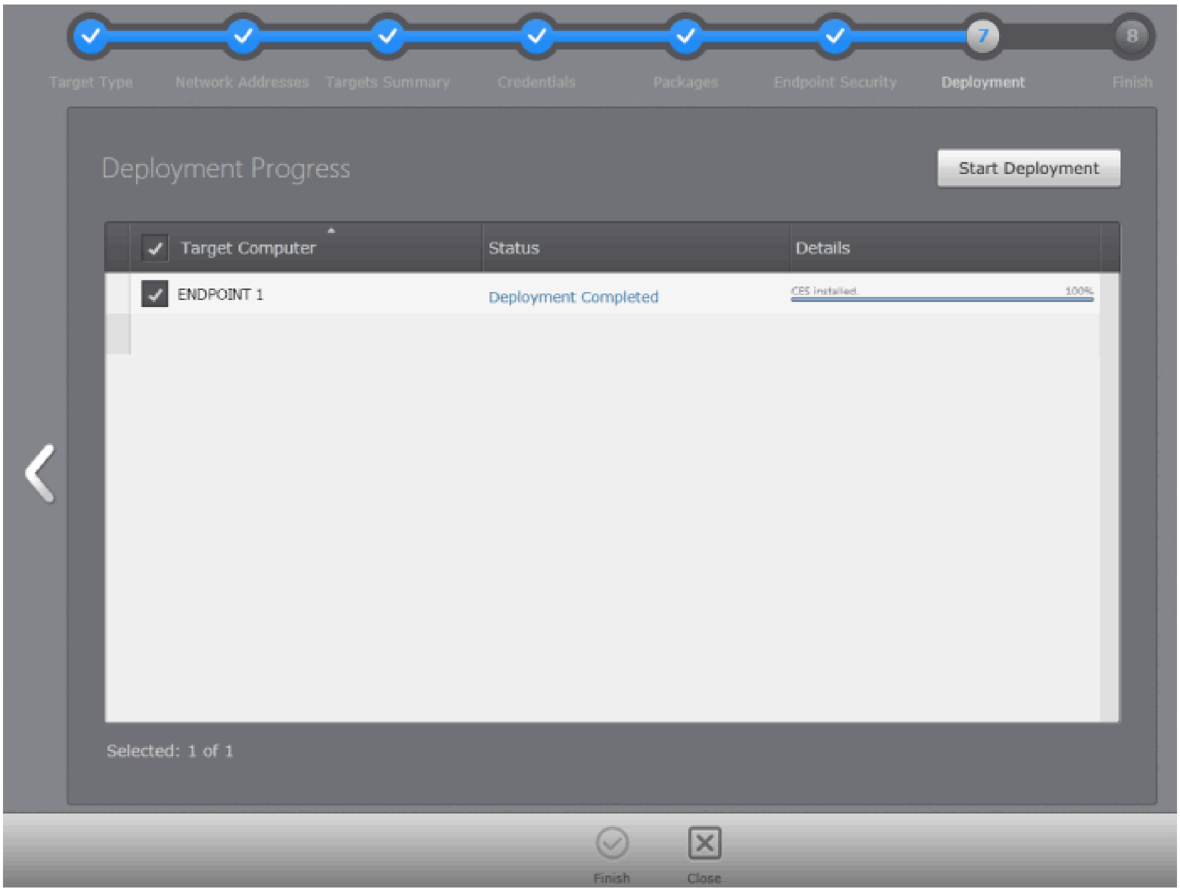
☑ Target Computer	Status	Details
☑ ENDPOINT 1	Installing Agent	Executing update script... 26%

Selected: 1 of 1

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 8 - Deployment Complete

On completion of installation, the results screen will appear.

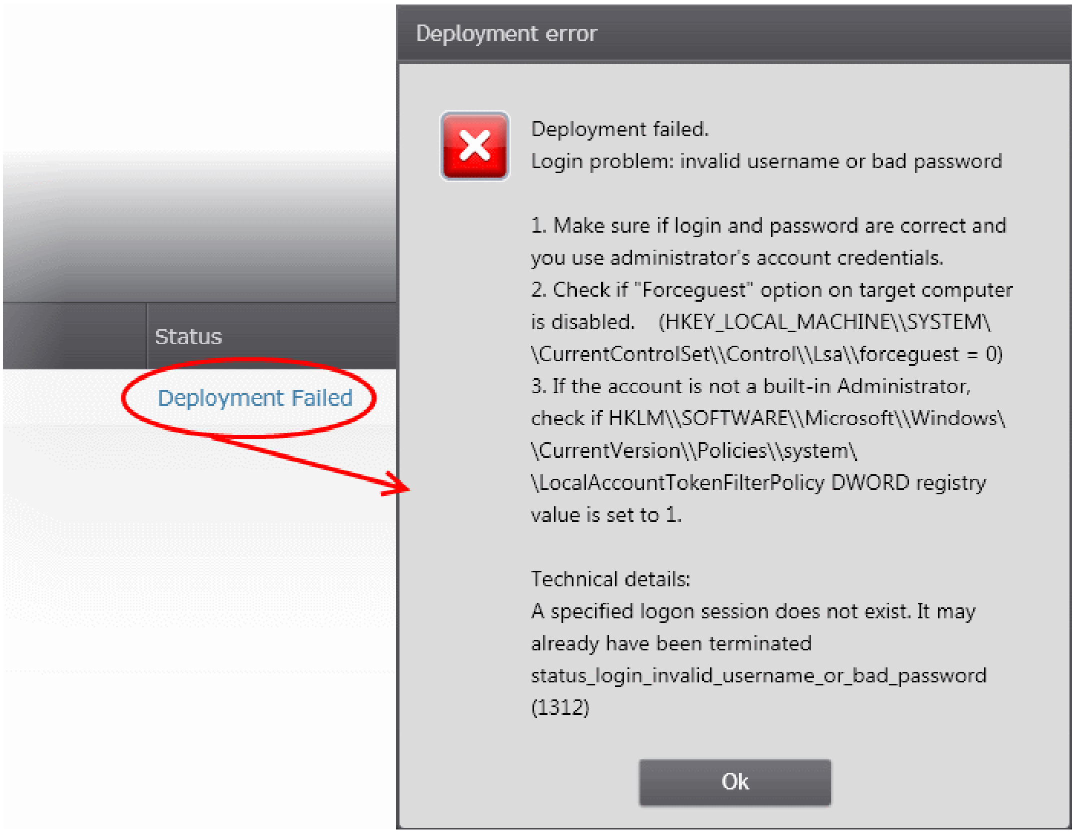


Deployment Progress

Target Computer	Status	Details
☑ ENDPOINT 1	Deployment Completed	CES installed. 100%

Selected: 1 of 1

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



Deployment error

Deployment failed.
Login problem: invalid username or bad password

1. Make sure if login and password are correct and you use administrator's account credentials.
2. Check if "Forceguest" option on target computer is disabled. (HKEY_LOCAL_MACHINE\\SYSTEM\\CurrentControlSet\\Control\\Lsa\\forceguest = 0)
3. 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.

Technical details:
A specified logon session does not exist. It may already have been terminated
status_login_invalid_username_or_bad_password (1312)

- 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, deploying agents, 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.

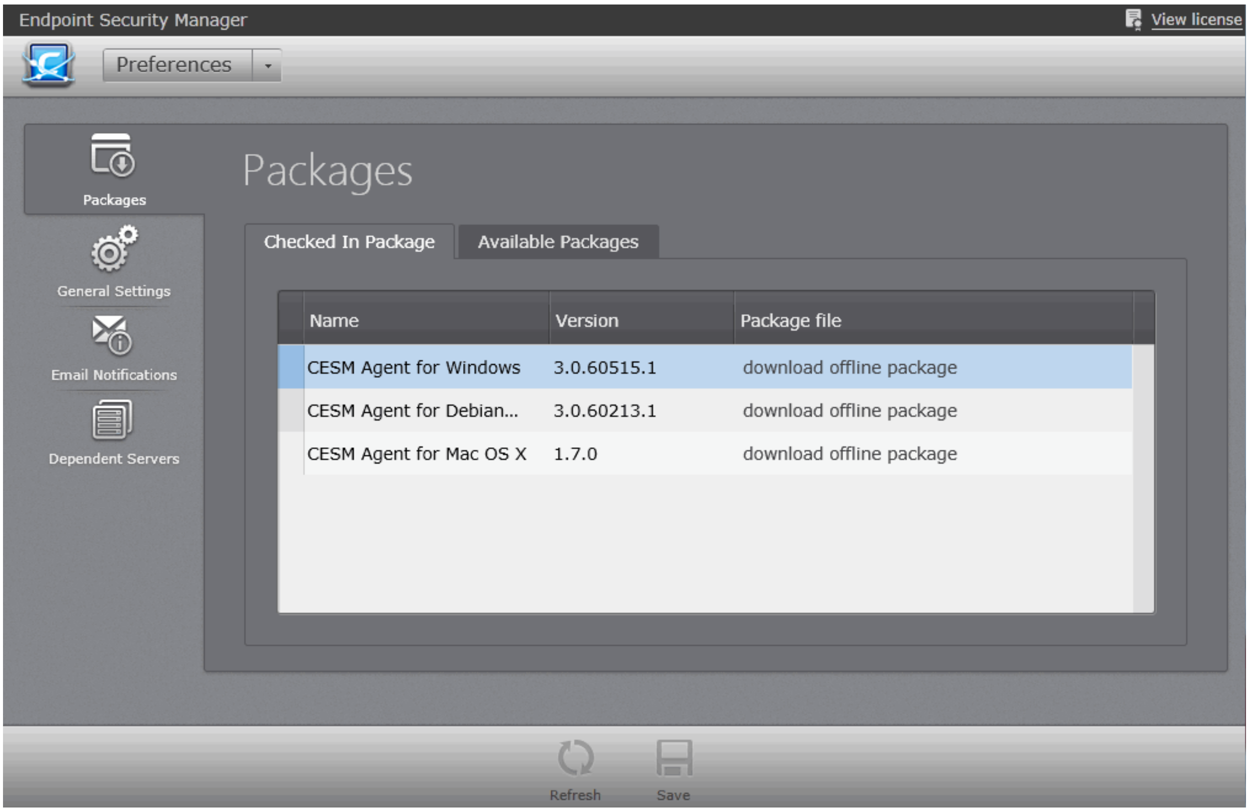
The newly added computer will be included to the default group 'Unassigned'. The administrator can then import the computer into the required group to which the computer is allotted.

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



Name	Version	Package file
CESM Agent for Windows	3.0.60515.1	download offline package
CESM Agent for Debian...	3.0.60213.1	download offline package
CESM Agent for Mac OS X	1.7.0	download offline package

- Select Agent setup file corresponding to the Operating System of the endpoint(s) onto which the agent has to be installed.

- Click 'Save' in the 'File Download' dialog and save the file in the location of your choice.

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:

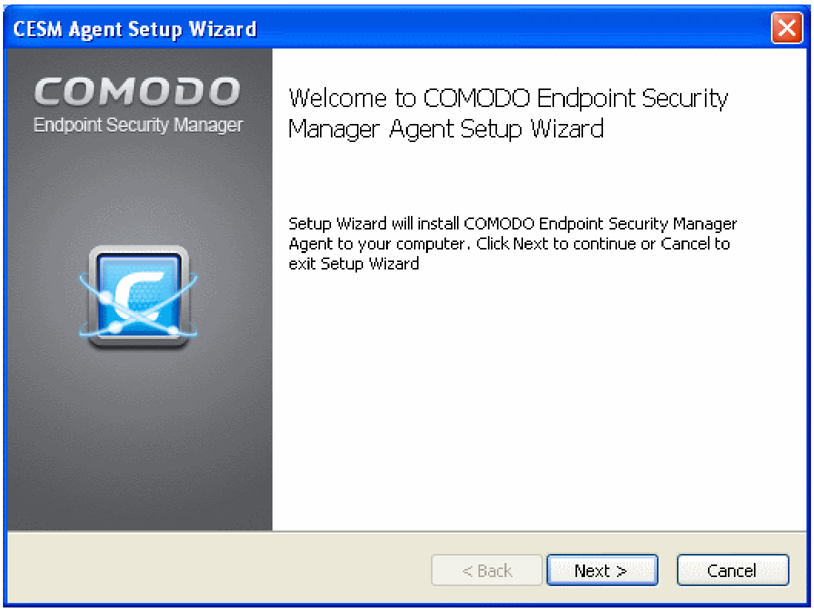
```
<file path in which agent setup file is stored>/ AgentSetup.exe /Options
```

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.

Step 1 - Welcome Screen

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


CESM Agent Setup Wizard

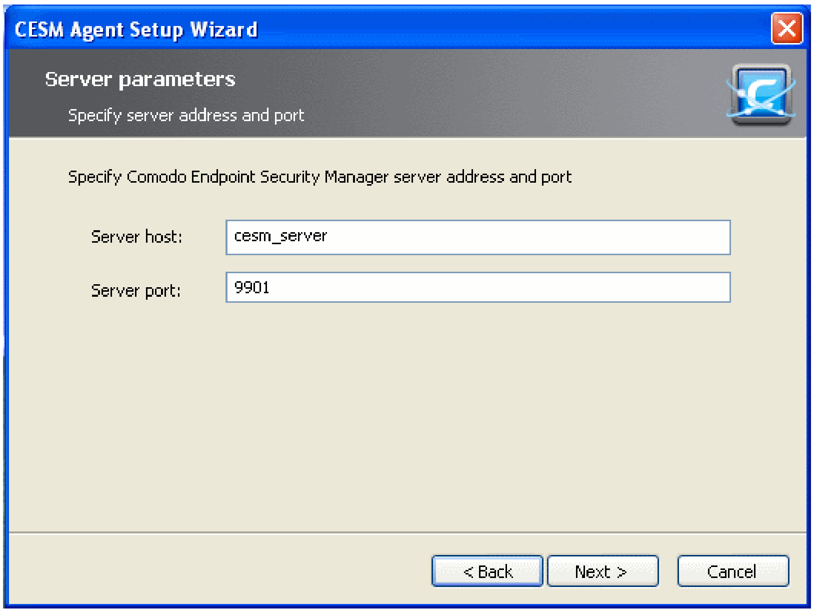
Welcome to COMODO Endpoint Security Manager Agent Setup Wizard

Setup Wizard will install COMODO Endpoint Security Manager Agent to your computer. Click Next to continue or Cancel to exit Setup Wizard

Click 'Next' to continue.

Step 2 – 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.


CESM Agent Setup Wizard

Server parameters

Specify server address and port

Specify Comodo Endpoint Security Manager server address and port

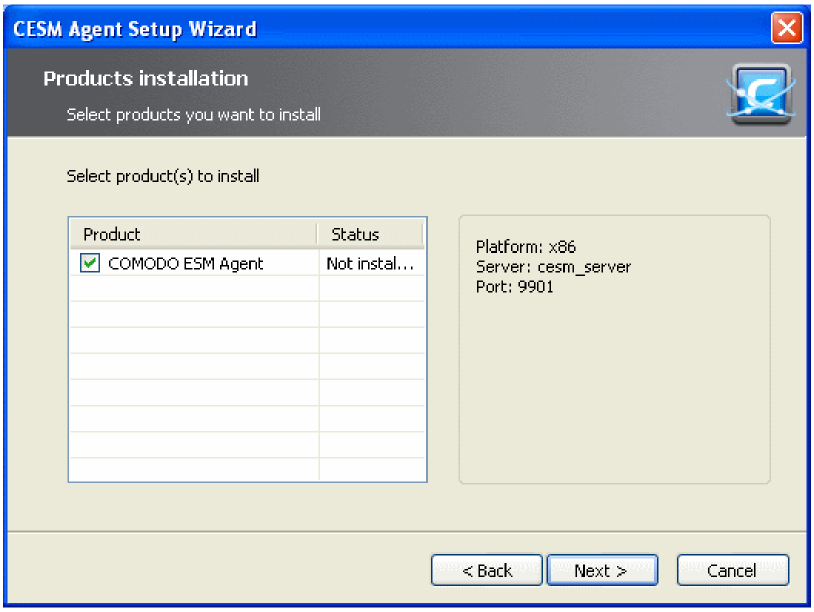
Server host: cesm_server

Server port: 9901

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 3 - 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.



CESM Agent Setup Wizard

Products installation

Select products you want to install

Select product(s) to install

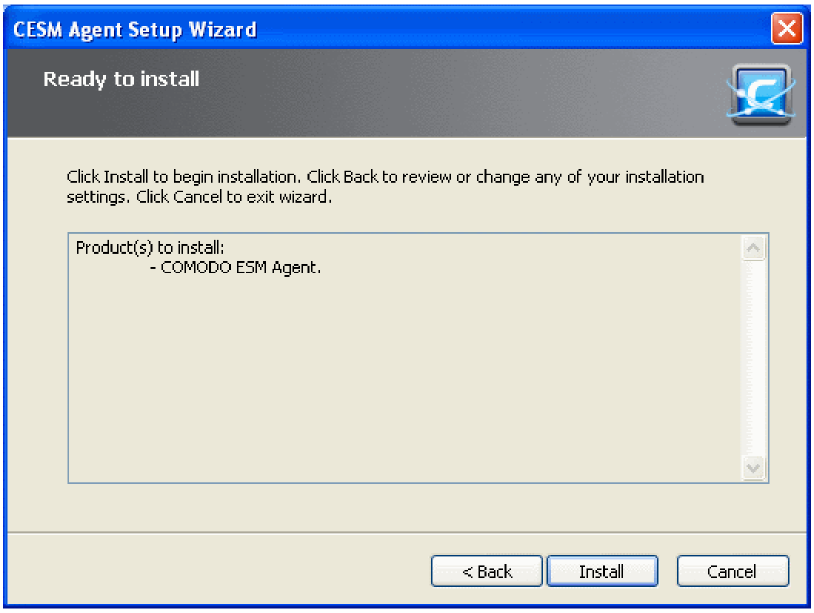
Product	Status
☑ COMODO ESM Agent	Not instal...

Platform: x86
Server: cesm_server
Port: 9901

Ensure that the required products are selected in then click 'Next'.

Step 4 - 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.



CESM Agent Setup Wizard

Ready to install

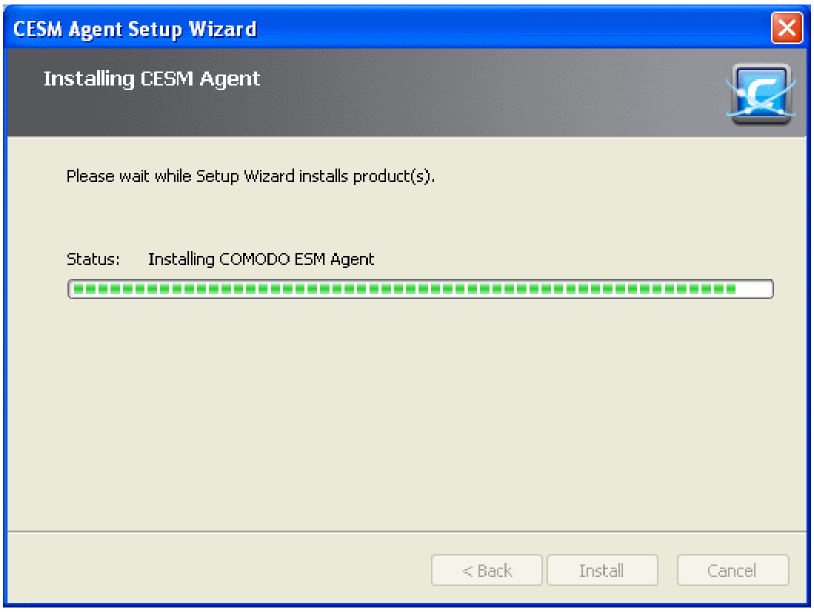
Click Install to begin installation. Click Back to review or change any of your installation settings. Click Cancel to exit wizard.

Product(s) to install:
- COMODO ESM Agent.

To commence the installation, click 'Install'.

Step 5 - Installation Progress

The installation progress will be displayed.



CESM Agent Setup Wizard

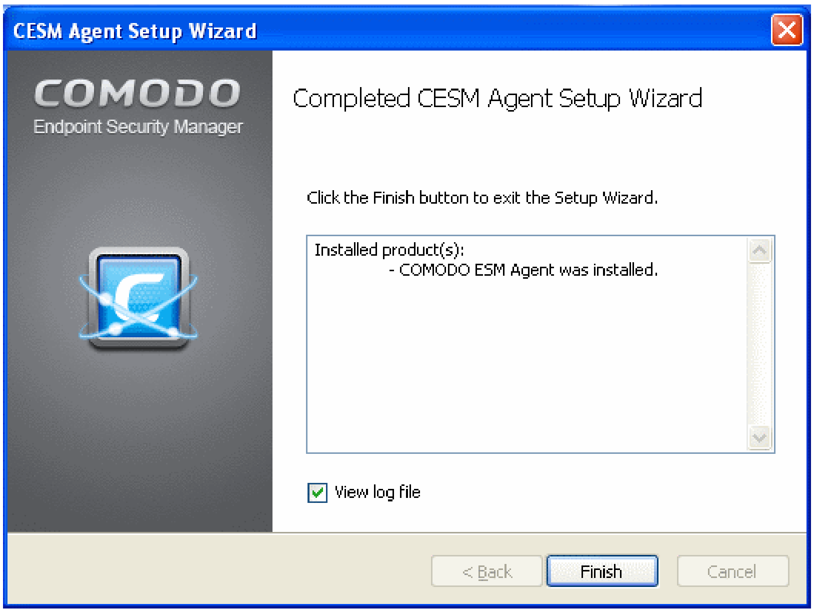
Installing CESM Agent

Please wait while Setup Wizard installs product(s).

Status: Installing COMODO ESM Agent

Step 6 - Installation Complete

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



CESM Agent Setup Wizard

Completed CESM Agent Setup Wizard

Click the Finish button to exit the Setup Wizard.

Installed product(s):
- COMODO ESM Agent was installed.

☑ View log file

- 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.

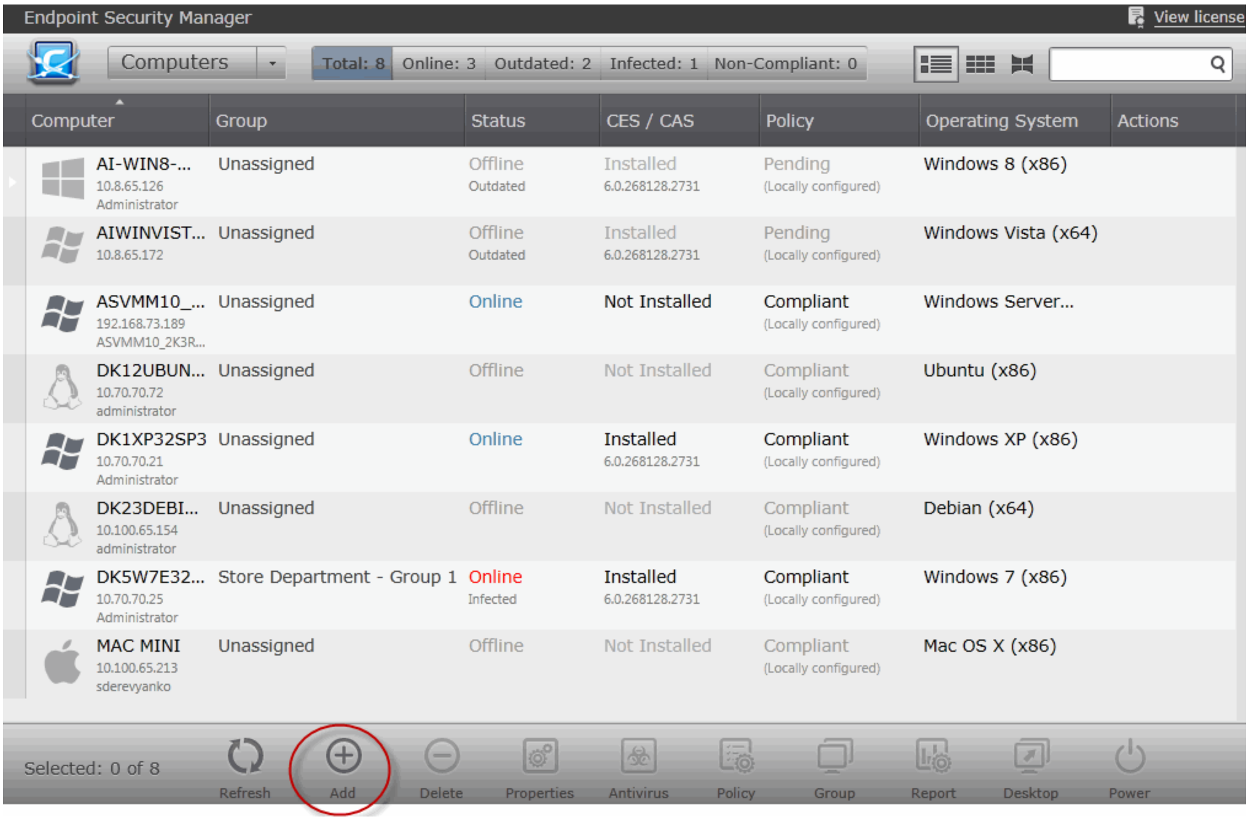
The agent will now automatically establish the connection to your CESM Service Server. Once the endpoint is connected, the administrator can start managing it and install CES on to it. Refer to **Updating Comodo Software on Managed Computers** for more details.

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 through the 'Add Computer' wizard.

To update software on managed computers

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

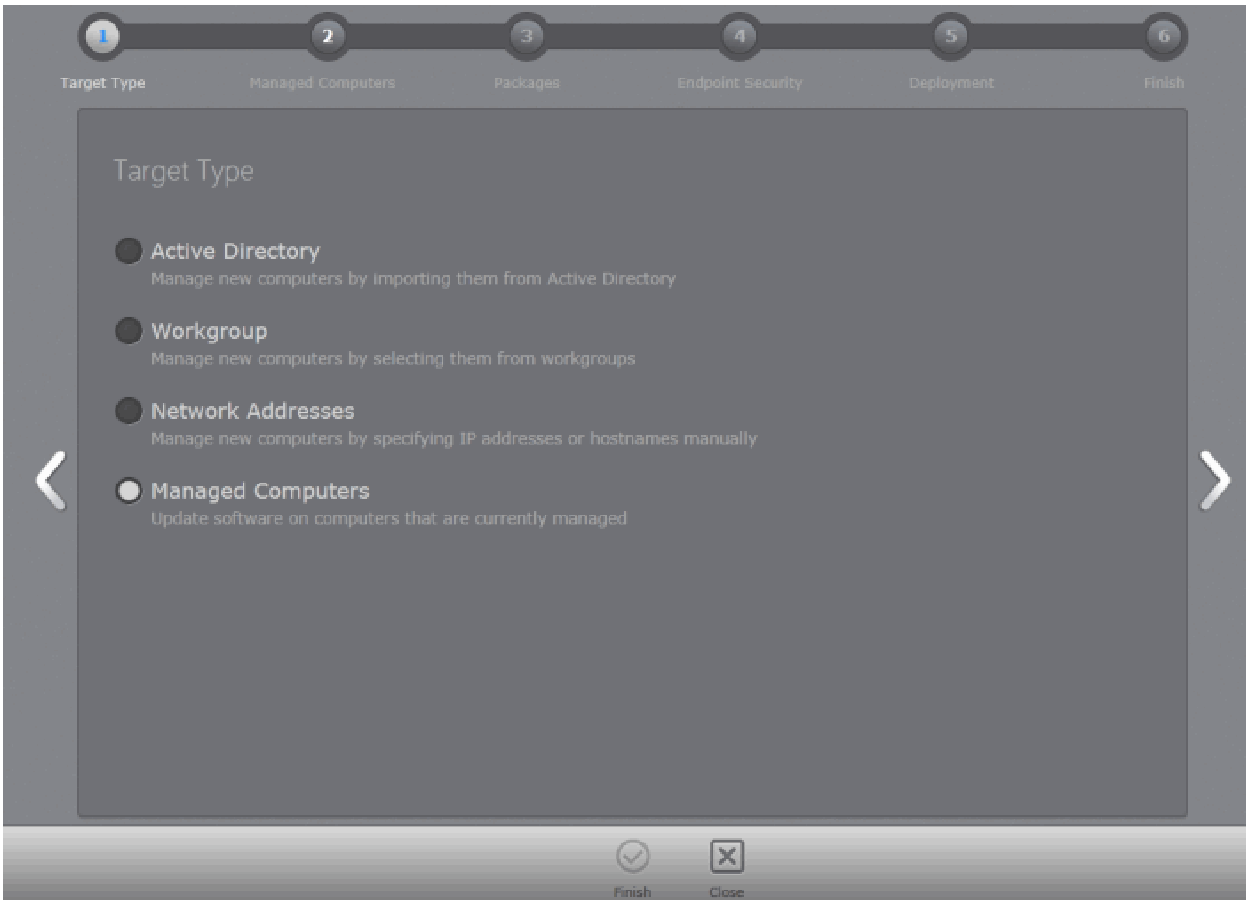


Total: 8 Online: 3 Outdated: 2 Infected: 1 Non-Compliant: 0

Computer	Group	Status	CES / CAS	Policy	Operating System	Actions
AI-WIN8-... 10.8.65.126 Administrator	Unassigned	Offline Outdated	Installed 6.0.268128.2731	Pending (Locally configured)	Windows 8 (x86)	
AIWINVIST... 10.8.65.172	Unassigned	Offline Outdated	Installed 6.0.268128.2731	Pending (Locally configured)	Windows Vista (x64)	
ASVMM10_... 192.168.73.189 ASVMM10_2K3R...	Unassigned	Online	Not Installed	Compliant (Locally configured)	Windows Server...	
DK12UBUN... 10.70.70.72 administrator	Unassigned	Offline	Not Installed	Compliant (Locally configured)	Ubuntu (x86)	
DK1XP32SP3 10.70.70.21 Administrator	Unassigned	Online	Installed 6.0.268128.2731	Compliant (Locally configured)	Windows XP (x86)	
DK23DEBI... 10.100.65.154 administrator	Unassigned	Offline	Not Installed	Compliant (Locally configured)	Debian (x64)	
DK5W7E32... 10.70.70.25 Administrator	Store Department - Group 1	Online Infected	Installed 6.0.268128.2731	Compliant (Locally configured)	Windows 7 (x86)	
MAC MINI 10.100.65.213 sderevyanko	Unassigned	Offline	Not Installed	Compliant (Locally configured)	Mac OS X (x86)	

Selected: 0 of 8

- Select 'Managed Computers' and click the right arrow or swipe left to proceed to the next step.



Target Type

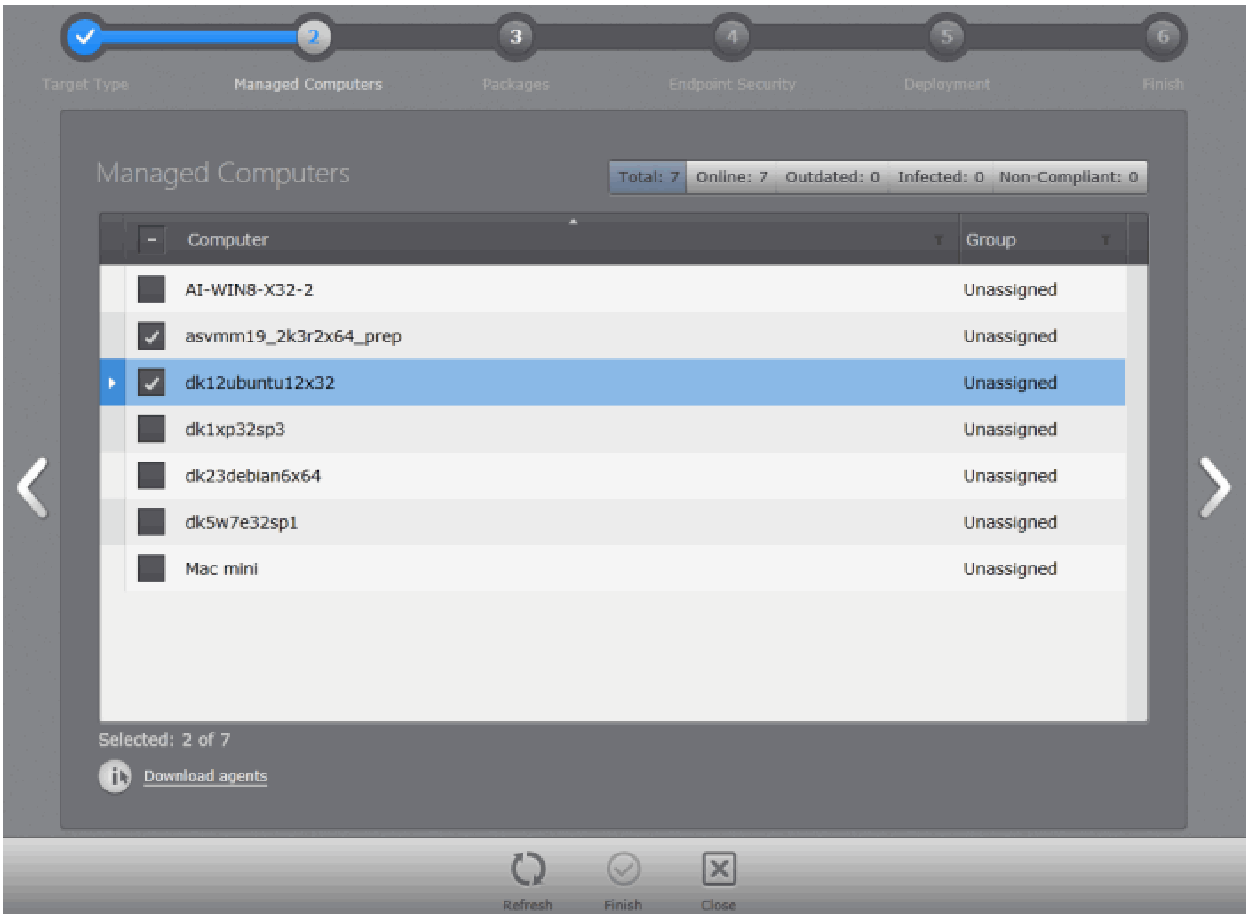
○ Active Directory
Manage new computers by importing them from Active Directory

○ Workgroup
Manage new computers by selecting them from workgroups

○ Network Addresses
Manage new computers by specifying IP addresses or hostnames manually

● Managed Computers
Update software on computers that are currently managed

All the managed computers will be listed.



Managed Computers

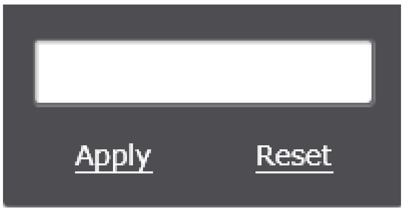
Total: 7 | Online: 7 | Outdated: 0 | Infected: 0 | Non-Compliant: 0

	Computer	Group
□	AI-WIN8-X32-2	Unassigned
☑	asvmm19_2k3r2x64_prep	Unassigned
☑	dk12ubuntu12x32	Unassigned
□	dk1xp32sp3	Unassigned
□	dk23debian6x64	Unassigned
□	dk5w7e32sp1	Unassigned
□	Mac mini	Unassigned

Selected: 2 of 7

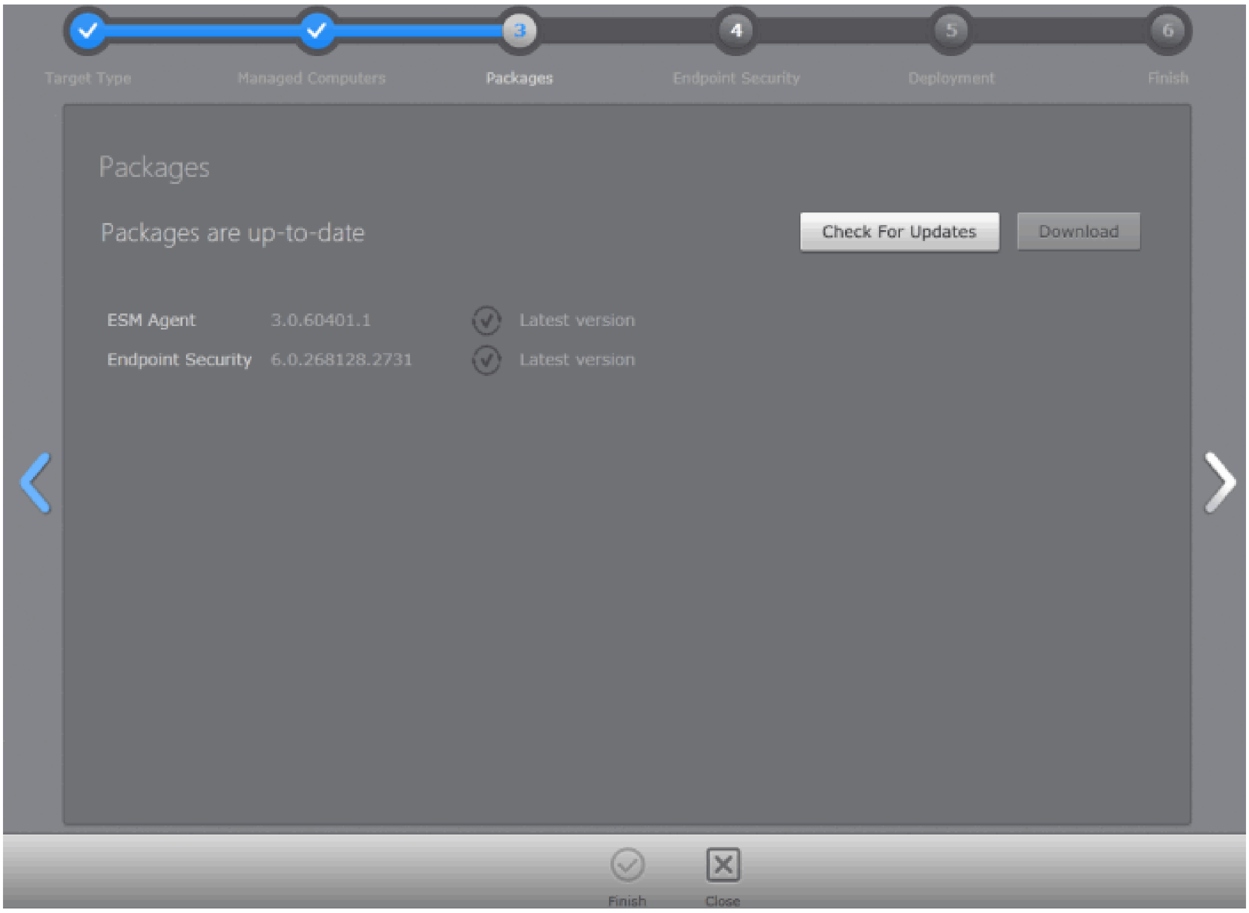
Download agents

- Select the endpoints that you want to check and update CESM Agent and CES application from the list.



- Click the filter icon in the 'Name' 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 stage 'Packages' displays the version details of ESM Agent and CES. You can also check for updates of these applications and download it in your server for deployment on to the selected endpoints.



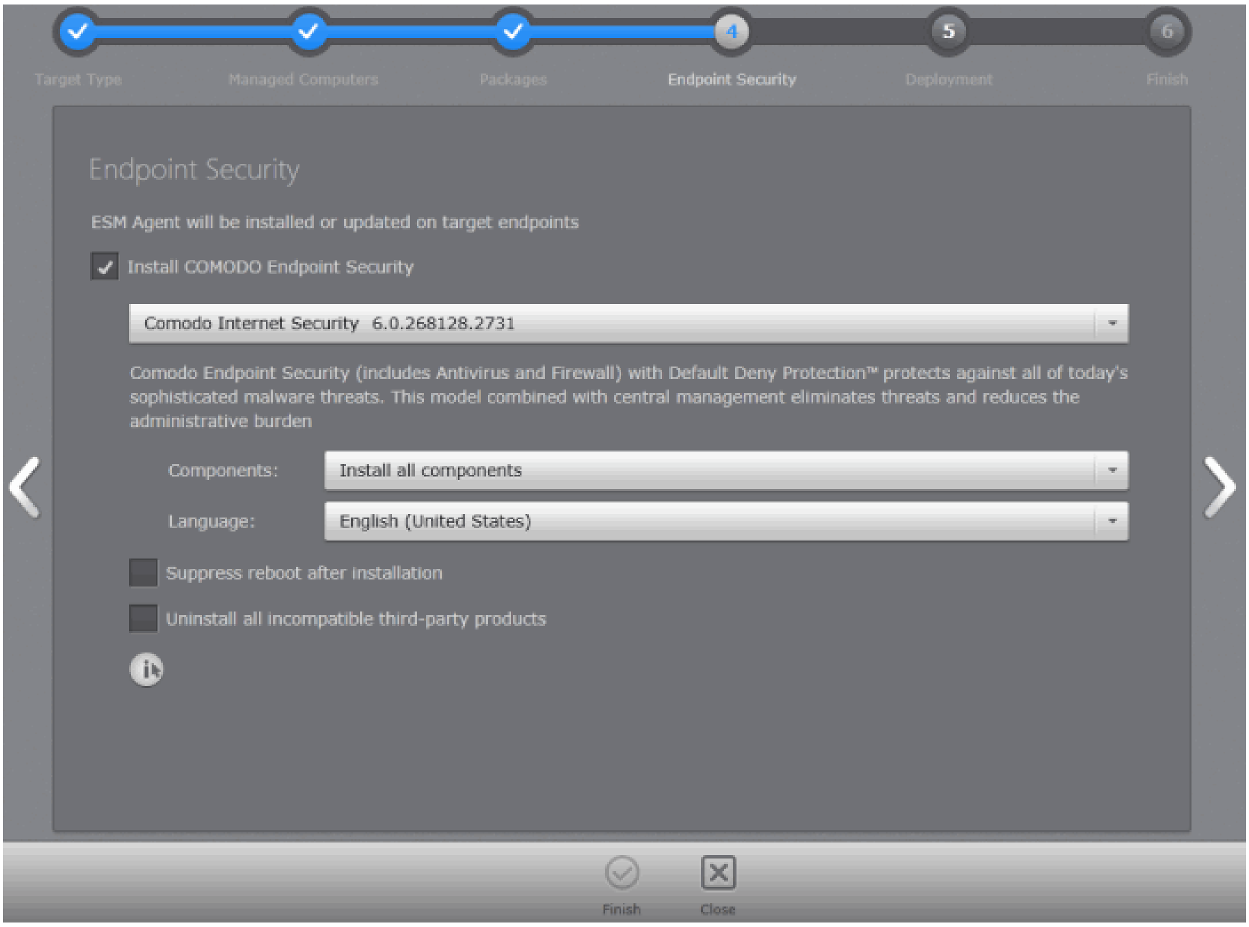
Packages

Packages are up-to-date

ESM Agent	3.0.60401.1	✓ Latest version
Endpoint Security	6.0.268128.2731	✓ Latest version

- Click 'Check for Updates' to find out if any newer version of CESM Agent and CES are available.
- If any newer versions are available, you can choose to download them to the CESM server by clicking 'Download' .
- 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):



Endpoint Security

ESM Agent will be installed or updated on target endpoints

☑ Install COMODO Endpoint Security

Comodo Internet Security 6.0.268128.2731

Comodo Endpoint Security (includes Antivirus and Firewall) with Default Deny Protection™ protects against all of today's sophisticated malware threats. This model combined with central management eliminates threats and reduces the administrative burden

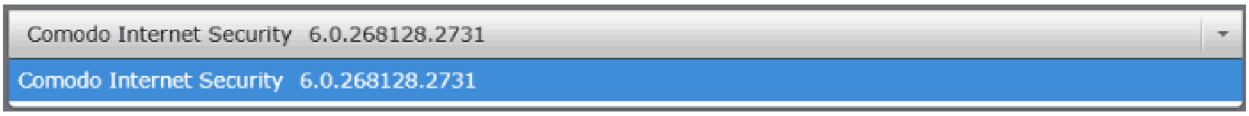
Components: Install all components

Language: English (United States)

□ Suppress reboot after installation

□ Uninstall all incompatible third-party products

- Select 'Install Comodo Endpoint Security' check box if you wish CES to be installed along with the agent.
- Select the version of CES you wish to install on the selected endpoints from the drop-down.



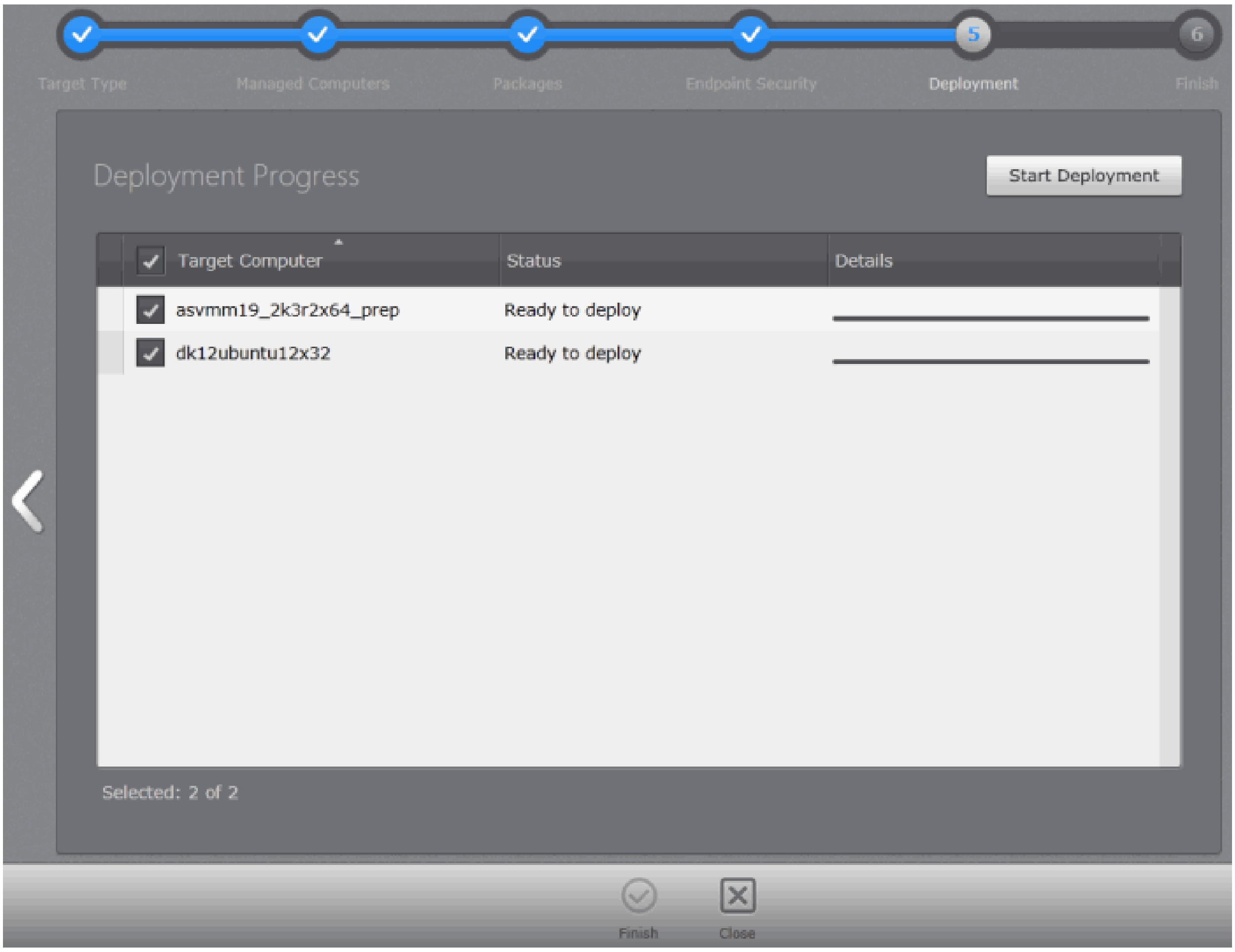
Comodo Internet Security 6.0.268128.2731

Comodo Internet Security 6.0.268128.2731

- Select whether you want to include all the components (Firewall and Antivirus), Antivirus only or Firewall only from the Components 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 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.



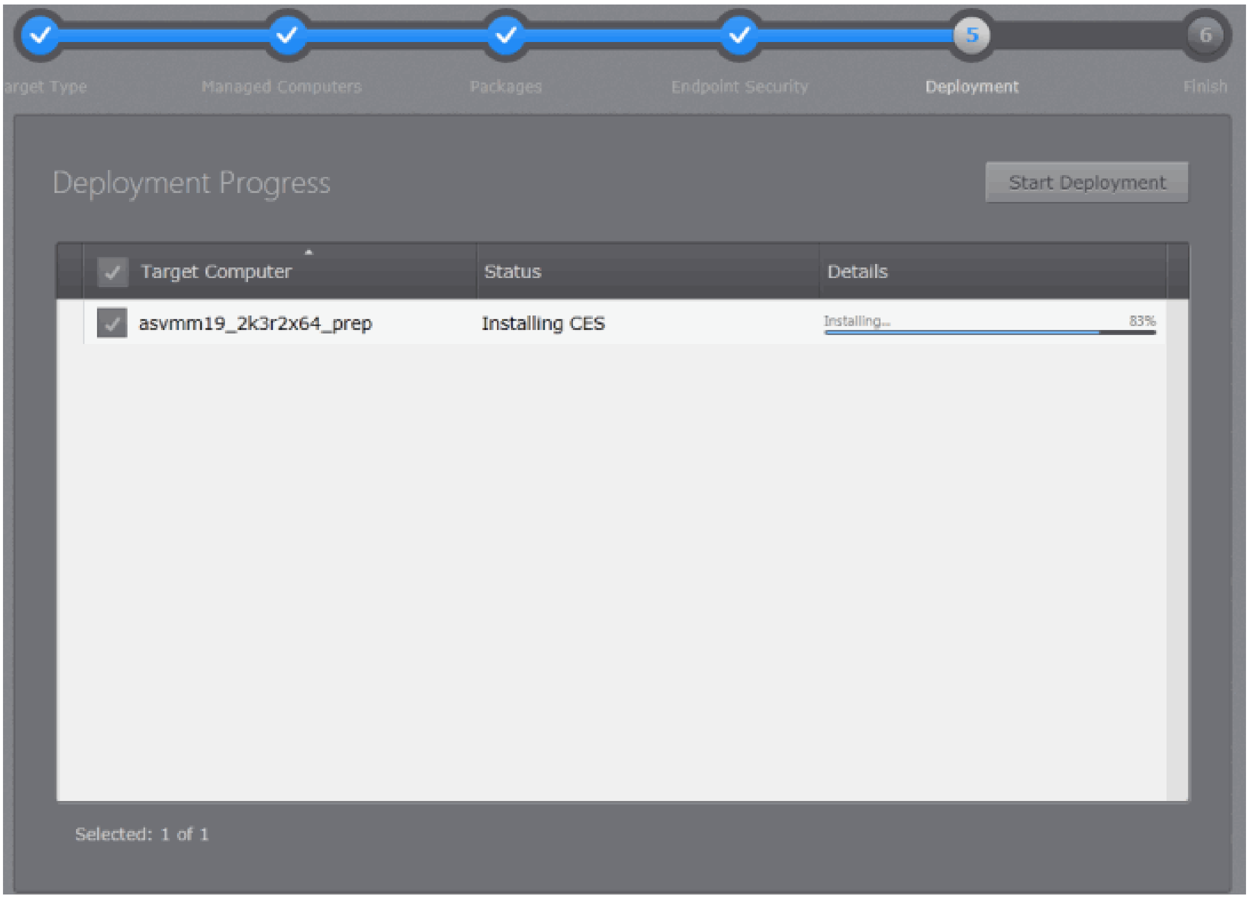
Deployment Progress

☑ Target Computer	Status	Details
☑ asvmm19_2k3r2x64_prep	Ready to deploy	
☑ dk12ubuntu12x32	Ready to deploy	

Selected: 2 of 2

- Click 'Start Deployment'.

The deployment progress will be displayed.

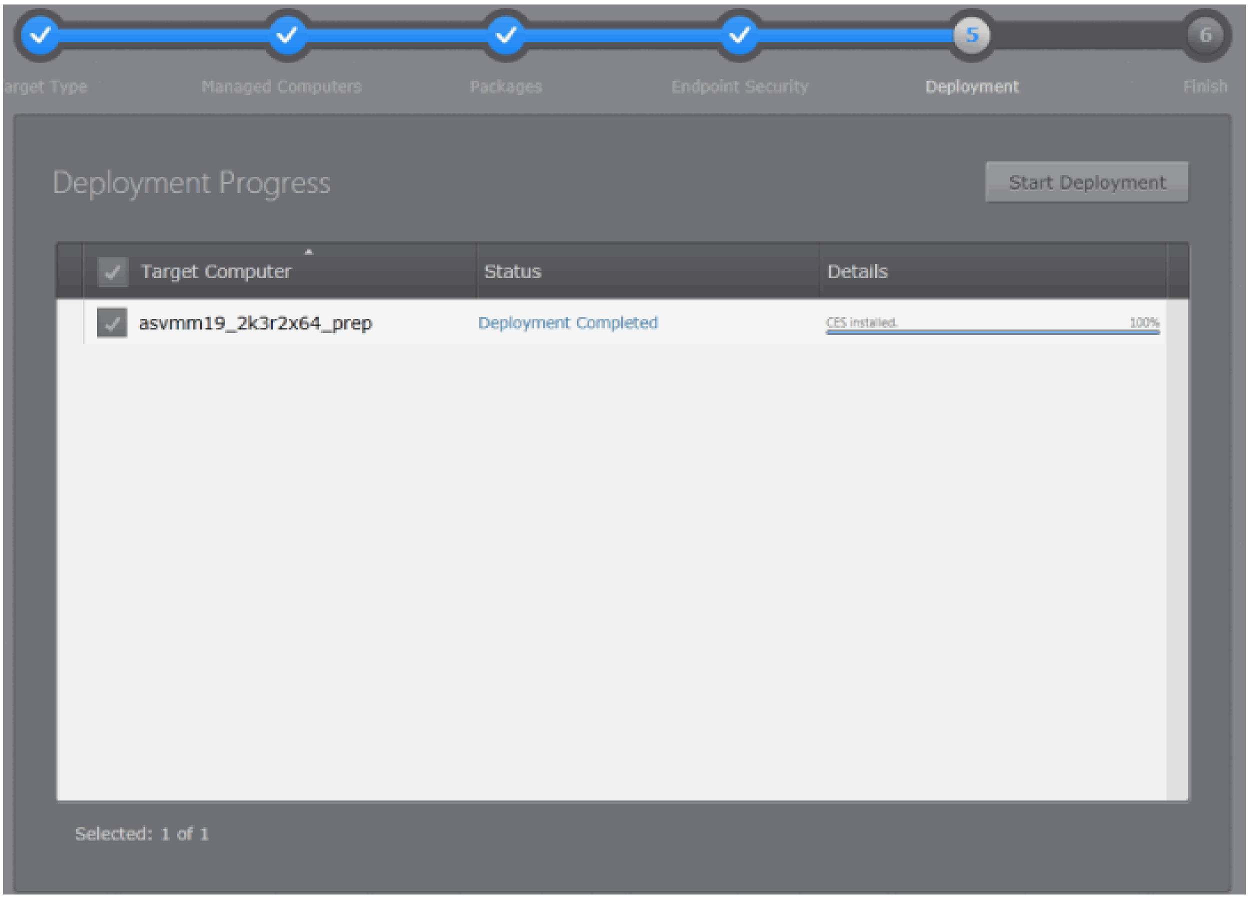


Deployment Progress

Target Computer	Status	Details
☑ asvmm19_2k3r2x64_prep	Installing CES	Installing... 83%

Selected: 1 of 1

On completion of installation, the results screen will appear.



Deployment Progress

Target Computer	Status	Details
☑ asvmm19_2k3r2x64_prep	Deployment Completed	CES installed. 100%

Selected: 1 of 1

- 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.

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.

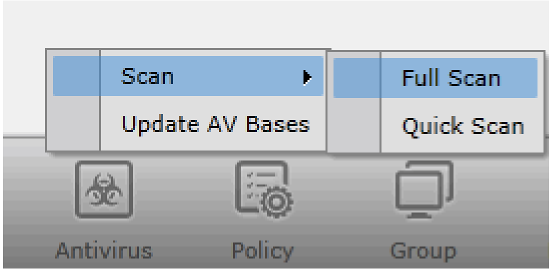
Tip: The administrators can also run a scan on a selected single endpoint from the **Computer Properties > Endpoint Security interface**. Refer to the section **Viewing and Managing Internet Security Software** for more details.

To run a full scan on selected endpoints

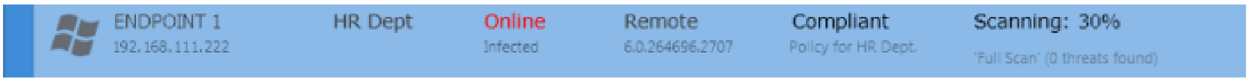
1. Select 'Computers' from the area selection drop-down menu to open the 'Computers' interface.
2. Choose the endpoints to be scanned. You can select multiple endpoints at once by pressing and holding the Ctrl or Shift key, from list, grid or 3D Panoramic view.

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.



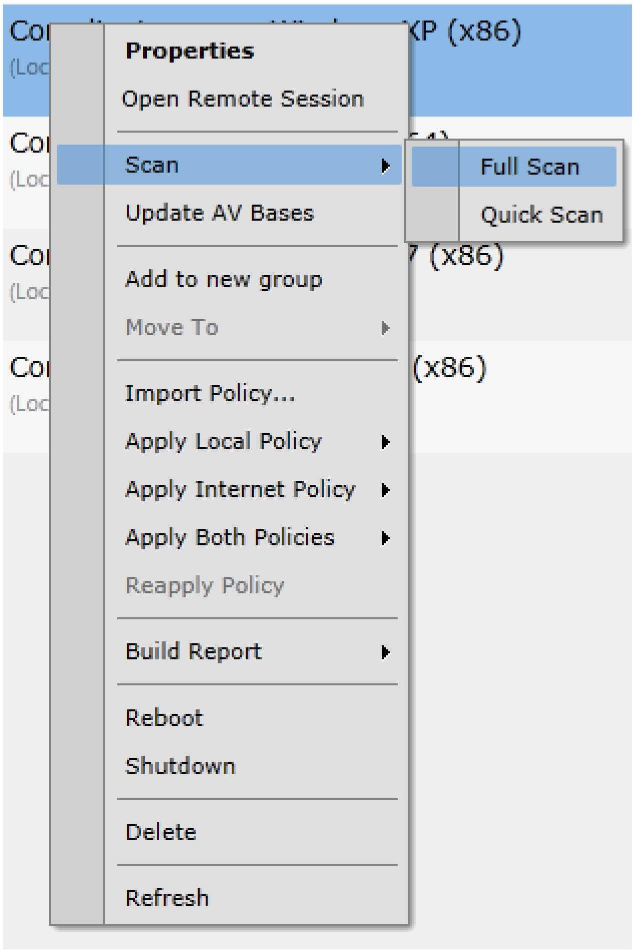
You can also run the scans from the right click options with choices to select the areas to be scanned in the endpoints.

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, grid 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.

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

- 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-72-1-451-4757-Custom-Scan-Settings.html**

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.

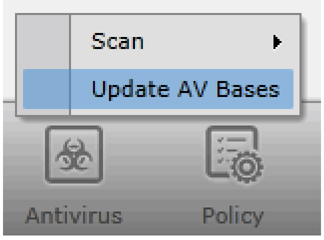
3.4. Updating Virus Database on Individual Endpoints

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

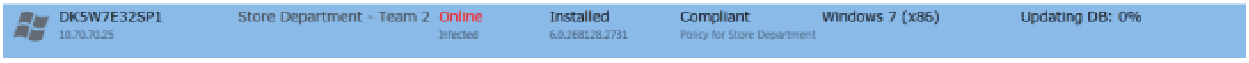
1. Select 'Computers' from the area selection drop-down menu to open the 'Computers' interface.

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.



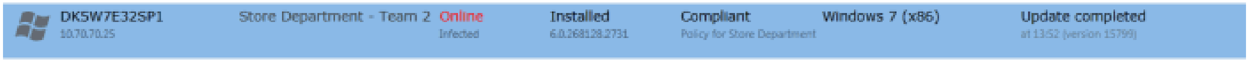
3. Click 'Antivirus'> 'Update AV Bases' from the bottom or right click on a selected endpoint and choose Update AV Bases from the context sensitive menu.

The Progress will be displayed.



DK5W7E325P1 10.70.70.25	Store Department - Team 2	Online Infected	Installed 6.0.268128.2731	Compliant Policy for Store Department	Windows 7 (x86)	Updating DB: 0%

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



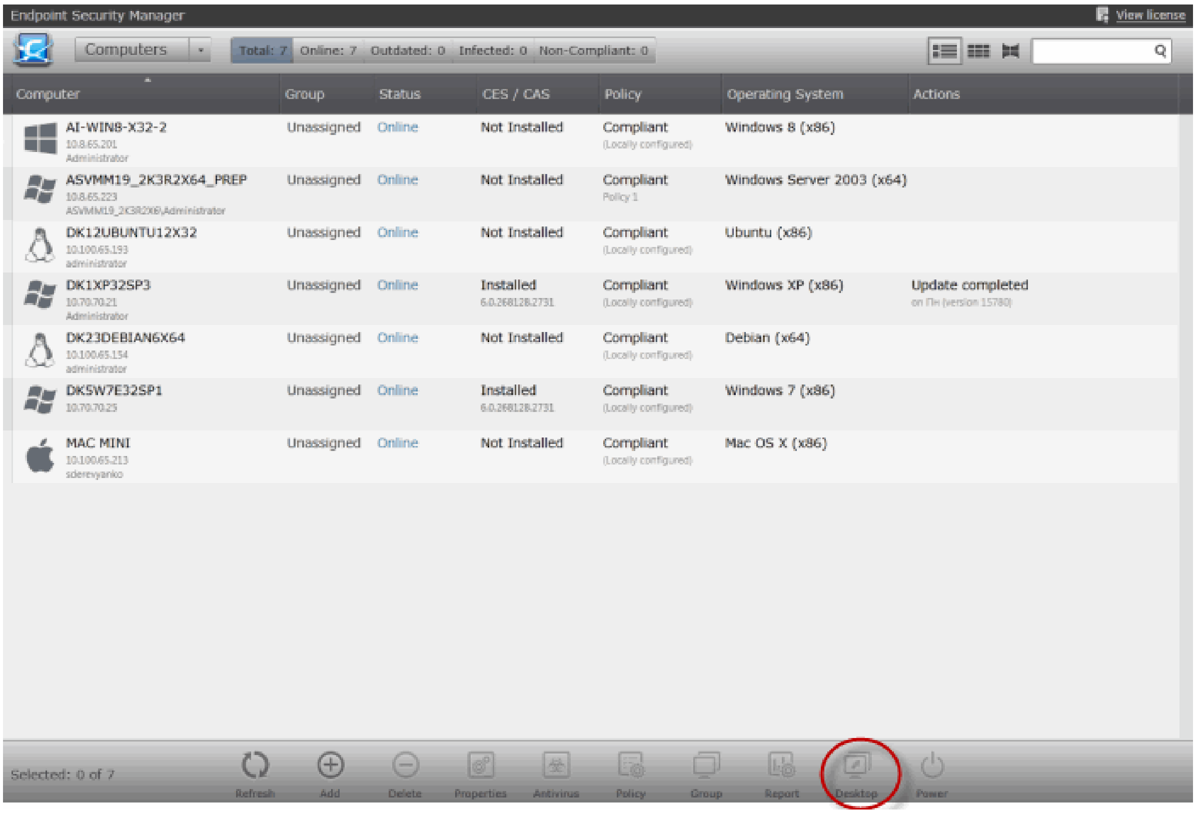
DK5W7E32SP1 10.70.70.25	Store Department - Team 2	Online Infected	Installed 6.0.268128.2731	Compliant Policy for Store Department	Windows 7 (x86)	Update completed at 13:52 (version 15799)

3.5. Accessing Endpoints through Remote Desktop Sharing Session

CESM allows the administrators to have a desktop sharing session with a remote computer for inspection, configuration, installing third party software or help the end user to solve any issues.

To start a remote sharing session

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



Endpoint Security Manager

Total: 7 | Online: 7 | Outdated: 0 | Infected: 0 | Non-Compliant: 0

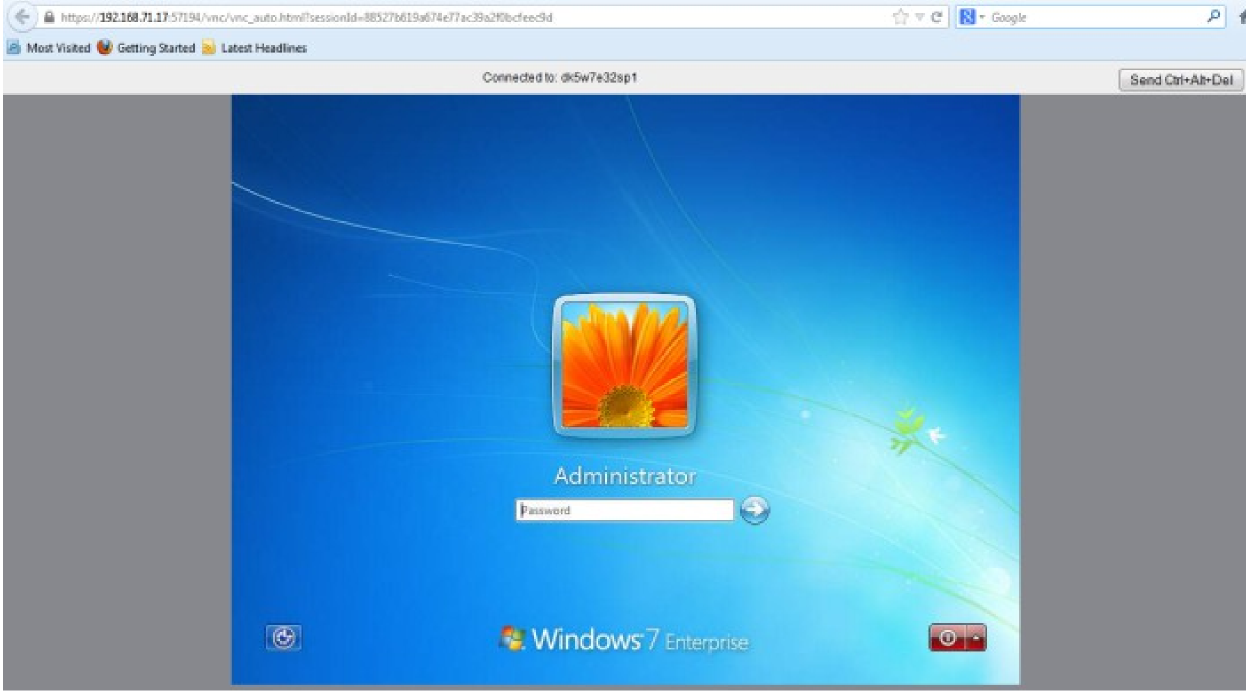
Computer	Group	Status	CES / CAS	Policy	Operating System	Actions
AI-WIN8-X32-2 10.8.65.201 Administrator	Unassigned	Online	Not Installed	Compliant (Locally configured)	Windows 8 (x86)	
ASVMM19_2K3R2X64_PREP 10.8.65.223 ASVMM19_2K3R2X6\Administrator	Unassigned	Online	Not Installed	Compliant Policy 1	Windows Server 2003 (x64)	
DK12UBUNTU12X32 10.100.65.193 administrator	Unassigned	Online	Not Installed	Compliant (Locally configured)	Ubuntu (x86)	
DK1XP32SP3 10.70.70.21 Administrator	Unassigned	Online	Installed 6.0.268128.2731	Compliant (Locally configured)	Windows XP (x86)	Update completed on Пн (version 15780)
DK23DEBIAN6X64 10.100.65.154 administrator	Unassigned	Online	Not Installed	Compliant (Locally configured)	Debian (x64)	
DK5W7E32SP1 10.70.70.25	Unassigned	Online	Installed 6.0.268128.2731	Compliant (Locally configured)	Windows 7 (x86)	
MAC MINI 10.100.65.213 sderevyanko	Unassigned	Online	Not Installed	Compliant (Locally configured)	Mac OS X (x86)	

Selected: 0 of 7

2. Select the endpoints to be controlled.

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

4. A new tab will be opened in the browser, displaying the desktop of the remote computer.



https://192.168.71.17:57194/vnc/vnc_auto.html?sessionId=88527b619a674e77ac39a2f0bcfeec9d

Connected to: dk5w7e32sp1

The administrator can take control of the remote computer, through the desktop sharing session.

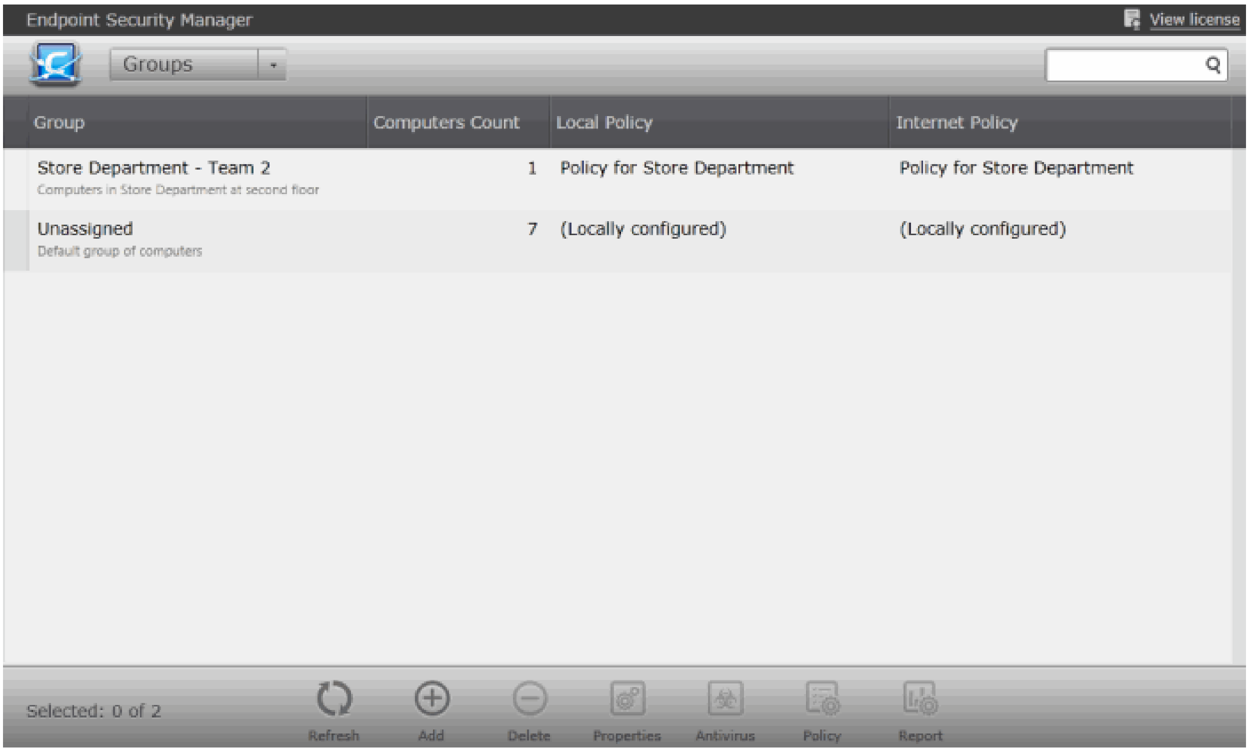
4. The Groups Area

Creating groups of computers allows the 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'. Once created, the administrator can manage all machines belonging to that group together. Some of the benefits of grouping the computers are:

- The CES security policies can be applied to the endpoints belonging to various groups as per their requirements
- Antivirus (AV) scans can be run on endpoints in a group together.
- The AV signature database in the endpoints can be updated together.
- Various reports can be generated for the endpoints belonging to a group as a single file.

CESM is shipped with a default group 'Unassigned'. All the computers which are imported into CESM and yet to be assigned to other groups, 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.



Group	Computers Count	Local Policy	Internet Policy
Store Department - Team 2 Computers in Store Department at second floor	1	Policy for Store Department	Policy for Store Department
Unassigned Default group of computers	7	(Locally configured)	(Locally configured)

Column Heading	Description
Group	Displays the name of the group
Computers Count	Displays the number of endpoints in the group
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**
- **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**

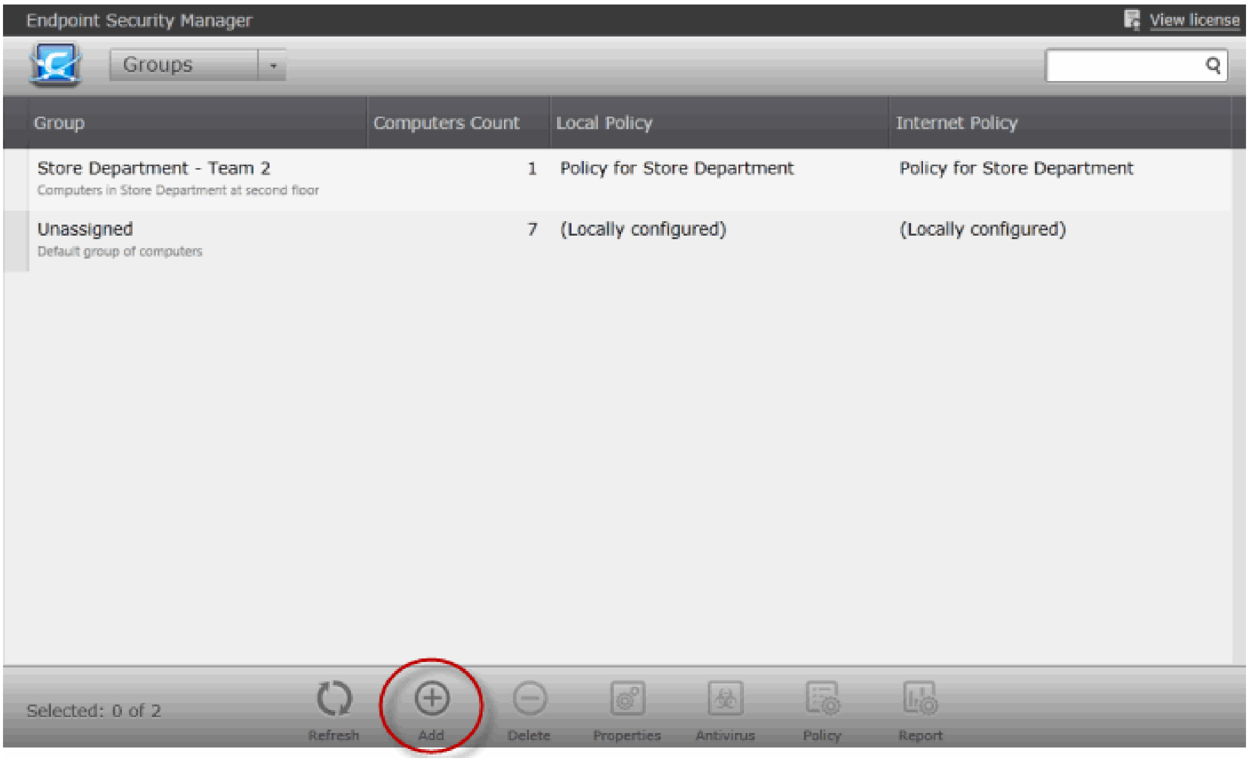
4.1. Creating New Groups and Importing Existing Endpoints

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

To create a new 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.

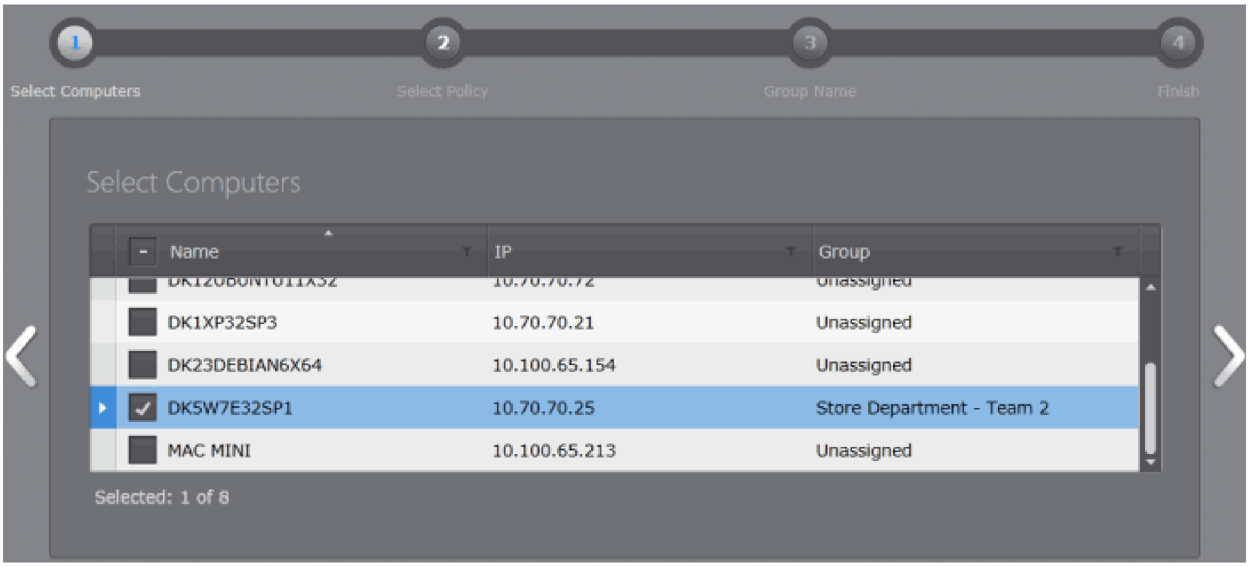


Group	Computers Count	Local Policy	Internet Policy
Store Department - Team 2 Computers in Store Department at second floor	1	Policy for Store Department	Policy for Store Department
Unassigned Default group of computers	7	(Locally configured)	(Locally configured)

2. Click 'Add' from the bottom to start the 'Create Group' Wizard.

Step 1 - Selecting Computers

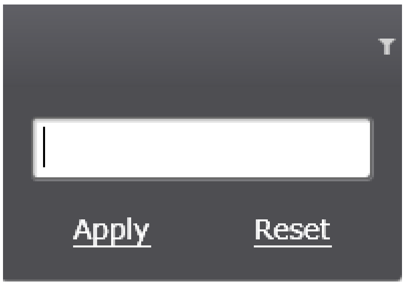
All the computers managed by CESM will be displayed as a list with their IP address and existing group details.



Select Computers

☐	Name	IP	Group
☐	DK12UBUNTU11X32	10.70.70.72	Unassigned
☐	DK1XP32SP3	10.70.70.21	Unassigned
☐	DK23DEBIAN6X64	10.100.65.154	Unassigned
☑	DK5W7E32SP1	10.70.70.25	Store Department - Team 2
☐	MAC MINI	10.100.65.213	Unassigned

Selected: 1 of 8

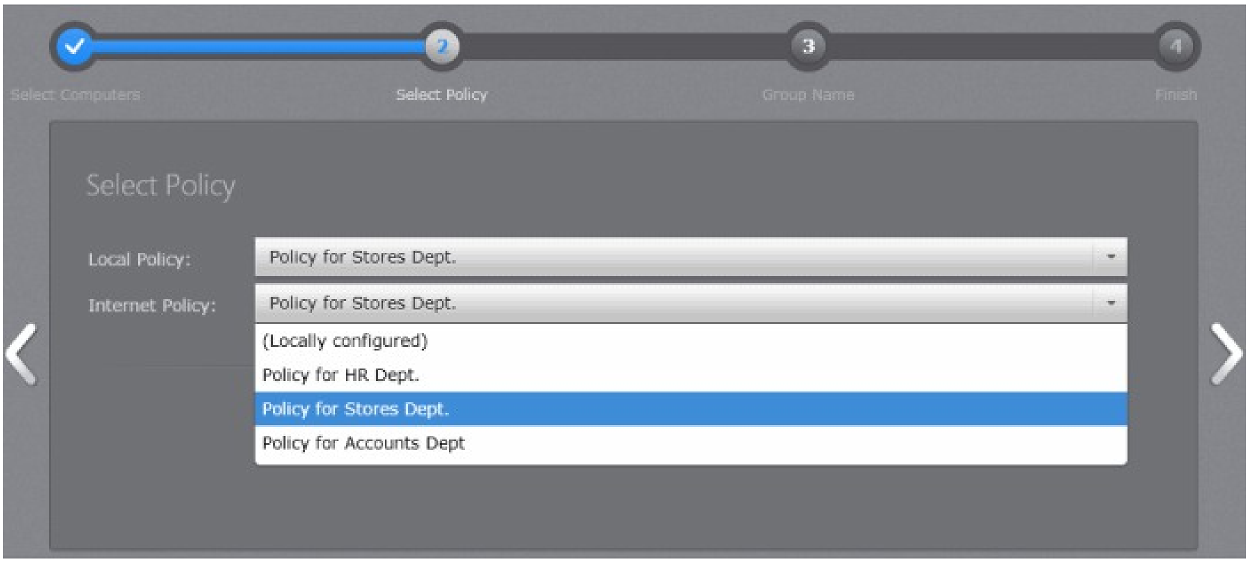


- Click the filter icon ▼ in the 'Name' column header to search for a particular endpoint and click 'Apply'.
- Click the filter icon ▼ in the 'IP' column header to search for endpoints with particular IP(s) and click 'Apply'.
- Click the filter icon ▼ in the 'Group' column header to search for endpoints belonging to a specific group and click 'Apply'.

- Select the endpoint computers to be added to the new group and click the right arrow/swipe the screen left to move to the next step.

Step 2 - Selecting Security Policy

The next step is to assign a security policy for the CES installations in the endpoints of the newly created group.



Select Policy

Local Policy: Policy for Stores Dept.

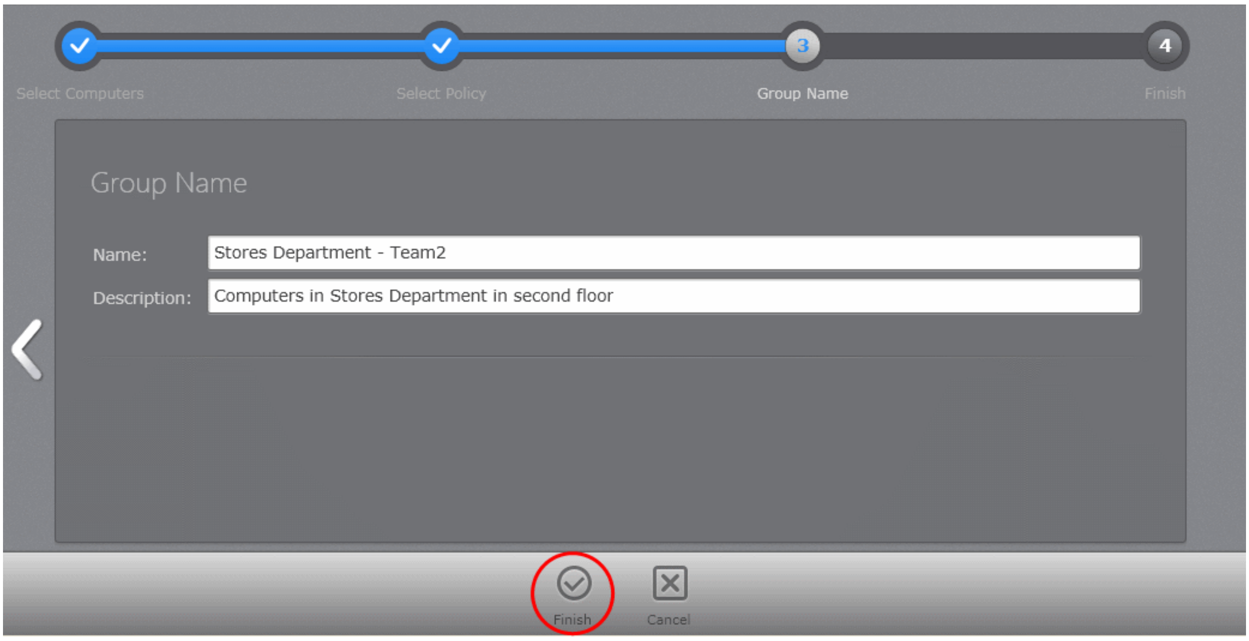
Internet Policy: Policy for Stores Dept.

(Locally configured)
Policy for HR Dept.
Policy for Stores Dept.
Policy for Accounts Dept

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 'Select Policy' step 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.

Step 3 - Naming the Group

The next step is to set a name for the created group.



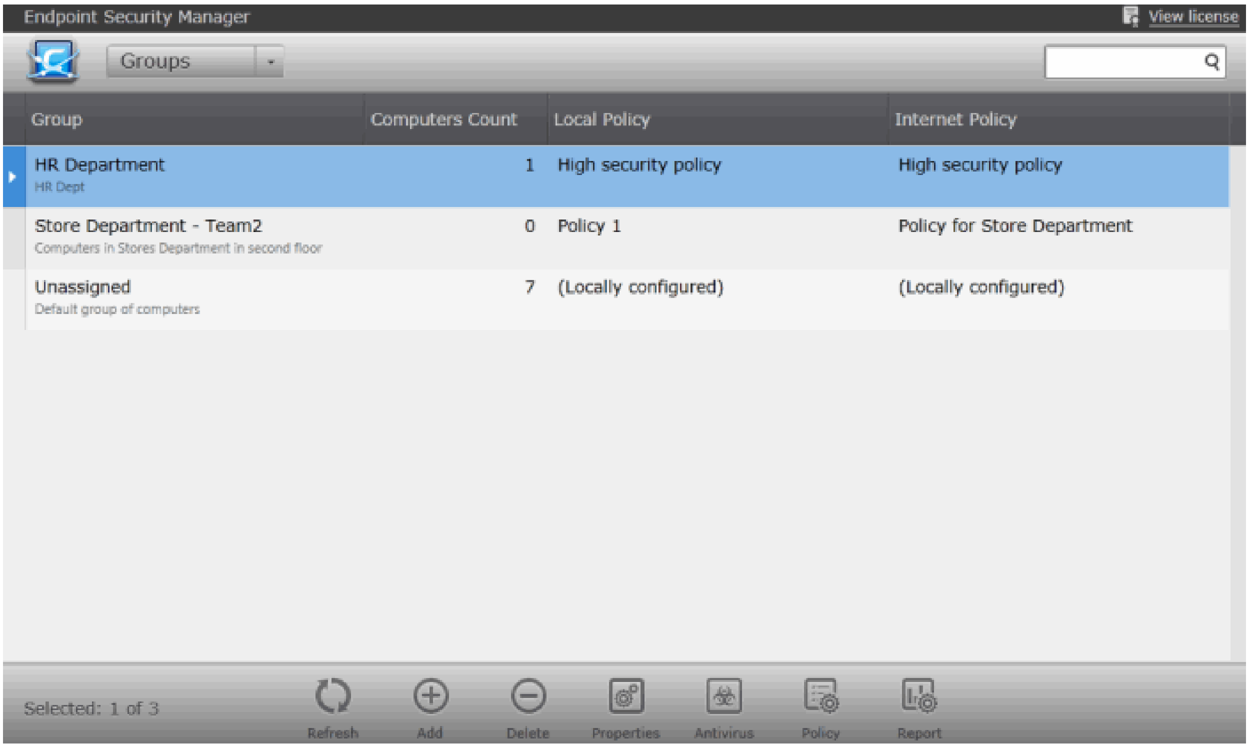
Group Name

Name: Stores Department - Team2

Description: Computers in Stores Department in second floor

- Enter a name as the group has to identified by CESM in the 'Name' text field.
- Select the Local Security Policy and Internet Security Policy for the CES installations from the respective drop-downs and click the right arrow to move to the next step. For more details on CESM policies, see the section '**The Policies Area**'.
- Enter a short description for the created group in the 'Description' text field. This description will appear in the 'Groups' area Interface.
- Click the 'Finish' from the bottom to exit the wizard.

The new group will be created with the endpoints selected in Step 1 as members. The CES installations in all the member endpoints will be applied with the security policy as chosen in step 2.



Group	Computers Count	Local Policy	Internet Policy
HR Department HR Dept	1	High security policy	High security policy
Store Department - Team2 Computers in Stores Department in second floor	0	Policy 1	Policy for Store Department
Unassigned Default group of computers	7	(Locally configured)	(Locally configured)

Selected: 1 of 3

Note: The policy can be changed for individual endpoints as desired from the '**Computers**' area.

4.2. Viewing and Managing Groups

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

From this interface the administrator can:

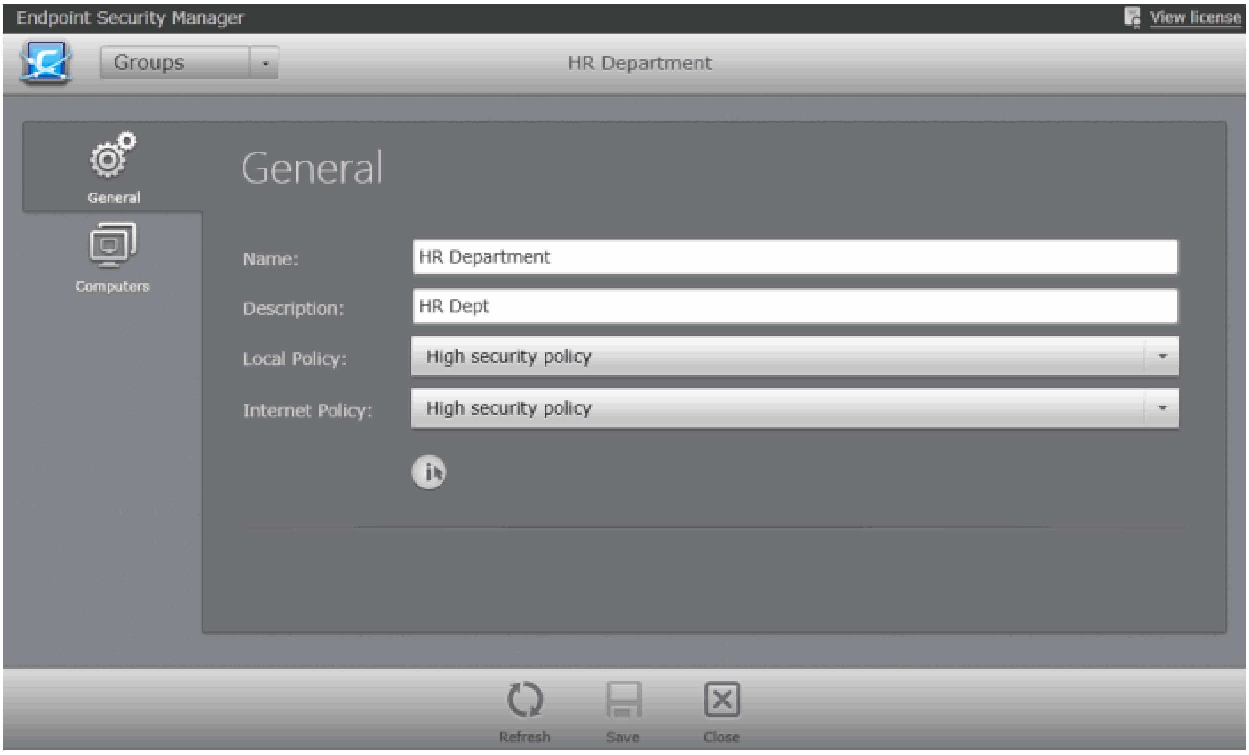
- View a summary on details such as security policy applied and the member endpoints of the selected group.
- Drive the CES installations of endpoints in local administration mode to remote administration mode.
- Edit a 'Group' to rename, add or remove member endpoints and to change default security policies assigned to the endpoints.
- Generate reports for the endpoints belonging to a group 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. Open the Group Properties interface for a selected group by:
   - Select the Group and click 'Properties' from the options at the bottom; or
   - Right on the Group and select 'Properties' from the context sensitive menu.



General

Name: HR Department

Description: HR Dept

Local Policy: High security policy

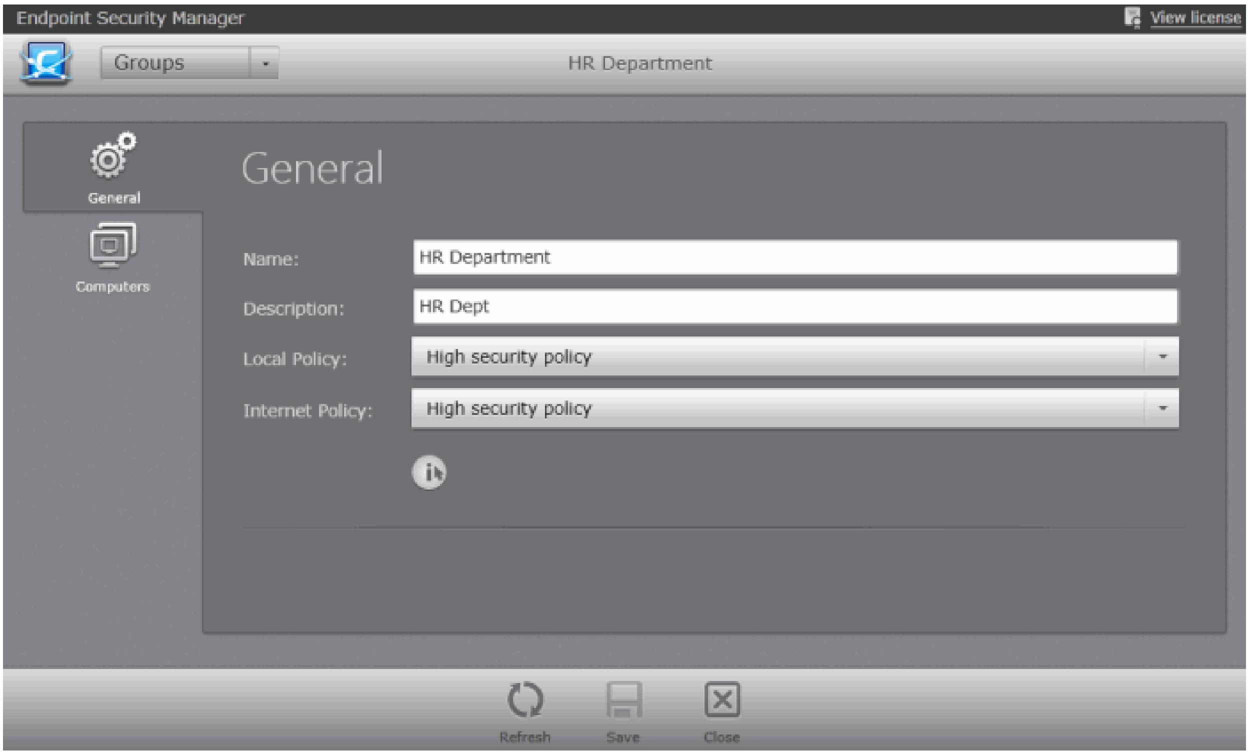
Internet Policy: High security policy

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

The General Properties screen displayed by clicking the 'General' tab from the left hand side navigation, shows the name and description of the group and allows the administrator to rename the group if required. 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.



Name: HR Department

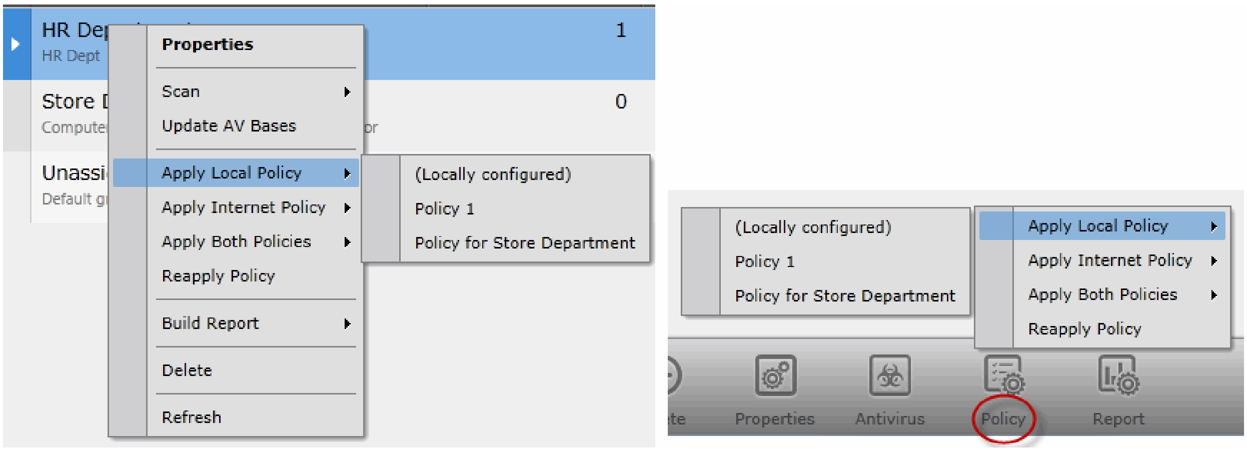
Description: HR Dept

Local Policy: High security policy

Internet Policy: High security policy

- 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.

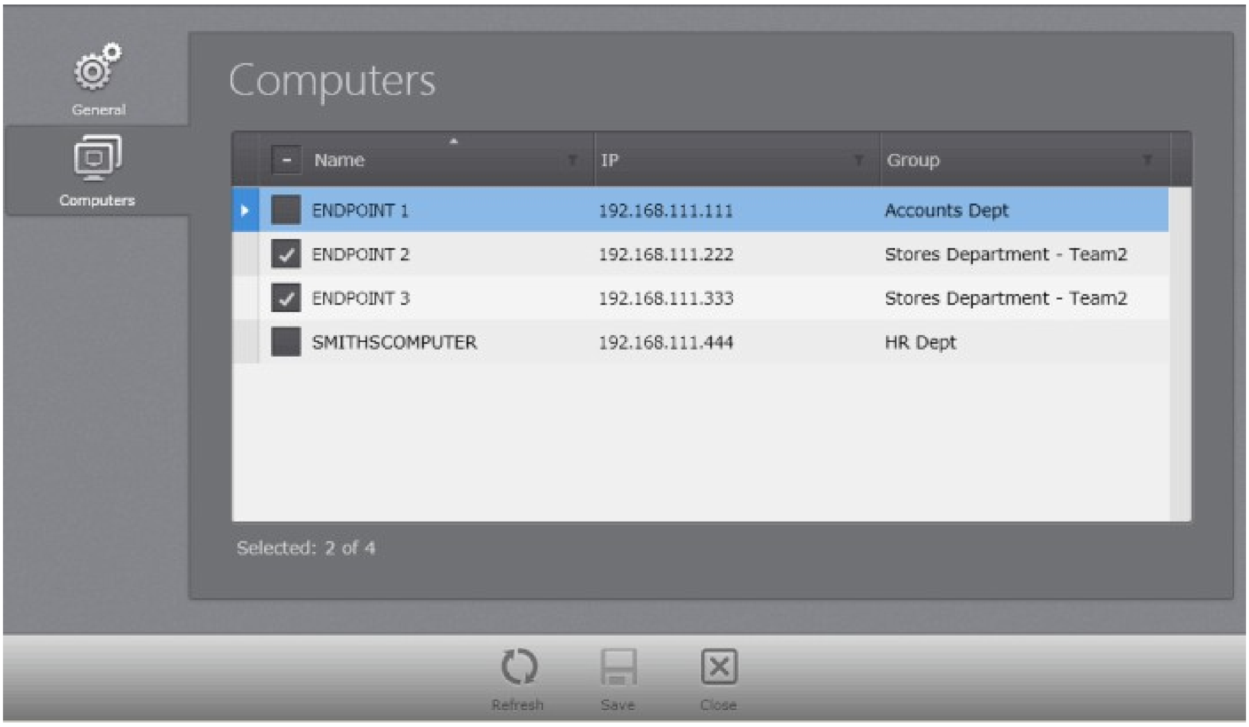
Alternatively, you can change the default security policy of a group directly by right clicking on it and selecting 'Apply Local Policy' or 'Apply Internet Policy' from the context sensitive menu and choosing the required policy from the sub menu or select the Groups, click Policy > 'Apply Local Policy', '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

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 they belong to, IP address. Endpoints that are member of the selected group are preselected.



Computers

☐ Name	IP	Group
□ ENDPOINT 1	192.168.111.111	Accounts Dept
☑ ENDPOINT 2	192.168.111.222	Stores Department - Team2
☑ ENDPOINT 3	192.168.111.333	Stores Department - Team2
□ SMITHSCOMPUTER	192.168.111.444	HR Dept

Selected: 2 of 4

  - 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. Running On-Demand Scan on Endpoint Groups

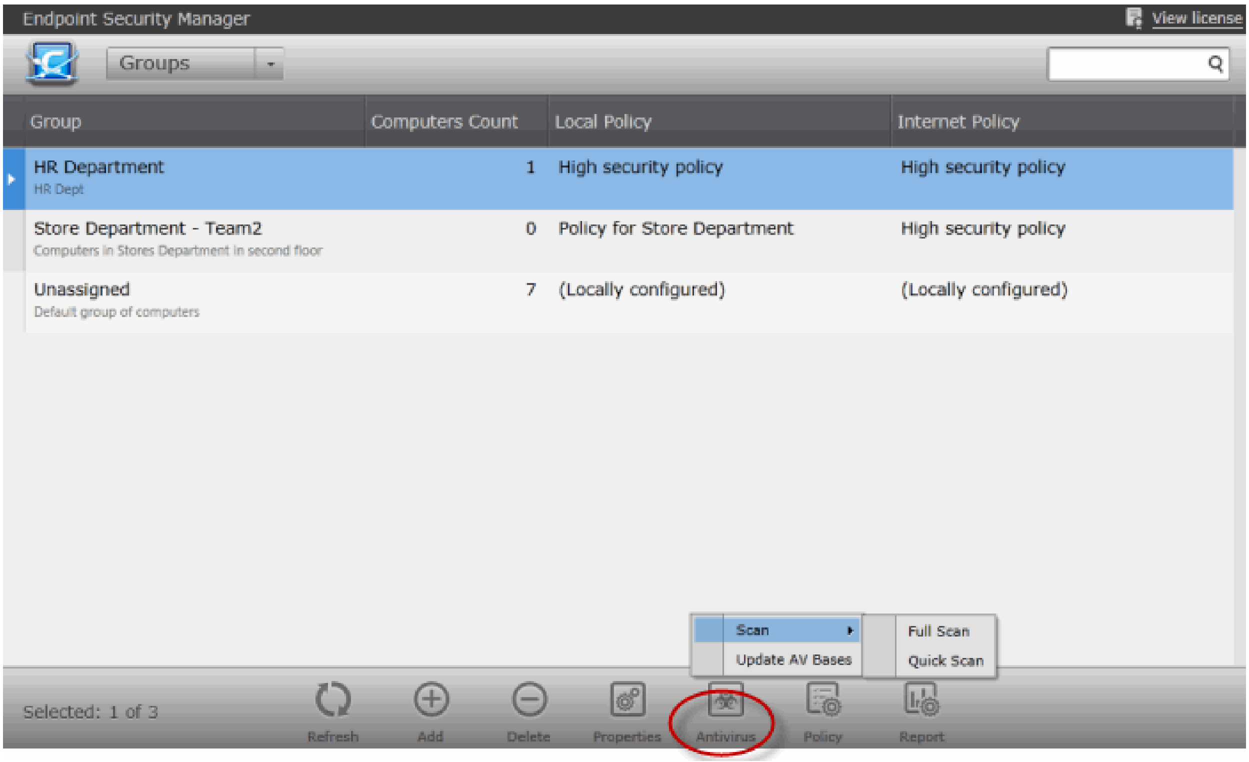
The 'Groups' area allows the administrator to run on-demand Antivirus (AV) scans on all the endpoints in selected Group(s) simultaneously. The administrator can choose to run a full scan or selected areas of the endpoints, by choosing a scan profile.

To run a full scan on the endpoints

1. Open the 'Groups' area by choosing Groups from the drop-down at the top left.
2. Select the 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 installed and AV enabled.

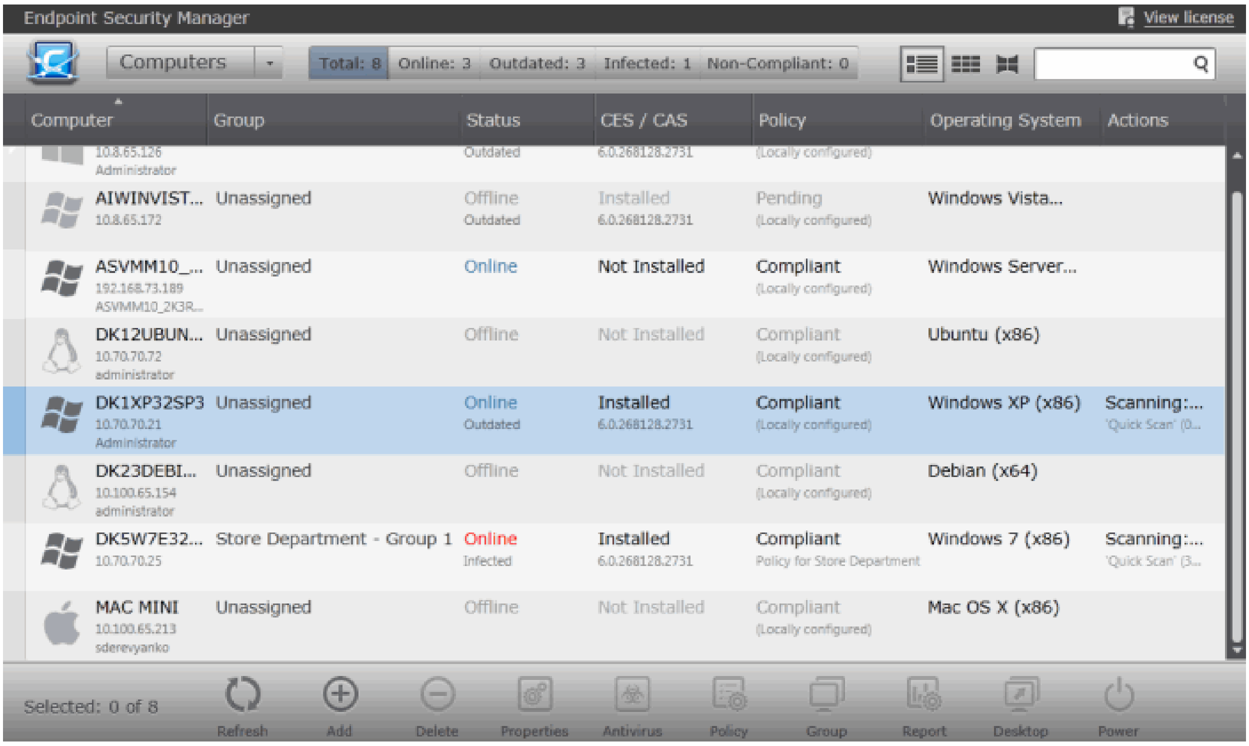
3. Click 'Antivirus' > 'Scan' > Full Scan/Quick Scan from the options at the bottom.



Group	Computers Count	Local Policy	Internet Policy
HR Department HR Dept	1	High security policy	High security policy
Store Department - Team2 Computers in Stores Department in second floor	0	Policy for Store Department	High security policy
Unassigned Default group of computers	7	(Locally configured)	(Locally configured)

Selected: 1 of 3

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



Total: 8 Online: 3 Outdated: 3 Infected: 1 Non-Compliant: 0

Computer	Group	Status	CES / CAS	Policy	Operating System	Actions
10.8.65.126 Administrator		Outdated	6.0.268128.2731	(Locally configured)		
AIWINVIST... 10.8.65.172	Unassigned	Offline Outdated	Installed 6.0.268128.2731	Pending (Locally configured)	Windows Vista...	
ASVMM10_... 192.168.73.189 ASVMM10_2K3R...	Unassigned	Online	Not Installed	Compliant (Locally configured)	Windows Server...	
DK12UBUN... 10.70.70.72 administrator	Unassigned	Offline	Not Installed	Compliant (Locally configured)	Ubuntu (x86)	
DK1XP32SP3 10.70.70.21 Administrator	Unassigned	Online Outdated	Installed 6.0.268128.2731	Compliant (Locally configured)	Windows XP (x86)	Scanning:... 'Quick Scan' (0...
DK23DEBI... 10.100.65.154 administrator	Unassigned	Offline	Not Installed	Compliant (Locally configured)	Debian (x64)	
DK5W7E32... 10.70.70.25	Store Department - Group 1	Online Infected	Installed 6.0.268128.2731	Compliant Policy for Store Department	Windows 7 (x86)	Scanning:... 'Quick Scan' (3...
MAC MINI 10.100.65.213 sderevyanko	Unassigned	Offline	Not Installed	Compliant (Locally configured)	Mac OS X (x86)	

Selected: 0 of 8

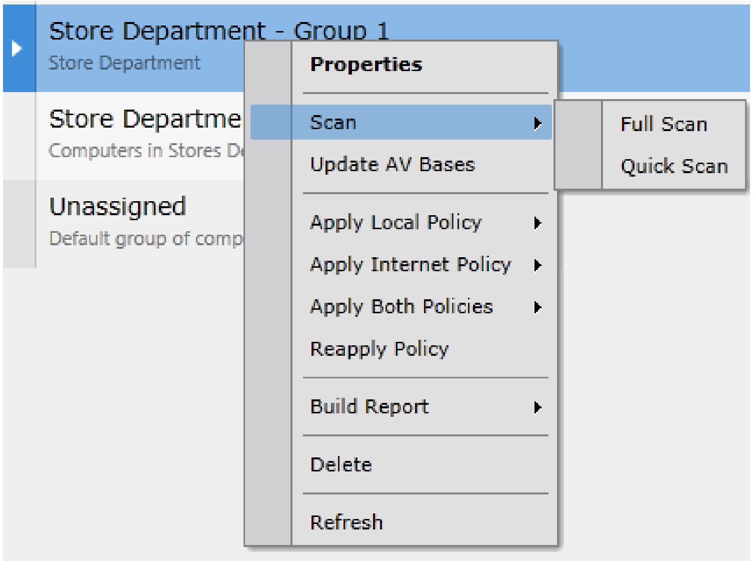
The administrator can also run the scans from the right click options with choices to select the areas to be scanned in the endpoints.

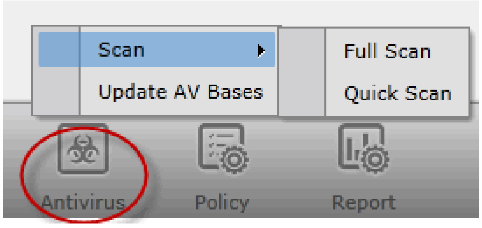
To run scan on selected areas of endpoints in a group

1. Open the 'Groups' area by choosing Groups from the drop-down at top left.
2. Select the 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 installed and AV enabled.

3. Right click and select 'Antivirus'> Scan from the context sensitive menu 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 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-72-1-451-4757-Custom-Scan-Settings.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.

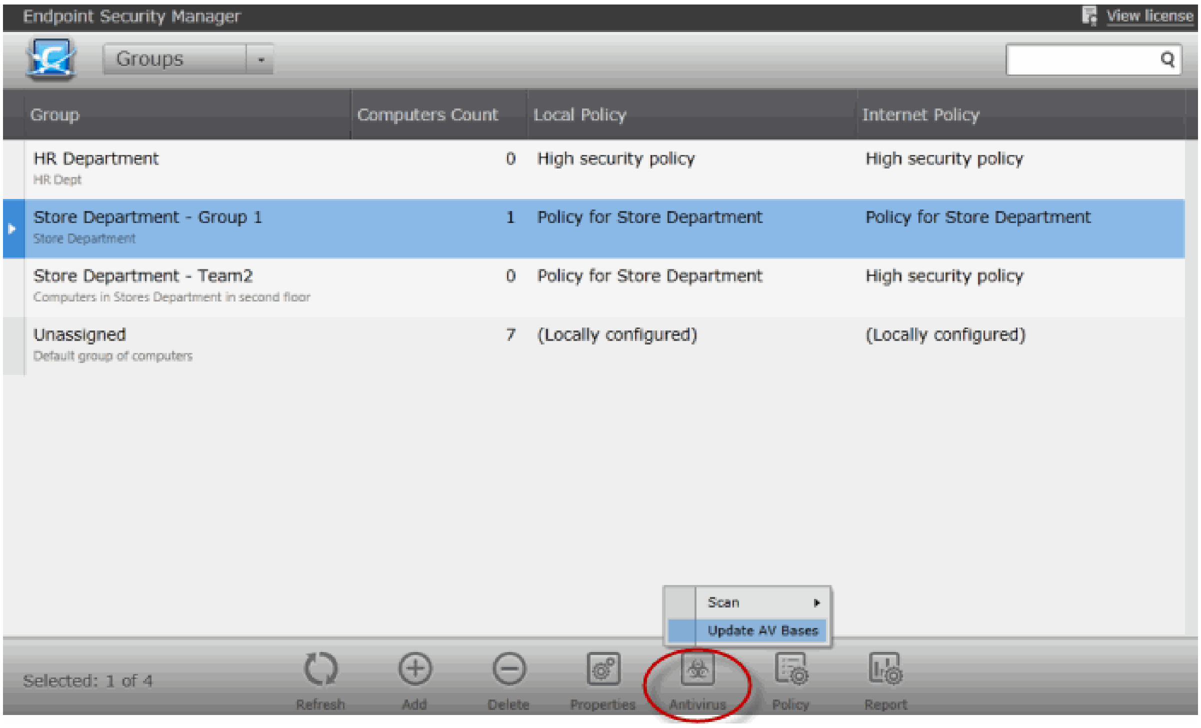
The results of the scan can be viewed as an Infection report from the Reports area - click 'Reports' then the 'Computer Infections'. The report can also be exported as a pdf file or a spreadsheet file for printing purposes. Refer to **Reports > Computer Infections** for more details.

4.4. 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), identified as outdated computers.

To update endpoints in a group

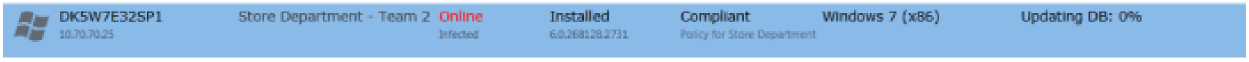
1. Open the 'Groups' area by choosing Groups from the drop-down at the top left.
2. Select the group(s) whose endpoints are to be updated. You can select multiple groups at once by pressing and holding the Ctrl or Shift key.



Group	Computers Count	Local Policy	Internet Policy
HR Department HR Dept	0	High security policy	High security policy
Store Department - Group 1 Store Department	1	Policy for Store Department	Policy for Store Department
Store Department - Team2 Computers in Stores Department in second floor	0	Policy for Store Department	High security policy
Unassigned Default group of computers	7	(Locally configured)	(Locally configured)

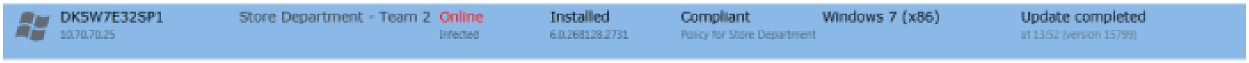
3. Click Update AV from the bottom or right click on a selected group and choose Update AV Bases from the context sensitive menu.

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



DK5W7E325P1 10.70.70.25	Store Department - Team 2	Online Infected	Installed 6.0.268128.2731	Compliant Policy for Store Department	Windows 7 (x86)	Updating DB: 0%

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



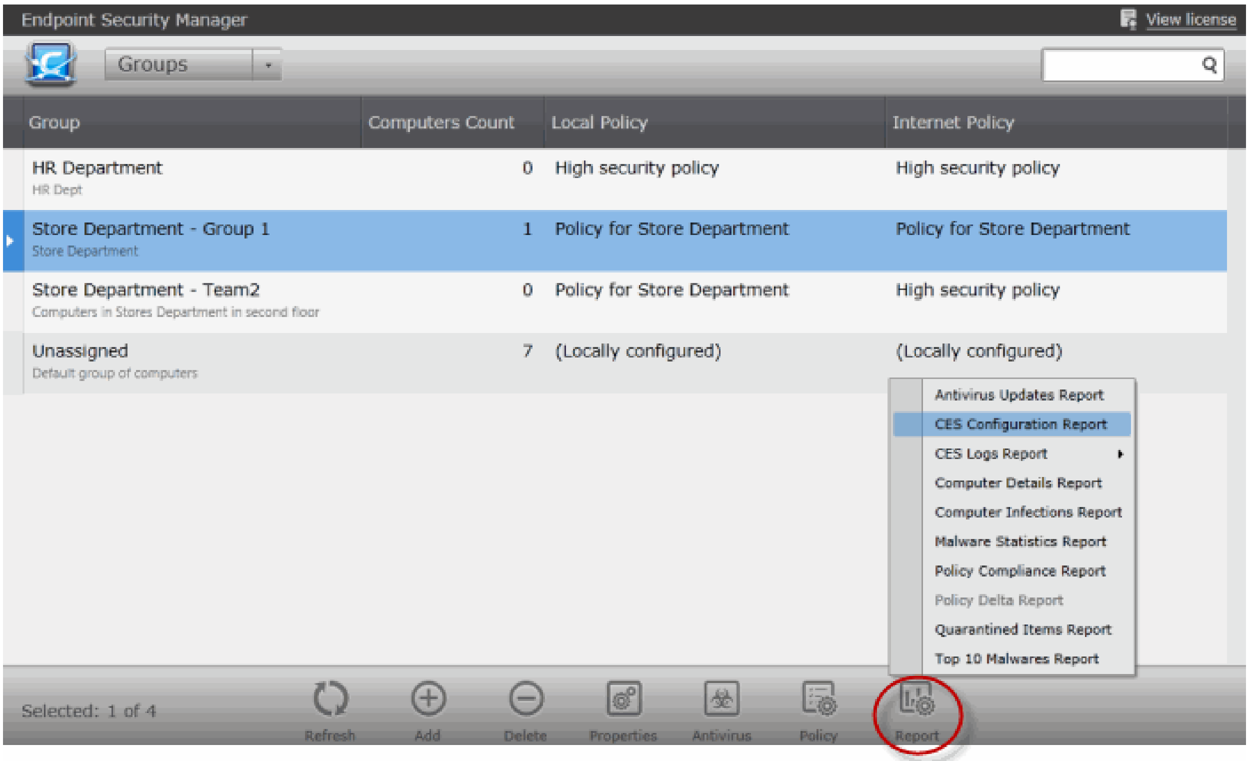
DK5W7E325P1 10.70.70.25	Store Department - Team 2	Online Infected	Installed 6.0.268128.2731	Compliant Policy for Store Department	Windows 7 (x86)	Update completed at 13:52 (version 15799)

4.5. Generating Reports for Selected Group

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

To generate reports on the endpoints in a group

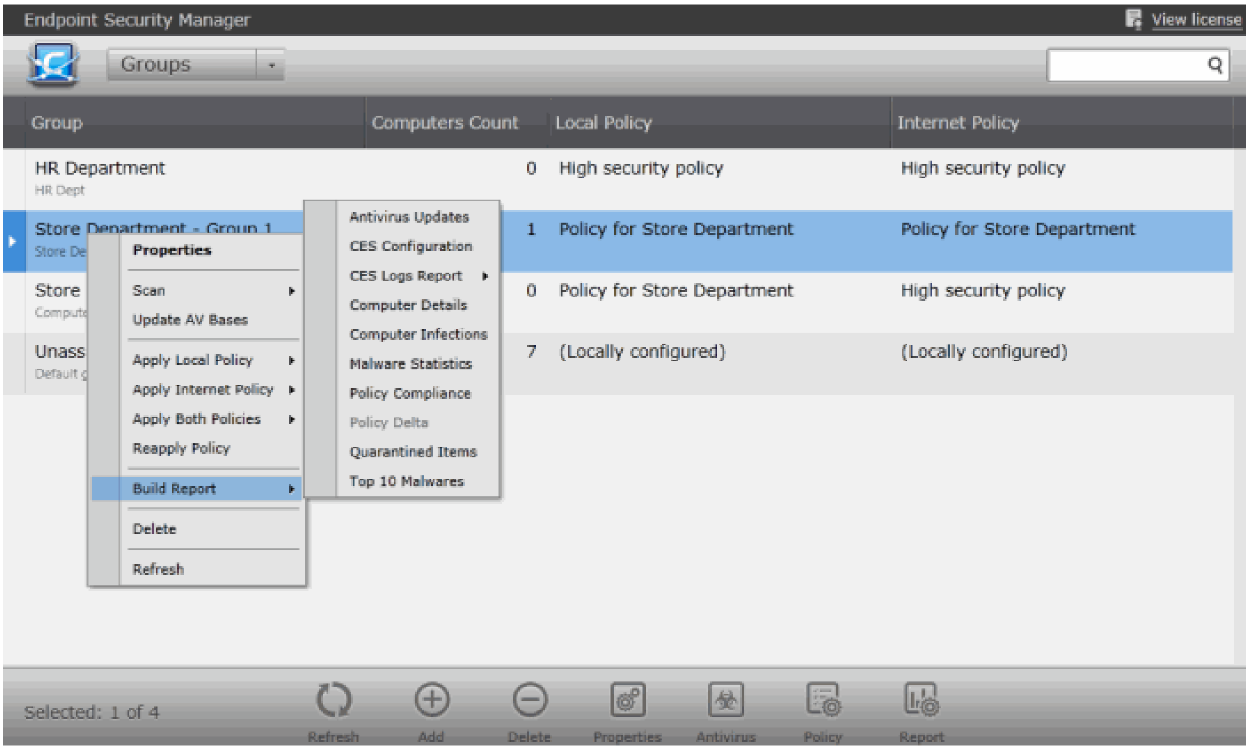
1. Open the 'Groups' area by choosing Groups from the drop-down at the top left.
2. Select the group(s) for which you wish to generate report. You can select multiple groups at once by pressing and holding the Ctrl or Shift key.



Group	Computers Count	Local Policy	Internet Policy
HR Department HR Dept	0	High security policy	High security policy
Store Department - Group 1 Store Department	1	Policy for Store Department	Policy for Store Department
Store Department - Team2 Computers in Stores Department in second floor	0	Policy for Store Department	High security policy
Unassigned Default group of computers	7	(Locally configured)	(Locally configured)

Selected: 1 of 4

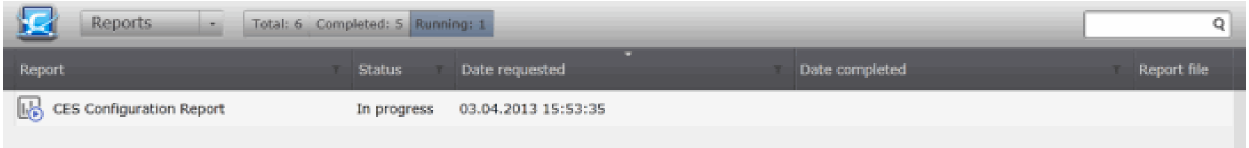
3. Click 'Report' and select the type of report to be generated. Alternatively, select the group(s), right click, choose 'Build Report' from the context sensitive menu and select the report to be generated.



Group	Computers Count	Local Policy	Internet Policy
HR Department HR Dept	0	High security policy	High security policy
Store Department - Group 1 Store De	1	Policy for Store Department	Policy for Store Department
Store Compute	0	Policy for Store Department	High security policy
Unass Default g	7	(Locally configured)	(Locally configured)

Selected: 1 of 4

The report generation will be started and the progress will be displayed in the Reports area.



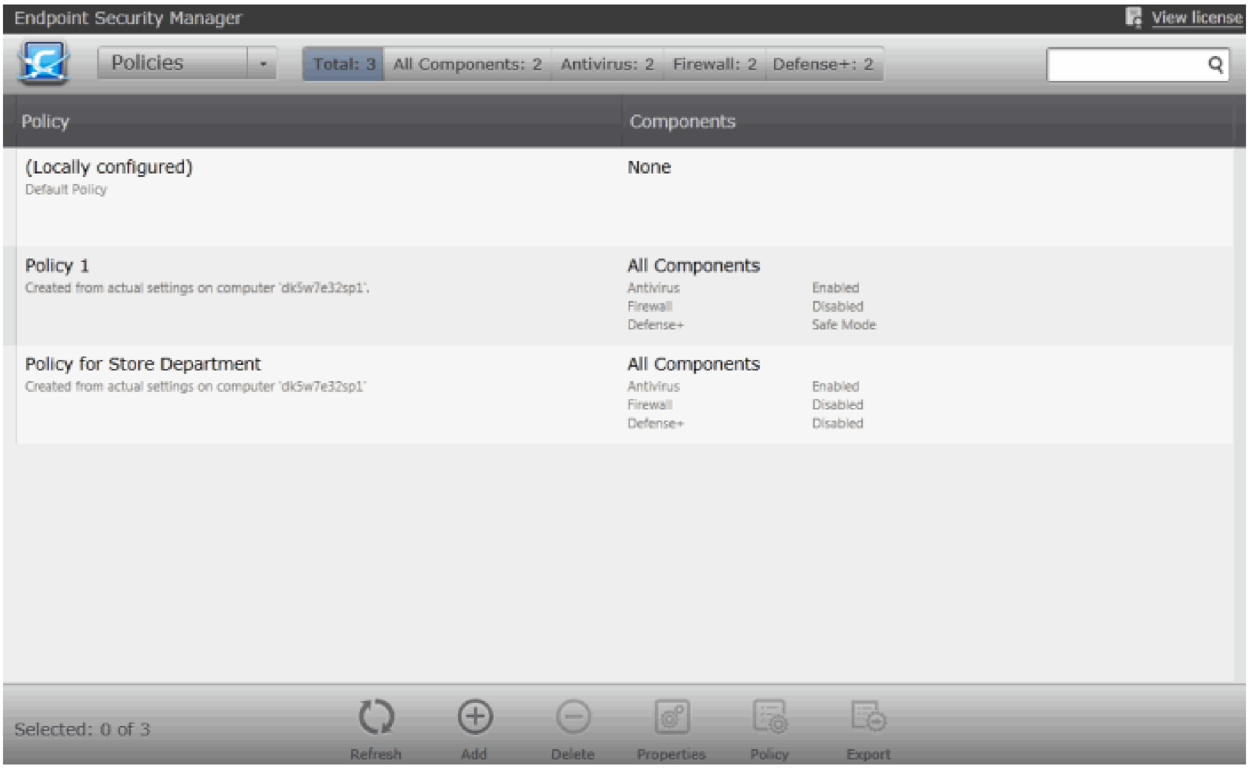
Report	Status	Date requested	Date completed	Report file
CES Configuration Report	In progress	03.04.2013 15:53:35		

On completion, the administrator can download the report from the Reports area. Refer to the Reports area for more details.

5. The Policies Area

A policy is the security configuration of Comodo Endpoint Security (CES) 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 import and manage security polices for endpoint machines.



Endpoint Security Manager

Policies

Total: 3 | All Components: 2 | Antivirus: 2 | Firewall: 2 | Defense+: 2

Policy	Components	
(Locally configured) Default Policy	None	
Policy 1 Created from actual settings on computer 'dk5w7e32sp1'.	All Components Antivirus Firewall Defense+	 Enabled Disabled Safe Mode
Policy for Store Department Created from actual settings on computer 'dk5w7e32sp1'	All Components Antivirus Firewall Defense+	 Enabled Disabled Disabled

Selected: 0 of 3

- **Create a new policy** - A step-by-step wizard that takes admins through the policy import, specification and deployment process.
- **View and managing security policies** - Allows administrators to view, reconfigure and export 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 configured and tested on a local machines via the standard CES interface.
- 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 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 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 installation. Only the agent applies the security policy settings to different components of the CES application and checks whether the application is compliant to policy.

- Each endpoint has two types of policy assigned to it: directly, or via the group that an endpoint is a member, 'Local Policy' and 'Internet Policy':
    - A 'local policy' which describes the CES security settings that will apply when the endpoint is within the local network.
    - An 'Internet policy' which 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. An endpoint can have any chosen policy and can be in either 'Remote' or 'Local' mode.
- 'Locally Configured' policy. 'Locally Configured' policy means that CES settings can be managed by the local user and policy compliance will not be enforced by ESM. Machines or groups with this policy will always report compliance status of 'OK'. Changes made to the CES settings on to the machine with 'Locally Configured' policy are dynamically stored in the policy. If a machine is switched back to 'Locally Configured' policy from an applied security policy, the last stored local CES configuration settings will be restored to it.

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. The new policies can be created by:

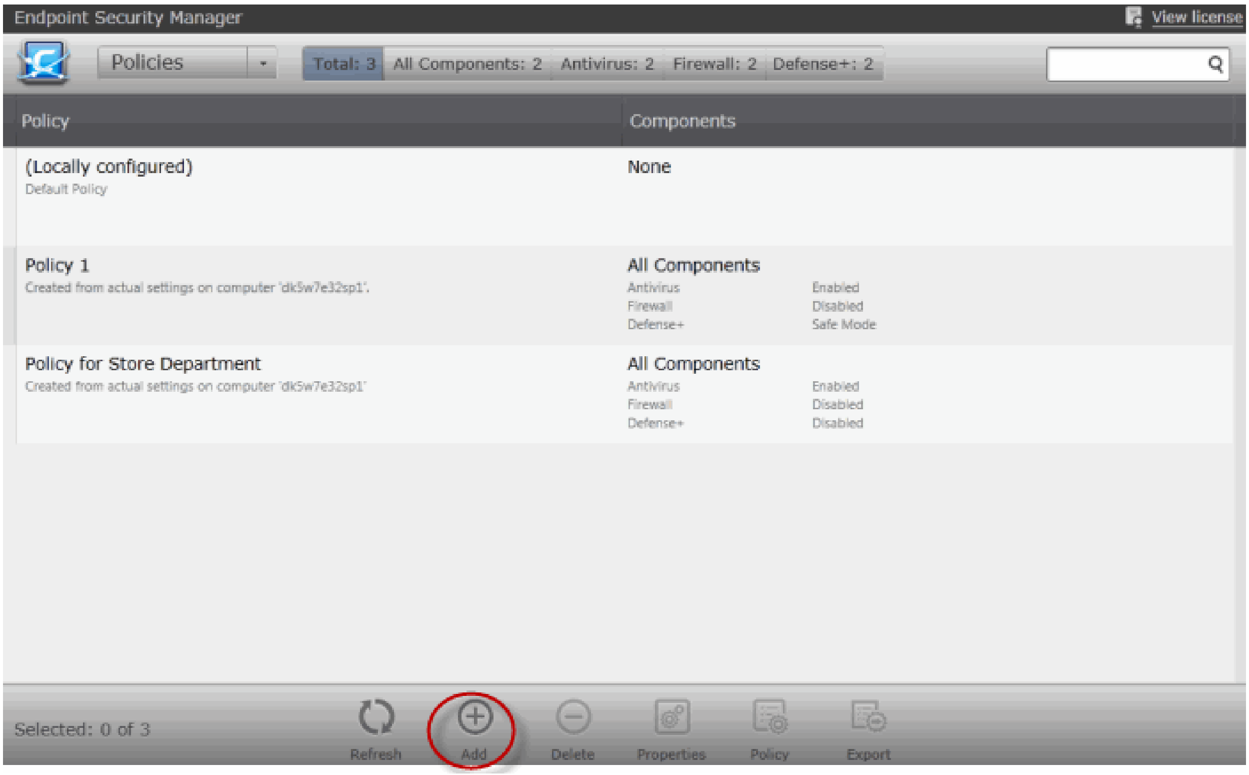
- Importing the local security settings from a computer.
- Using another, pre-existing, policy as a base.
- Importing from a saved .xml file.

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.

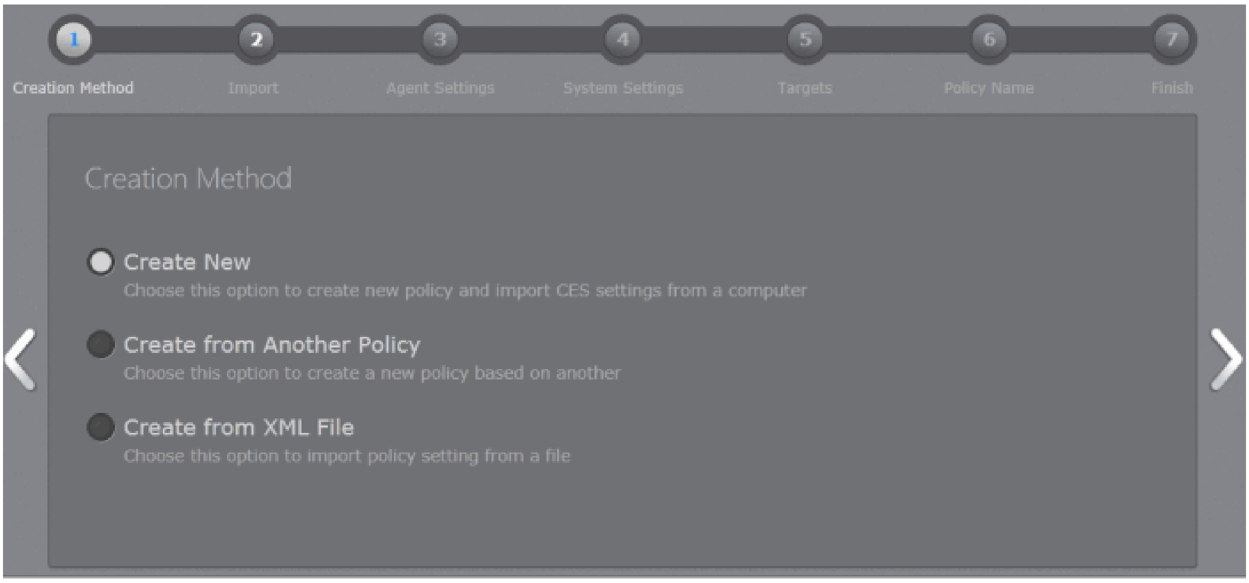
To start the 'Create Policy' wizard

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



Policy	Components
(Locally configured) Default Policy	None
Policy 1 Created from actual settings on computer 'dk5w7e32sp1'.	All Components Antivirus Enabled Firewall Disabled Defense+ Safe Mode
Policy for Store Department Created from actual settings on computer 'dk5w7e32sp1'	All Components Antivirus Enabled Firewall Disabled Defense+ Disabled

The wizard will start with Step 1- Create. The remaining 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.



Creation Method

○ Create New
Choose this option to create new policy and import CES settings from a computer

● Create from Another Policy
Choose this option to create a new policy based on another

● Create from XML File
Choose this option to import policy setting from a file

Step 1 – Create a New Policy

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.

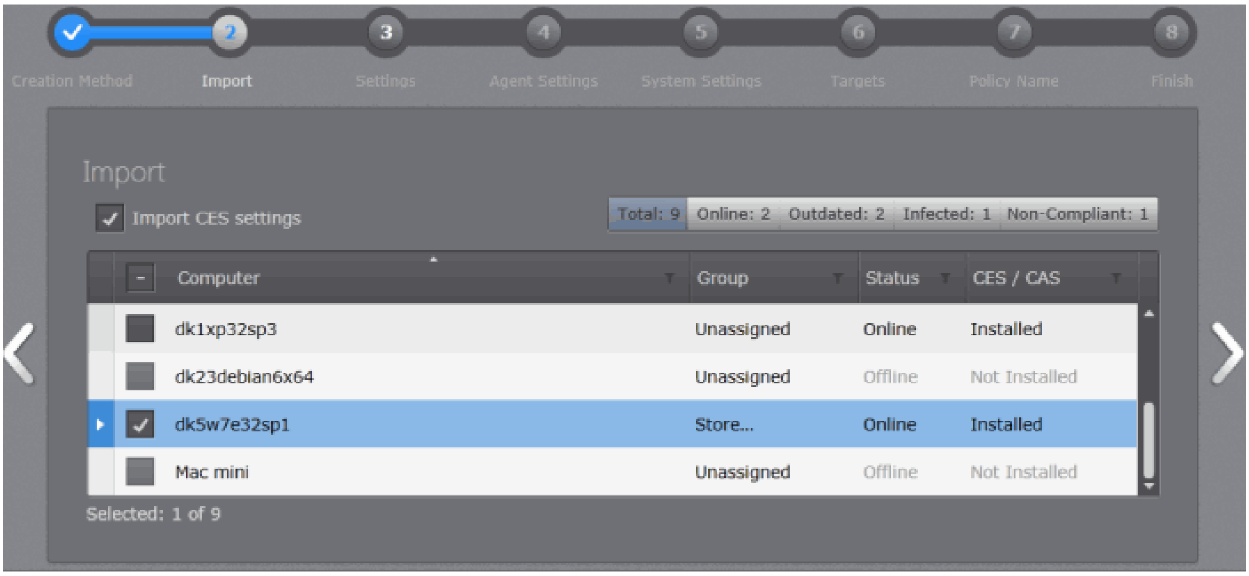
Tip: You might create a policy from another policy if you want to exclude a CES component from policy but use the settings in other components, or change the agent-specific settings of the policy(such as to have a different compliance polling interval, or to disallow local mode access) for a particular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



Import

☑ Import CES settings

Total: 9 | Online: 2 | Outdated: 2 | Infected: 1 | Non-Compliant: 1

	Computer	Group	Status	CES / CAS
□	dk1xp32sp3	Unassigned	Online	Installed
□	dk23debian6x64	Unassigned	Offline	Not Installed
☑	dk5w7e32sp1	Store...	Online	Installed
□	Mac mini	Unassigned	Offline	Not Installed

Selected: 1 of 9

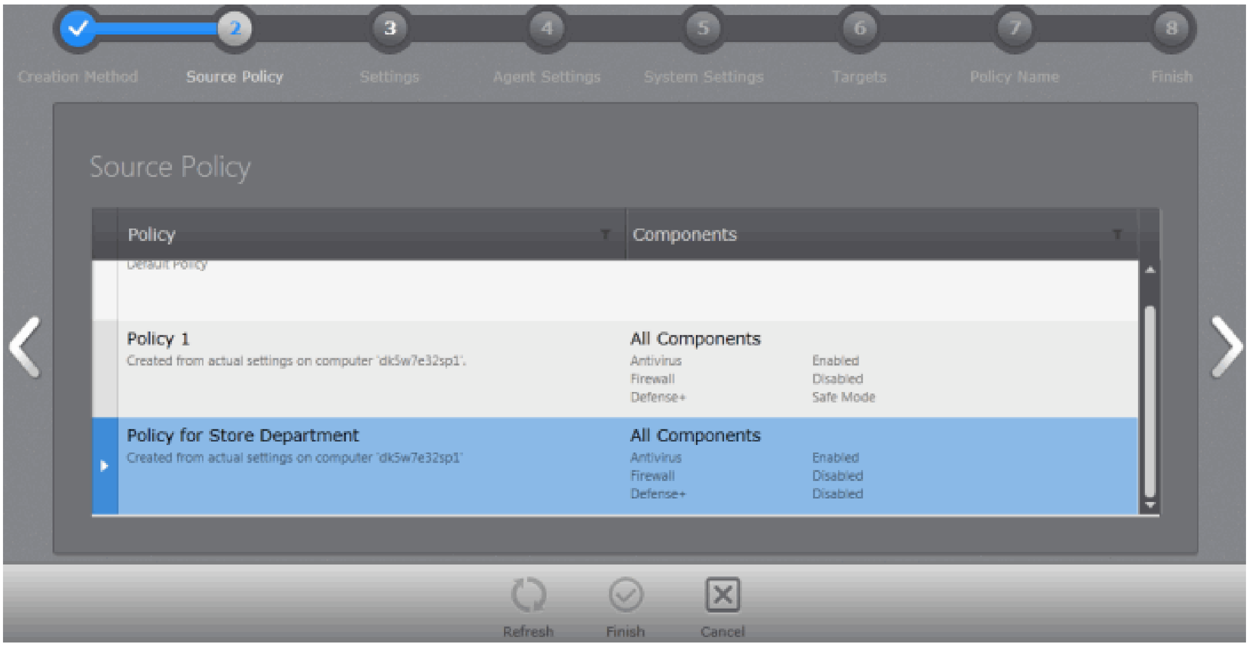
- Click the filter icon in the 'Computer' column header to search for a particular endpoint, enter its name partially or fully and click 'Apply'.
- Click the filter icon in the 'Group' column header to search for an endpoint belonging to particular group, enter its name partially or fully and click 'Apply'.
- Click the filter icon in the 'Status' column header to search for an endpoint with a particular status, select the status and click 'Apply'.
- Click the filter icon in the 'CES Mode' column header to search for endpoints with CES in Local, Remote or Unknown mode and click 'Apply'.
- Click 'Reset' to display all the items.
- Select the computer from which you wish to import the settings. The computer should have CES installed and be in local mode, configured as per requirements, and should be online to enable ESM to import the settings.
- Options:
  - **Force source computer to be remotely managed after policy import is complete** - To configure the settings locally, the source computer would have been switched to local administration mode. If you wish the computer to be switched to Remote administration mode after policy is read, select this option.
- Click the right arrow to move to **Step 3 – Settings**.

Importing from Another Policy

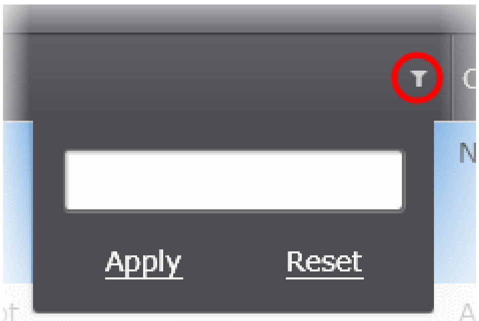
- Choose 'Create from Another Policy' if you wish to import the security settings from an existing Policy and click the right arrow to move to Step 2 - Selecting Source Policy.

Step 2 - Selecting Source Policy

A list of all the existing policies with their descriptions and the CES components configured by them are displayed.



Policy	Components
Default Policy	
Policy 1 Created from actual settings on computer 'dk5w7e32sp1'.	All Components Antivirus Enabled Firewall Disabled Defense+ Safe Mode
Policy for Store Department Created from actual settings on computer 'dk5w7e32sp1'	All Components Antivirus Enabled Firewall Disabled Defense+ Disabled

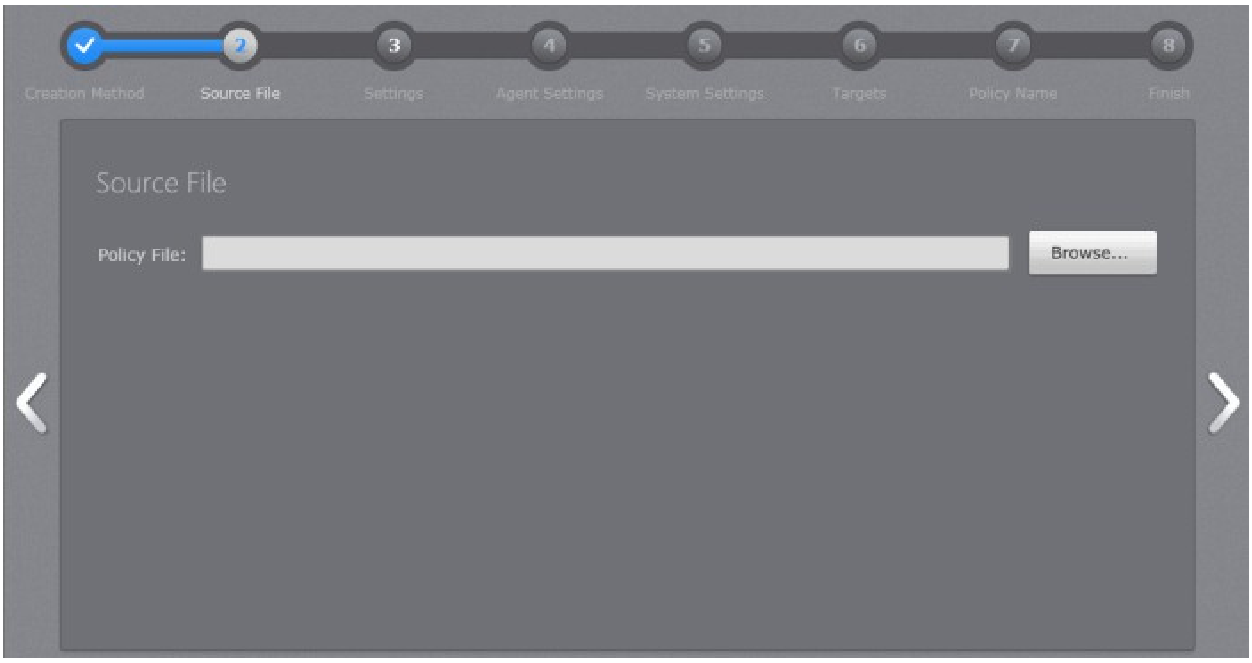


- Click the filter icon in the respective column header to search for a particular policy or component, enter its name partially or fully click 'Apply'.
- Click 'Reset' to display all the items.
- Select the source policy from which you wish to create a new policy and click the right arrow to move to **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.

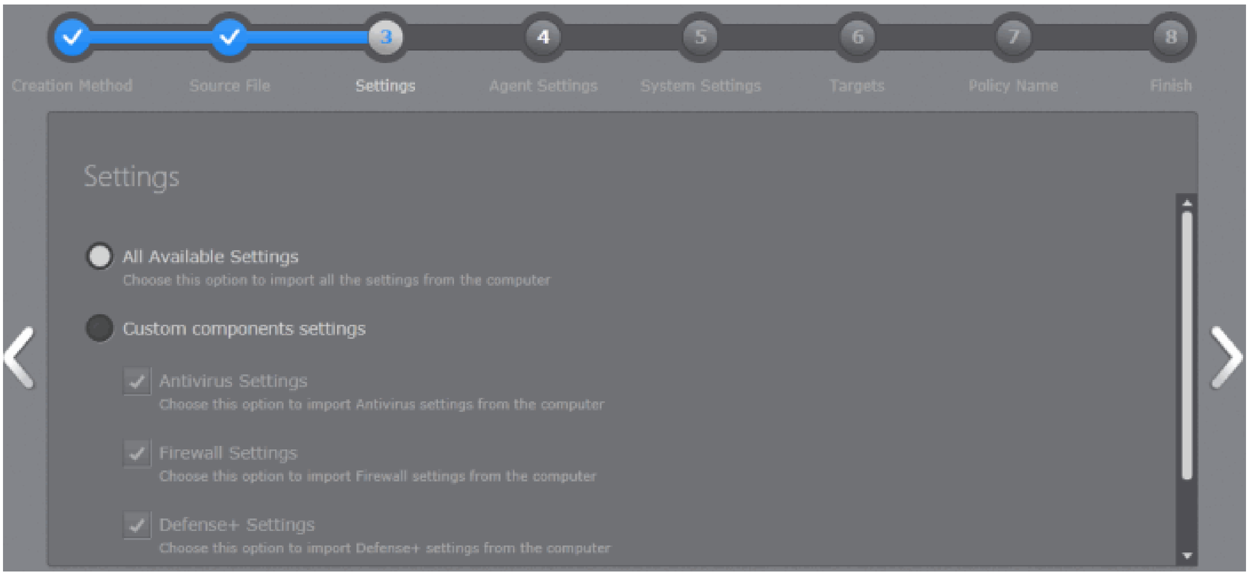
Step 2 - Selecting Source File



- 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 - CES Settings

The next step is to select the components of CES for which the security settings are to be imported into the policy.



Settings

○ All Available Settings
Choose this option to import all the settings from the computer

● Custom components settings

☑ Antivirus Settings
Choose this option to import Antivirus settings from the computer

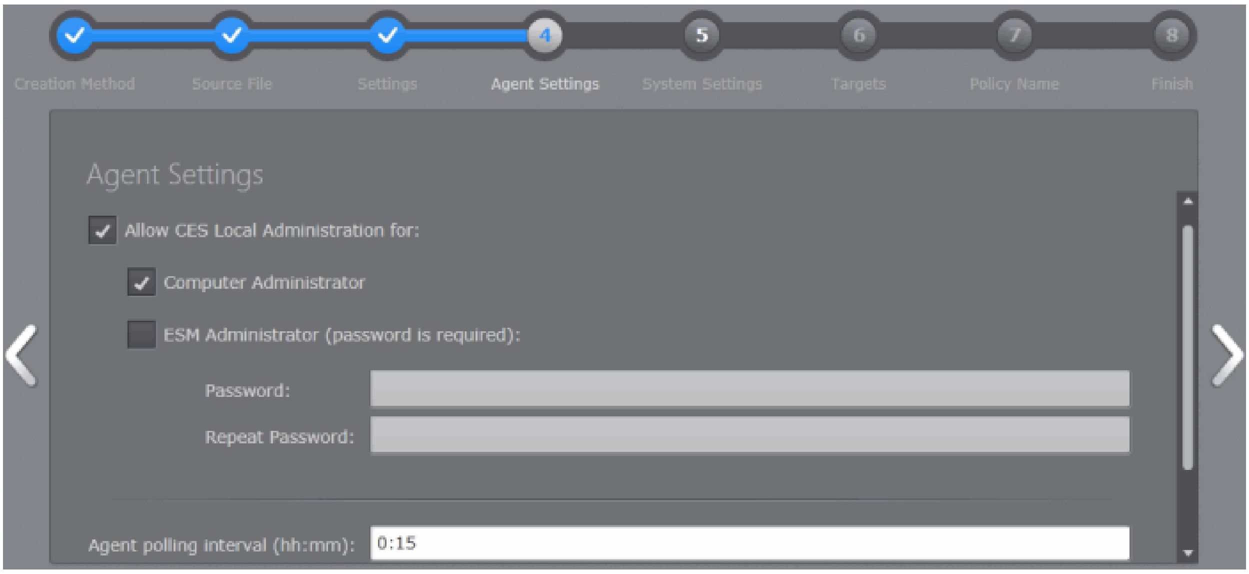
☑ Firewall Settings
Choose this option to import Firewall settings from the computer

☑ Defense+ Settings
Choose this option to import Defense+ settings from the computer

- **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 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.
  - **Include Trusted Vendors** - Imports trusted vendors, if any, from the source policy.
  - **Include Trusted Files** - Imports trusted files, if any, from the source policy.
- 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 Settings

☑ Allow CES Local Administration for:

☑ Computer Administrator

□ ESM Administrator (password is required):

Password:

Repeat Password:

Agent polling interval (hh:mm): 0:15

- **Allow CES Local Administration** - Configures the agent to allow the CES 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 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 to local administration mode.
- **Local Server Address** - The administrator can specify the address of the server machine in the local network, on which the ESM central service is installed.
- **Internet Server Address** - The administrator can specify the address of the external server on which the ESM central service is installed if the endpoint should connect to the ESM server through Internet.
- **Policy compliance polling interval** - The administrator can set the time interval (in hours and minutes) for the agent to periodically check whether the CES 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).

Tip: Local Server Address and Internet Server Address values are used by the Agent to determine when Local Policy or Internet Policy should be applied. What's more, these addresses have a priority over addresses that are in the Server Network Addresses list specified in the Configuration Tool such that:

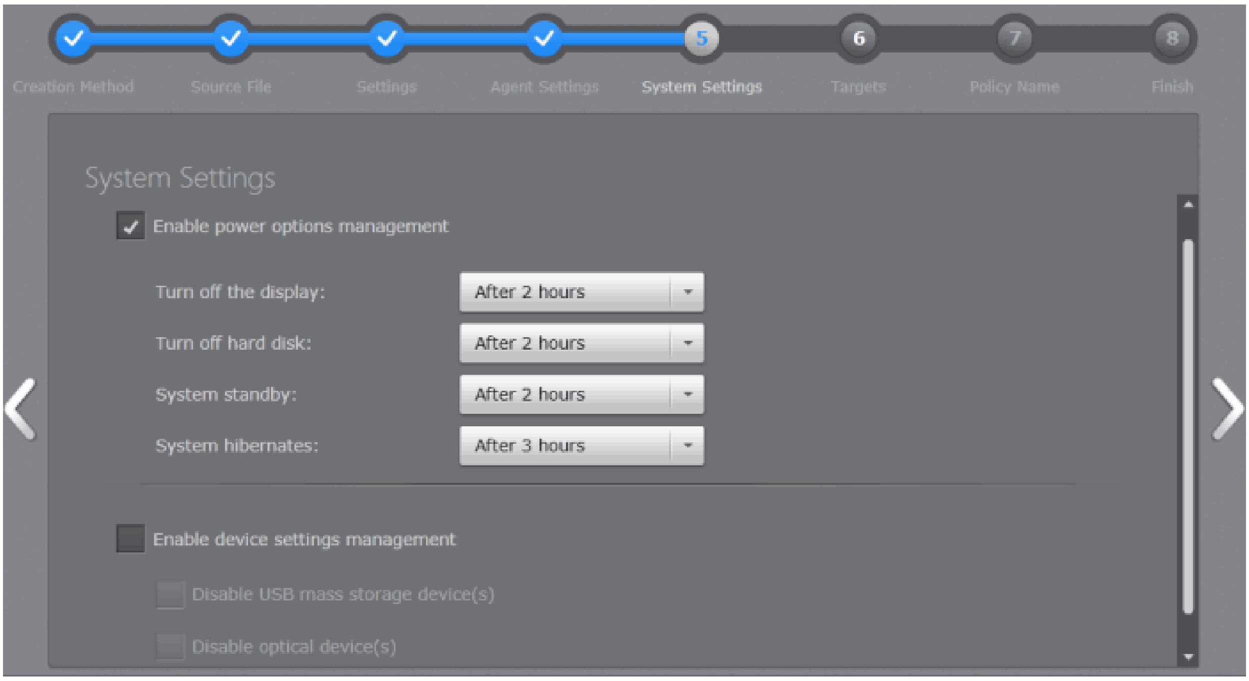
1. The Local Server Address value, mandatory in policy settings, specifies that if this connection is established Local Policy should be applied.
2. Internet Server Address value is optional in policy settings. If specified it is tried to be reached ONLY if the specified local address connection fails, Internet Policy should be applied.

If none of these addresses succeeded or if Internet Server Address value wasn't specified, the Agent will try the remaining hosts in the Server Network Addresses list, applying the corresponding policy based upon analysis per RFC 3330 of a connection succeeding via a special use address as indicating Local policy, and a public address indicating Internet policy.

- 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 at the target computers, for which the policy has to be applied.



System Settings

☑ Enable power options management

Turn off the display: After 2 hours

Turn off hard disk: After 2 hours

System standby: After 2 hours

System hibernates: After 3 hours

□ Enable device settings management

□ Disable USB mass storage device(s)

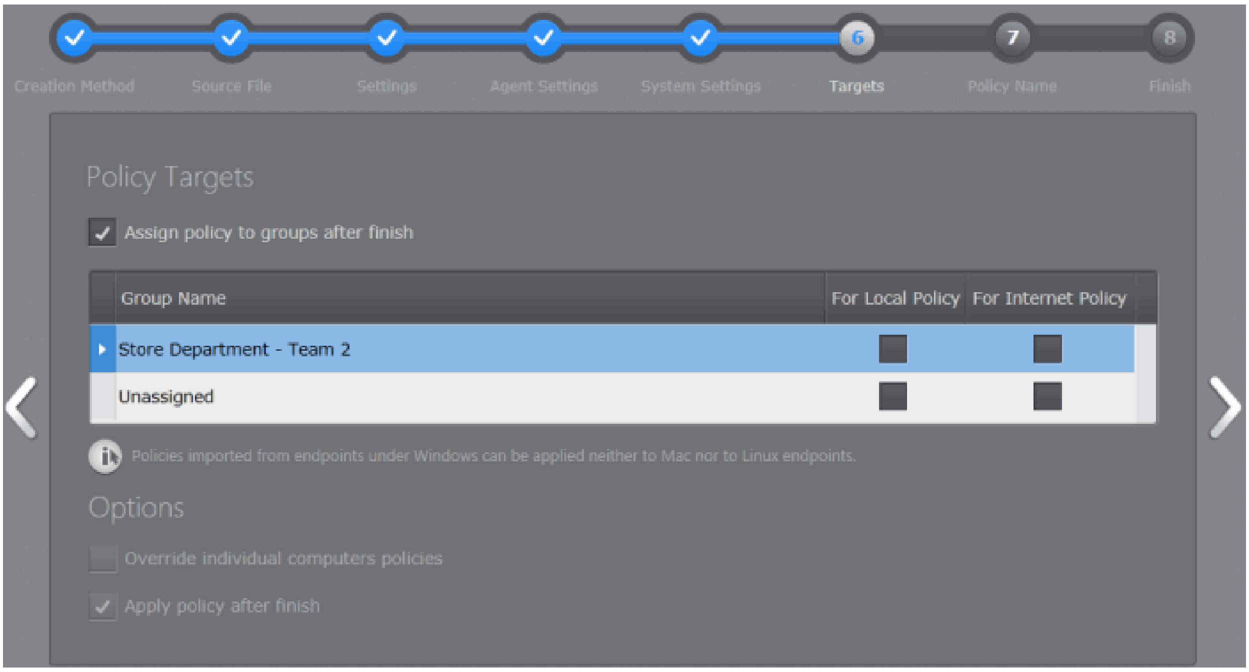
□ Disable optical device(s)

- **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.
- **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.
  - **Disable floppy device(s)** - Selecting this option will disable floppy devices at the target computers.

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) onto which the created policy has to be applied.



Policy Targets

☑ Assign policy to groups after finish

Group Name	For Local Policy	For Internet Policy
Store Department - Team 2	□	□
Unassigned	□	□

Policies imported from endpoints under Windows can be applied neither to Mac nor to Linux endpoints.

Options

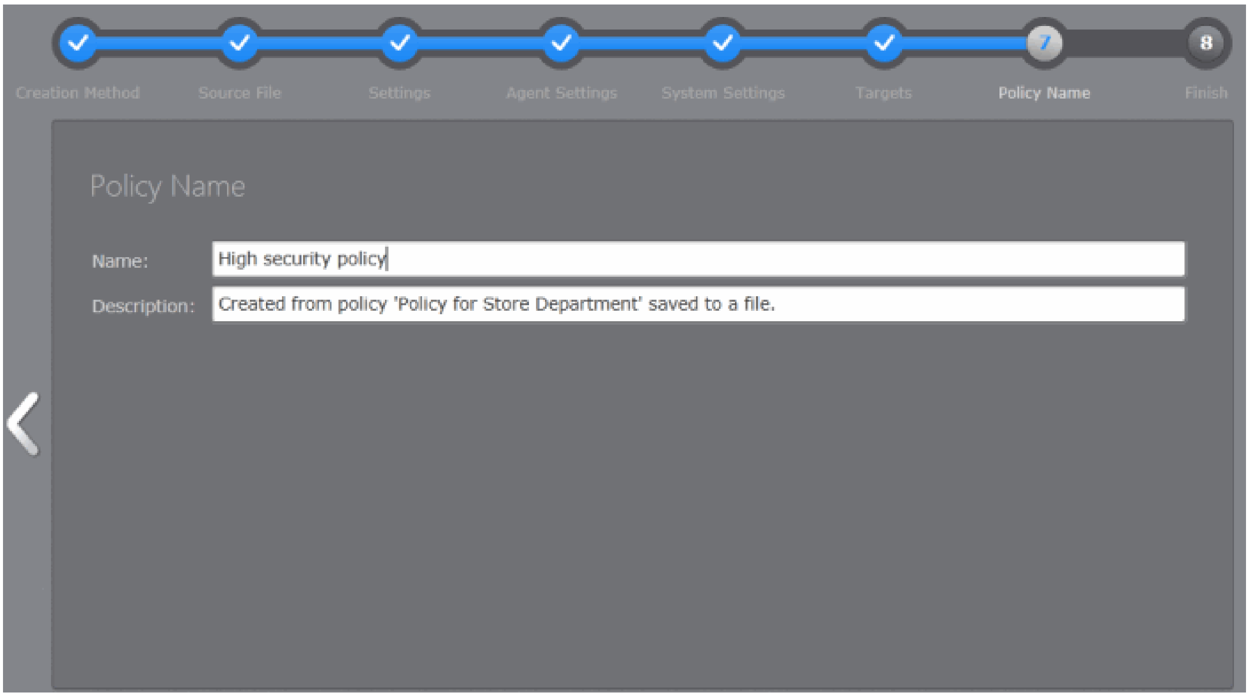
□ Override individual computers policies

☑ Apply policy after finish

- 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) of computers connected through the local network you wish to apply the new policy, select 'For Local Policy' check box.
- For the 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** - Selecting this option will apply the new policy onto target computers in the selected groups that currently have individual policies that differ from the group policy, thereby reverting their policies to come from their group membership.
  - **Apply policy after finish** - Selecting this option will apply newly created policy to all it's targets right after policy creation is finished.
- 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.



Policy Name

Name: High security policy

Description: Created from policy 'Policy for Store Department' saved to a file.

- **Name** - Enter a name according to criteria deemed suitable to the security settings.
- **Description** - Enter short text that best describes the policy.
- Make your selection and click the 'Finish' icon ✓ or swipe the screen to left to complete the policy creation process. On completion:
    - The 'Policy' interface will open with the new policy added.

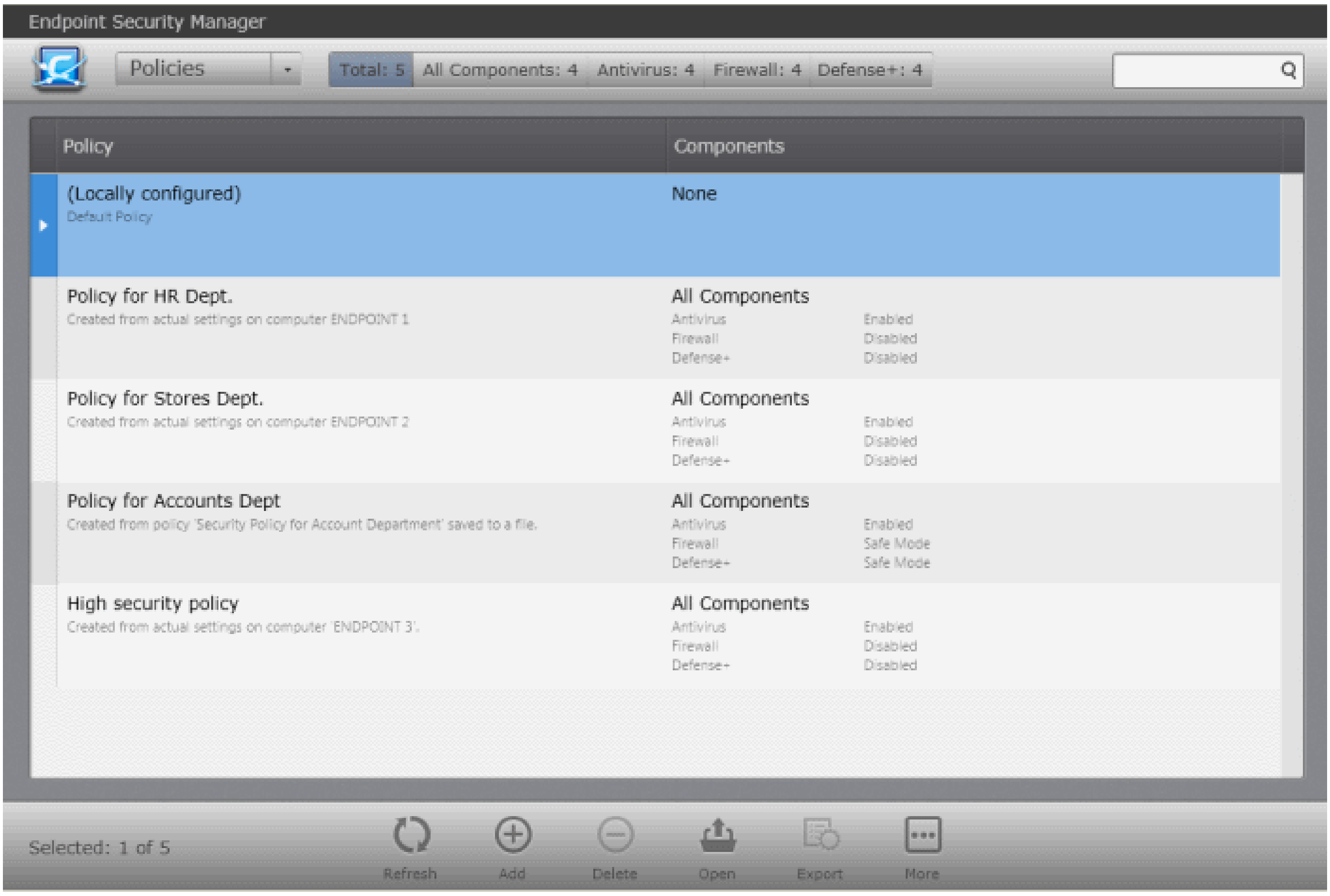
The new policy will be applied to the target computers selected in step 6 as per the options selected in the same.

5.2. Editing a Security Policy

The 'Policies' interface enables the administrator to:

- View a list of all policies along with their descriptions and the CES component covered by the policy.
- View and modify the details of any policy - including name, description, CES components, target computers and whether the policy should allow local configuration.
- Configure various settings such as Antivirus settings, Firewall settings, Defense+ settings, General CES settings, Agent settings and System 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:



Policy	Components
(Locally configured) Default Policy	None
Policy for HR Dept. Created from actual settings on computer ENDPOINT 1	All Components Antivirus Enabled Firewall Disabled Defense+ Disabled
Policy for Stores Dept. Created from actual settings on computer ENDPOINT 2	All Components Antivirus Enabled Firewall Disabled Defense+ Disabled
Policy for Accounts Dept Created from policy 'Security Policy for Account Department' saved to a file.	All Components Antivirus Enabled Firewall Safe Mode Defense+ Safe Mode
High security policy Created from actual settings on computer 'ENDPOINT 3'.	All Components Antivirus Enabled Firewall Disabled Defense+ Disabled

At the top of the interface a summary of policies including the total number of policies, the number of components used for the policies are displayed.

To search for a particular policy, enter the name of the policy fully or partially in the search box at the top right side of the interface and either press the enter button or wait for few seconds for the searched policy to be displayed. Delete the entered text in the search box to view all the policies again.

View All Policies Interface - Table of Column Descriptions

Column Heading	Description
Policy	Displays the name of the Policy.
Components	Indicates the components of CES for which the policy applies the configuration settings.

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, edit 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

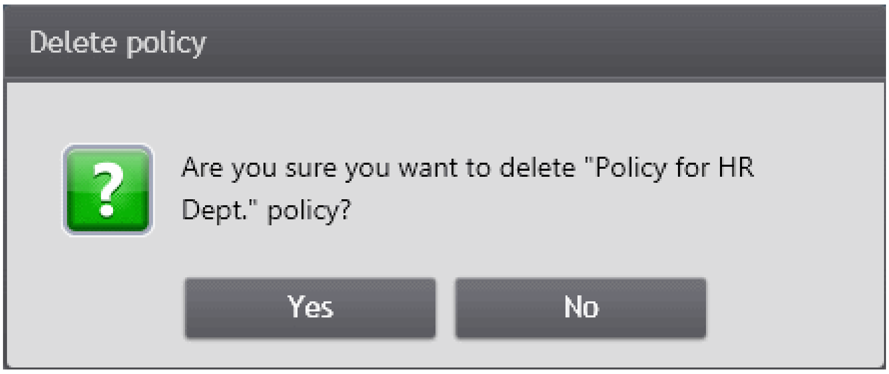
- Select the policy by clicking or touching the desired policy from 'Policies' interface to highlight it. Click the Export icon . Alternatively, right click on the selected policy and select 'Export...' from the context sensitive menu. The Windows 'Save As' dialog will appear.
- Select the destination 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.



Are you sure you want to delete "Policy for HR Dept." policy?

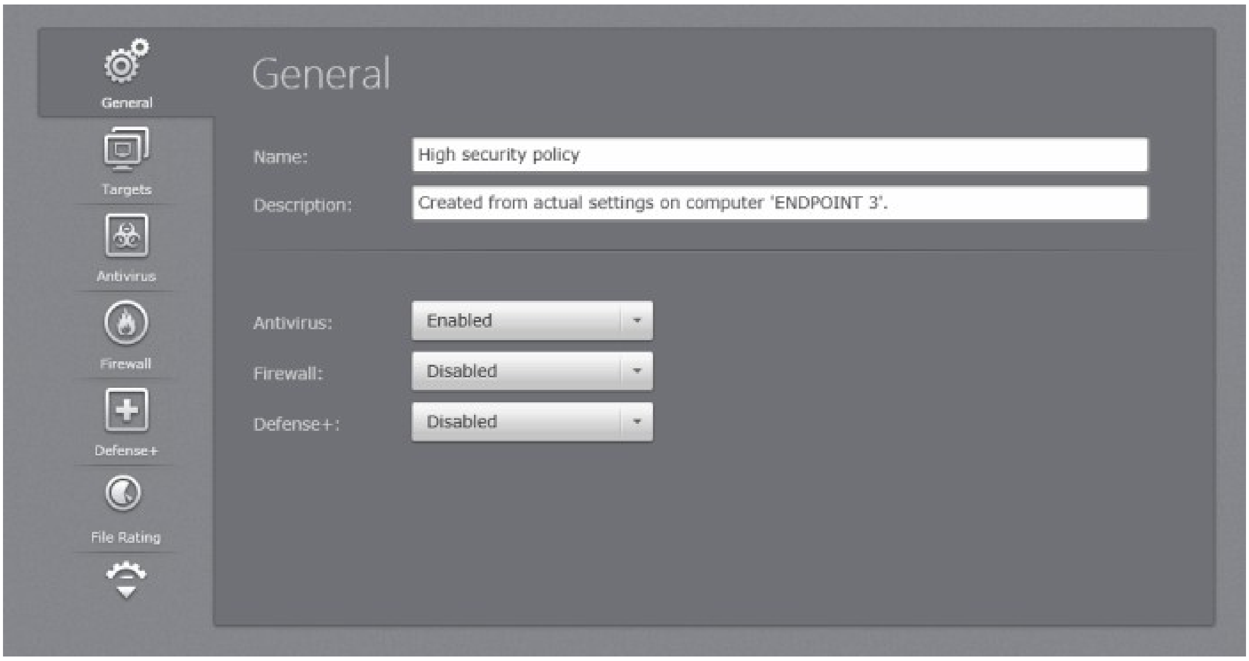
- Click 'Yes' to remove the selected item(s).

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.

Tip: Hold Shift or CTRL to select multiple items.

Viewing details and reconfiguring a policy

Selecting a policy and clicking the Properties 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 settings, File Rating, Agent settings and System settings for the selected policy. The policy can also be assigned to other groups from this interface.



General

Name: High security policy

Description: Created from actual settings on computer 'ENDPOINT 3'.

Antivirus: Enabled

Firewall: Disabled

Defense+: Disabled

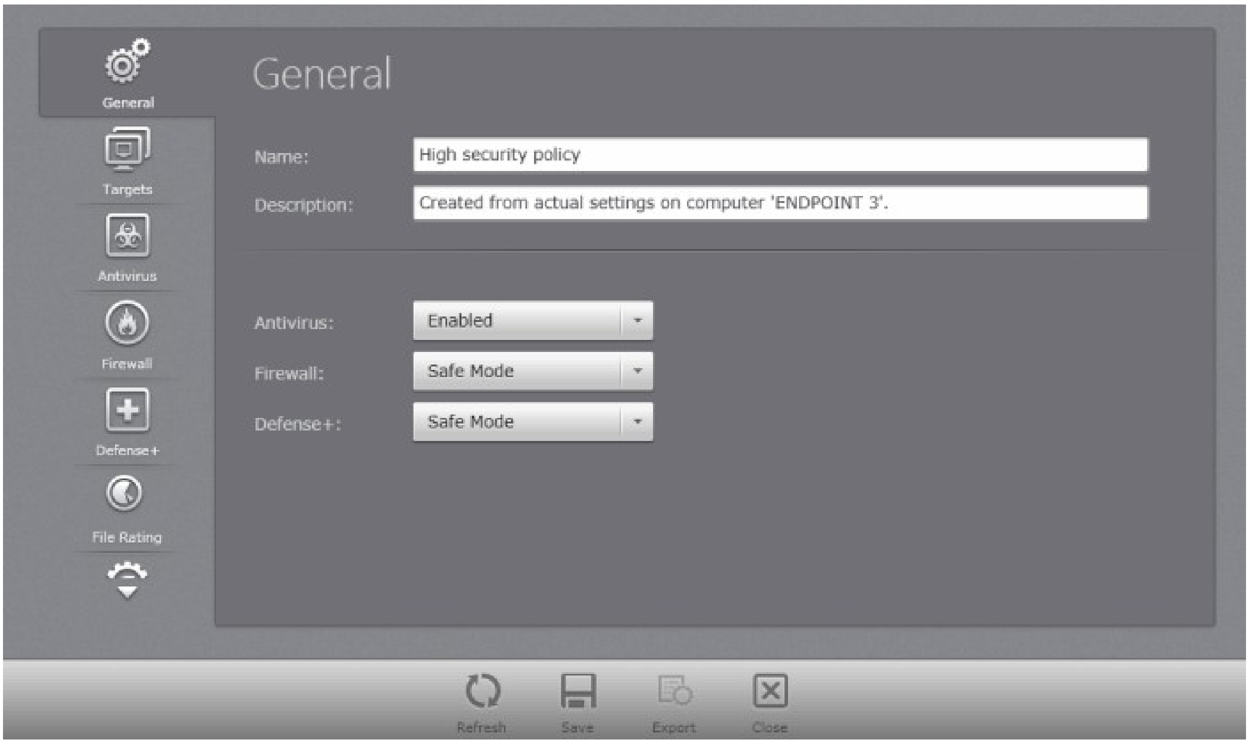
Refer to the following sections for more details.

- **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 Antivirus settings for the policy.
- **Firewall Settings** - Enables the administrator to configure Firewall settings for the policy.
- **Defense+ Settings** - Enables the administrator to configure Defense+ settings for the policy.
- **File Rating** - Enables the administrator to configure File Rating settings for the policy.
- **General CES Settings** - Enables the administrator to configure General CES settings for the policy.
- **Agent Settings** - Enables the administrator to configure the ESM agent deployed onto the endpoints as per the policy.
- **System Settings** - Enables the administrator to Power and Device management settings fro the policy.

The administrator can switch between these areas by using the up or down arrow located at the top and bottom in the left pane.

5.2.1. General Properties

The General screen shows the name and description of the policy as well as the CES 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

Name: High security policy

Description: Created from actual settings on computer 'ENDPOINT 3'.

Antivirus: Enabled

Firewall: Safe Mode

Defense+: Safe Mode

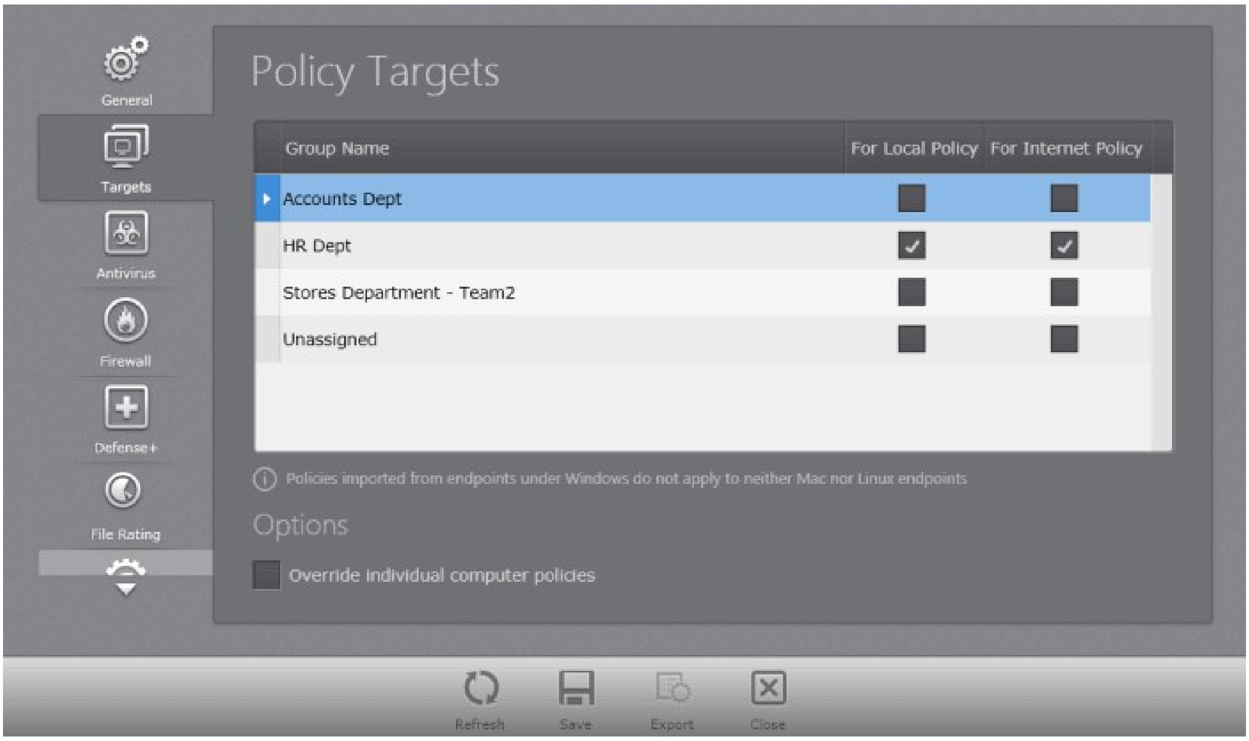
To change these details, the administrator can directly edit the respective text boxes in the upper pane and click the 'Save' icon at the bottom of the page. The lower pane displays the details of the security settings. You can change the security settings in this screen or in the '**Antivirus Settings**', '**Firewall Settings**' and '**Defense+ Settings**' screens for more granular configuration.

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.
- Remove the policy from already applied groups.

To open the interface, click on the 'Targets' icon in the left pane. All the groups configured in CESM will be displayed.



Policy Targets

Group Name	For Local Policy	For Internet Policy
Accounts Dept	□	□
HR Dept	☑	☑
Stores Department - Team2	□	□
Unassigned	□	□

Policies imported from endpoints under Windows do not apply to neither Mac nor Linux endpoints

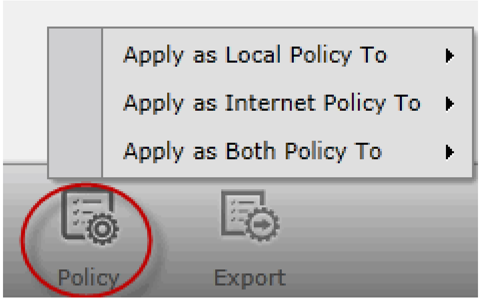
Options

□ Override individual computer policies

- For the 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) of computers connected through the Internet you wish to apply the new policy, select 'For Internet Policy' check box.
- **Options**:
  - **Override individual computers policy** - Selecting this option will apply the new policy onto target computers in the selected groups that currently have individual policies that differ from the group policy, thereby reverting their policies to come from their group membership.

- Click the 'Save' icon for any changes to the settings to take effect.

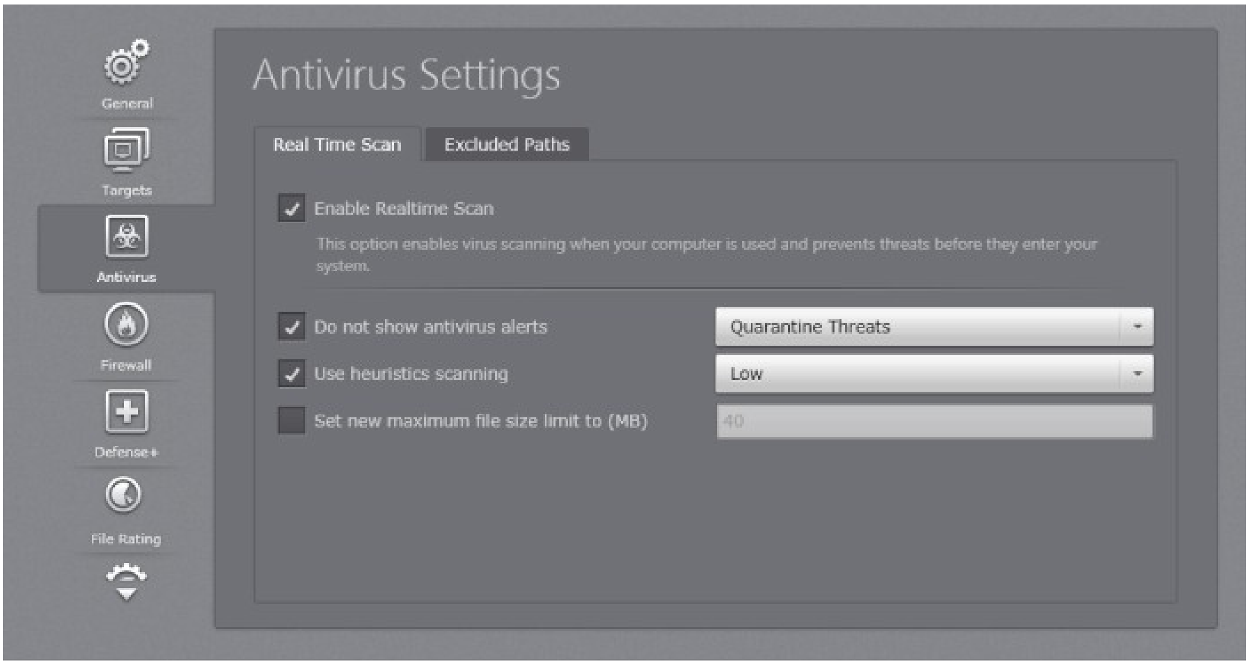
Alternatively, a policy can also be applied to different groups by using right-click options and selecting the group from the context sensitive menu or by clicking the 'Policy' icon in the Policies screen and selecting the group from the menu.



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) and Exclusions (a list of the files you consider safe).

To open the interface, click on the 'Antivirus' icon in the left pane. The Antivirus Settings screen will be displayed.



Antivirus Settings

☑ Enable Realtime Scan

This option enables virus scanning when your computer is used and prevents threats before they enter your system.

☑ Do not show antivirus alerts — Quarantine Threats

☑ Use heuristics scanning — Low

□ Set new maximum file size limit to (MB) — 40

The options that can be configured in the Antivirus settings screen are:

- **Real Time Scanning** - To set the parameters for on-access scanning.
- **Exclusions** - To add trusted files and applications for excluding from a virus scan.

Real Time Scanning

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 you real time protection against threats.

You also have options to automatically remove the threats found during scanning and to update virus database before scanning. It is highly recommended that you enable the Real Time Scanner to ensure the endpoints remains continually free of infection.

- **Enable Realtime Scan** - Allows the administrator to enable or disable real-time scanning. Comodo recommends to leave this option selected.(***Default=Enabled***)
- **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. If you choose not to show alerts then you have a choice of default responses that CES should automatically take – either 'Block Threats' or 'Quarantine Threats'.
  - **Quarantine Threats** - Moves the detected threat(s) to quarantine for your later assessment and action. ***(Default)***
  - **Block Threats** - Stops the application or file from execution, if a threat is detected in it.
- **Use heuristics scanning** - Allows the administrator to enable or disable Heuristics scanning and define scanning level. (***Default = Enabled***)

  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.

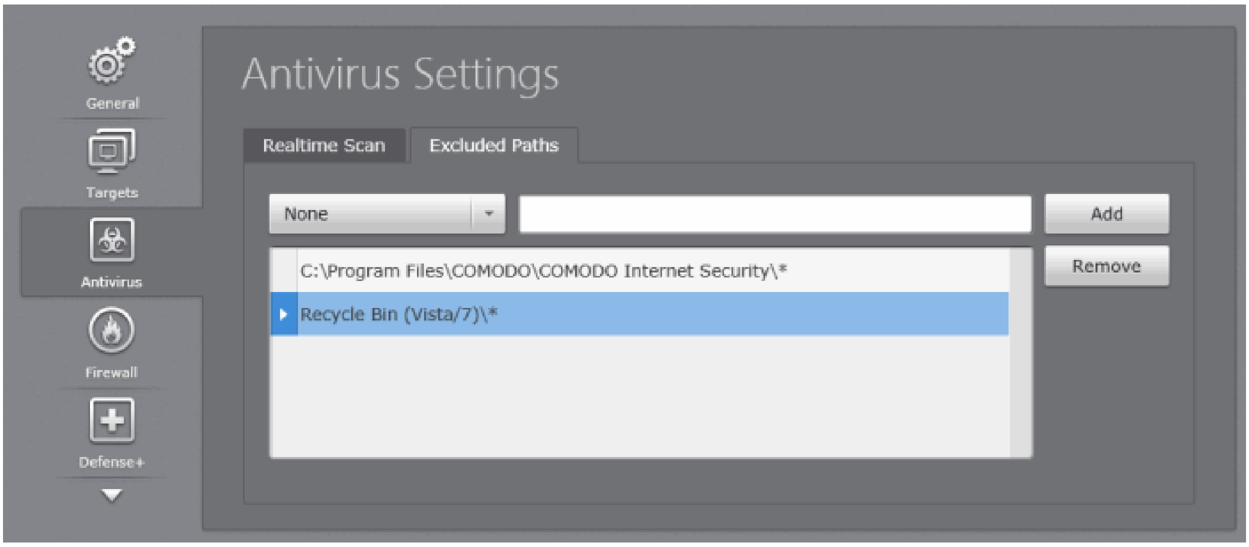
  Leave this option selected to keep Heuristics scanning enabled. Else, deselect this checkbox. If enabled, you can select the level of Heuristic scanning from the drop-down:

  - **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. (***Default***)

    - **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.
- **Set new maximum file size limit to** - 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. (***Default = 40 MB***)

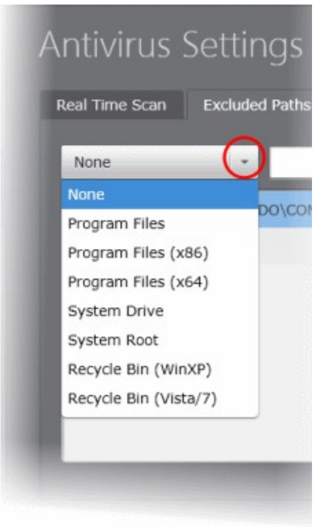
Exclusions

In the Excluded Paths area, you can specify files and folders that you trust and want to exclude them from all future scans of all types.



C:\Program Files\COMODO\COMODO Internet Security*
Recycle Bin (Vista/7)*

You can add files and folders in Exclusions list by selecting the folder from the drop-down and entering the path in the text field or enter the entire path in the field after selecting 'None' in the drop-down.



- Click the 'Add' button.

If you want to remove an item from the list, select it and click the 'Remove' button.

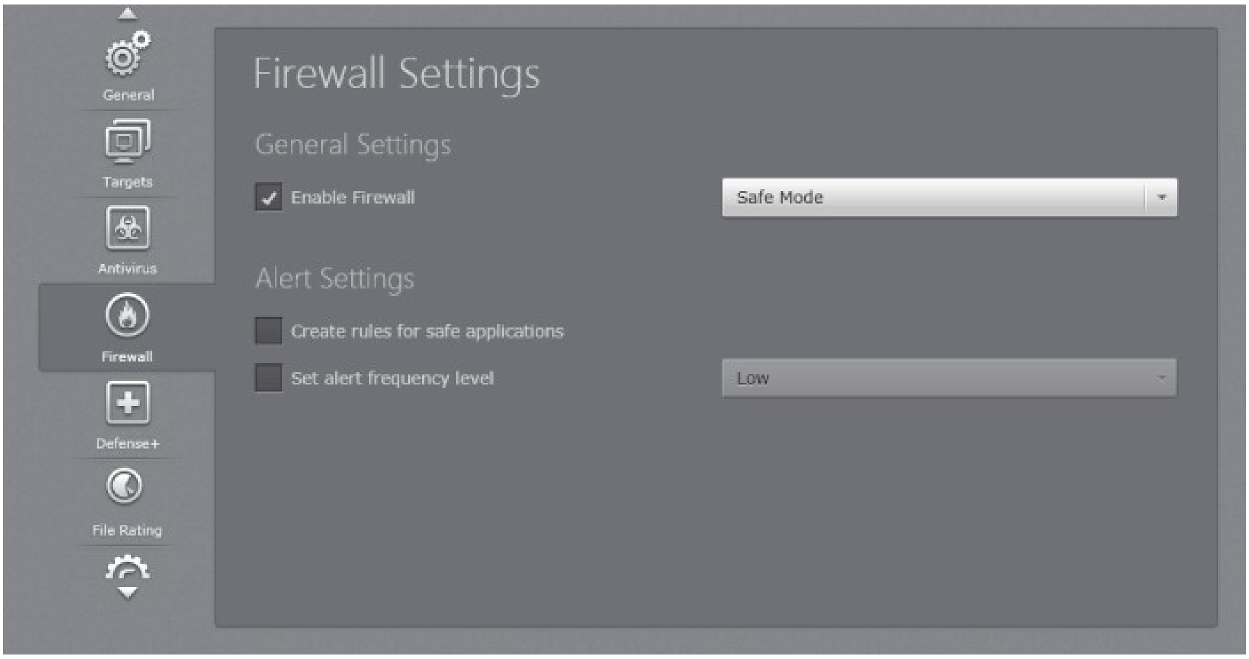
Click the 'Save' icon for any changes to the settings to take effect.

For more details on the Antivirus Settings, see **http://help.comodo.com/** for Comodo Endpoint Security.

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.

To open the Firewall Settings interface, click on the 'Firewall' icon in the left pane. The Firewall Settings screen will be displayed.



Firewall Settings

General Settings

☑ Enable Firewall — Safe Mode

Alert Settings

□ Create rules for safe applications

□ Set alert frequency level — Low

Click the links below for more details:

- **General Settings**
- **Alert Settings**

General Settings

The Enable Firewall check box is enabled by default and if disabled, all incoming and outgoing connections are allowed irrespective of the restrictions set by the user. Comodo strongly advise against this setting 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
- Custom Ruleset
- Safe Mode
- Training Mode

- **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 does not automatically create 'allow' rules for safe applications. This helps saving the resource usage, simplifies the rules interface by reducing the number of 'Allowed' rules in it, reduces the number of pop-up alerts and is beneficial to beginners who find difficulties in setting up the rules.

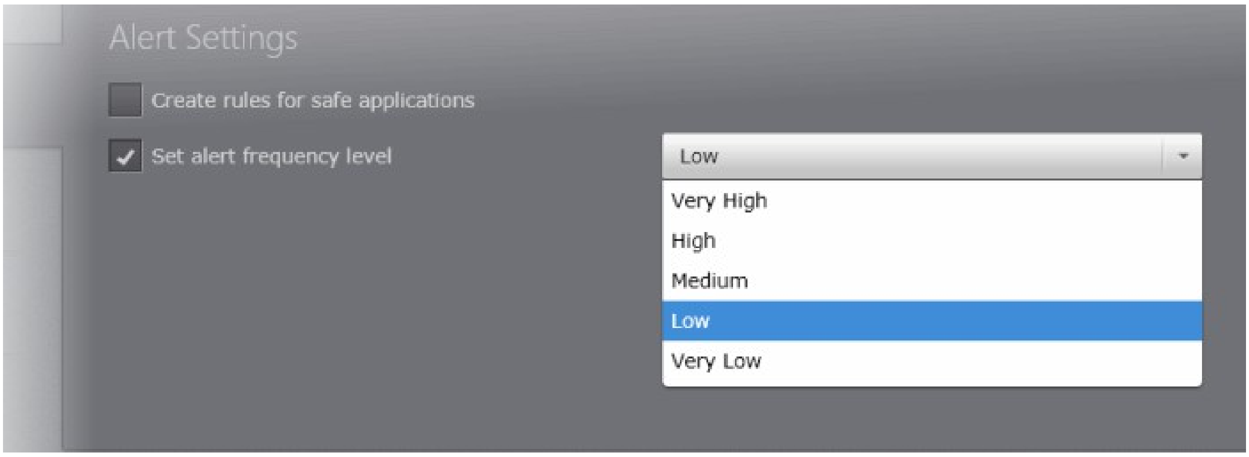
Enabling this check box instructs CES to begin learning the behavior of safe applications so that it can automatically generate the 'Allow' rules. These rules are listed in the Application Rules interface of CES. The Advanced users can edit/modify the rules as they wish.

Background Note: Prior to version 4.x, CES would automatically add an allow rule for 'safe' files to the rules interface. This allowed advanced users to have granular control over rules but could also lead to a cluttered rules interface. The constant addition of these 'allow' rules and the corresponding requirement to learn the behavior of applications that are already considered 'safe' also took a toll on system resources. In version 4.x and above, 'allow' rules for applications considered 'safe' are not automatically created - simplifying the rules interface and cutting resource overhead with no loss in security. Advanced users can re-enable this setting if they require the ability to edit rules for safe applications (or, informally, if they preferred the way rules were created in CES version 3.x).

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.



Alert Settings

□ Create rules for safe applications

☑ Set alert frequency level — Low

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.
- **Very Low**: The firewall shows only one alert for an application.

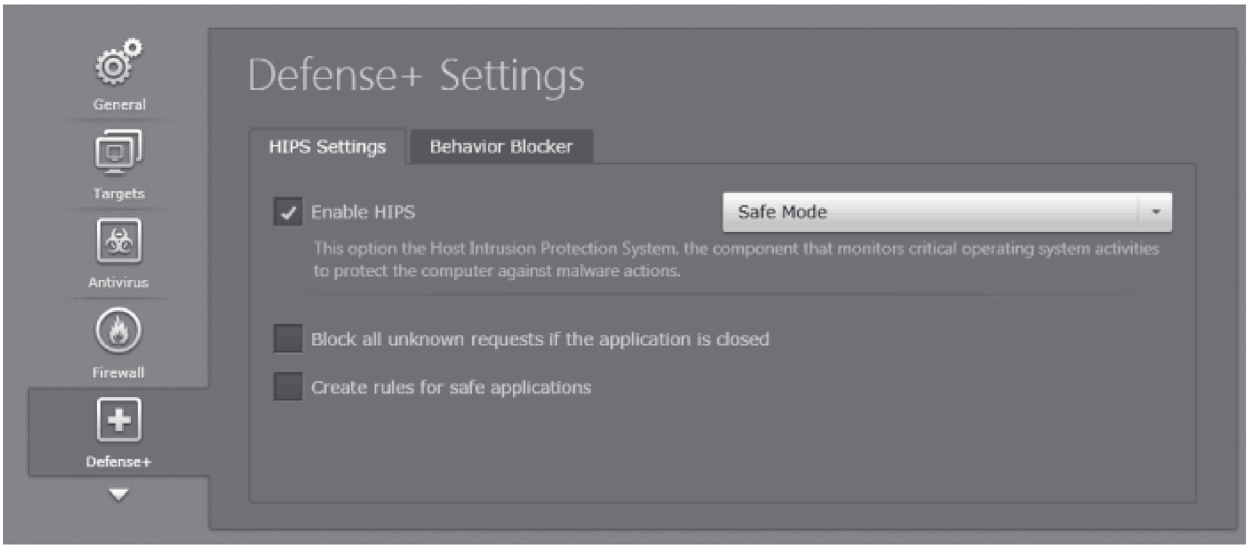
Click the 'Save' icon for any changes to the settings to take effect.

For more details on the Firewall Settings, see **http://help.comodo.com/** for Comodo Endpoint Security.

5.2.5. Configuring Defense+ Settings

Defense+ is a collective term that covers the Host Intrusion Prevention (HIPS), sandboxing and behavior blocker components of Comodo Endpoint Security. 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.

To open the Defense+ Settings interface, click on the 'Defense+' icon ⊞ in the left pane. The Defense+ Settings screen will be displayed.



Defense+ Settings

☑ Enable HIPS — Safe Mode

This option the Host Intrusion Protection System, the component that monitors critical operating system activities to protect the computer against malware actions.

□ Block all unknown requests if the application is closed

□ Create rules for safe applications

The Defense+ settings area allows an administrator to configure the following:

- **HIPS Behavior Settings**
- **Behavior Blocker**

HIPS Behavior Settings

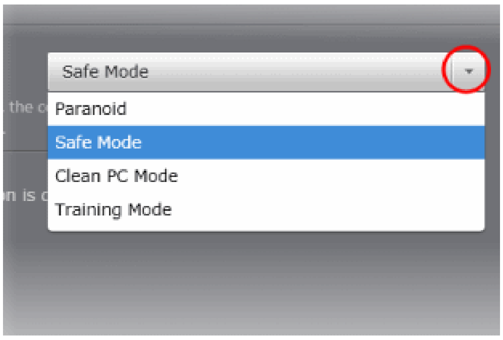
HIPS constantly monitors system activity and only allows executables and processes to run if they comply with the prevailing security rules that have been enforced by the user. For the average user, Comodo Endpoint Security ships with a default HIPS ruleset that works 'out of the box' - providing extremely 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.

- **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. Comodo Endpoint Security 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 Comodo Endpoint Security 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.

Checkbox Options

- **Block all unknown requests if the application is closed** - Selecting this option blocks all unknown execution requests if Comodo Endpoint Security 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 security settings then it is OK to leave this box unchecked. ***(Default = Disabled)***
- **Create rules for safe applications** - Automatically creates rules for safe applications in HIPS Ruleset. ***(Default = Disabled)***

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.

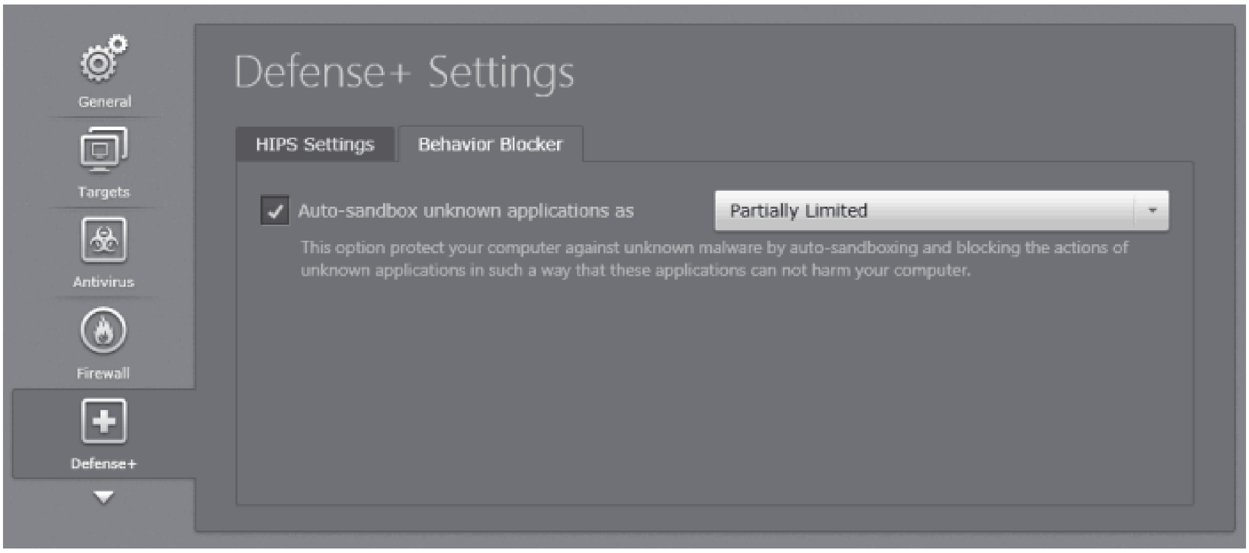
By default, CES does not automatically create 'allow' rules for safe applications. This helps saving the resource usage, simplifies the rules interface by reducing the number of 'Allowed' rules in it, reduces the number of pop-up alerts and is beneficial to beginners who find difficulties in setting up the rules.

Enabling this checkbox instructs CES to begin learning the behavior of safe applications so that it can automatically generate the 'Allow' rules. These rules are listed in the HIPS Rules interface. Administrators can edit / modify the rules as they wish.

Behavior Blocker

The Behavior Blocker is an integral part of the Defense+ engine and is responsible for authenticating every executable image that is loaded into the memory. The Behavior Blocker intercepts all files before they are loaded into memory and intercepts prefetching/caching attempts for those files. It calculates the hash of the executable at the point it attempts to load into the memory. It then compares this hash with the list of known / recognized applications that are on the Comodo safe list. If the hash matches the one on record for the executable, then the application is safe and the Behavior Blocker allows it to run. If no matching hash is found on the safelist, then the executable is 'unrecognized' and is run inside the auto-sandbox. You will be notified via an alert when this happens.

To access the Behavior Blocker settings screen, click the 'Behavior Blocker' tab in the 'Defense+ Settings' interface.



Defense+ Settings

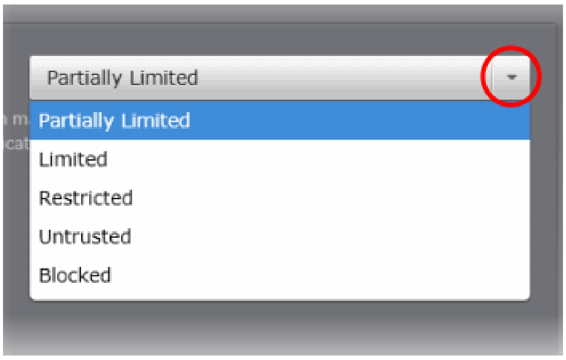
☑ Auto-sandbox unknown applications as: Partially Limited

This option protect your computer against unknown malware by auto-sandboxing and blocking the actions of unknown applications in such a way that these applications can not harm your computer.

- **Auto-sandbox unknown applications as** - Allows the administrator to enable or disable the Behavior Blocker. If enabled, the Behavior Blocker runs unrecognized applications inside the auto-sandbox with the access restriction as selected in the drop down menu. (***Default = 'Enabled' with 'Partially Limited'***)

Note: The 'auto-sandbox' referred to here is distinct to the fully virtualized sandbox/Virtual Kiosk discussed in Sandbox Tasks in CES. The 'auto-sandbox' is a non-virtual environment under which unrecognized applications are run allowed to run under a set of access restrictions (default='Partially Limited'). These restrictions prevent the application from taking actions that are damaging to your system. Advanced users can, however, make a registry change to enable 'Full Virtualization' of auto-sandboxed files.

Access restriction levels determine the amount of privileges an auto-sandboxed application has to access other software and hardware resources on your computer:



- **Partially Limited -** The application is allowed to access all operating system files and resources like the clipboard. Modification of protected files/registry keys are 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.
- **Blocked -** The application is not allowed to run at all.
- **Fully Virtualized** - This option is not available by default but can be enabled by adding a registry key (advanced users only). To do this, open the registry editor and browse to HKLM >SYSTEM > software > Comodo > Firewall Pro. Add a DWORD key to this hive named EnableDefaultVirtualization and set the value to 1. 'Fully Virtualized' will now be listed in the auto-sandbox restriction level drop down.

Click the 'Save' icon for any changes to the settings to take effect.

For more details on the Defense+ Settings, see **http://help.comodo.com/** for Comodo Endpoint Security.

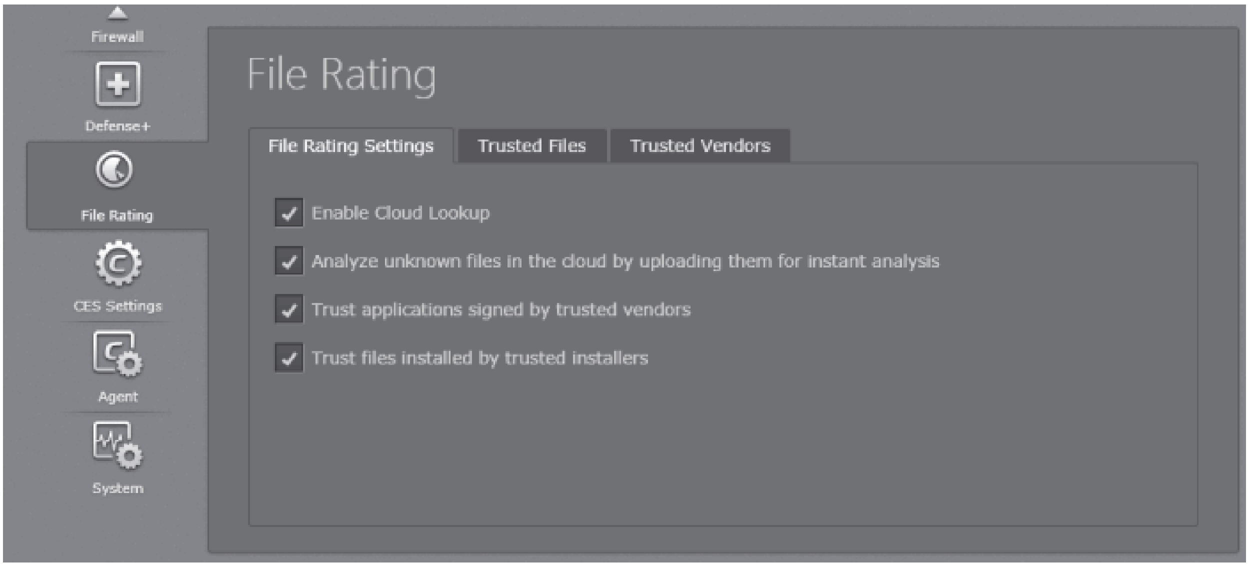
5.2.6. Configuring File Rating Settings

The CES 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 will check the file against our master whitelist and blacklists and will award it trusted status 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.

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 added to the Blocked Files list and denied all access rights from other processes or users - effectively cutting them off from the rest of your system. Files which could not be recognized by the rating system are added to the list of 'Unrecognized Files'. You can review files on the unrecognized list and manually choose to trust/block/delete them or investigate further by sending them to Comodo for analysis/running another file lookup.

To open the File Rating interface, click on the 'File Rating' icon in the left pane. The File Rating screen will be displayed.



☑ Enable Cloud Lookup

☑ Analyze unknown files in the cloud by uploading them for instant analysis

☑ Trust applications signed by trusted vendors

☑ Trust files installed by trusted installers

The 'File Rating' area allows you to view and manage the list of Trusted Files and Trusted Vendors. Click on the following links for more details:

- **File Rating Settings**
- **Trusted Files**
- **Trusted Vendors**

File Rating Settings

The File Rating Settings screen allows you to configure the overall behavior of File Rating feature of Comodo Endpoint Security.

Check box options:

- **Enable Cloud Lookup** - Allows you to enable or disable File Rating.(***Default and recommended =Enabled***)
- **Analyze unknown files in the cloud by uploading them for instant analysis** - Instructs CES 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 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 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***)

Trusted Files

Files added to the Trusted Files list 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, you 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'.

CES allows you to 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. Files can be transferred into this module by clicking the 'Move to' button in the 'Unrecognized Files' area.

Adding files to Trusted Files list

CES allows you to add files and executables to the list of Trusted Files so that those files will be given Trusted status. 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. However you can also add files by their file names, but if you happen to change the file name later, it looses its 'Trusted' status.

To add new file(s) to Trusted Files list

- Click the 'Add Local' button to add files from the computer through which the console is accessed.
- Click the 'Add Remote' button to add files from the endpoints that are connected to CESM.

Navigate to the file(s) that you want to add and click 'Open'. The selected file(s) will be added to the Trusted Files list.

To remove an included entry from the Trusted Files list

- Select the entry to be removed from the 'Trusted Files' list. You can select several entries to be removed at once by using Shift or Ctrl keys.
- Click the Remove button.
- Click 'Save' for the changes to take effect.

Trusted Vendors

In Comodo Endpoint Security, 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 Comodo Endpoint Security (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.

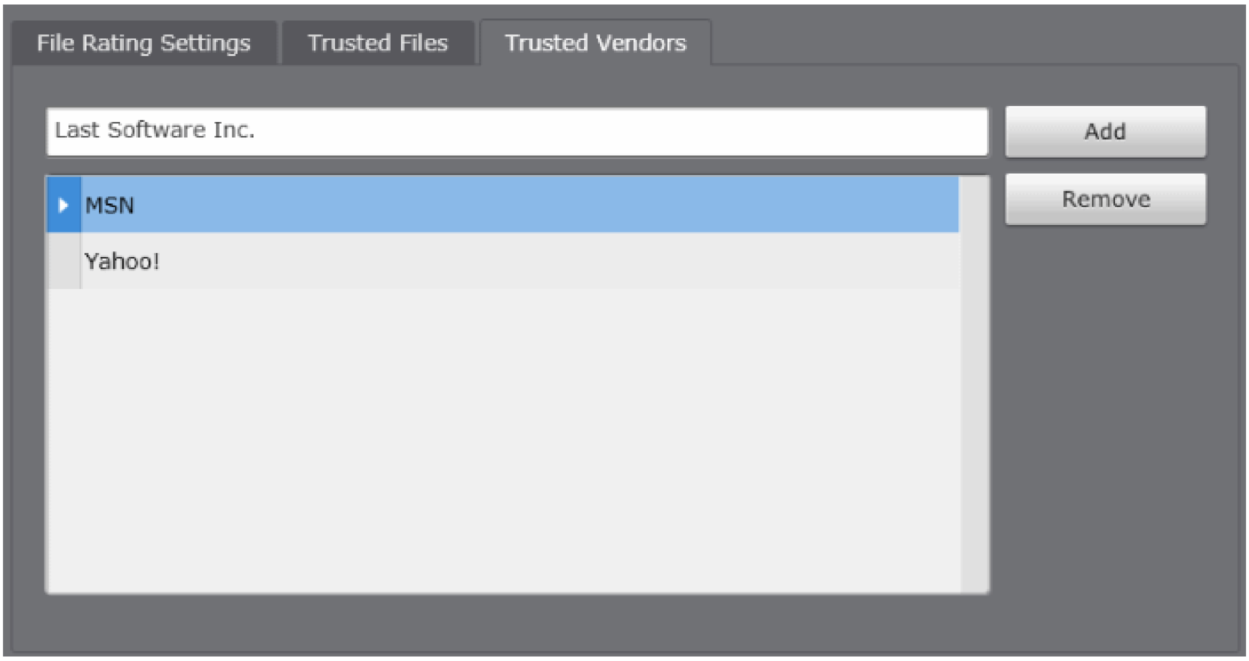
- Browse to the folder containing the .exe file.
- Right click on the .exe file.
- Select 'Properties' from the menu.
- Click the tab 'Digital Signatures (if there is no such tab then the software has not been signed).

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.

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.

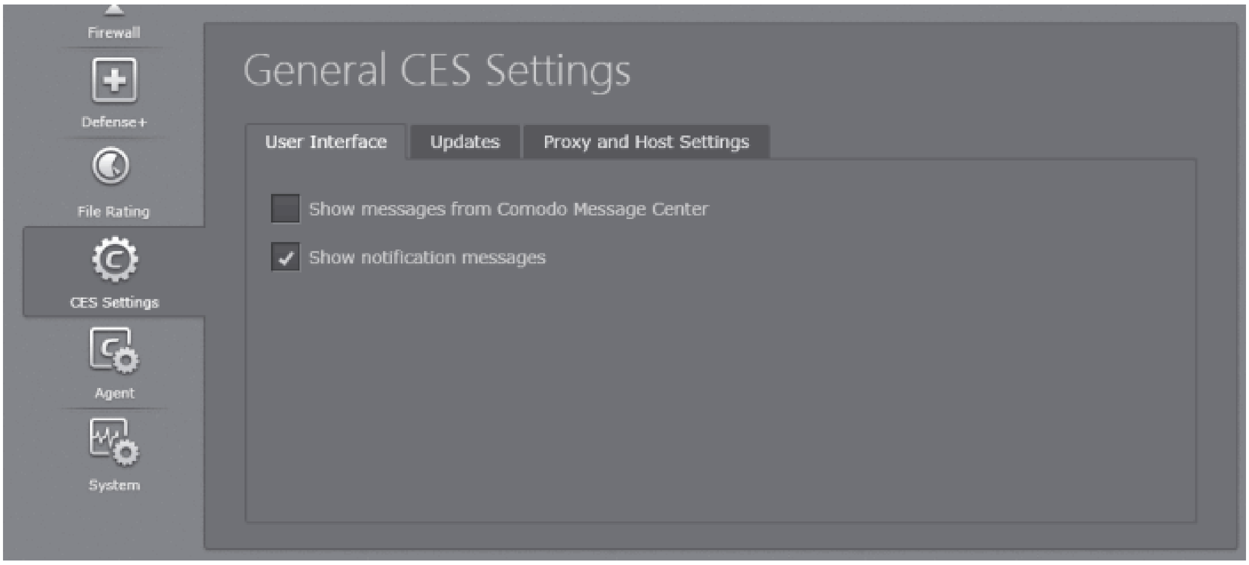
Click the 'Save' icon for any changes to the settings to take effect.

For more details on the File Rating Settings, see **http://help.comodo.com/** for Comodo Endpoint Security.

5.2.7. Configuring General CES Settings

In the General CES Settings screen, administrators can configure various options related to the operation of Comodo Endpoint Security.

To open the General CES Settings interface, click on the 'CES Settings' icon in the left pane. The General CES Settings screen will be displayed.



□ Show messages from Comodo Message Center

☑ Show notification messages

Click the following links for more details:

- User Interface
- Updates
- Proxy and Host Settings

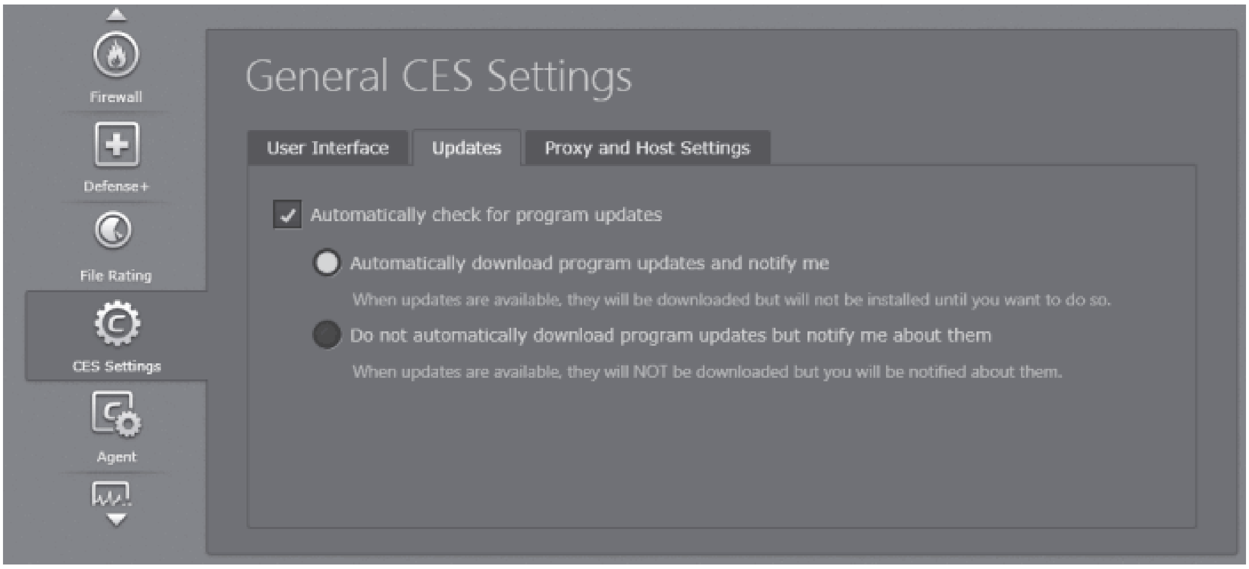
User Interface Settings

The 'User Interface' tab allows the administrator to enable / disable CES notification messages and / or messages from Comodo Message Center.

- **Show messages from COMODO Message Center** - If enabled, Comodo Message Center messages will periodically appear to keep you abreast of news in the Comodo world. 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 = Enabled***)
- **Show notification messages** - These are the CES system notices that appear in the bottom right hand corner of your screen (just above the tray icons) and inform you about the actions that CES is taking and any CES status updates. For example ' Comodo Firewall is learning ' or 'Defense+ is learning ' are generated when these modules are learning the activity of previously unknown components of trusted applications. Antivirus notifications will also be displayed if you have selected 'Do not show antivirus alerts' check box in Antivirus > Real-time Scan settings screen. Clear this check box if you do not want to see these system messages. (***Default = Enabled***)

Update Settings

The 'Updates' area allows the administrator to configure settings that govern CES program and virus database updates.



☑ Automatically check for program updates

○ Automatically download program updates and notify me

When updates are available, they will be downloaded but will not be installed until you want to do so.

● Do not automatically download program updates but notify me about them

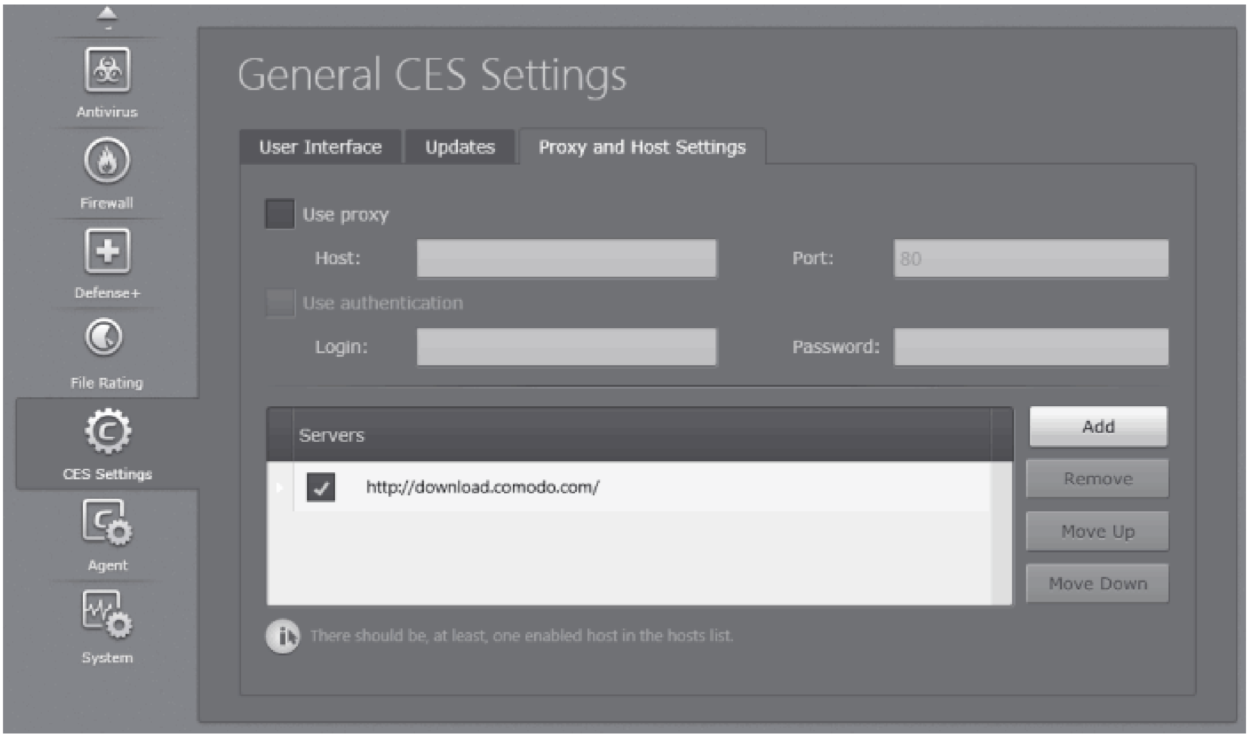
When updates are available, they will NOT be downloaded but you will be notified about them.

- **Automatically check for updates** - If this is option is enabled, CES automatically checks for program and virus database updates automatically. You can also specify which servers and connections to use for updates in Proxy and Host Settings screen. Comodo recommends automatic update checks are left enabled to ensure your system enjoys maximum protection against the latest threats.(***Default=Enabled***)
  - **Automatically download program updates and notify me** - Instructs CES to automatically download program and virus database updates as soon as they are available then notify you that they are ready for installation. (***Default=Enabled***)
  - **Do not automatically download updates but notify me about them** - Selecting this option means CES will notify you when updates are available but will not download them until after your approval.

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 default, CES 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 installations collect the updates from there. The 'Proxy and Host Settings' interface allows you to point CES at this proxy/staging server. This helps conserve overall bandwidth consumption and accelerates the update process when large number of endpoints are involved.

Note: You first need to install Comodo Offline Updater in order to download updates to your proxy server. This can be downloaded from **http://enterprise.comodo.com/security-solutions/endpoint-security/endpoint-security-manager/free-trial.php**



□ Use proxy

Host:

Port: 80

□ Use authentication

Login:

Password:

Servers

☑ http://download.comodo.com/

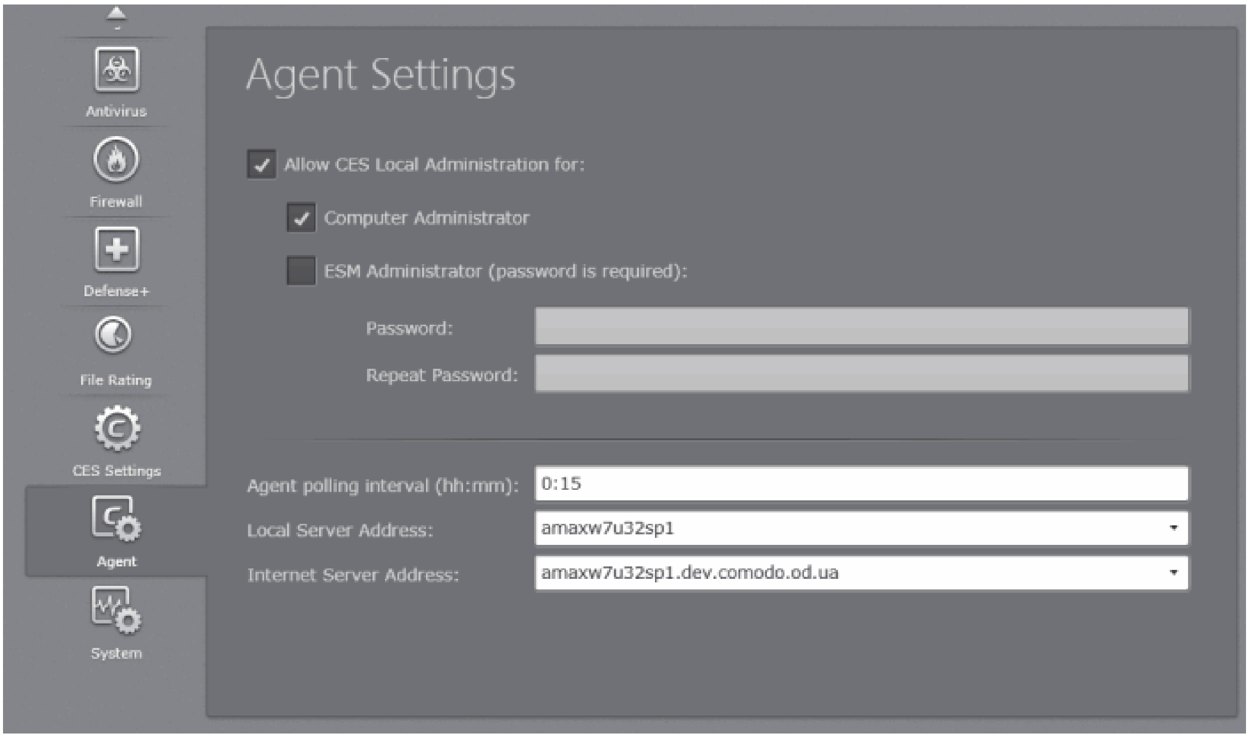
There should be, at least, one enabled host in the hosts list.

- Select '**Use proxy**' check box if you want Comodo Endpoint Security 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 will commence downloading from the first server that contains new updates.

5.2.8. Configuring Agent Settings

In the Agent Settings screen, administrators can edit the Agent settings for the selected policy.

To open the Agent Settings interface, click on the 'Agent' icon in the left pane. The Agent Settings screen will be displayed.



Agent Settings

☑ Allow CES Local Administration for:

☑ Computer Administrator

□ ESM Administrator (password is required):

Password:

Repeat Password:

Agent polling interval (hh:mm): 0:15

Local Server Address: amaxw7u32sp1

Internet Server Address: amaxw7u32sp1.dev.comodo.od.ua

- **Allow CES Local Administration for**- Configures the agent to allow the CES 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 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 to local administration mode.
- **Policy compliance polling interval** - The administrator can set the time interval (in hours and minutes) for the agent to periodically check whether the CES 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).
- **Local Server Address** - The administrator can specify the address of the server machine in the local network, on which the ESM central service is installed.
- **Internet Server Address** - The administrator can specify the address of the external server on which the ESM central service is installed if the endpoint should connect to the ESM server through Internet.

Tip: Local Server Address and Internet Server Address values are used by the Agent to determine when Local Policy or Internet Policy should be applied. What's more, these addresses have a priority over addresses that are in the Server Network Addresses list specified in the Configuration Tool such that:

1. The Local Server Address value, mandatory in policy settings, specifies that if this connection is established Local Policy should be applied.
2. Internet Server Address value is optional in policy settings. If specified it is tried to be reached ONLY if the specified local address connection fails, Internet Policy should be applied.

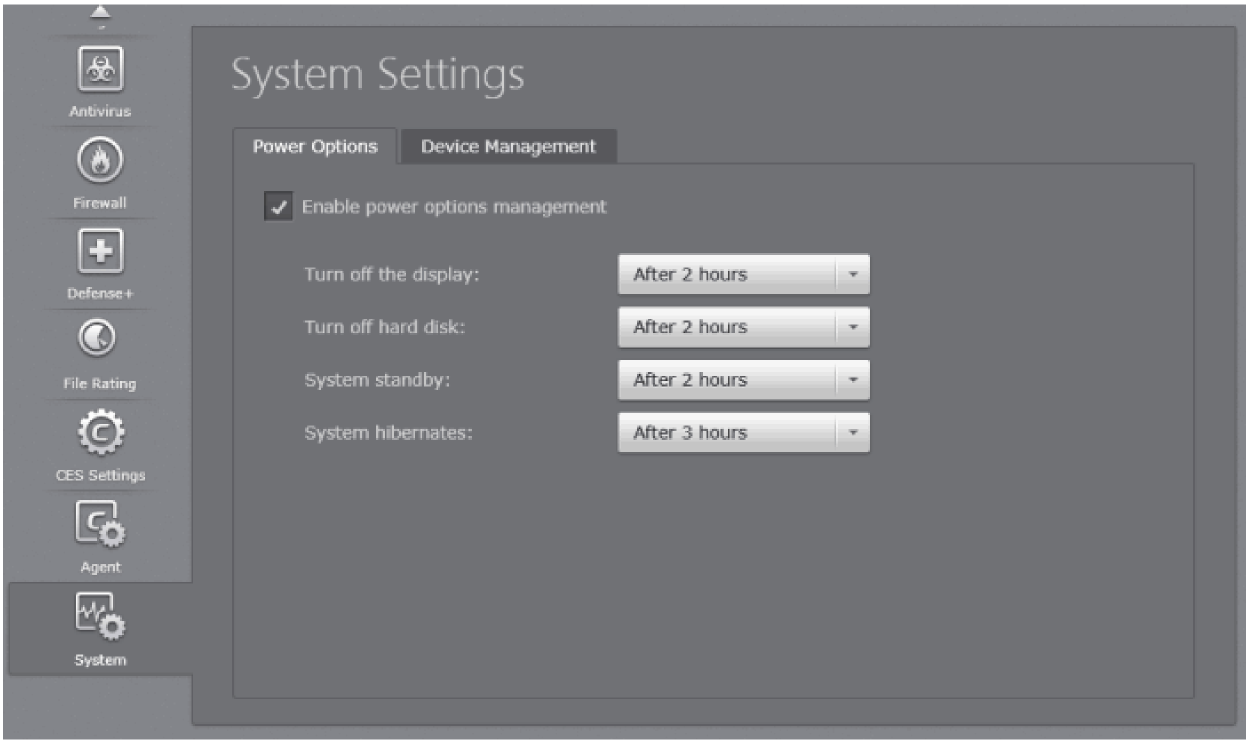
If none of these addresses succeeded or if Internet Server Address value wasn't specified, the Agent will try the remaining hosts in the Server Network Addresses list, applying the corresponding policy based upon analysis per RFC 3330 of a connection succeeding via a special use address as indicating Local policy, and a public address indicating Internet policy.

- Click 'Save' for any changes to take effect.

5.2.9. Configuring System Settings

The System Settings screen allows the administrator to edit the system settings configured for the selected policy.

To open the System Settings interface, click on the 'System' icon in the left pane. The System Settings screen with Power Options interface will be displayed.



☑ Enable power options management

Turn off the display: After 2 hours

Turn off hard disk: After 2 hours

System standby: After 2 hours

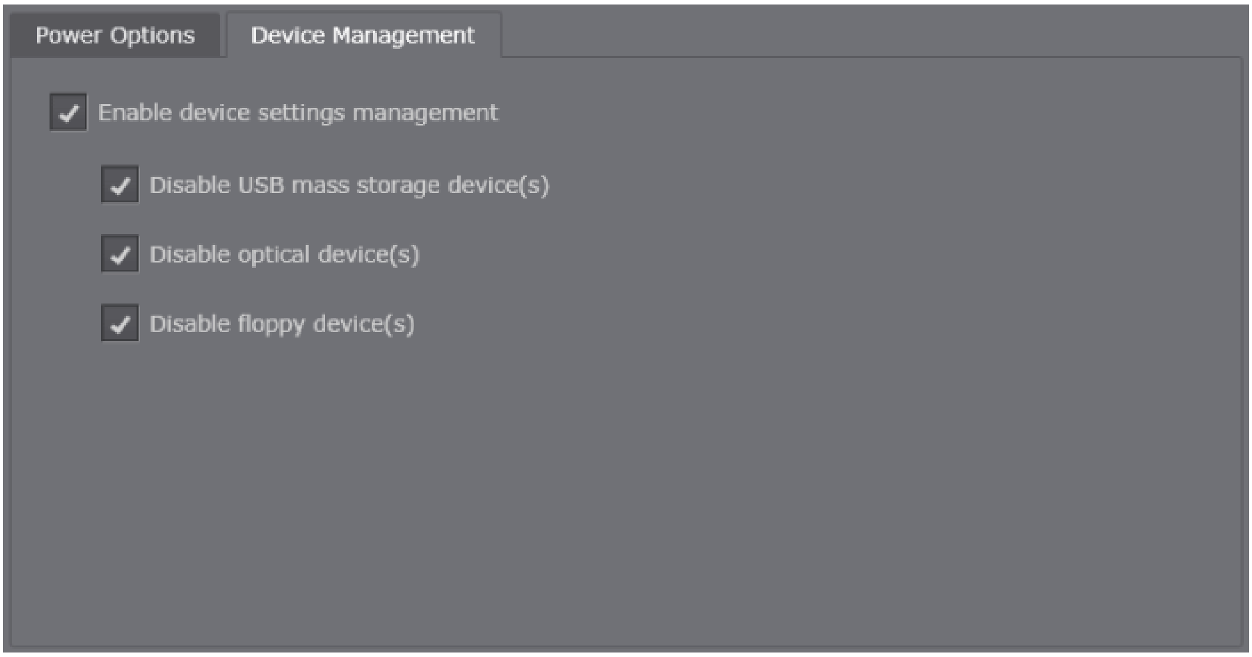
System hibernates: After 3 hours

Power Options

- **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.

Devices Management

- Click the 'Device Management' tab to open the device settings interface.



☑ Enable device settings management

☑ Disable USB mass storage device(s)

☑ Disable optical device(s)

☑ Disable floppy device(s)

- **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.
    - **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 More 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.

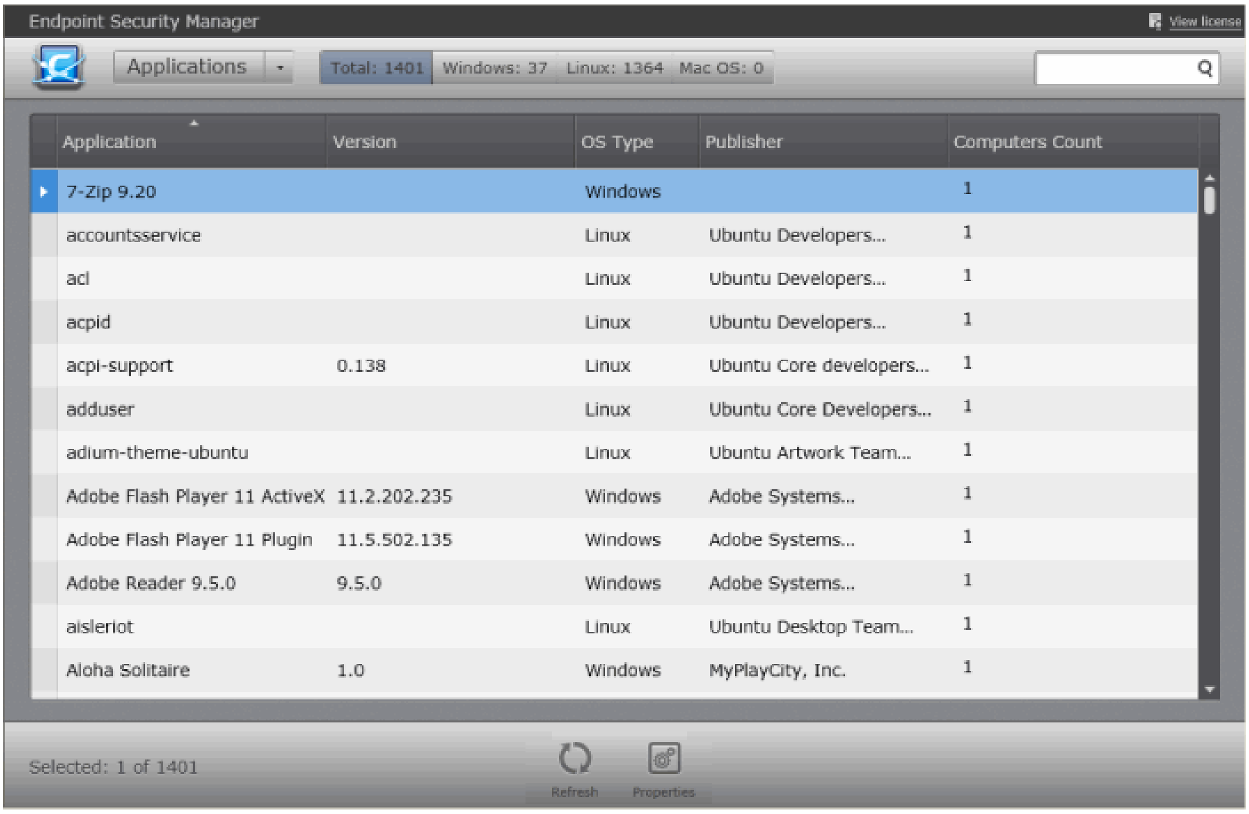
- Advanced screen of the Computers interface. (Refer to the section **Viewing and Managing Group and Security Policy Details** for more details).
- Using the More icon in the Computers interface.

6. 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.



Application	Version	OS Type	Publisher	Computers Count
7-Zip 9.20		Windows		1
accountsservice		Linux	Ubuntu Developers...	1
acl		Linux	Ubuntu Developers...	1
acpid		Linux	Ubuntu Developers...	1
acpi-support	0.138	Linux	Ubuntu Core developers...	1
adduser		Linux	Ubuntu Core Developers...	1
adium-theme-ubuntu		Linux	Ubuntu Artwork Team...	1
Adobe Flash Player 11 ActiveX	11.2.202.235	Windows	Adobe Systems...	1
Adobe Flash Player 11 Plugin	11.5.502.135	Windows	Adobe Systems...	1
Adobe Reader 9.5.0	9.5.0	Windows	Adobe Systems...	1
aisleriot		Linux	Ubuntu Desktop Team...	1
Aloha Solitaire	1.0	Windows	MyPlayCity, Inc.	1

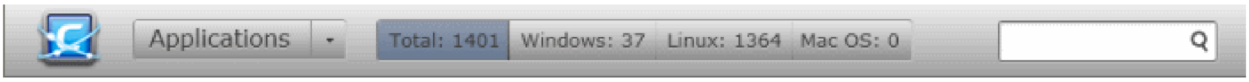
Selected: 1 of 1401

Column Heading	Description
Application	Displays the name of the application.
Version	Displays the version number of the application.
OS Type	Displayes 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

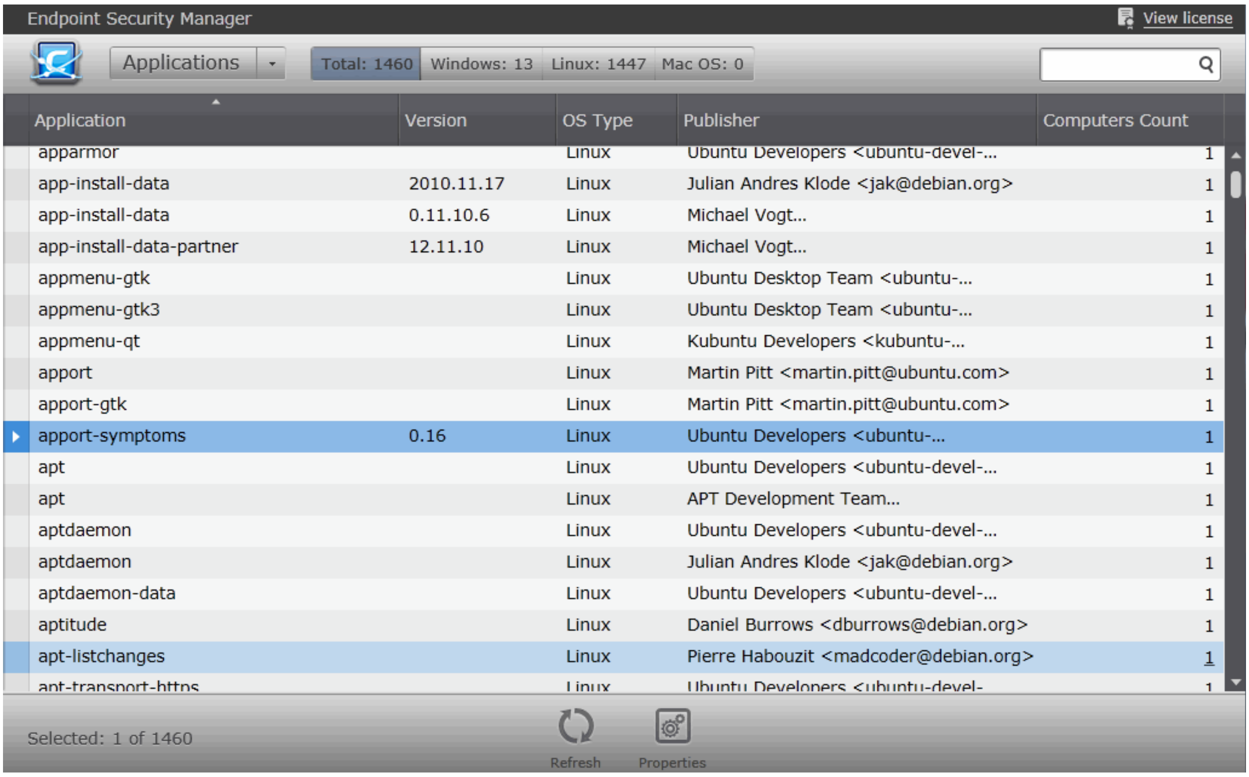
The filter options in the gray stripe, gives at-a-glance statistics of the number of applications identified from computers running on different Operating Systems and allow the administrator to filter the computers based on the criteria.

The search field in the right allows the administrator to search for a specific application by entering its name partially or fully.



Managing Applications

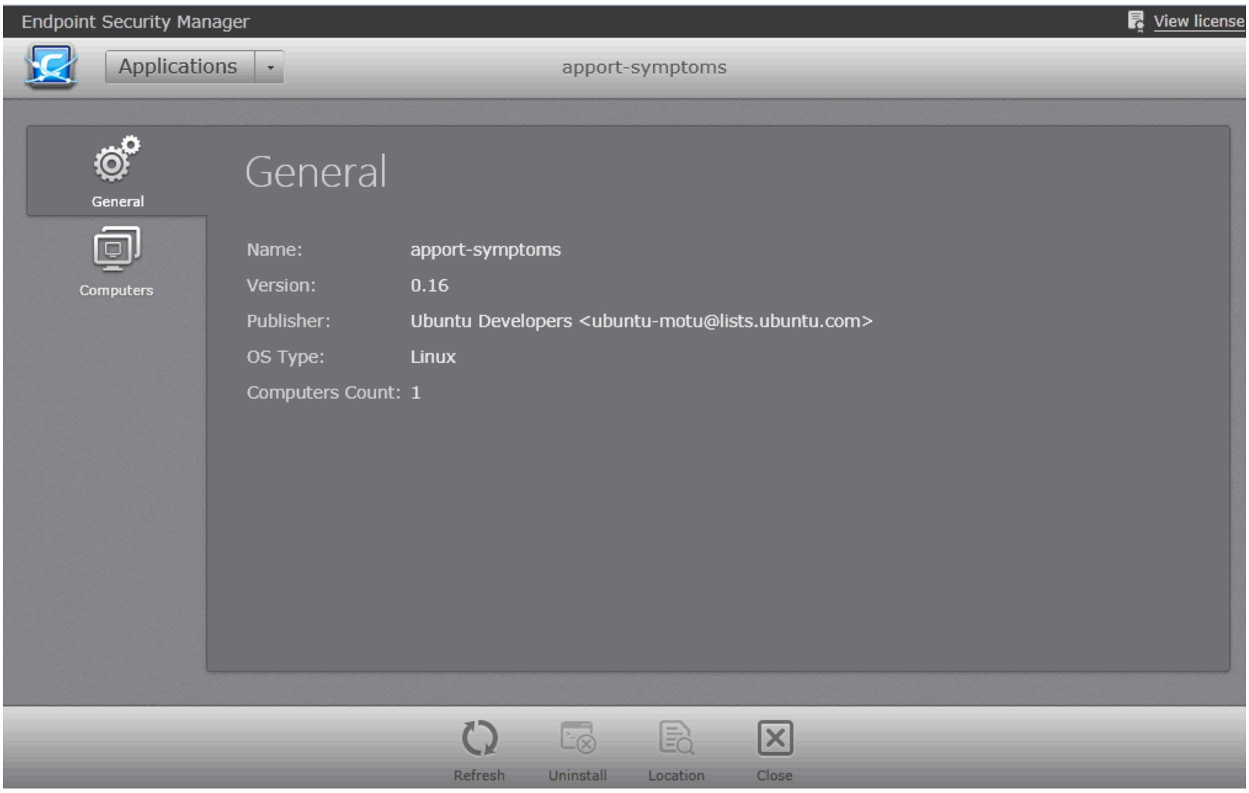
To view the details of a selected application, select the application and click 'Properties' or right click on the application and choose 'Properties' from the context sensitive menu.



Application	Version	OS Type	Publisher	Computers Count
apparmor		Linux	Ubuntu Developers <ubuntu-devel-...	1
app-install-data	2010.11.17	Linux	Julian Andres Klode <jak@debian.org>	1
app-install-data	0.11.10.6	Linux	Michael Vogt...	1
app-install-data-partner	12.11.10	Linux	Michael Vogt...	1
appmenu-gtk		Linux	Ubuntu Desktop Team <ubuntu-...	1
appmenu-gtk3		Linux	Ubuntu Desktop Team <ubuntu-...	1
appmenu-qt		Linux	Kubuntu Developers <kubuntu-...	1
apport		Linux	Martin Pitt <martin.pitt@ubuntu.com>	1
apport-gtk		Linux	Martin Pitt <martin.pitt@ubuntu.com>	1
apport-symptoms	0.16	Linux	Ubuntu Developers <ubuntu-...	1
apt		Linux	Ubuntu Developers <ubuntu-devel-...	1
apt		Linux	APT Development Team...	1
aptdaemon		Linux	Ubuntu Developers <ubuntu-devel-...	1
aptdaemon		Linux	Julian Andres Klode <jak@debian.org>	1
aptdaemon-data		Linux	Ubuntu Developers <ubuntu-devel-...	1
aptitude		Linux	Daniel Burrows <dburrows@debian.org>	1
apt-listchanges		Linux	Pierre Habouzit <madcoder@debian.org>	1
apt-transport-https		Linux	Ubuntu Developers <ubuntu-devel-	1

Selected: 1 of 1460

The Application Properties interface will open.


Endpoint Security Manager

Name: apport-symptoms

Version: 0.16

Publisher: Ubuntu Developers <ubuntu-motu@lists.ubuntu.com>

OS Type: Linux

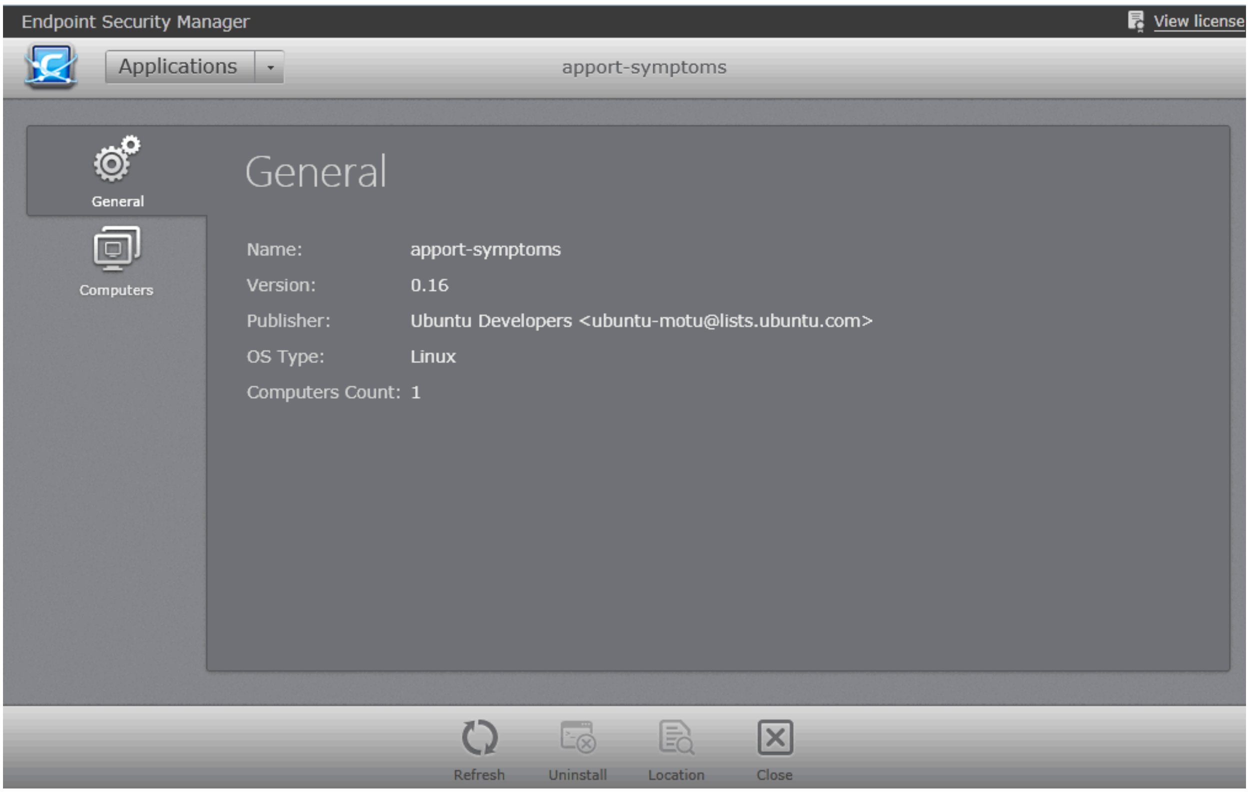
Computers Count: 1

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.


Endpoint Security Manager

Name: apport-symptoms

Version: 0.16

Publisher: Ubuntu Developers <ubuntu-motu@lists.ubuntu.com>

OS Type: Linux

Computers Count: 1

The General Properties screen displays the details on name, version number, publisher, OS and number of endpoints on which the application was identified.

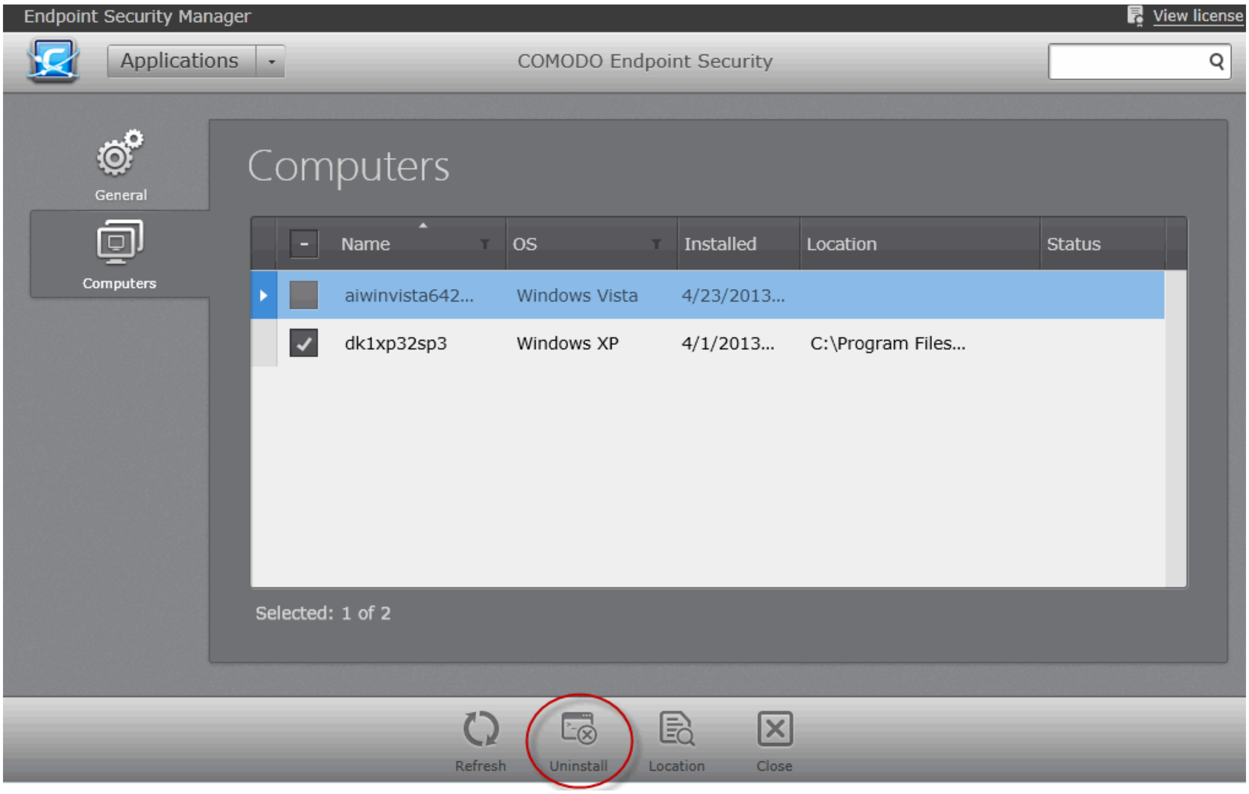
Computers Screen

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 uninstall the application, if it is an unwanted one.

To uninstall the application from selected endpoints

1. Select the endpoints. You can select multiple endpoints simultaneously by pressing and holding the 'Ctrl' or 'Shift' keys in the key board.



	Name	OS	Installed	Location	Status
□	aiwinvista642...	Windows Vista	4/23/2013...		
☑	dk1xp32sp3	Windows XP	4/1/2013...	C:\Program Files...	

Selected: 1 of 2

2. Click 'Uninstall'.

The application will be uninstalled from the selected endpoints immediately.

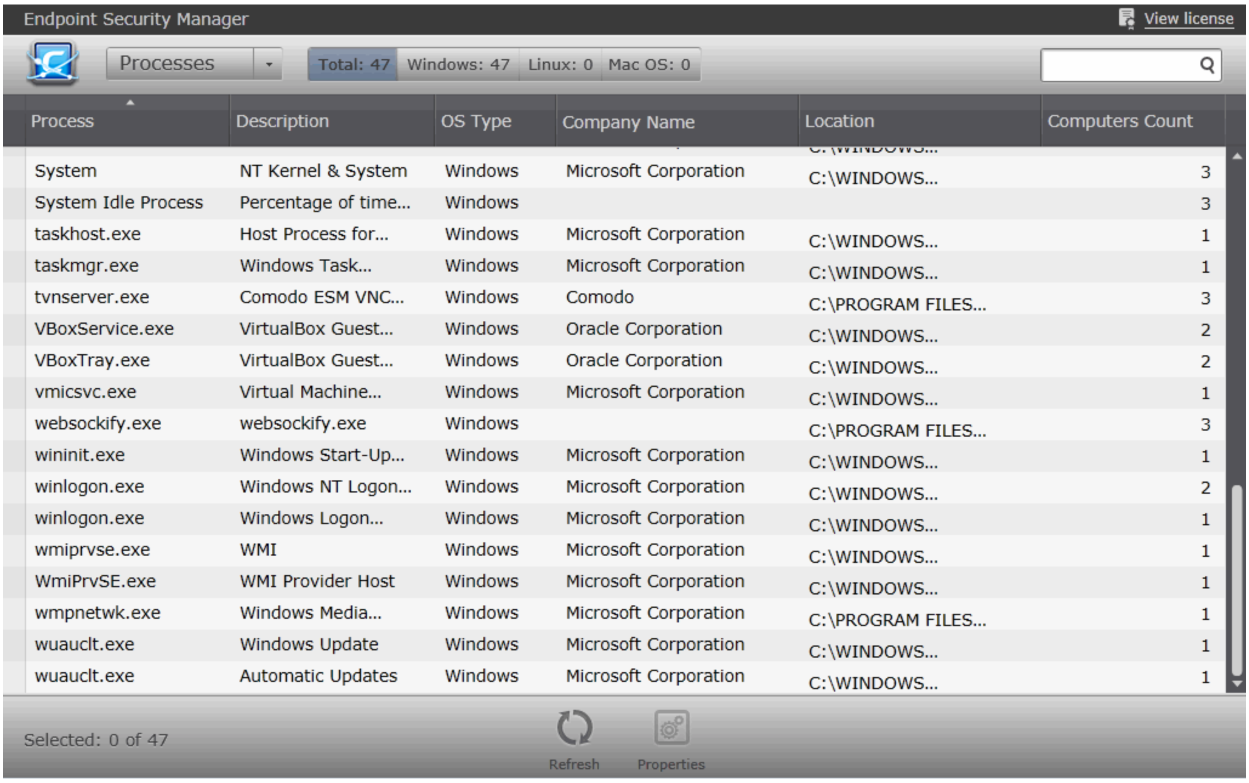
Note: You can uninstall only MSI based applications from this interface.

Clicking the 'Location' will open the File System. Click **Viewing and Managing Drives and Storage** for more details.

7. 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.



Process	Description	OS Type	Company Name	Location	Computers Count
System	NT Kernel & System	Windows	Microsoft Corporation	C:\WINDOWS...	3
System Idle Process	Percentage of time...	Windows			3
taskhost.exe	Host Process for...	Windows	Microsoft Corporation	C:\WINDOWS...	1
taskmgr.exe	Windows Task...	Windows	Microsoft Corporation	C:\WINDOWS...	1
tvnserver.exe	Comodo ESM VNC...	Windows	Comodo	C:\PROGRAM FILES...	3
VBoxService.exe	VirtualBox Guest...	Windows	Oracle Corporation	C:\WINDOWS...	2
VBoxTray.exe	VirtualBox Guest...	Windows	Oracle Corporation	C:\WINDOWS...	2
vmicsvc.exe	Virtual Machine...	Windows	Microsoft Corporation	C:\WINDOWS...	1
websockify.exe	websockify.exe	Windows		C:\PROGRAM FILES...	3
wininit.exe	Windows Start-Up...	Windows	Microsoft Corporation	C:\WINDOWS...	1
winlogon.exe	Windows NT Logon...	Windows	Microsoft Corporation	C:\WINDOWS...	2
winlogon.exe	Windows Logon...	Windows	Microsoft Corporation	C:\WINDOWS...	1
wmiprvse.exe	WMI	Windows	Microsoft Corporation	C:\WINDOWS...	1
WmiPrvSE.exe	WMI Provider Host	Windows	Microsoft Corporation	C:\WINDOWS...	1
wmpnetwk.exe	Windows Media...	Windows	Microsoft Corporation	C:\PROGRAM FILES...	1
wuauclt.exe	Windows Update	Windows	Microsoft Corporation	C:\WINDOWS...	1
wuauclt.exe	Automatic Updates	Windows	Microsoft Corporation	C:\WINDOWS...	1

Selected: 0 of 47

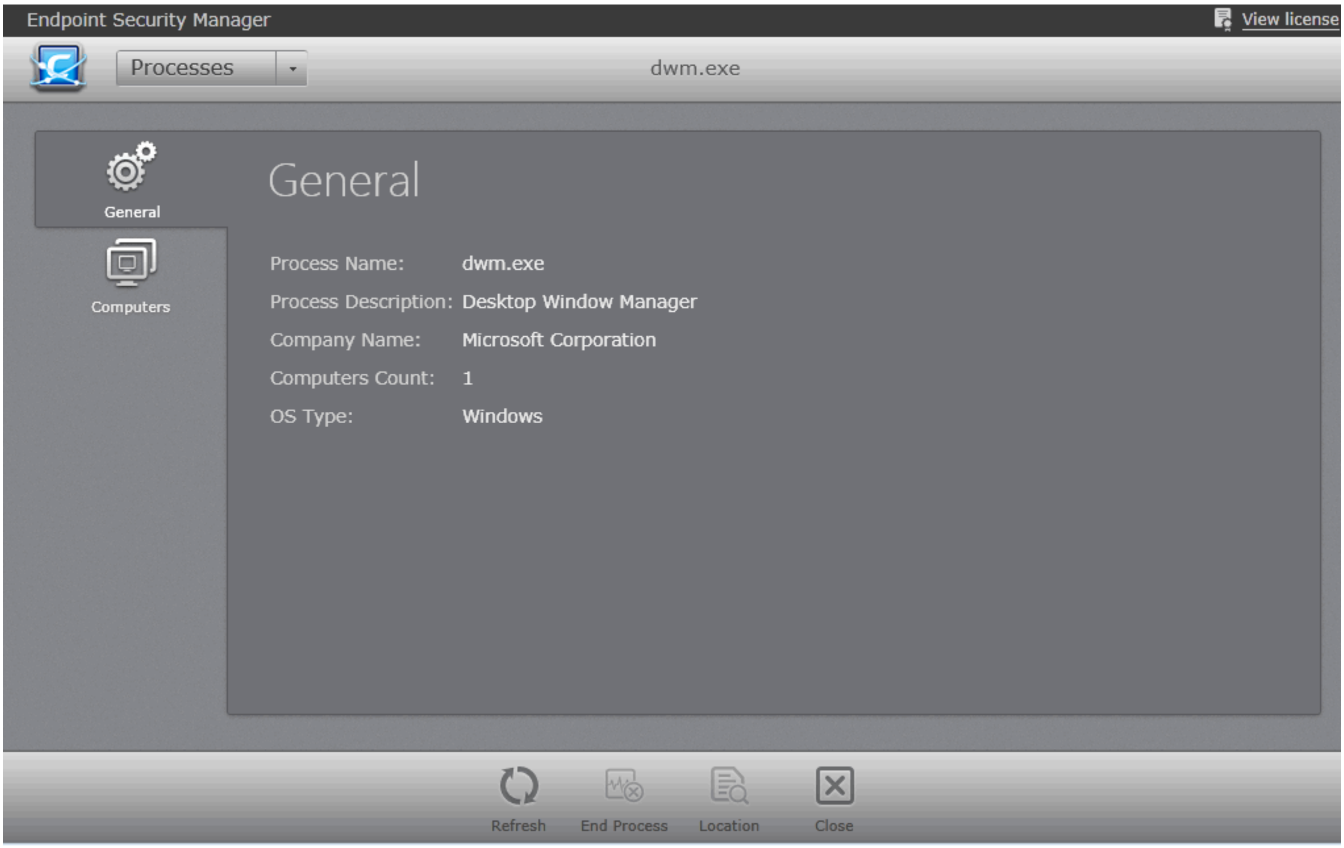
Column Heading	Description
Process	Displays the name of the process.
Description	Displays a short description of the process.
OS Type	Displays the Operating System of the endpoint(s) on which the process is running.
Location	Displays the process location.
Computers Count	Indicates the number of endpoint computers on which the process is running

To view process properties

- 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

Process Name: dwm.exe

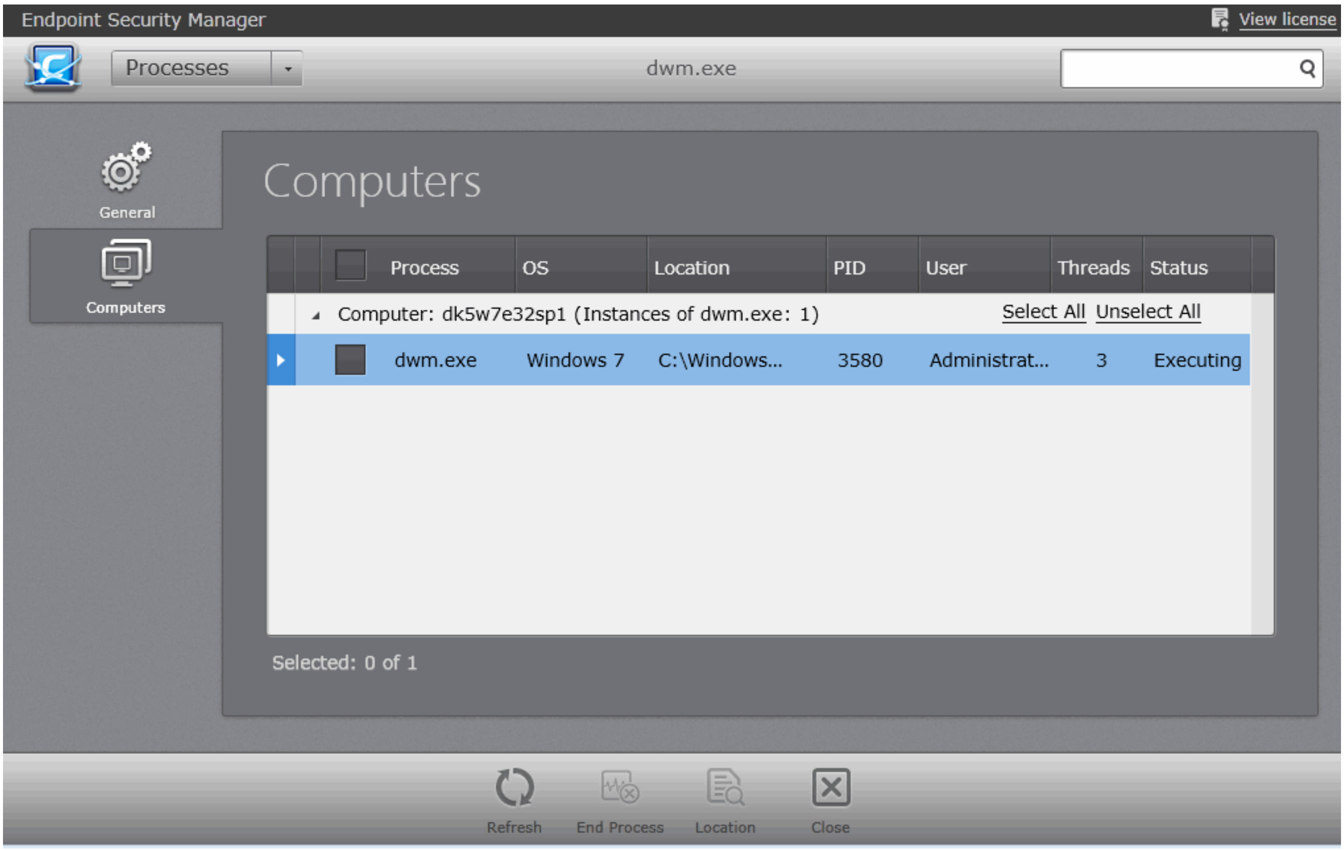
Process Description: Desktop Window Manager

Company Name: Microsoft Corporation

Computers Count: 1

OS Type: Windows

- **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.



Computer: dk5w7e32sp1 (Instances of dwm.exe: 1)

☐	Process	OS	Location	PID	User	Threads	Status
☐	dwm.exe	Windows 7	C:\Windows...	3580	Administrat...	3	Executing

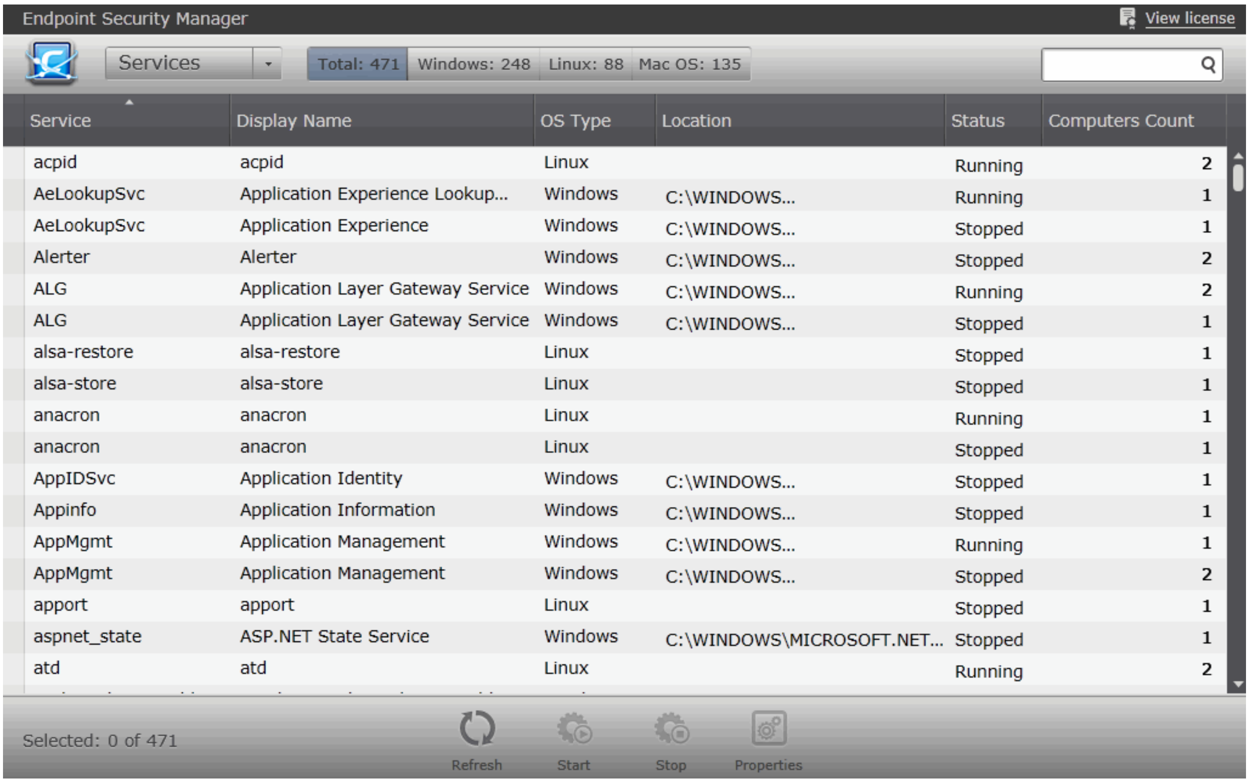
Selected: 0 of 1

- To terminate the process from selected endpoints, select the endpoints and click the 'End Process' from the options at the bottom.

8. 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.



Service	Display Name	OS Type	Location	Status	Computers Count
acpid	acpid	Linux		Running	2
AeLookupSvc	Application Experience Lookup...	Windows	C:\WINDOWS...	Running	1
AeLookupSvc	Application Experience	Windows	C:\WINDOWS...	Stopped	1
Alerter	Alerter	Windows	C:\WINDOWS...	Stopped	2
ALG	Application Layer Gateway Service	Windows	C:\WINDOWS...	Running	2
ALG	Application Layer Gateway Service	Windows	C:\WINDOWS...	Stopped	1
alsa-restore	alsa-restore	Linux		Stopped	1
alsa-store	alsa-store	Linux		Stopped	1
anacron	anacron	Linux		Running	1
anacron	anacron	Linux		Stopped	1
AppIDSvc	Application Identity	Windows	C:\WINDOWS...	Stopped	1
Appinfo	Application Information	Windows	C:\WINDOWS...	Stopped	1
AppMgmt	Application Management	Windows	C:\WINDOWS...	Running	1
AppMgmt	Application Management	Windows	C:\WINDOWS...	Stopped	2
apport	apport	Linux		Stopped	1
aspnet_state	ASP.NET State Service	Windows	C:\WINDOWS\MICROSOFT.NET...	Stopped	1
atd	atd	Linux		Running	2

Selected: 0 of 471

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 service location.
Status	Displays the service status.
Computers Count	Indicates the number of endpoint computers on which the service is loaded

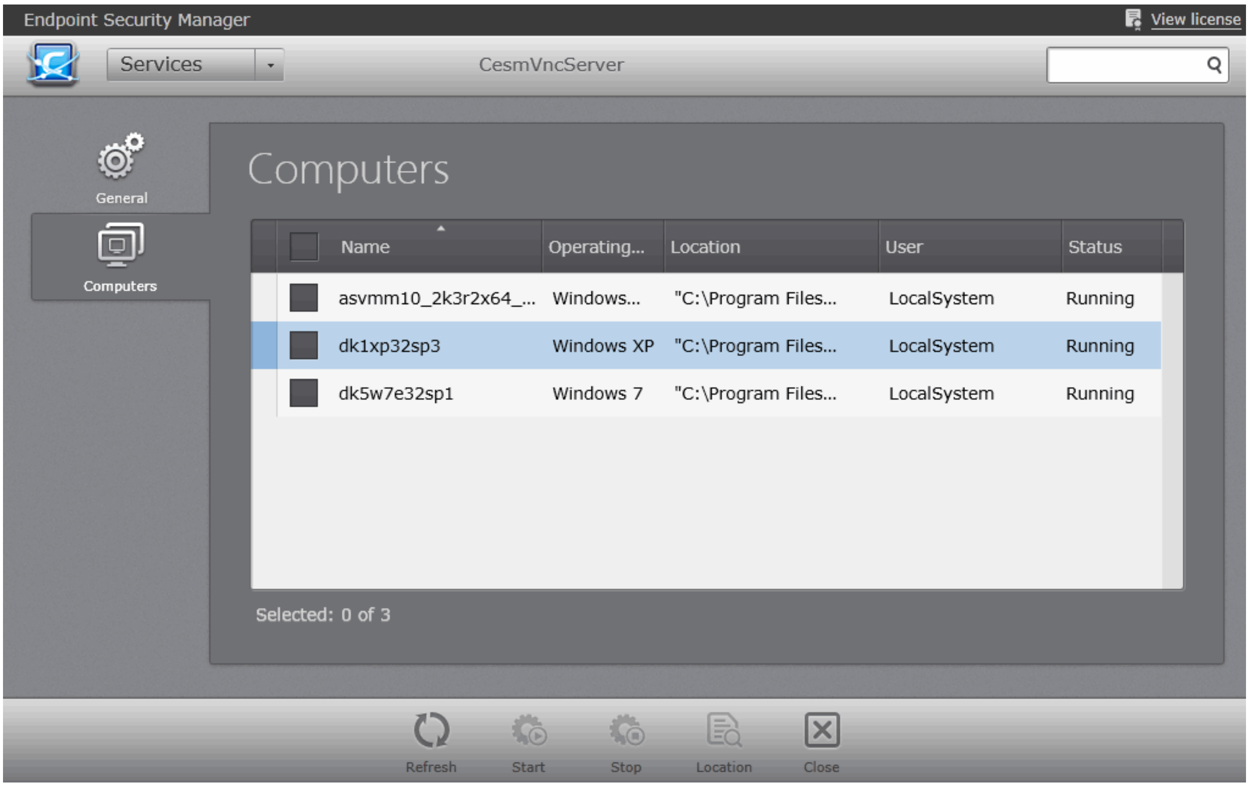
To view process properties

- Select a 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.

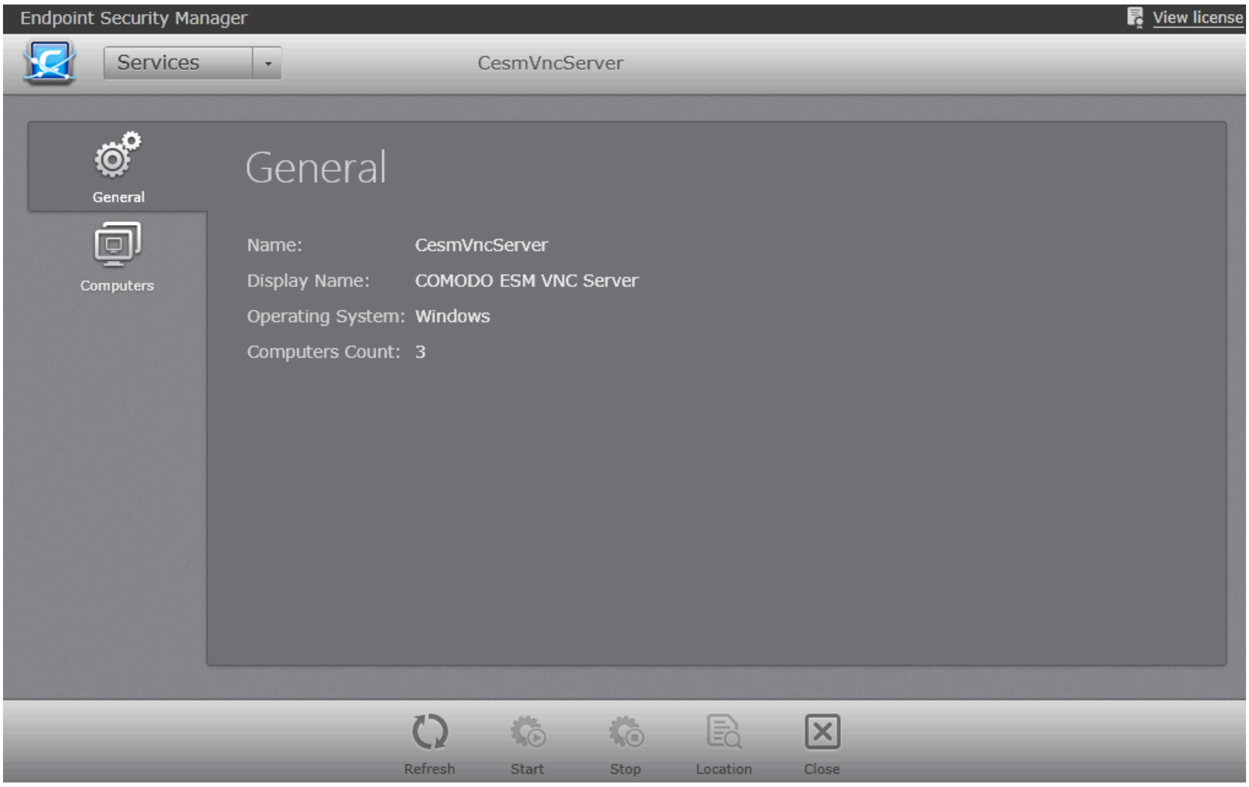


Computers

□	Name	Operating...	Location	User	Status
□	asvmm10_2k3r2x64_...	Windows...	"C:\Program Files...	LocalSystem	Running
□	dk1xp32sp3	Windows XP	"C:\Program Files...	LocalSystem	Running
□	dk5w7e32sp1	Windows 7	"C:\Program Files...	LocalSystem	Running

Selected: 0 of 3

- To stop a running service, select the computer and click 'Stop' from the options at the bottom.
- To start a stopped service, select the computer and click 'Start' from the options at the bottom.
- To open service location, select the computer and click 'Location' at the bottom.



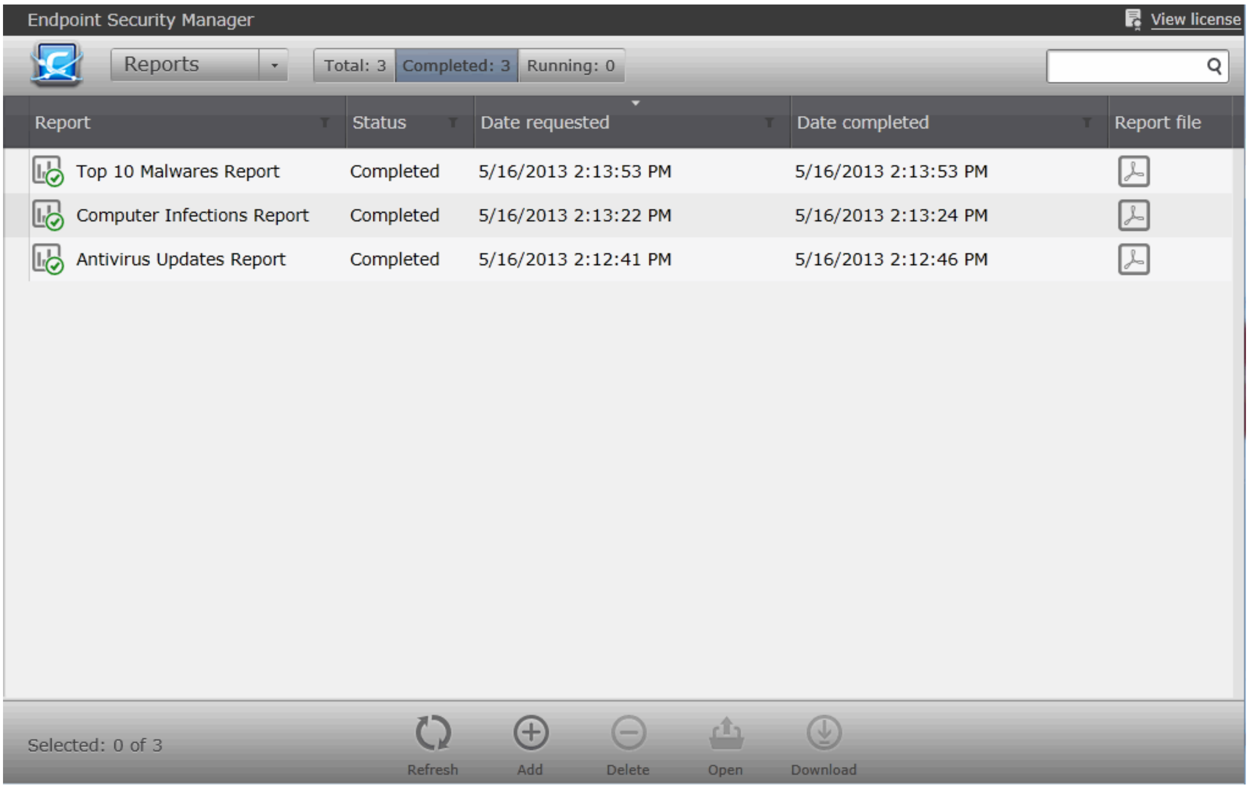
General

Name: CesmVncServer
Display Name: COMODO ESM VNC Server
Operating System: Windows
Computers Count: 3

9. 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.



Report	Status	Date requested	Date completed	Report file
Top 10 Malwares Report	Completed	5/16/2013 2:13:53 PM	5/16/2013 2:13:53 PM	
Computer Infections Report	Completed	5/16/2013 2:13:22 PM	5/16/2013 2:13:24 PM	
Antivirus Updates Report	Completed	5/16/2013 2:12:41 PM	5/16/2013 2:12:46 PM	

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.

Report Types

- **Antivirus Updates** - Information on versions of AV signature databases at the endpoints.
- **CES Configuration** - Information on components of CES installed at the endpoints and their configuration status.
- **CES Log** - Logs of events related to CES 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 CES and the endpoints affected by them.

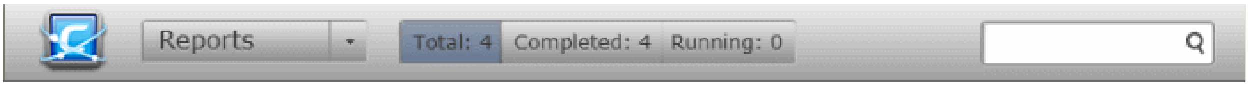
- **Malware Statistics** - Statistical information on the malware detected at various AV scans run on the target endpoint(s), with the actions taken against them.
- **Policy Compliance** - A summary of compliance of the endpoints to their assigned security policies and a detailed information on the security 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.

Filter Options

The filter options in the gray stripe, gives at-a-glance statistics of the reports requested, completed and under generation.

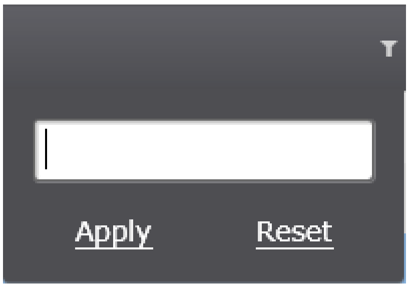
Clicking a category displays only the reports falling into that category.

The search field lets the administrator search for report(s) by endpoint or report completion/request date.

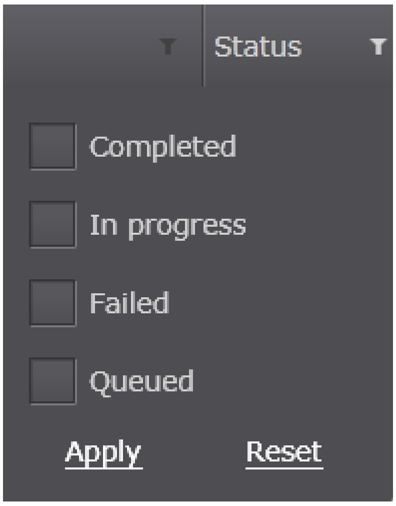


More filters can be applied by clicking the funnel icon beside the column heading.

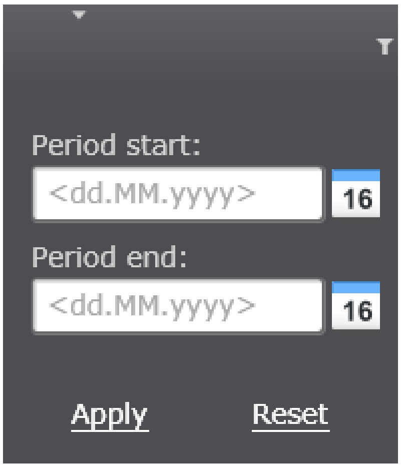
- Click the filter icon in the 'Report' column header to search for a specific report type:



- 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' column header to search for reports that were requested within a specific date range.



Period start:

<dd.MM.yyyy>

Period end:

<dd.MM.yyyy>

- Click the filter icon ▼ in the 'Date Completed' column header to search for reports that were completed within a specific date range.
- Click 'Reset' to display all the items.

Generating a Report

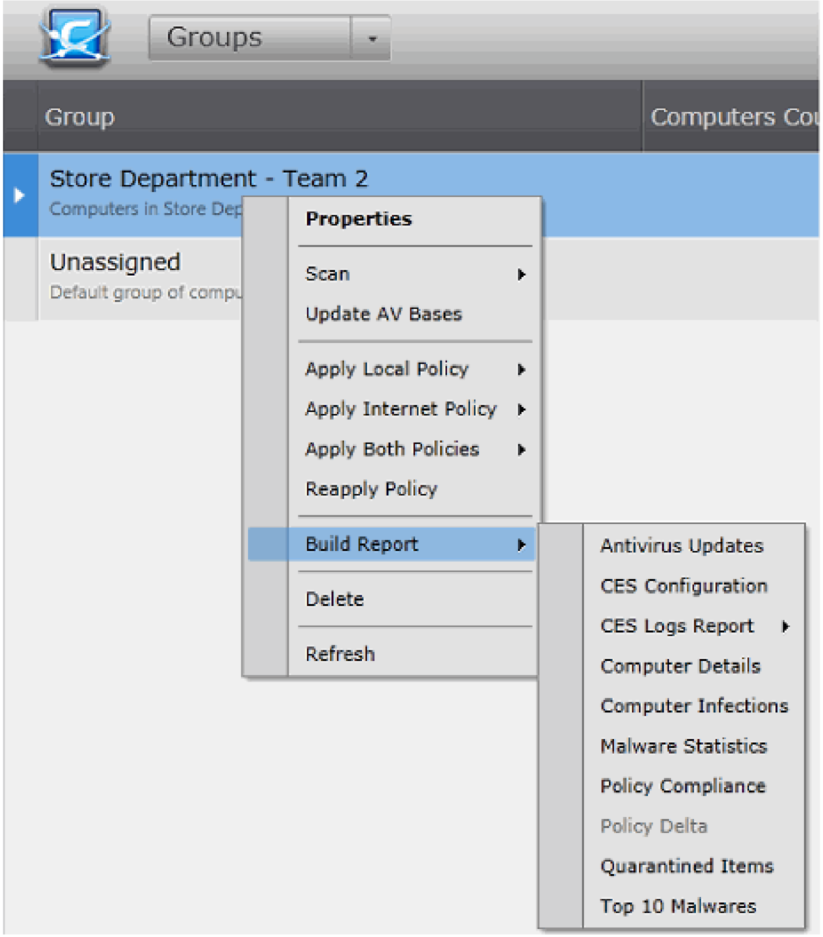
Administrators can generate reports for defined groups of endpoints, individual endpoints or selected endpoints. Group reports can be generated from the 'Groups' area, Reports for individual endpoints can be generated from the 'Computers' area.

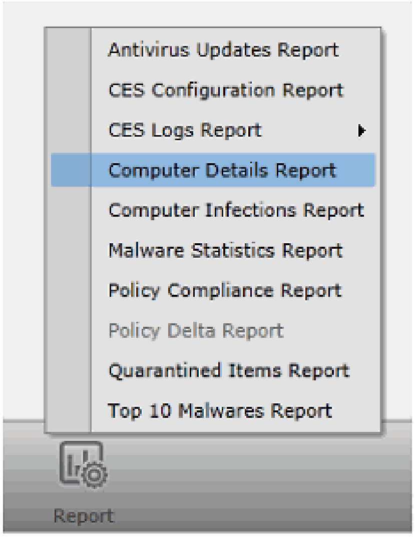
To generate reports for a selected group

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 group, select 'Report' from the bottom of the interface and choose the report type.

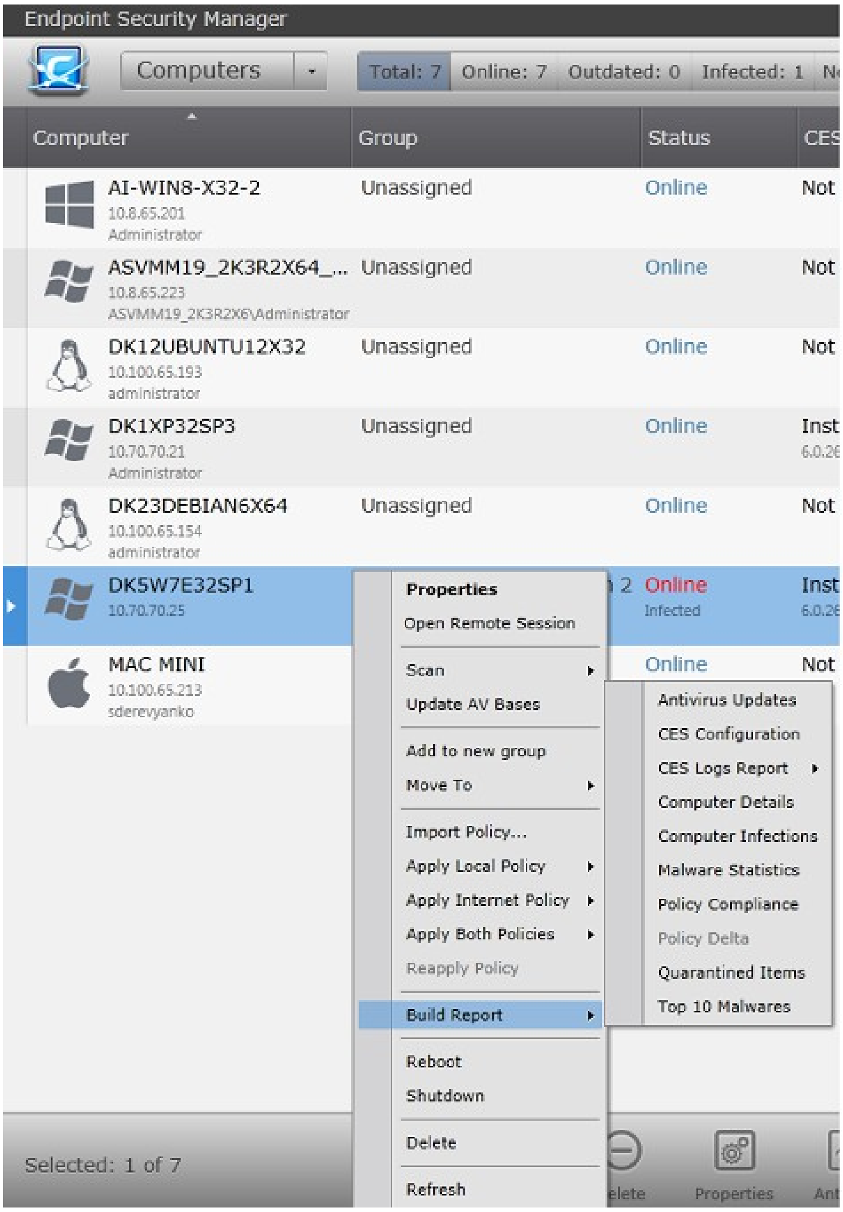




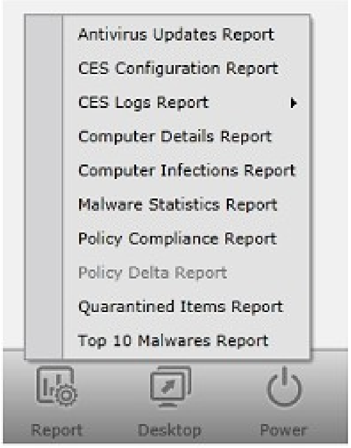
The report generation will be started or added to the queue. The progress will be displayed in the 'Reports' area. On completion, the report can be opened from the 'Reports' area. Refer to the sections below for detailed explanations on each report type.

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.



Computer	Group	Status	CES
AI-WIN8-X32-2 10.8.65.201 Administrator	Unassigned	Online	Not
ASVMM19_2K3R2X64_... 10.8.65.223 ASVMM19_2K3R2X6\Administrator	Unassigned	Online	Not
DK12UBUNTU12X32 10.100.65.193 administrator	Unassigned	Online	Not
DK1XP32SP3 10.70.70.21 Administrator	Unassigned	Online	Inst 6.0.26
DK23DEBIAN6X64 10.100.65.154 administrator	Unassigned	Online	Not
DK5W7E32SP1 10.70.70.25		Online Infected	Inst 6.0.26
MAC MINI 10.100.65.213 sderevyanko		Online	Not



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. The administrator can choose the printable file to be generated in portable document (.pdf) or spreadsheet (.xls) format.

Viewing the Report

Selecting a report from the list and clicking 'Open' from the options at the bottom or right clicking a report and choosing 'Open' from the context sensitive menu will open the report.

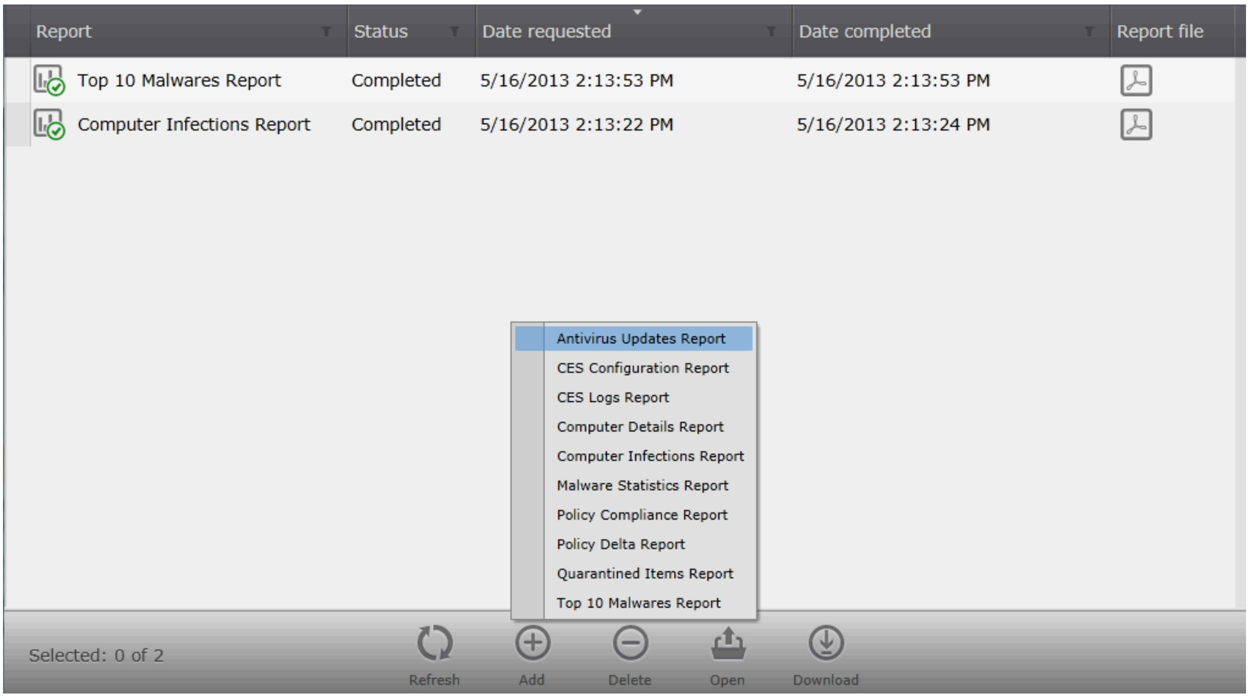
The following sections explain each of these report types in detail.

9.1. 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.

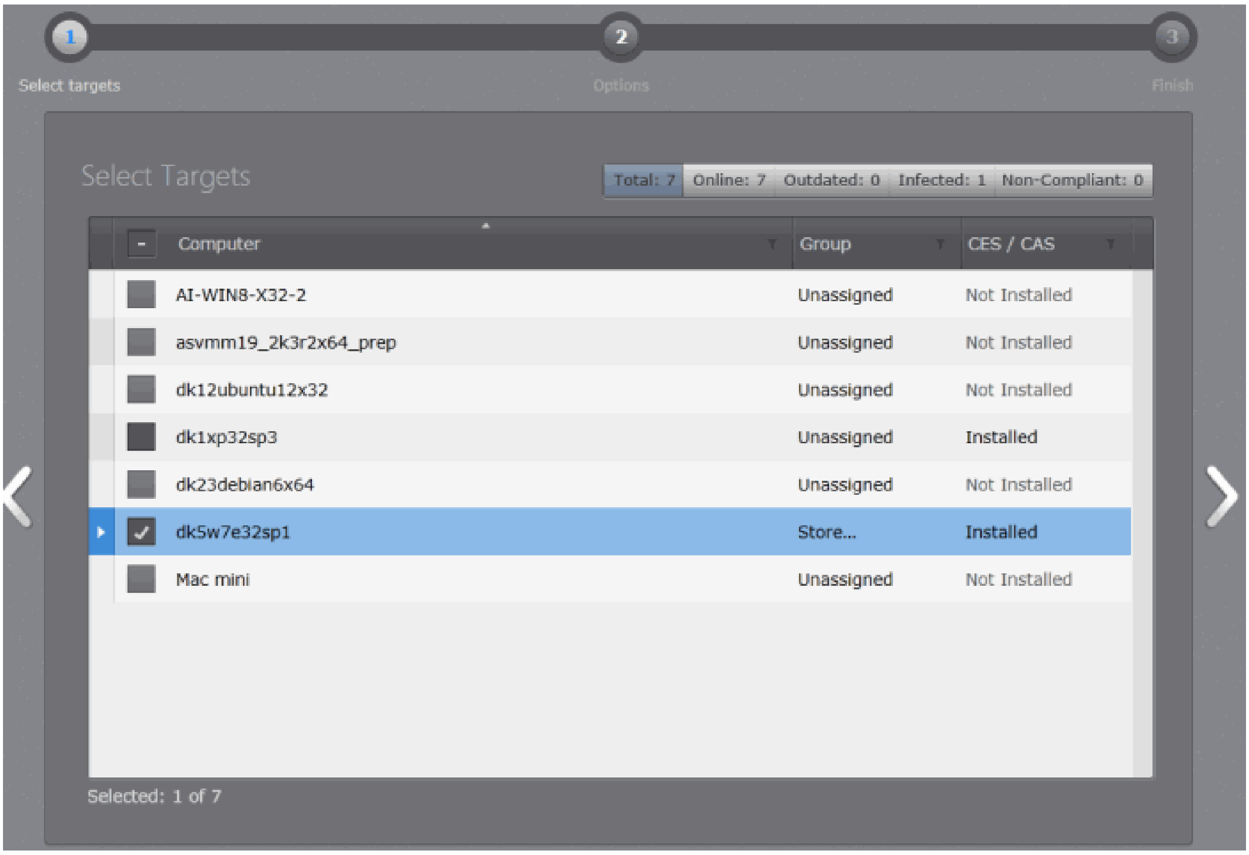


Report	Status	Date requested	Date completed	Report file
Top 10 Malwares Report	Completed	5/16/2013 2:13:53 PM	5/16/2013 2:13:53 PM	
Computer Infections Report	Completed	5/16/2013 2:13:22 PM	5/16/2013 2:13:24 PM	

- 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.



	Computer	Group	CES / CAS
□	AI-WIN8-X32-2	Unassigned	Not Installed
□	asvmm19_2k3r2x64_prep	Unassigned	Not Installed
□	dk12ubuntu12x32	Unassigned	Not Installed
□	dk1xp32sp3	Unassigned	Installed
□	dk23debian6x64	Unassigned	Not Installed
☑	dk5w7e32sp1	Store...	Installed
□	Mac mini	Unassigned	Not Installed

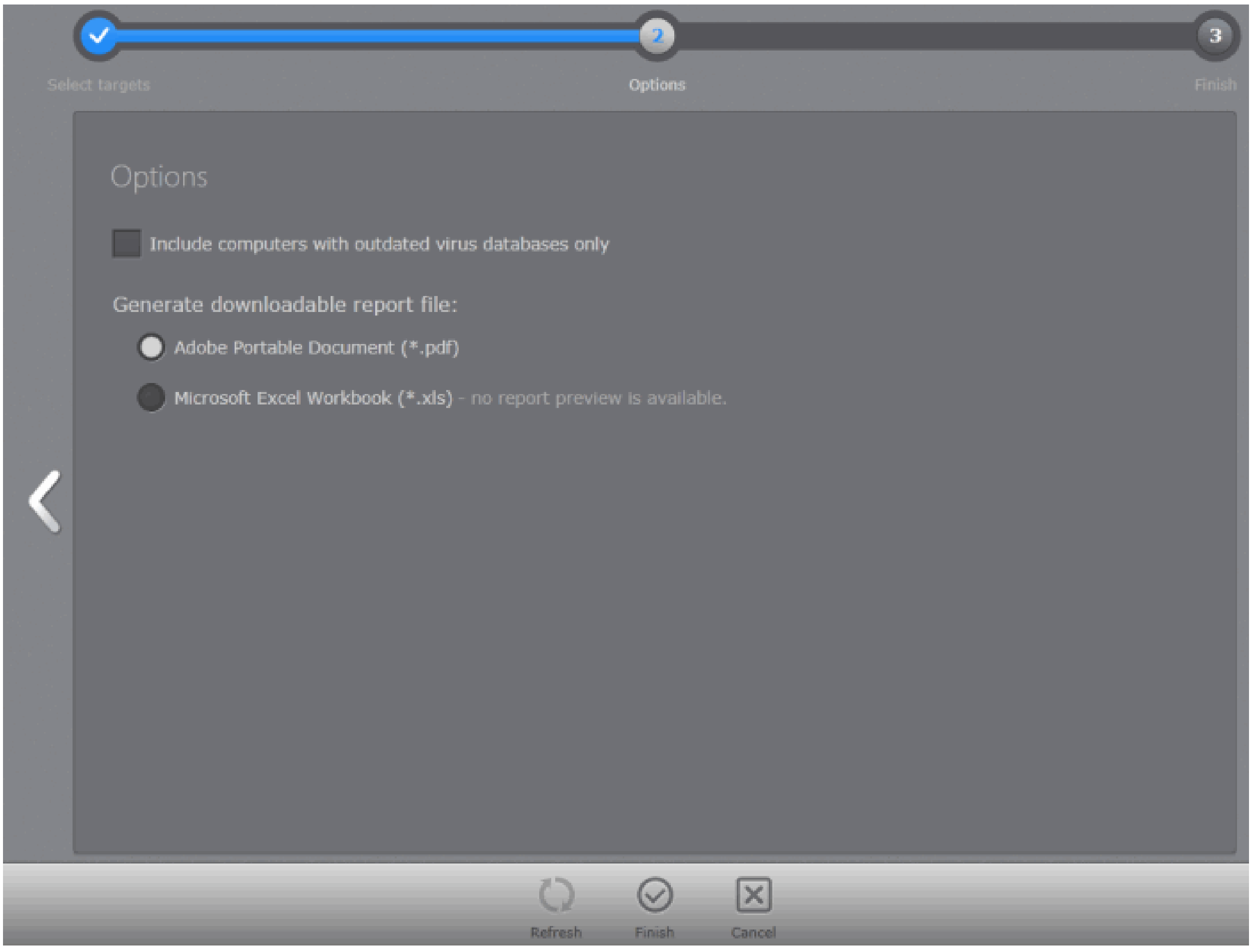
- Select the endpoint(s) for which you wish to generate the AV Updates report. The filter options in the header provides at-a-glance statistics of the computers in the network and allow the administrator to filter the computers based on the criteria. You can also filter the computers by clicking the 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 downloaded to the administrator's computer.

- Select required options



Options

□ Include computers with outdated virus databases only

Generate downloadable report file:

○ Adobe Portable Document (*.pdf)

● Microsoft Excel Workbook (*.xls) - no report preview is available.

- Click the 'Finish' icon to start generating the report.

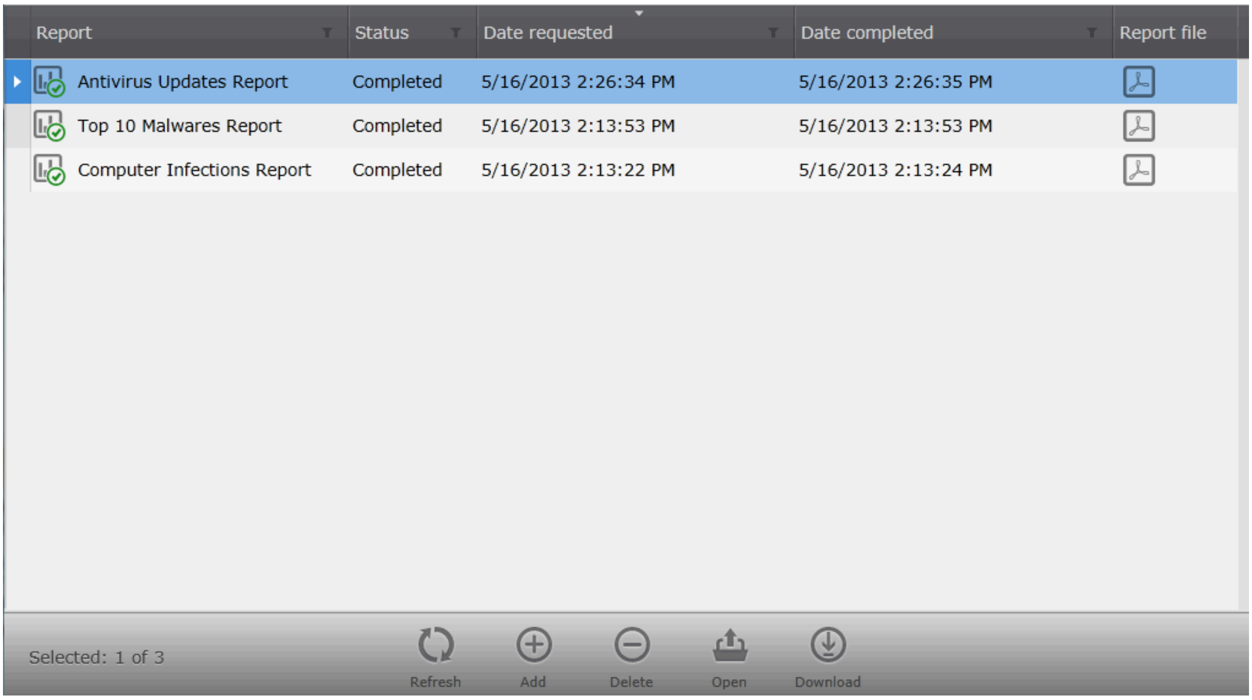
The report generation will be started or added to the queue. The progress will be displayed in the 'Reports' area.

View the Report

The administrator can view the report at anytime after the completion.

To view the report

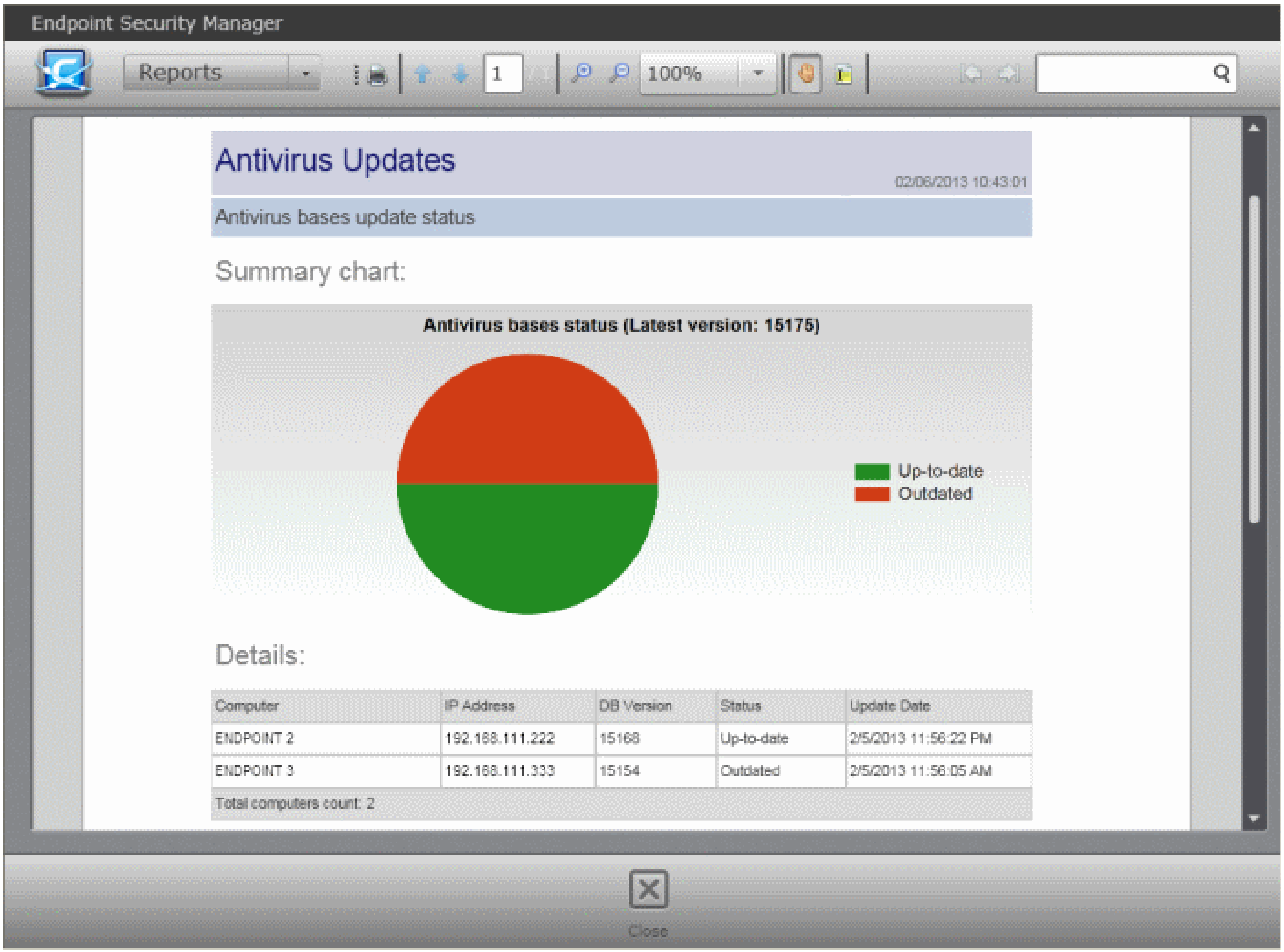
- Select the report and click Open or right click on the report and choose Open from the context sensitive menu.



Report	Status	Date requested	Date completed	Report file
Antivirus Updates Report	Completed	5/16/2013 2:26:34 PM	5/16/2013 2:26:35 PM	
Top 10 Malwares Report	Completed	5/16/2013 2:13:53 PM	5/16/2013 2:13:53 PM	
Computer Infections Report	Completed	5/16/2013 2:13:22 PM	5/16/2013 2:13:24 PM	

Selected: 1 of 3

The report will contain the AV signature database update details at each endpoint selected in step 1.



Endpoint Security Manager
Reports
1
100%

Antivirus Updates

02/06/2013 10:43:01

Antivirus bases update status

Summary chart:

Antivirus bases status (Latest version: 15175)
Up-to-date
Outdated

Details:

Computer	IP Address	DB Version	Status	Update Date
ENDPOINT 2	192.168.111.222	15168	Up-to-date	2/5/2013 11:56:22 PM
ENDPOINT 3	192.168.111.333	15154	Outdated	2/5/2013 11:56:05 AM
Total computers count: 2				

- 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.

Downloading the Report

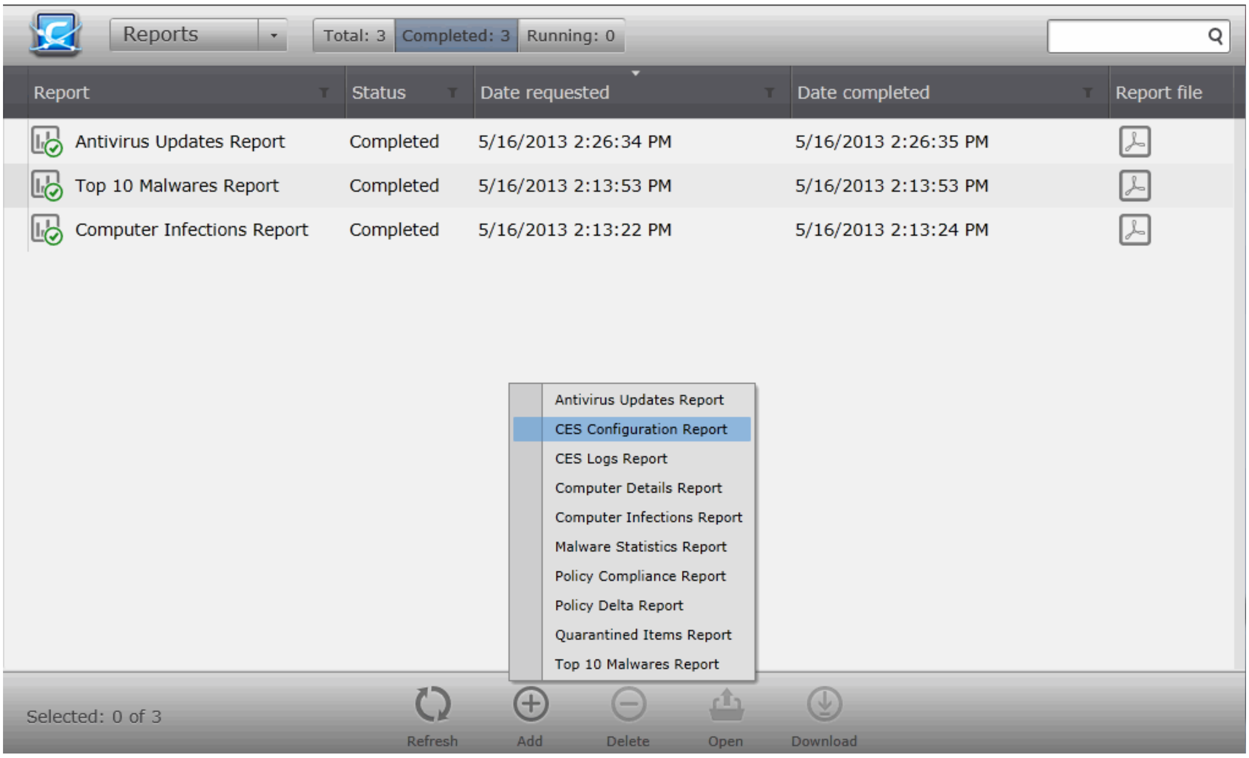
If the administrator had opted for generating a downloadable report, it can be downloaded by selecting the Report in the 'Reports' area and clicking the download icon ⬇ at the bottom.

9.2. CES Configuration Report

The 'CES Configuration' report provides information on components of CES installed and enabled on the target computers according to their applied policies.

To generate a CES Configuration report

- Open the 'Reports' area by choosing 'Reports' from the drop-down at the top left.



Reports

Total: 3 Completed: 3 Running: 0

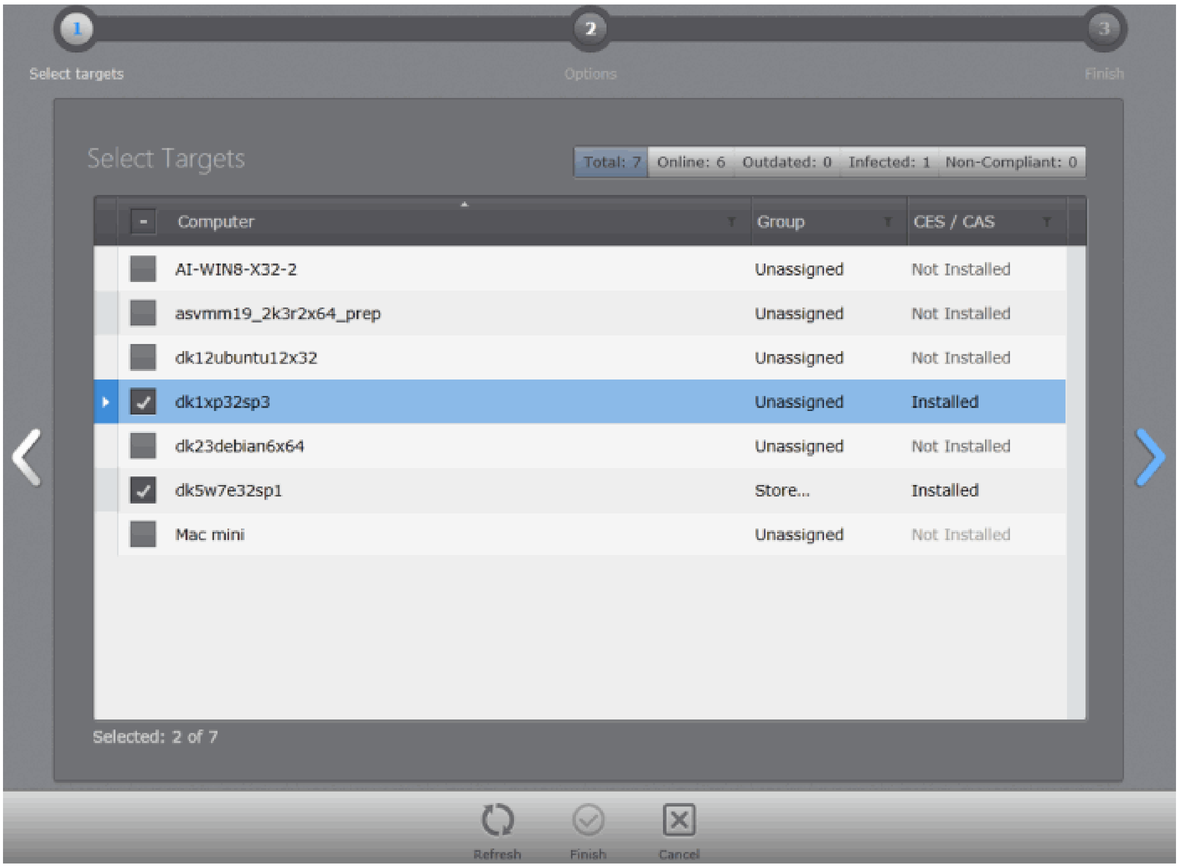
Report	Status	Date requested	Date completed	Report file
Antivirus Updates Report	Completed	5/16/2013 2:26:34 PM	5/16/2013 2:26:35 PM	
Top 10 Malwares Report	Completed	5/16/2013 2:13:53 PM	5/16/2013 2:13:53 PM	
Computer Infections Report	Completed	5/16/2013 2:13:22 PM	5/16/2013 2:13:24 PM	

Selected: 0 of 3

- Click 'Add' and choose 'CES Configuration Report'. The 'Create CES Configuration Report' wizard will start.

Step 1 - Selecting Targets

The list of all the endpoint computers connected to CESM is displayed.



Select Targets

Total: 7 | Online: 6 | Outdated: 0 | Infected: 1 | Non-Compliant: 0

	Computer	Group	CES / CAS
□	AI-WIN8-X32-2	Unassigned	Not Installed
□	asvmm19_2k3r2x64_prep	Unassigned	Not Installed
□	dk12ubuntu12x32	Unassigned	Not Installed
☑	dk1xp32sp3	Unassigned	Installed
□	dk23debian6x64	Unassigned	Not Installed
☑	dk5w7e32sp1	Store...	Installed
□	Mac mini	Unassigned	Not Installed

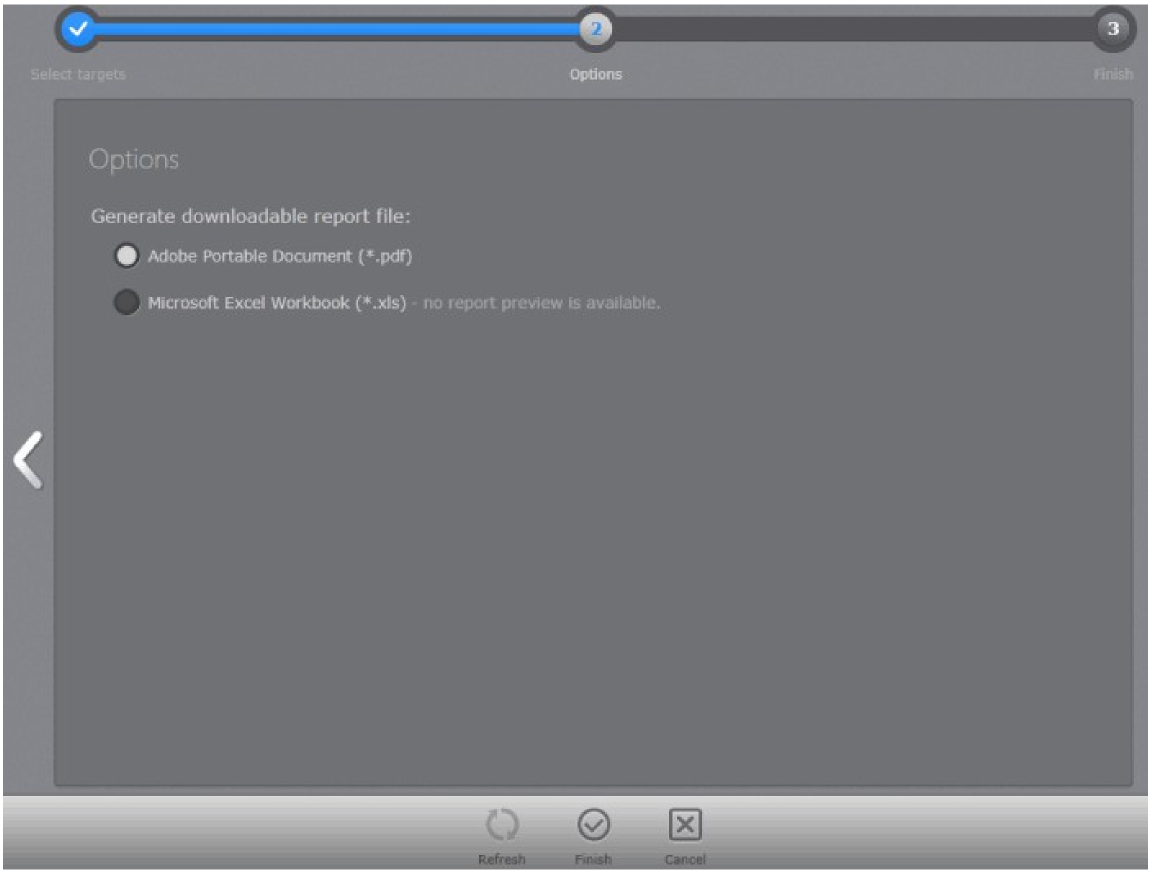
Selected: 2 of 7

- Select the endpoint(s) for which you wish to generate the CES 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 downloaded to the administrator's computer.
- Select required options.



Options

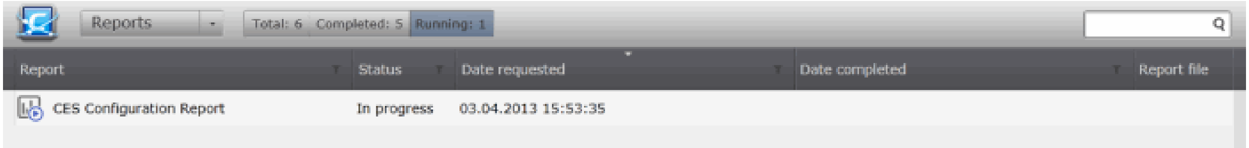
Generate downloadable report file:

○ Adobe Portable Document (*.pdf)

● Microsoft Excel Workbook (*.xls) - no report preview is available.

- 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.



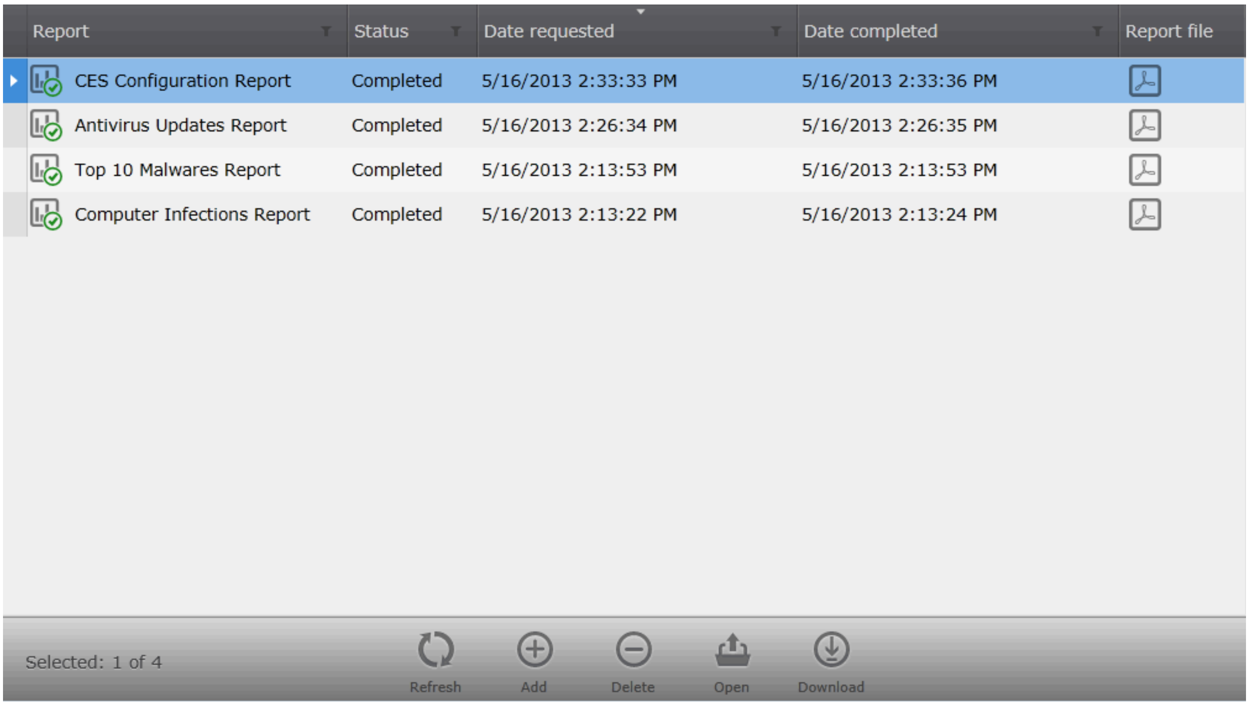
Report	Status	Date requested	Date completed	Report file
CES Configuration Report	In progress	03.04.2013 15:53:35		

View the Report

The administrator can view the report at anytime after the completion.

To view the report

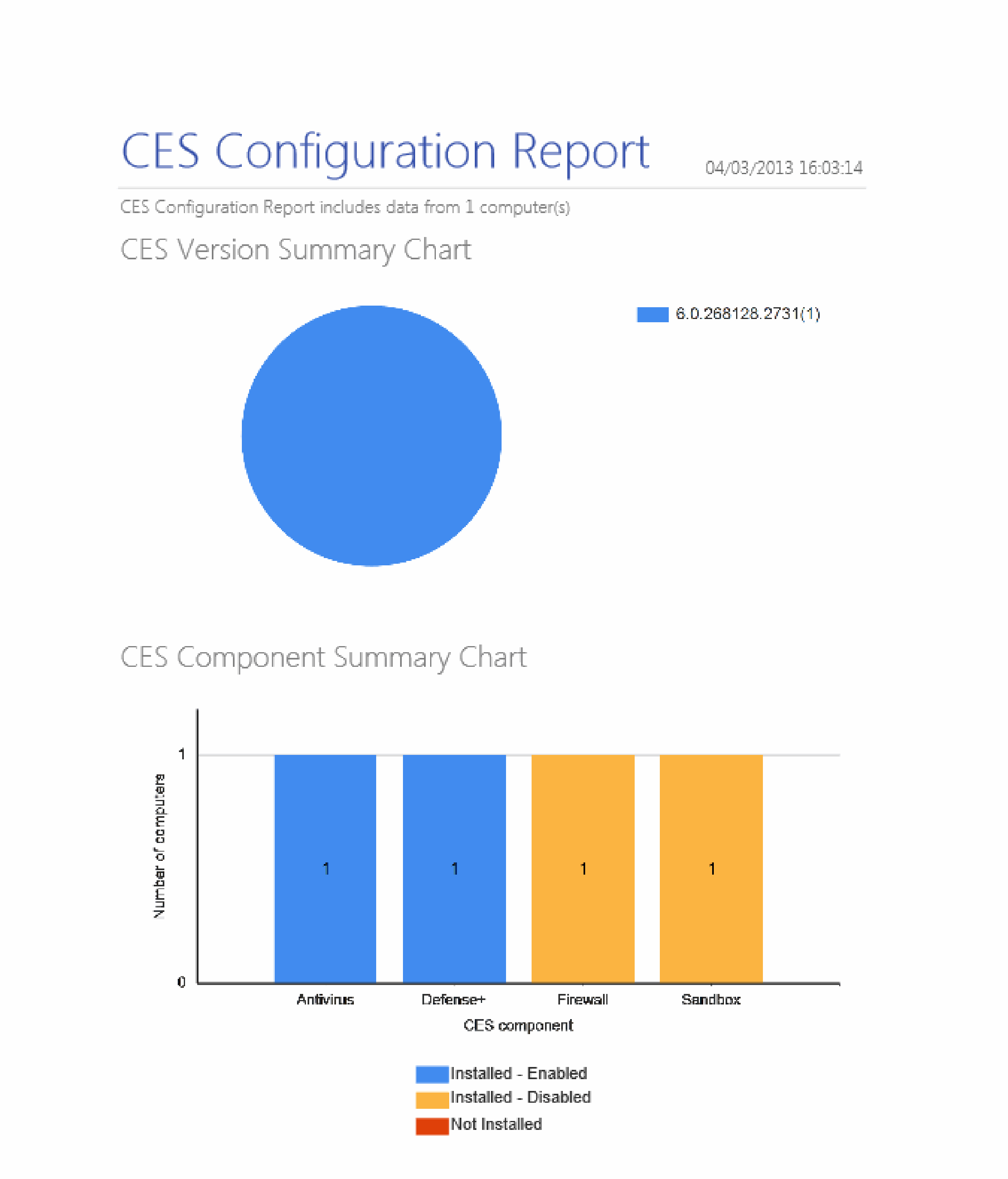
- Select the report and click 'Open' or right click on the report and choose 'Open' from the context sensitive menu.



Report	Status	Date requested	Date completed	Report file
CES Configuration Report	Completed	5/16/2013 2:33:33 PM	5/16/2013 2:33:36 PM	
Antivirus Updates Report	Completed	5/16/2013 2:26:34 PM	5/16/2013 2:26:35 PM	
Top 10 Malwares Report	Completed	5/16/2013 2:13:53 PM	5/16/2013 2:13:53 PM	
Computer Infections Report	Completed	5/16/2013 2:13:22 PM	5/16/2013 2:13:24 PM	

Selected: 1 of 4

The report will contain the details on CES versions and CES components installed/activated on the endpoints selected in step 1.



CES Configuration Report 04/03/2013 16:03:14

CES Configuration Report includes data from 1 computer(s)

CES Version Summary Chart

CES Component Summary Chart

- The summary pie chart in the upper portion provides an at-a-glance information of CES versions installed in the selected endpoints.
- The bar-graph displays a comparison of CES components installed and activated in the selected endpoints
- Following the graphical summary, details of each computer, with CES versions, installed and enabled components are displayed.

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.

9.3. CES Log Report

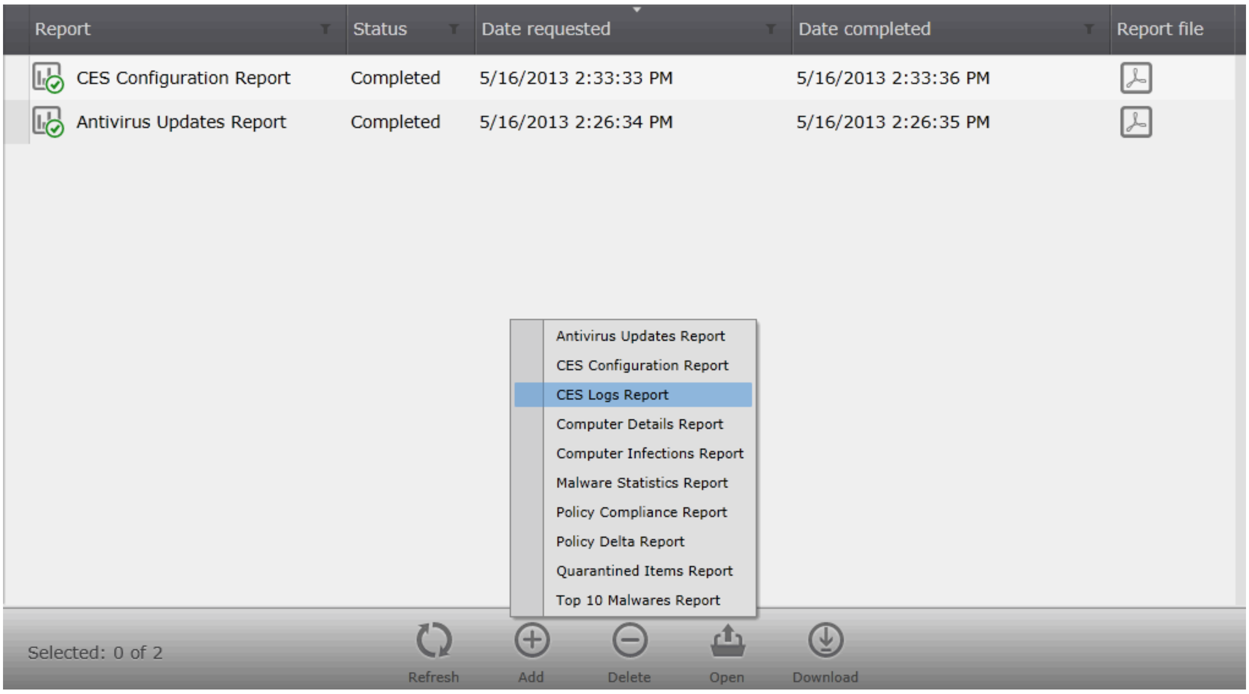
The CES installation in each target computer maintains a log of events for each of the Antivirus, Firewall and Defense+ components.

- **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.

The CES Log 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 CES Logs report

- Open the 'Reports' area by choosing 'Reports' from the drop-down at the top left.



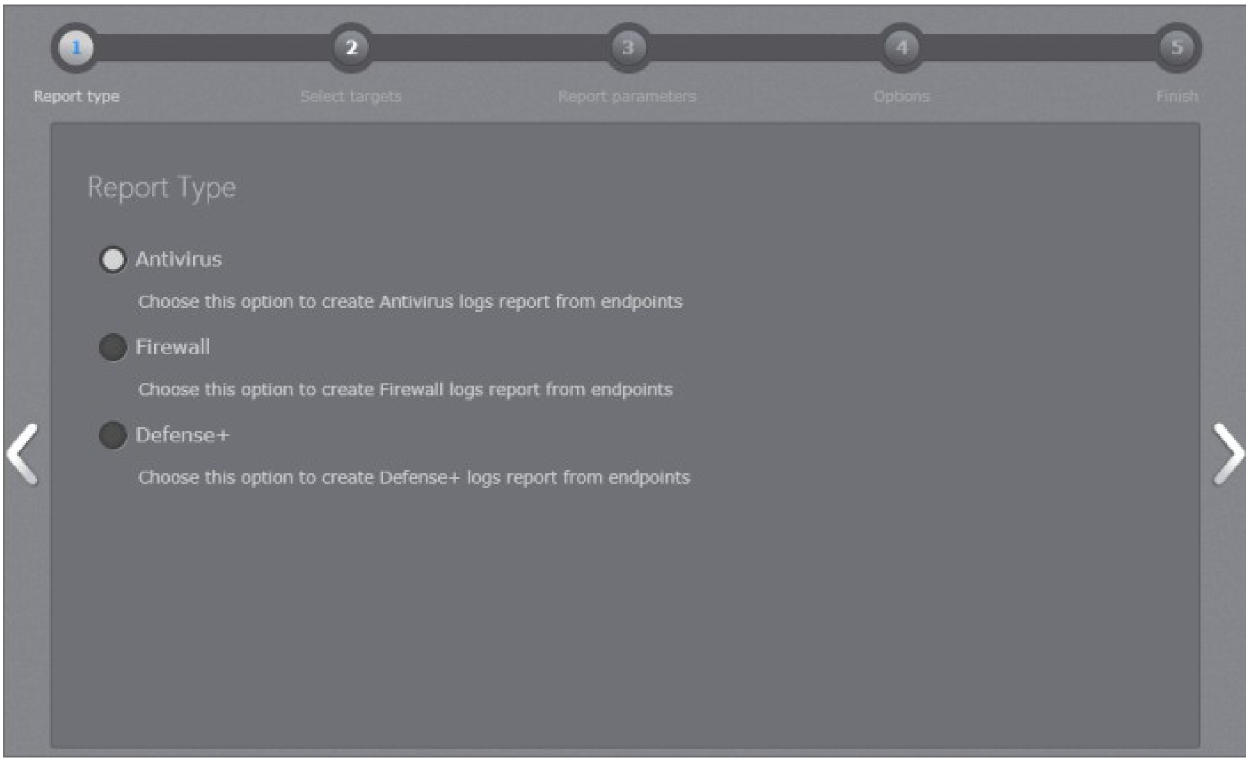
Report	Status	Date requested	Date completed	Report file
CES Configuration Report	Completed	5/16/2013 2:33:33 PM	5/16/2013 2:33:36 PM	
Antivirus Updates Report	Completed	5/16/2013 2:26:34 PM	5/16/2013 2:26:35 PM	

Selected: 0 of 2

- Click 'Add' and choose 'CES Logs Report'. The 'Create CES Logs Report' wizard will start.

Step 1 - Select Report Type

The first step is to choose the CES component for which you want to generate a log report.



Report Type

○ Antivirus

Choose this option to create Antivirus logs report from endpoints

● Firewall

Choose this option to create Firewall logs report from endpoints

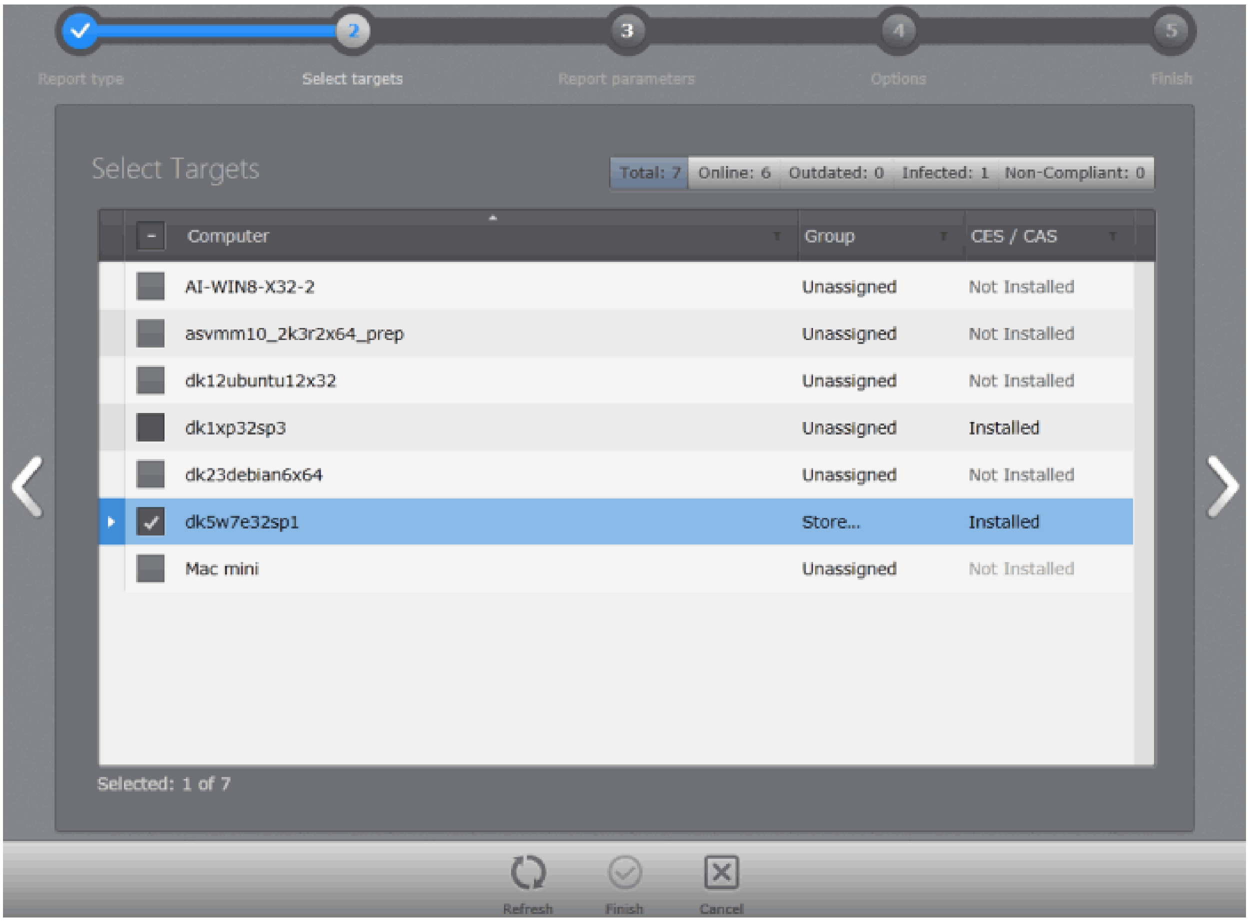
● Defense+

Choose this option to create Defense+ logs report from endpoints

- 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 Targets

Total: 7 | Online: 6 | Outdated: 0 | Infected: 1 | Non-Compliant: 0

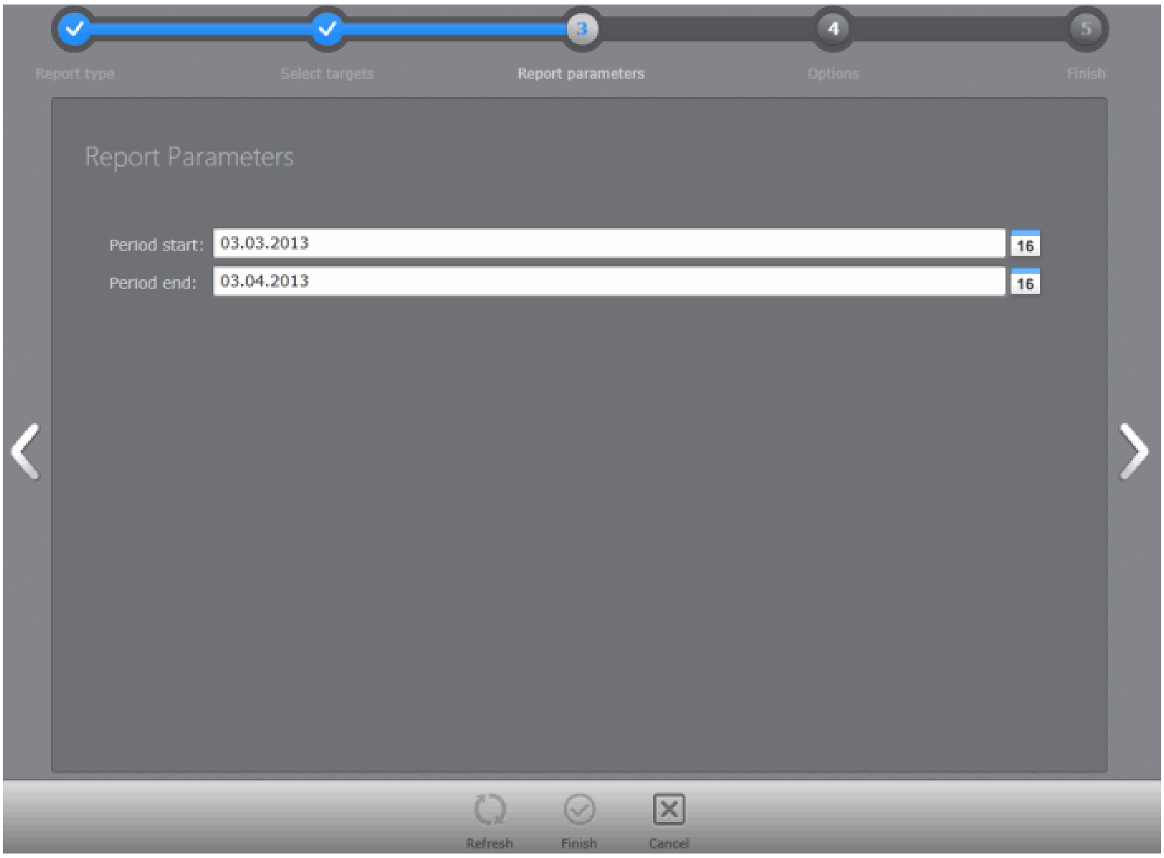
	Computer	Group	CES / CAS
□	AI-WIN8-X32-2	Unassigned	Not Installed
□	asvmm10_2k3r2x64_prep	Unassigned	Not Installed
□	dk12ubuntu12x32	Unassigned	Not Installed
□	dk1xp32sp3	Unassigned	Installed
□	dk23debian6x64	Unassigned	Not Installed
☑	dk5w7e32sp1	Store...	Installed
□	Mac mini	Unassigned	Not Installed

Selected: 1 of 7

- Select the endpoint(s) for which you wish to generate the CES 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 3 – Report Parameters

The next step is to choose the time period, that the report should include the log saved during it.



Report Parameters

Period start: 03.03.2013

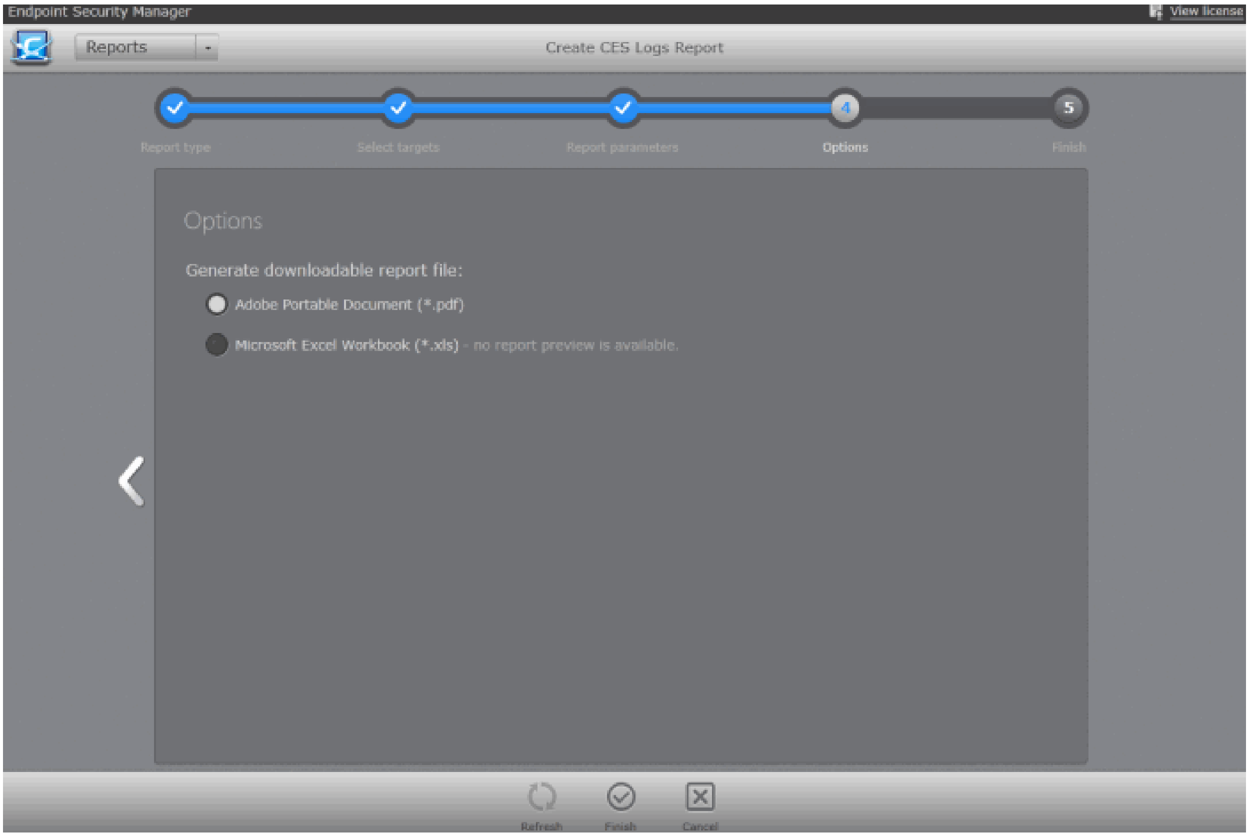
Period end: 03.04.2013

- 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 downloaded to the administrator's computer.
- Select required options.



Options

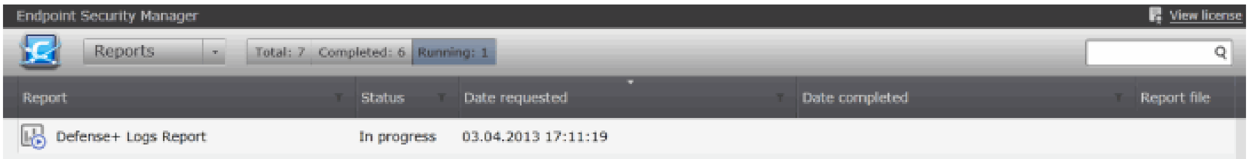
Generate downloadable report file:

○ Adobe Portable Document (*.pdf)

○ Microsoft Excel Workbook (*.xls) - no report preview is available.

- 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.

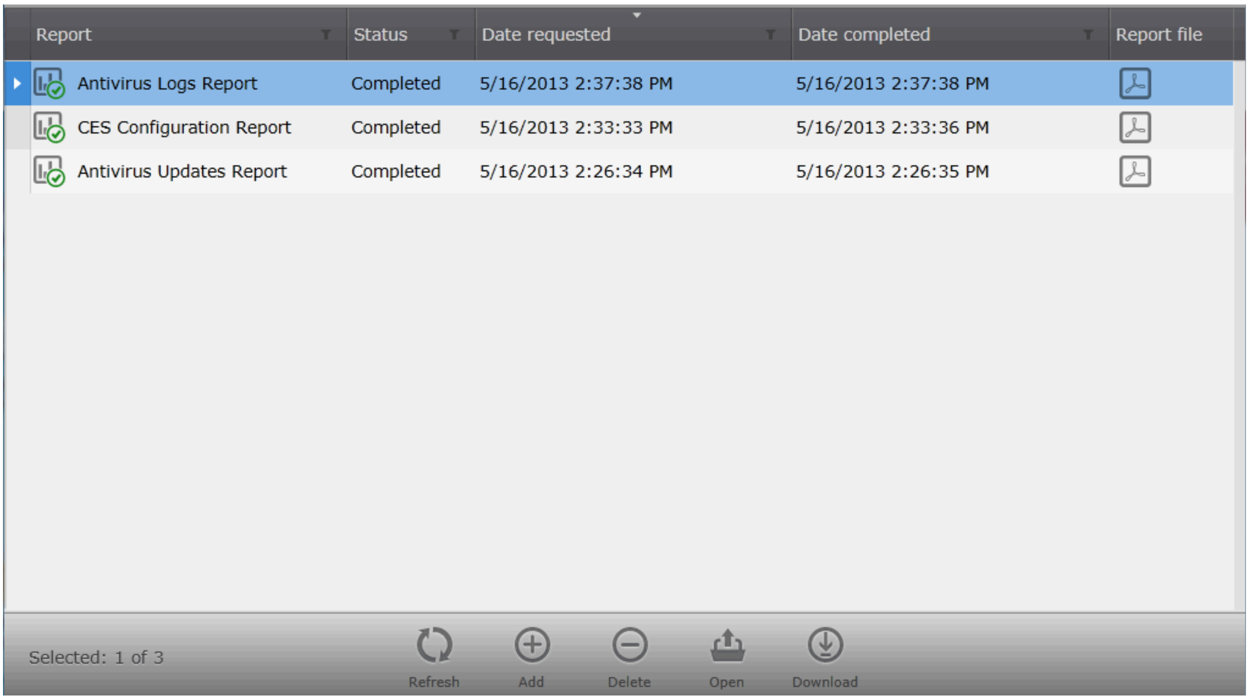


Report	Status	Date requested	Date completed	Report file
Defense+ Logs Report	In progress	03.04.2013 17:11:19		

View the Report

The administrator can view the report at anytime after the completion.

To view the report



Report	Status	Date requested	Date completed	Report file
Antivirus Logs Report	Completed	5/16/2013 2:37:38 PM	5/16/2013 2:37:38 PM	
CES Configuration Report	Completed	5/16/2013 2:33:33 PM	5/16/2013 2:33:36 PM	
Antivirus Updates Report	Completed	5/16/2013 2:26:34 PM	5/16/2013 2:26:35 PM	

Selected: 1 of 3

- Select the report and click Open or right click on the report and choose Open from the context sensitive menu.

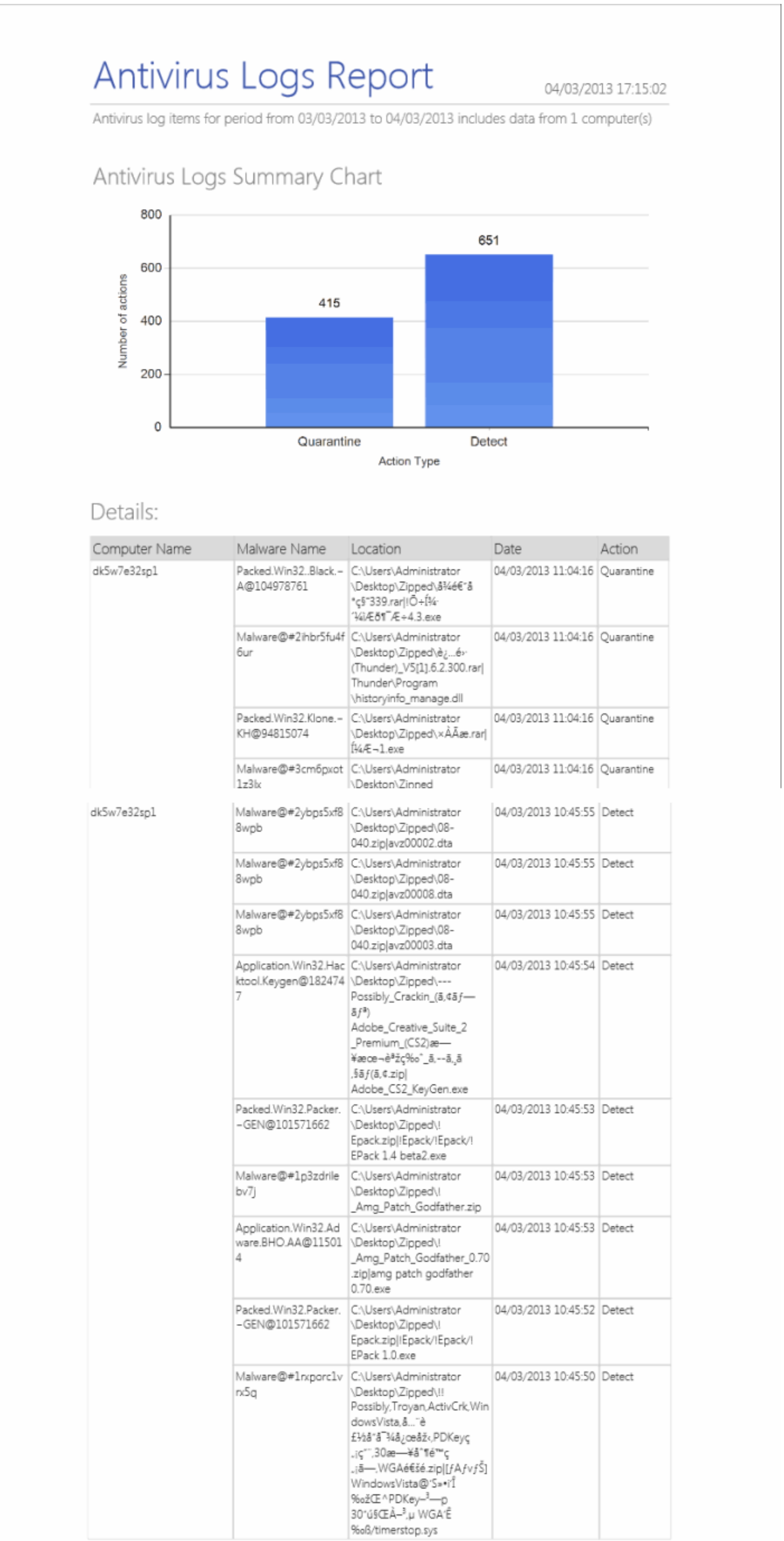
The report will contain the log entries for the component selected in step 1, recorded at the target endpoints selected at step 2 for the time period selected in step 3. If more than one computer is selected in step 2, the log reports are given for them one by one.

Examples of:

- **Antivirus Log Report**
- **Firewall Log Report** and
- **Defense+ Log Report**

... are shown below.

Antivirus Log Report



Antivirus Logs Report 04/03/2013 17:15:02

Antivirus log items for period from 03/03/2013 to 04/03/2013 includes data from 1 computer(s)

Antivirus Logs Summary Chart

Details:

Computer Name	Malware Name	Location	Date	Action
dk5w7e32sp1	Packed.Win32..Black.–A@104978761	C:\Users\Administrator\Desktop\Zipped\å¾é€˜å*ç§˜339.rar|!Õ÷Í¾·˜¼¡Æõ¶¯Æ÷4.3.exe	04/03/2013 11:04:16	Quarantine
	Malware@#2ihbr5fu4f6ur	C:\Users\Administrator\Desktop\Zipped\è¿…é›·(Thunder)_V5[1].6.2.300.rar|Thunder\Program\historyinfo_manage.dll	04/03/2013 11:04:16	Quarantine
	Packed.Win32.Klone.–KH@94815074	C:\Users\Administrator\Desktop\Zipped\×ÀÃæ.rar|Í¼Æ¬1.exe	04/03/2013 11:04:16	Quarantine
	Malware@#3cm6pxot1z3lx	C:\Users\Administrator\Deskton\Zinned	04/03/2013 11:04:16	Quarantine
dk5w7e32sp1	Malware@#2ybps5xf88wpb	C:\Users\Administrator\Desktop\Zipped\08-040.zip|avz00002.dta	04/03/2013 10:45:55	Detect
	Malware@#2ybps5xf88wpb	C:\Users\Administrator\Desktop\Zipped\08-040.zip|avz00008.dta	04/03/2013 10:45:55	Detect
	Malware@#2ybps5xf88wpb	C:\Users\Administrator\Desktop\Zipped\08-040.zip|avz00003.dta	04/03/2013 10:45:55	Detect
	Application.Win32.Hacktool.Keygen@1824747	C:\Users\Administrator\Desktop\Zipped\---Possibly_Crackin_(ã‚¢ãƒ—ãƒª)Adobe_Creative_Suite_2_Premium_(CS2)æ—¥æœ¬èªžç‰ˆ_ã‚--ã‚¸ã‚§ãƒ(ã‚¢.zip|Adobe_CS2_KeyGen.exe	04/03/2013 10:45:54	Detect
	Packed.Win32.Packer.–GEN@101571662	C:\Users\Administrator\Desktop\Zipped\!Epack.zip|!Epack/!Epack/!EPack 1.4 beta2.exe	04/03/2013 10:45:53	Detect
	Malware@#1p3zdrilebv7j	C:\Users\Administrator\Desktop\Zipped\!_Amg_Patch_Godfather.zip	04/03/2013 10:45:53	Detect
	Application.Win32.Adware.BHO.AA@115014	C:\Users\Administrator\Desktop\Zipped\!_Amg_Patch_Godfather_0.70.zip|amg patch godfather 0.70.exe	04/03/2013 10:45:53	Detect
	Packed.Win32.Packer.–GEN@101571662	C:\Users\Administrator\Desktop\Zipped\!Epack.zip|!Epack/!Epack/!EPack 1.0.exe	04/03/2013 10:45:52	Detect
	Malware@#1rxporc1vrx5q	C:\Users\Administrator\Desktop\Zipped\!!Possibly,Troyan,ActivCrk,WindowsVista,å…¨è£½å“ã‚¯ãƒ©ãƒƒã‚¯,PDKeyç„¡ç””,30æ—¥å‹•ä½œç„¡ã—,WGAé€šé.zip|[ƒAƒvƒŠ]WindowsVista@'S»•iÎ‰ožŒ^PDKey–³—p30“ú§ŒÀ–³,µ WGA'Ê‰ß/timerstop.sys	04/03/2013 10:45:50	Detect

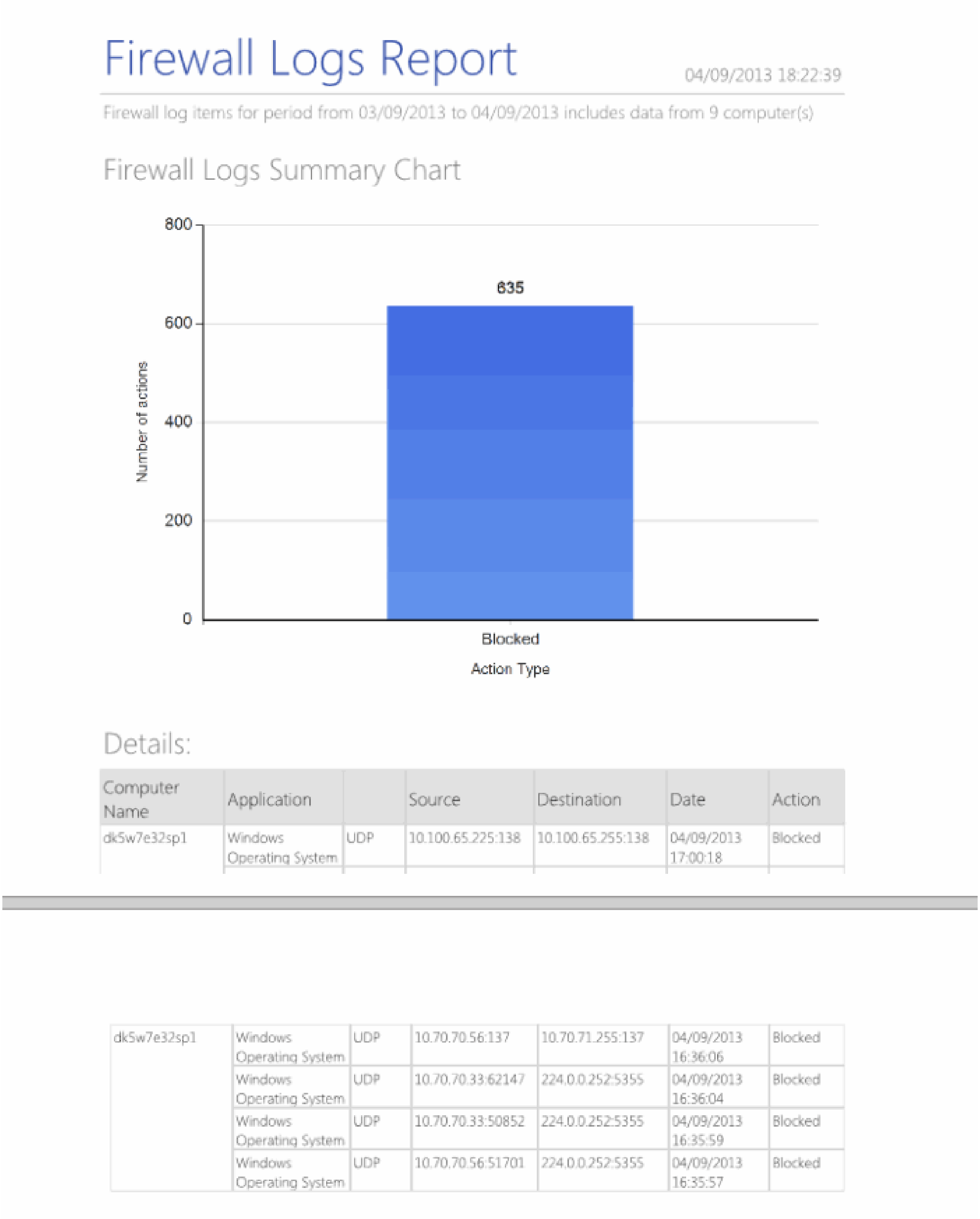
- The summary bar-graph in the upper portion provides an at-a-glance information of number of different AV events at the selected endpoints.

- 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.
  - 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.

Firewall Log Report



Firewall Logs Report

04/09/2013 18:22:39

Firewall log items for period from 03/09/2013 to 04/09/2013 includes data from 9 computer(s)

Firewall Logs Summary Chart

Details:

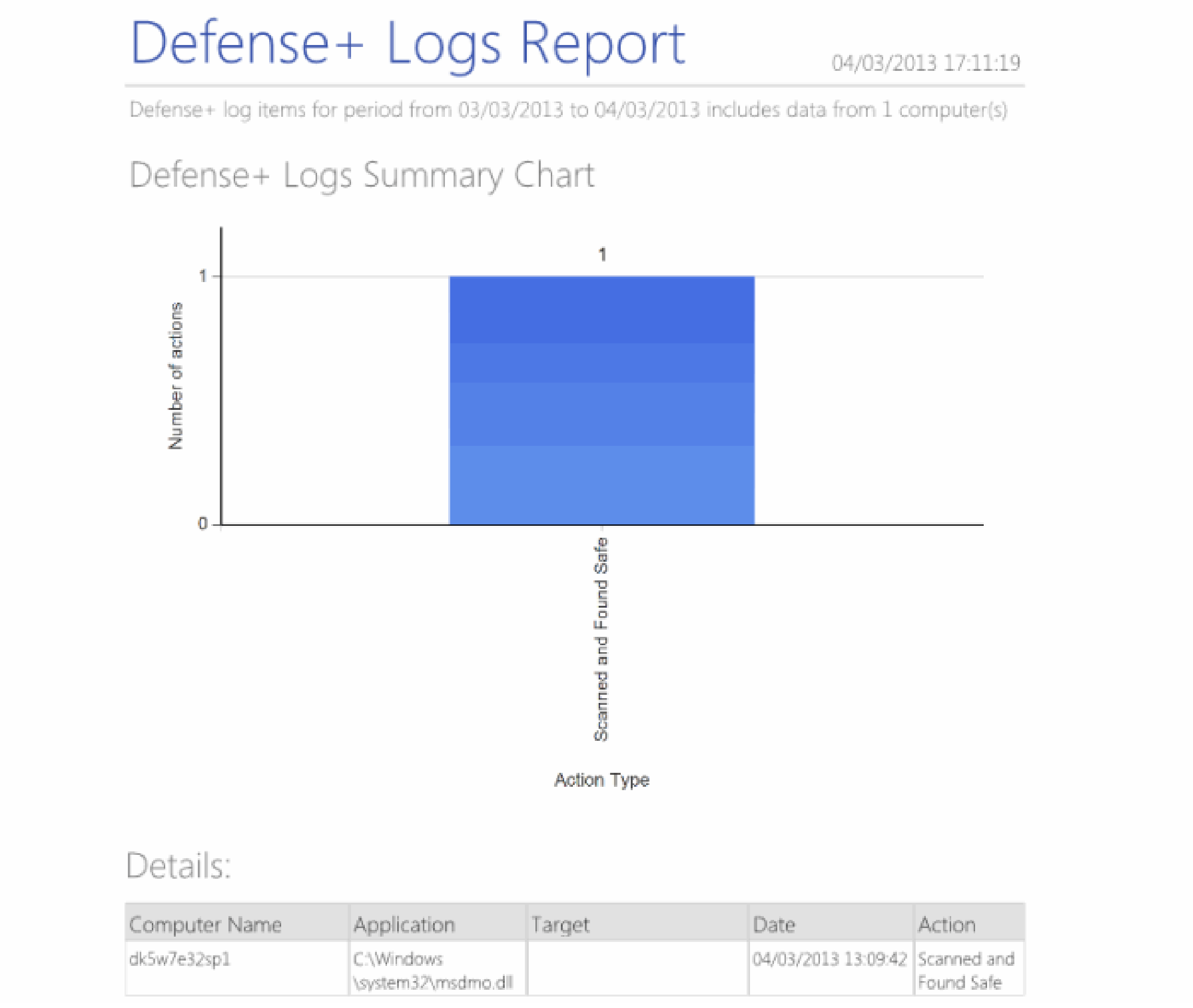
Computer Name	Application		Source	Destination	Date	Action
dk5w7e32sp1	Windows Operating System	UDP	10.100.65.225:138	10.100.65.255:138	04/09/2013 17:00:18	Blocked
dk5w7e32sp1	Windows Operating System	UDP	10.70.70.56:137	10.70.71.255:137	04/09/2013 16:36:06	Blocked
	Windows Operating System	UDP	10.70.70.33:62147	224.0.0.252:5355	04/09/2013 16:36:04	Blocked
	Windows Operating System	UDP	10.70.70.33:50852	224.0.0.252:5355	04/09/2013 16:35:59	Blocked
	Windows Operating System	UDP	10.70.70.56:51701	224.0.0.252:5355	04/09/2013 16:35:57	Blocked

- The summary bar-graph in the upper portion provides an at-a-glance information of 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.
  - Application - Name of the application or program that initiated the connection attempt.
  - Protocol - The protocol of 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.

Defense+ Log Report



Defense+ Logs Report 04/03/2013 17:11:19

Defense+ log items for period from 03/03/2013 to 04/03/2013 includes data from 1 computer(s)

Defense+ Logs Summary Chart

Details:

Computer Name	Application	Target	Date	Action
dk5w7e32sp1	C:\Windows \system32\msdmo.dll		04/03/2013 13:09:42	Scanned and Found Safe

- 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

  - Application - Indicates which application or process propagated the event.

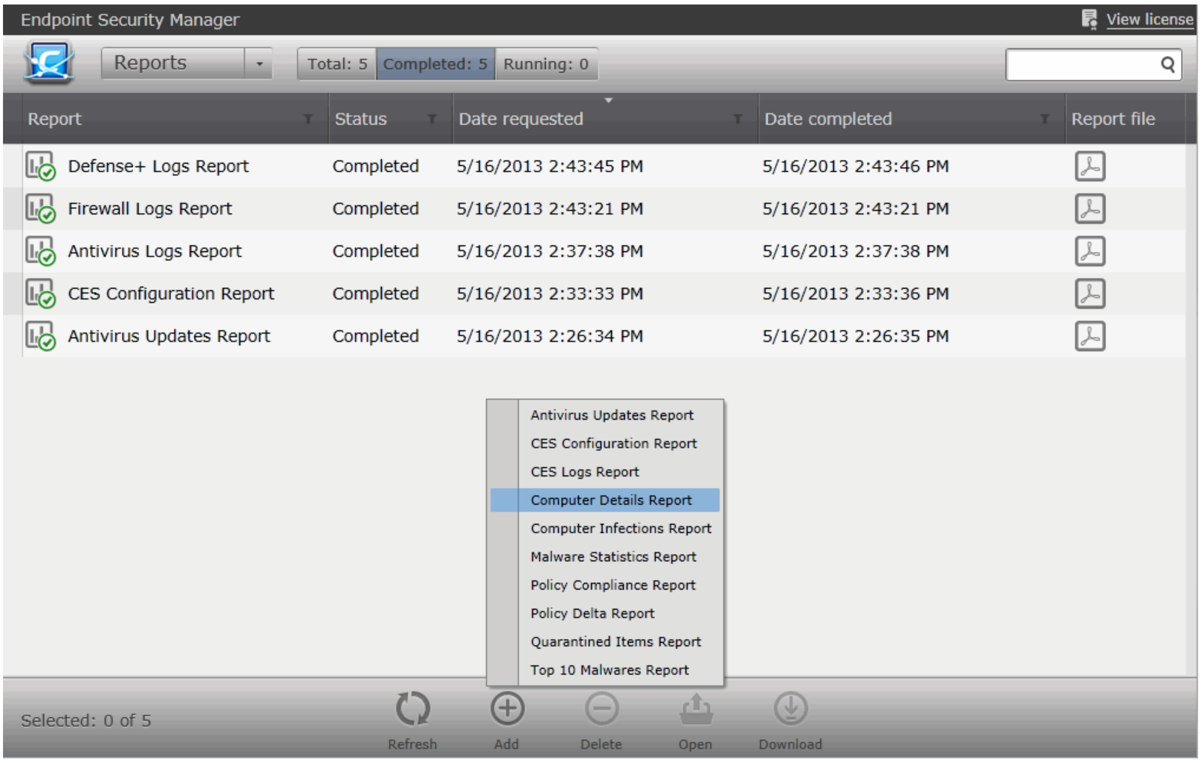
- Target - Represents the location of the target file.
- Date - Contains precise details of the date and time of the access attempt.
- Action - Indicates action taken against the access attempt.

9.4. 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.

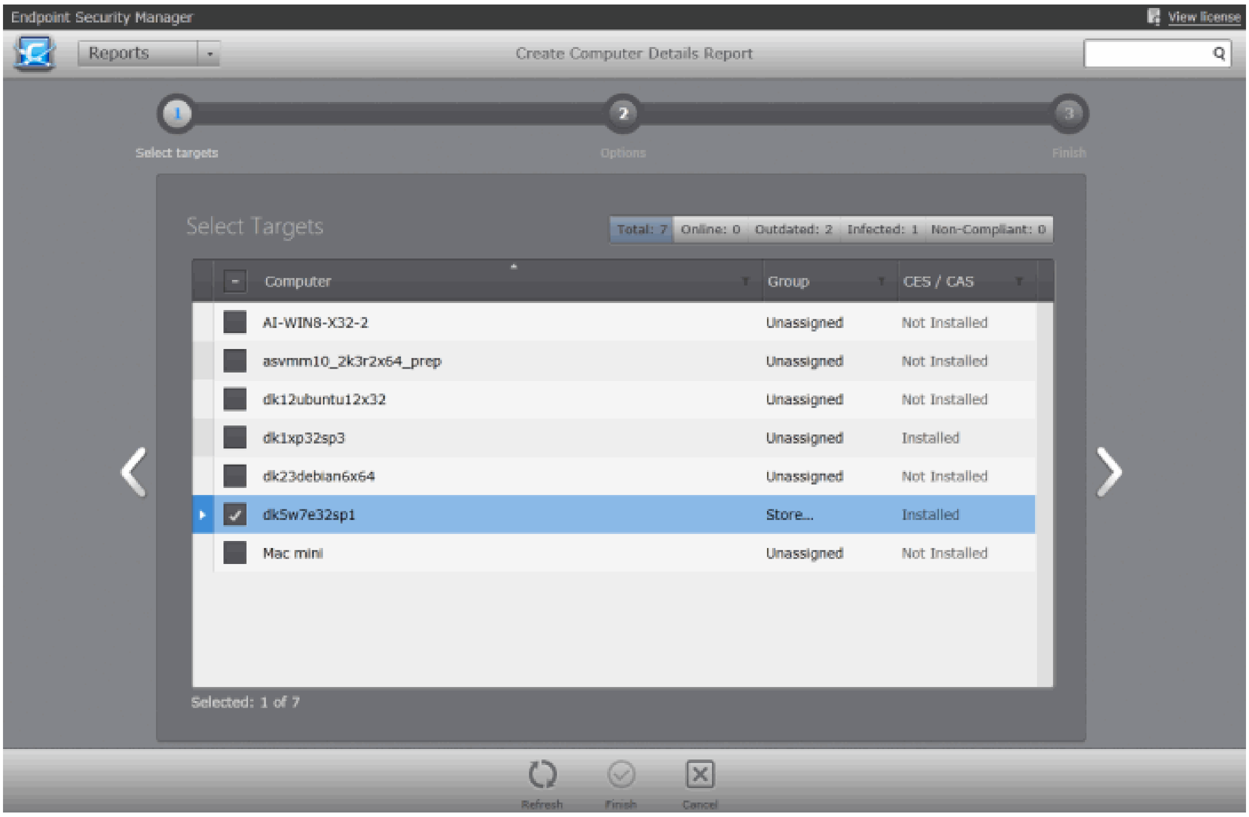


Report	Status	Date requested	Date completed	Report file
Defense+ Logs Report	Completed	5/16/2013 2:43:45 PM	5/16/2013 2:43:46 PM	
Firewall Logs Report	Completed	5/16/2013 2:43:21 PM	5/16/2013 2:43:21 PM	
Antivirus Logs Report	Completed	5/16/2013 2:37:38 PM	5/16/2013 2:37:38 PM	
CES Configuration Report	Completed	5/16/2013 2:33:33 PM	5/16/2013 2:33:36 PM	
Antivirus Updates Report	Completed	5/16/2013 2:26:34 PM	5/16/2013 2:26:35 PM	

- 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 Targets

Total: 7 | Online: 0 | Outdated: 2 | Infected: 1 | Non-Compliant: 0

	Computer	Group	CES / CAS
□	AI-WIN8-X32-2	Unassigned	Not Installed
□	asvmm10_2k3r2x64_prep	Unassigned	Not Installed
□	dk12ubuntu12x32	Unassigned	Not Installed
□	dk1xp32sp3	Unassigned	Installed
□	dk23debian6x64	Unassigned	Not Installed
☑	dk5w7e32sp1	Store...	Installed
□	Mac mini	Unassigned	Not Installed

Selected: 1 of 7

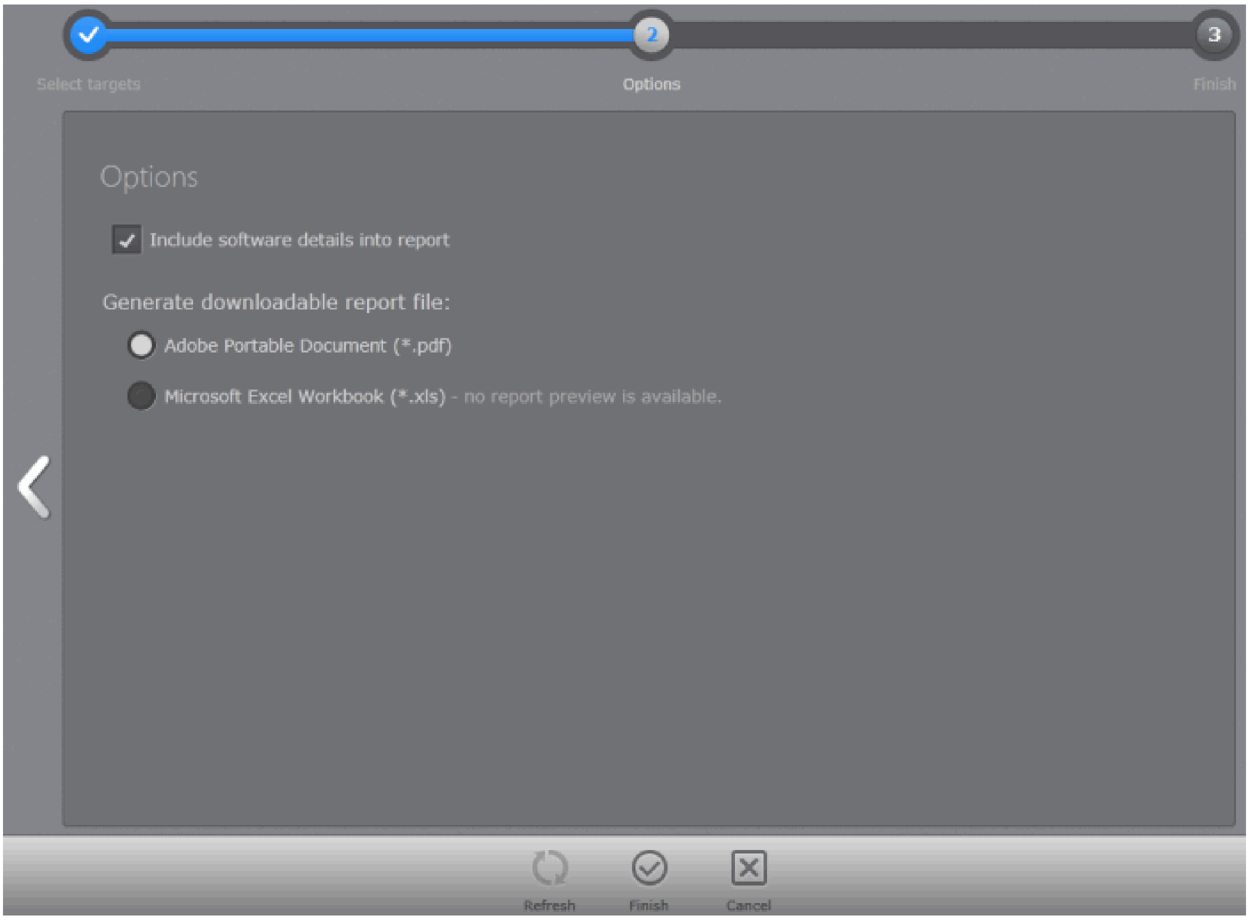
- Select the endpoint(s) for which you wish to generate the Computer Details report. The filter options in the header provides at-a-glance statistics of the computers in the network and allow the administrator to filter the computers based on the criteria. You can also filter the computers by clicking 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



Options

☑ Include software details into report

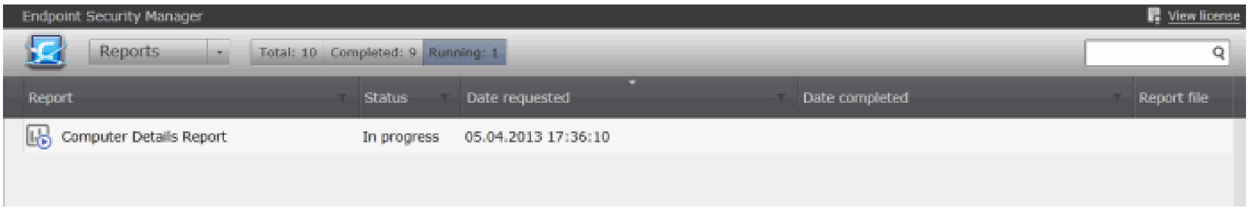
Generate downloadable report file:

○ Adobe Portable Document (*.pdf)

● Microsoft Excel Workbook (*.xls) - no report preview is available.

- 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.



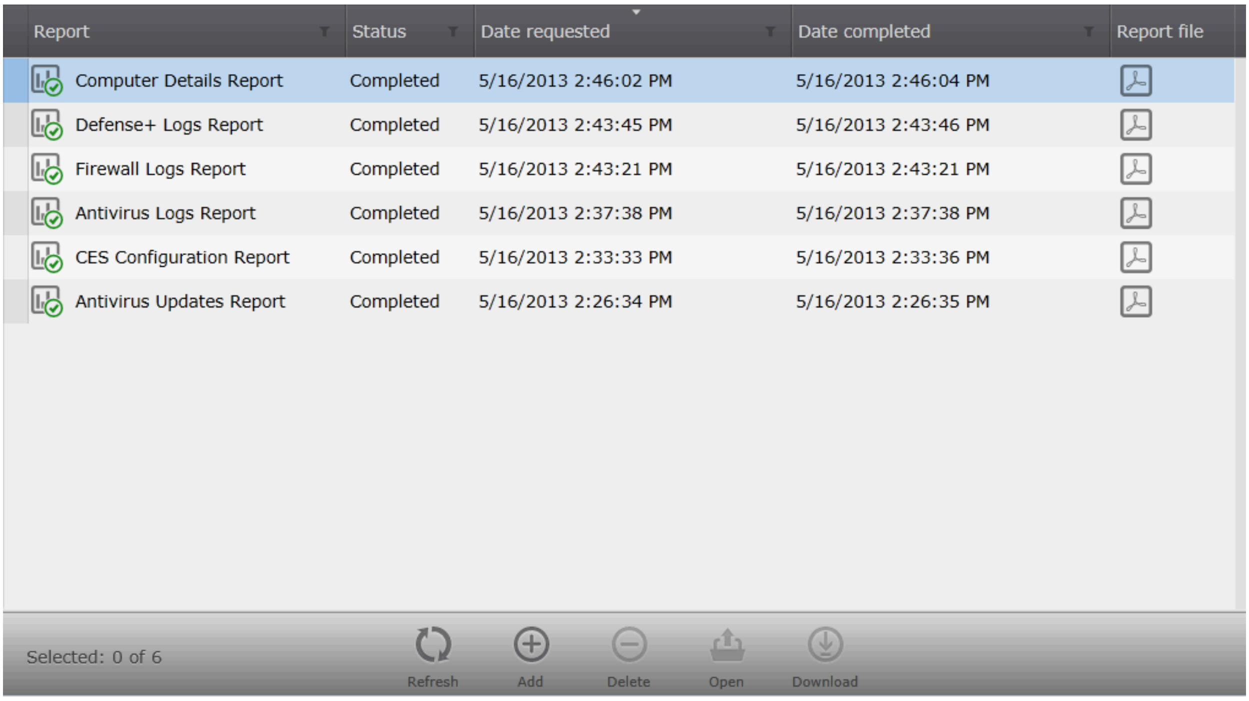
Report	Status	Date requested	Date completed	Report file
Computer Details Report	In progress	05.04.2013 17:36:10		

View the Report

The administrator can view the report at anytime after the completion.

To view the report

- Select the report and click 'Open' or right click on the report and choose 'Open' from the context sensitive menu.



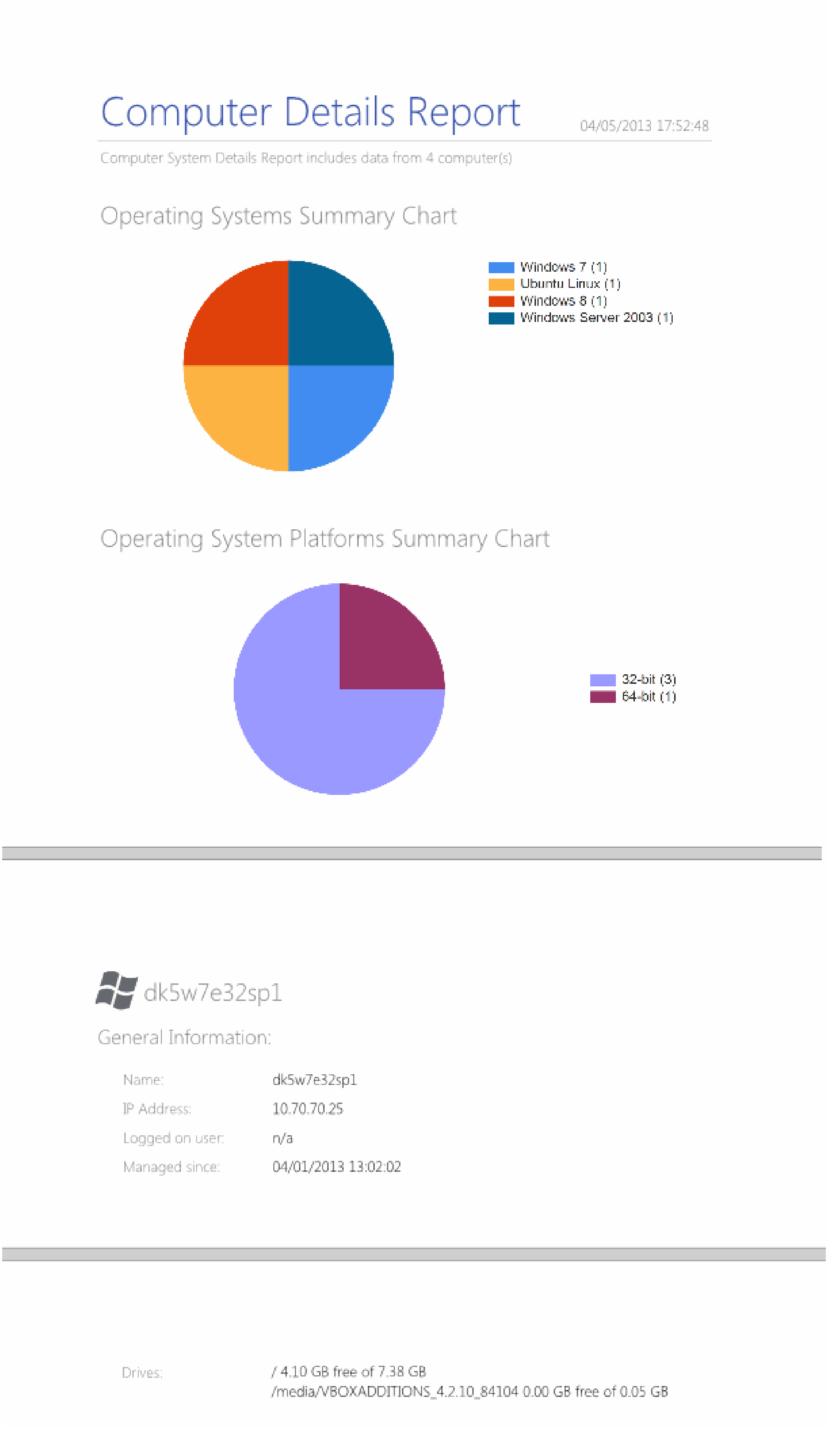
Report	Status	Date requested	Date completed	Report file
Computer Details Report	Completed	5/16/2013 2:46:02 PM	5/16/2013 2:46:04 PM	
Defense+ Logs Report	Completed	5/16/2013 2:43:45 PM	5/16/2013 2:43:46 PM	
Firewall Logs Report	Completed	5/16/2013 2:43:21 PM	5/16/2013 2:43:21 PM	
Antivirus Logs Report	Completed	5/16/2013 2:37:38 PM	5/16/2013 2:37:38 PM	
CES Configuration Report	Completed	5/16/2013 2:33:33 PM	5/16/2013 2:33:36 PM	
Antivirus Updates Report	Completed	5/16/2013 2:26:34 PM	5/16/2013 2:26:35 PM	

Selected: 0 of 6

The report will contain 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 will contain pie charts providing a comparison of versions of Operating Systems (OS) of the selected target endpoints.
- The successive pages will contain:
  - 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.



Computer Details Report 04/05/2013 17:52:48

Computer System Details Report includes data from 4 computer(s)

Operating Systems Summary Chart

Operating System Platforms Summary Chart

dk5w7e32sp1

General Information:

Name:	dk5w7e32sp1
IP Address:	10.70.70.25
Logged on user:	n/a
Managed since:	04/01/2013 13:02:02
Drives:	/ 4.10 GB free of 7.38 GB /media/VBOXADDITIONS_4.2.10_84104 0.00 GB free of 0.05 GB

Downloading the Report

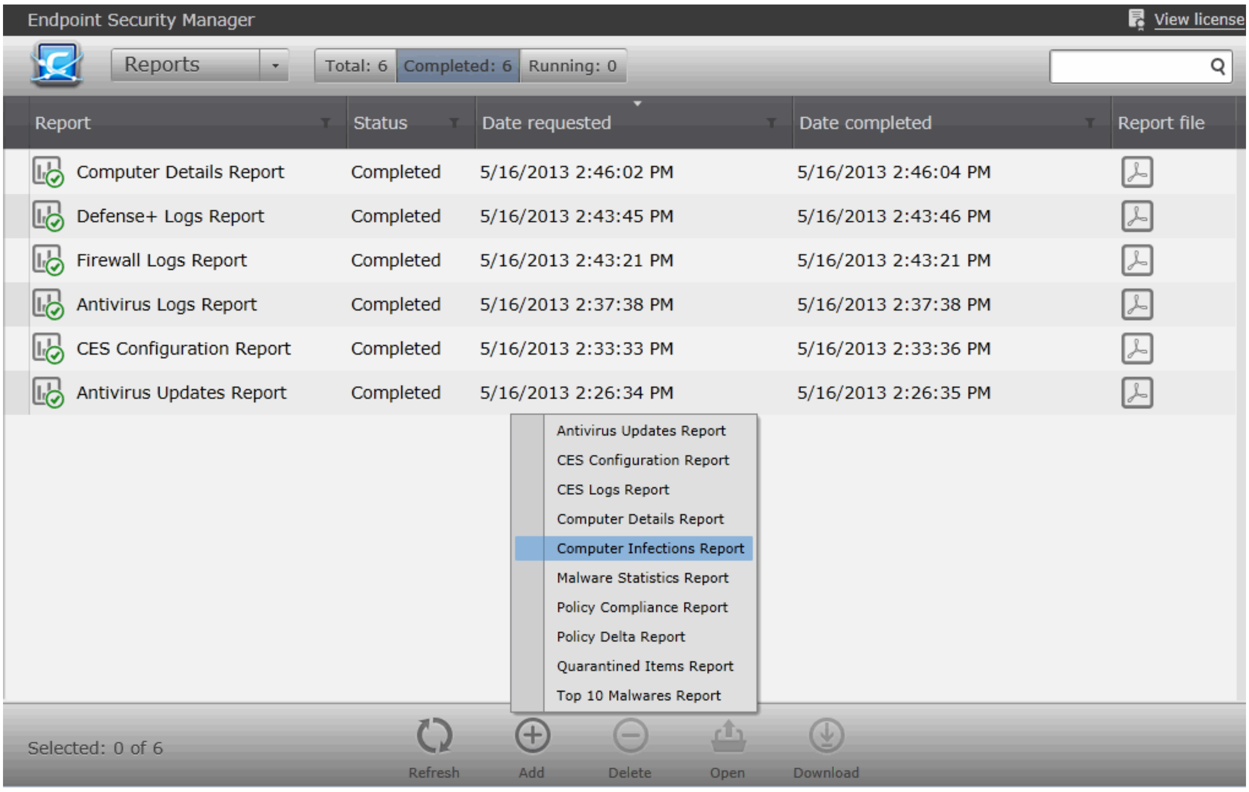
If the administrator had opted for generating a downloadable report, it can be downloaded by selecting the Report in the'Reports' area and clicking the download icon at the bottom.

9.5. 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.

To generate a Computer Infections report

- Open the 'Reports' area by choosing 'Reports' from the drop-down at the top left.



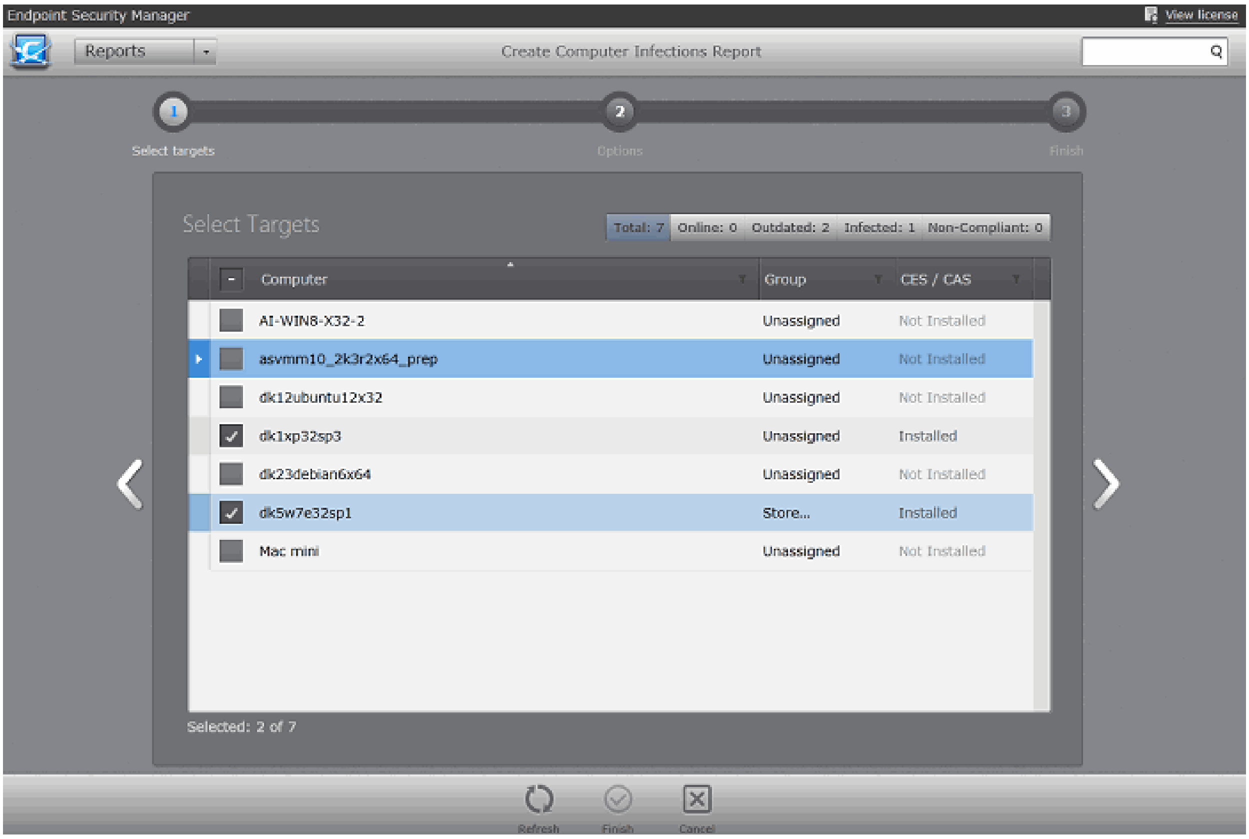
Report	Status	Date requested	Date completed	Report file
Computer Details Report	Completed	5/16/2013 2:46:02 PM	5/16/2013 2:46:04 PM	
Defense+ Logs Report	Completed	5/16/2013 2:43:45 PM	5/16/2013 2:43:46 PM	
Firewall Logs Report	Completed	5/16/2013 2:43:21 PM	5/16/2013 2:43:21 PM	
Antivirus Logs Report	Completed	5/16/2013 2:37:38 PM	5/16/2013 2:37:38 PM	
CES Configuration Report	Completed	5/16/2013 2:33:33 PM	5/16/2013 2:33:36 PM	
Antivirus Updates Report	Completed	5/16/2013 2:26:34 PM	5/16/2013 2:26:35 PM	

Selected: 0 of 6

- 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 Targets

Total: 7 | Online: 0 | Outdated: 2 | Infected: 1 | Non-Compliant: 0

	Computer	Group	CES / CAS
□	AI-WIN8-X32-2	Unassigned	Not Installed
□	asvmm10_2k3r2x64_prep	Unassigned	Not Installed
□	dk12ubuntu12x32	Unassigned	Not Installed
☑	dk1xp32sp3	Unassigned	Installed
□	dk23debian6x64	Unassigned	Not Installed
☑	dk5w7e32sp1	Store...	Installed
□	Mac mini	Unassigned	Not Installed

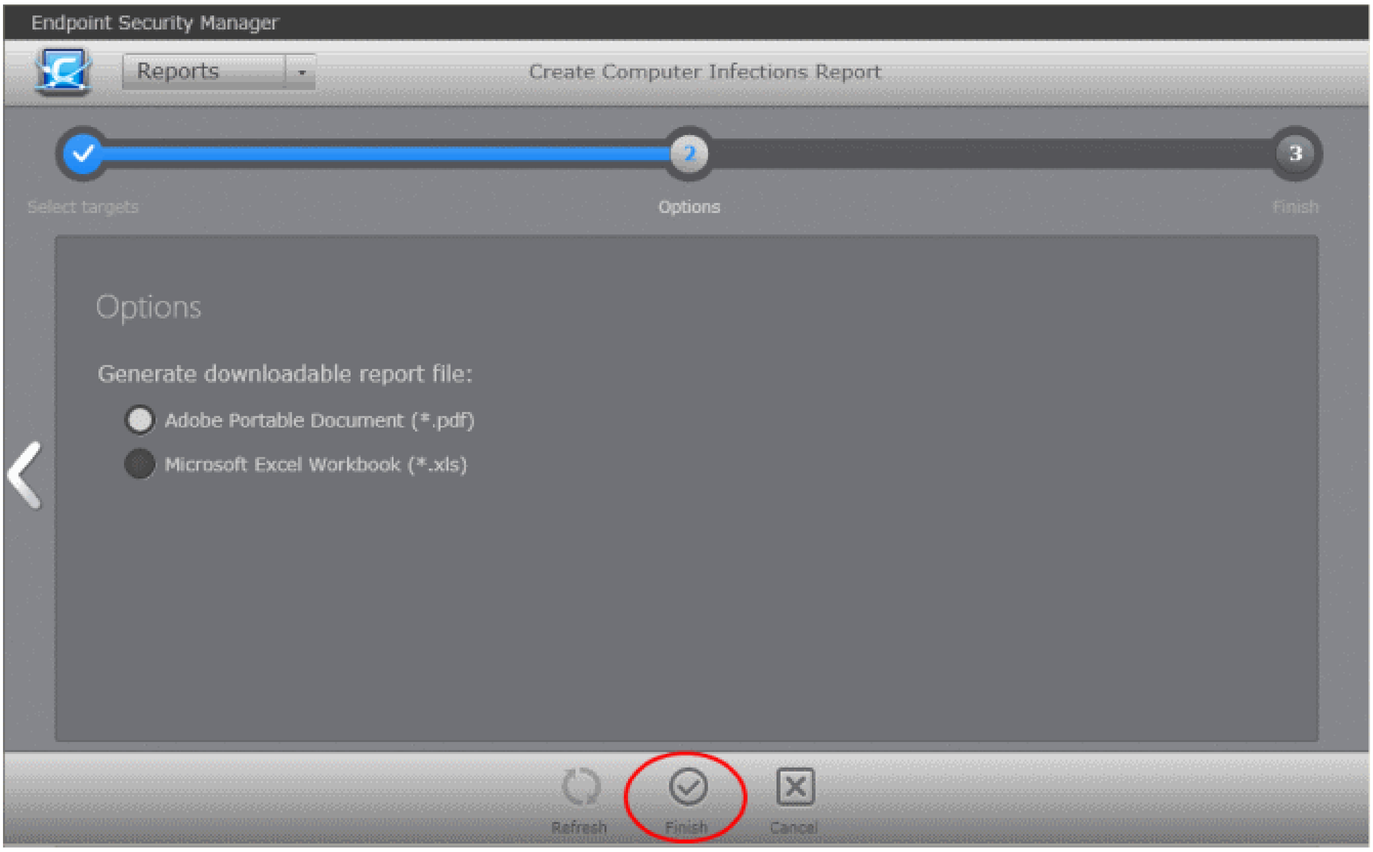
Selected: 2 of 7

- 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.



Options

Generate downloadable report file:

○ Adobe Portable Document (*.pdf)

● Microsoft Excel Workbook (*.xls)

- Click the 'Finish' icon to start generating the report.

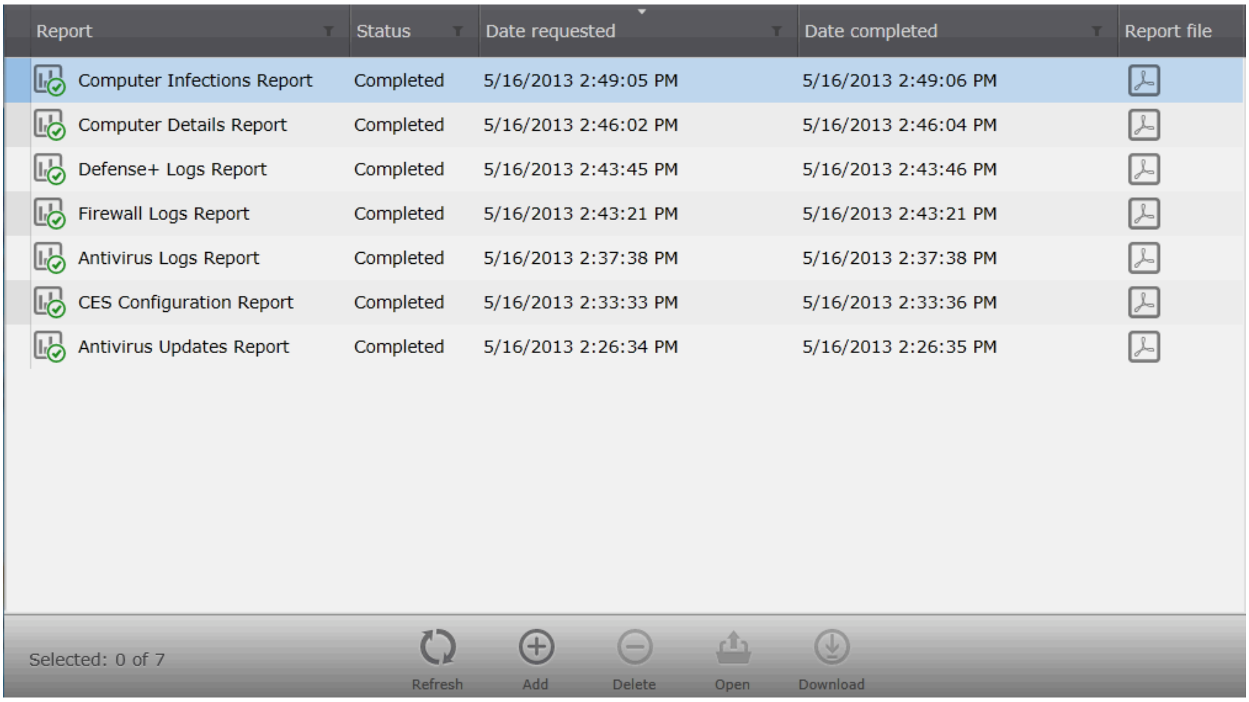
The report generation will be started or added to the queue. The progress will be displayed in the 'Reports' area.

View the Report

The administrator can view the report at anytime after the completion.

To view the report

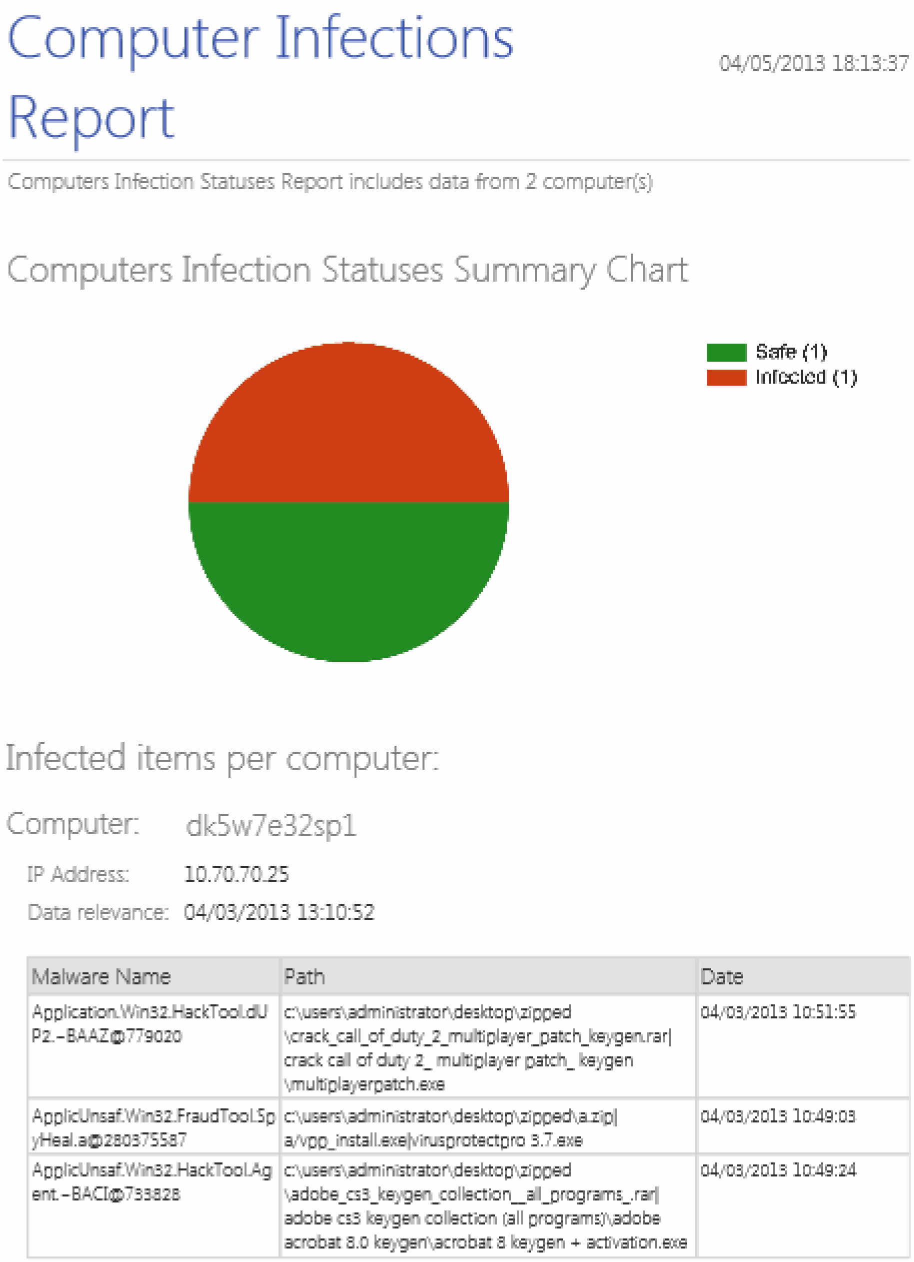
- Select the report and click Open or right click on the report and choose Open from the context sensitive menu.



Report	Status	Date requested	Date completed	Report file
Computer Infections Report	Completed	5/16/2013 2:49:05 PM	5/16/2013 2:49:06 PM	
Computer Details Report	Completed	5/16/2013 2:46:02 PM	5/16/2013 2:46:04 PM	
Defense+ Logs Report	Completed	5/16/2013 2:43:45 PM	5/16/2013 2:43:46 PM	
Firewall Logs Report	Completed	5/16/2013 2:43:21 PM	5/16/2013 2:43:21 PM	
Antivirus Logs Report	Completed	5/16/2013 2:37:38 PM	5/16/2013 2:37:38 PM	
CES Configuration Report	Completed	5/16/2013 2:33:33 PM	5/16/2013 2:33:36 PM	
Antivirus Updates Report	Completed	5/16/2013 2:26:34 PM	5/16/2013 2:26:35 PM	

Selected: 0 of 7

- The report will contain a pie chart that provides an at-a-glance comparison of computers that are affected/not affected by malware from the selected target endpoints.
- 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.



Computer Infections Report

04/05/2013 18:13:37

Computers Infection Statuses Report includes data from 2 computer(s)

Computers Infection Statuses Summary Chart

🟩 Safe (1)
🟥 Infected (1)

Infected items per computer:

Computer: dk5w7e32sp1

IP Address: 10.70.70.25

Data relevance: 04/03/2013 13:10:52

<table>
<tr><th>Malware Name</th><th>Path</th><th>Date</th></tr>
<tr><td>Application.Win32.HackTool.dUP2.–BAAZ@779020</td><td>c:\users\administrator\desktop\zipped\crack_call_of_duty_2_multiplayer_patch_keygen.rar|crack call of duty 2_ multiplayer patch_ keygen\multiplayerpatch.exe</td><td>04/03/2013 10:51:55</td></tr>
<tr><td>ApplicUnsaf.Win32.FraudTool.SpyHeal.a@280375587</td><td>c:\users\administrator\desktop\zipped\a.zip|a/vpp_install.exe|virusprotectpro 3.7.exe</td><td>04/03/2013 10:49:03</td></tr>
<tr><td>ApplicUnsaf.Win32.HackTool.Agent.–BACI@733828</td><td>c:\users\administrator\desktop\zipped\adobe_cs3_keygen_collection__all_programs_.rar|adobe cs3 keygen collection (all programs)\adobe acrobat 8.0 keygen\acrobat 8 keygen + activation.exe</td><td>04/03/2013 10:49:24</td></tr>
</table>

Downloading the Report

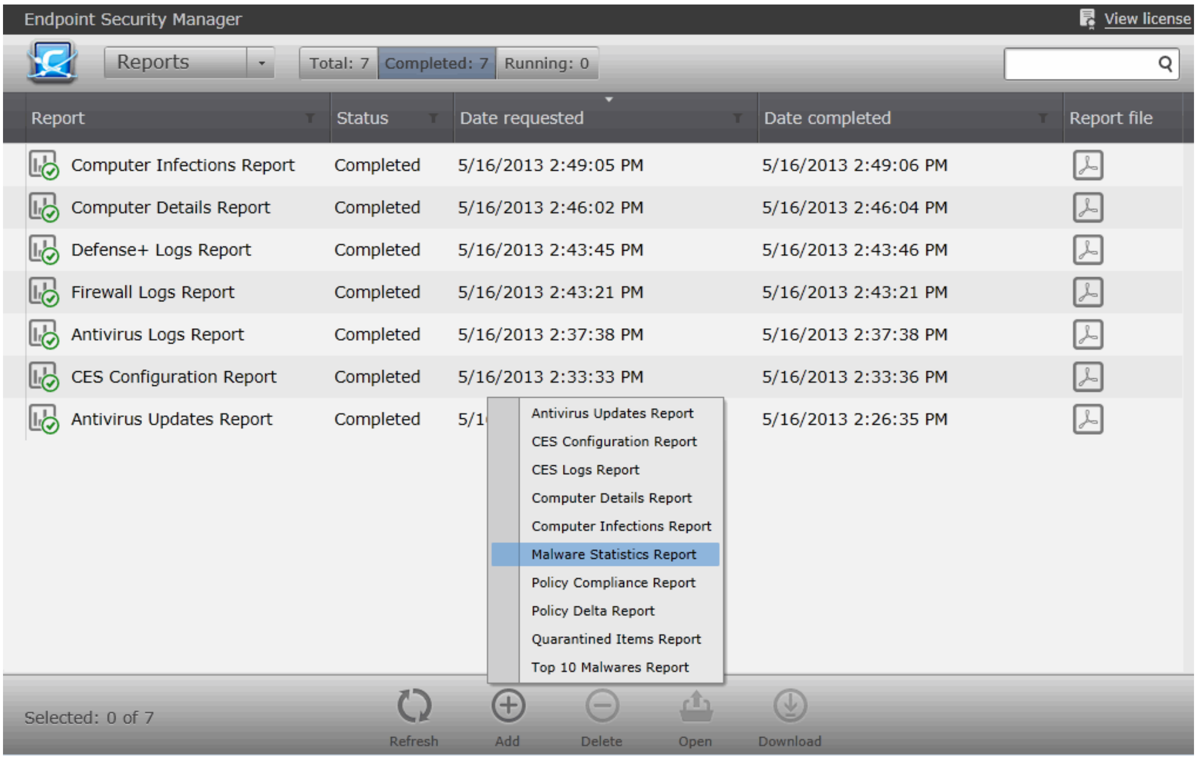
If the administrator had opted for generating a downloadable report, it can be downloaded by selecting the Report in the 'Reports' area and clicking the download icon ⬇ at the bottom.

9.6. 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 CES 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.

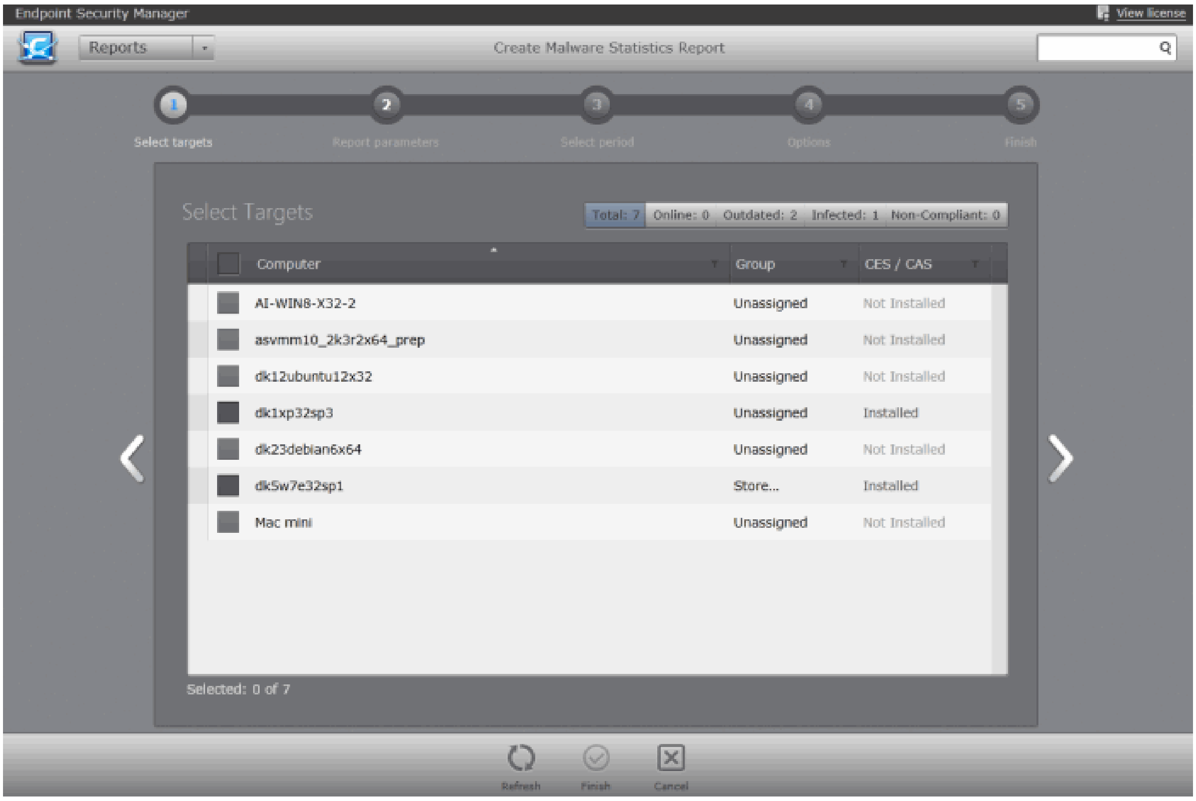


Report	Status	Date requested	Date completed	Report file
Computer Infections Report	Completed	5/16/2013 2:49:05 PM	5/16/2013 2:49:06 PM	
Computer Details Report	Completed	5/16/2013 2:46:02 PM	5/16/2013 2:46:04 PM	
Defense+ Logs Report	Completed	5/16/2013 2:43:45 PM	5/16/2013 2:43:46 PM	
Firewall Logs Report	Completed	5/16/2013 2:43:21 PM	5/16/2013 2:43:21 PM	
Antivirus Logs Report	Completed	5/16/2013 2:37:38 PM	5/16/2013 2:37:38 PM	
CES Configuration Report	Completed	5/16/2013 2:33:33 PM	5/16/2013 2:33:36 PM	
Antivirus Updates Report	Completed	5/1	5/16/2013 2:26:35 PM	

- 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.



Select Targets

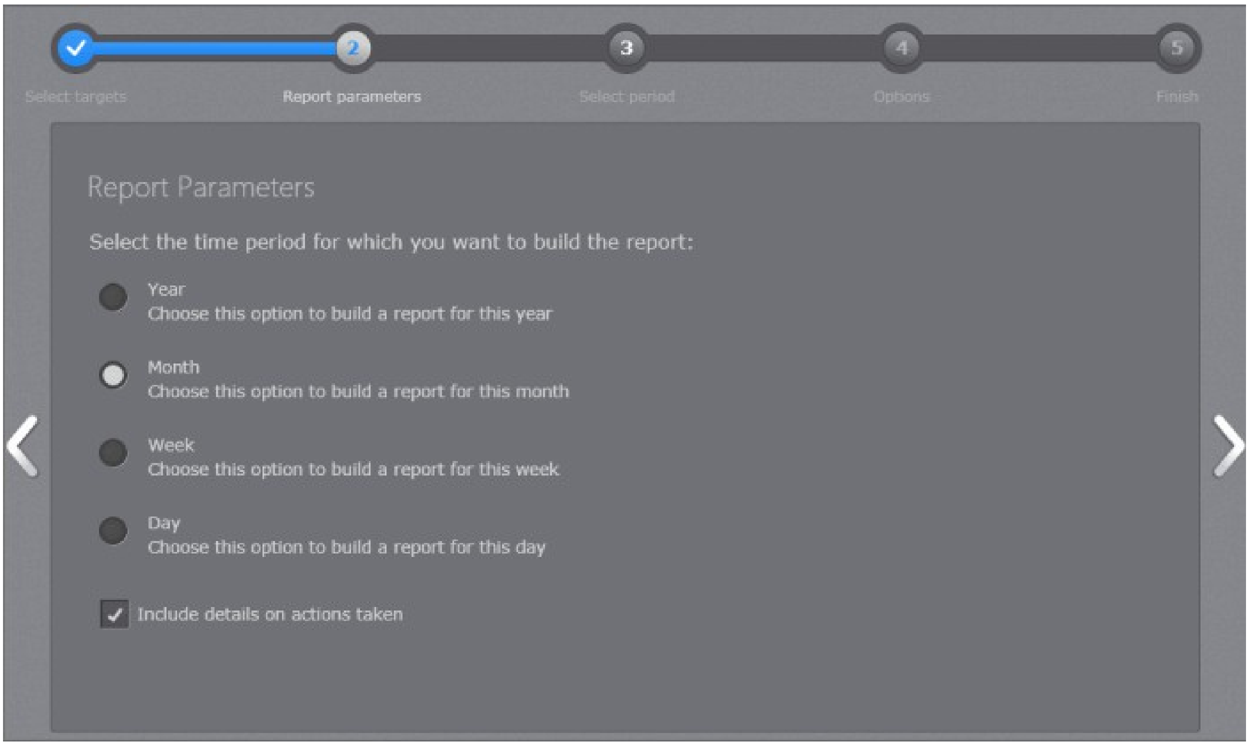
Total: 7 | Online: 0 | Outdated: 2 | Infected: 1 | Non-Compliant: 0

□ Computer	Group	CES / CAS
□ AI-WIN8-X32-2	Unassigned	Not Installed
□ asvmm10_2k3r2x64_prep	Unassigned	Not Installed
□ dk12ubuntu12x32	Unassigned	Not Installed
□ dk1xp32sp3	Unassigned	Installed
□ dk23debian6x64	Unassigned	Not Installed
□ dk5w7e32sp1	Store...	Installed
□ Mac mini	Unassigned	Not Installed

Selected: 0 of 7

Step 2 - Selecting Report Duration

The next step is to select the period for which you wish the report to be created.



Report Parameters

Select the time period for which you want to build the report:

○ Year
Choose this option to build a report for this year

● Month
Choose this option to build a report for this month

○ Week
Choose this option to build a report for this week

○ Day
Choose this option to build a report for this day

☑ Include details on actions taken

- The time period options available are:
  - Year - Generates statistics from any year (from 1st January YYYY).
  - Month - Generates statistics from the beginning of the current month (from 1st MM YYYY).
  - 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'.

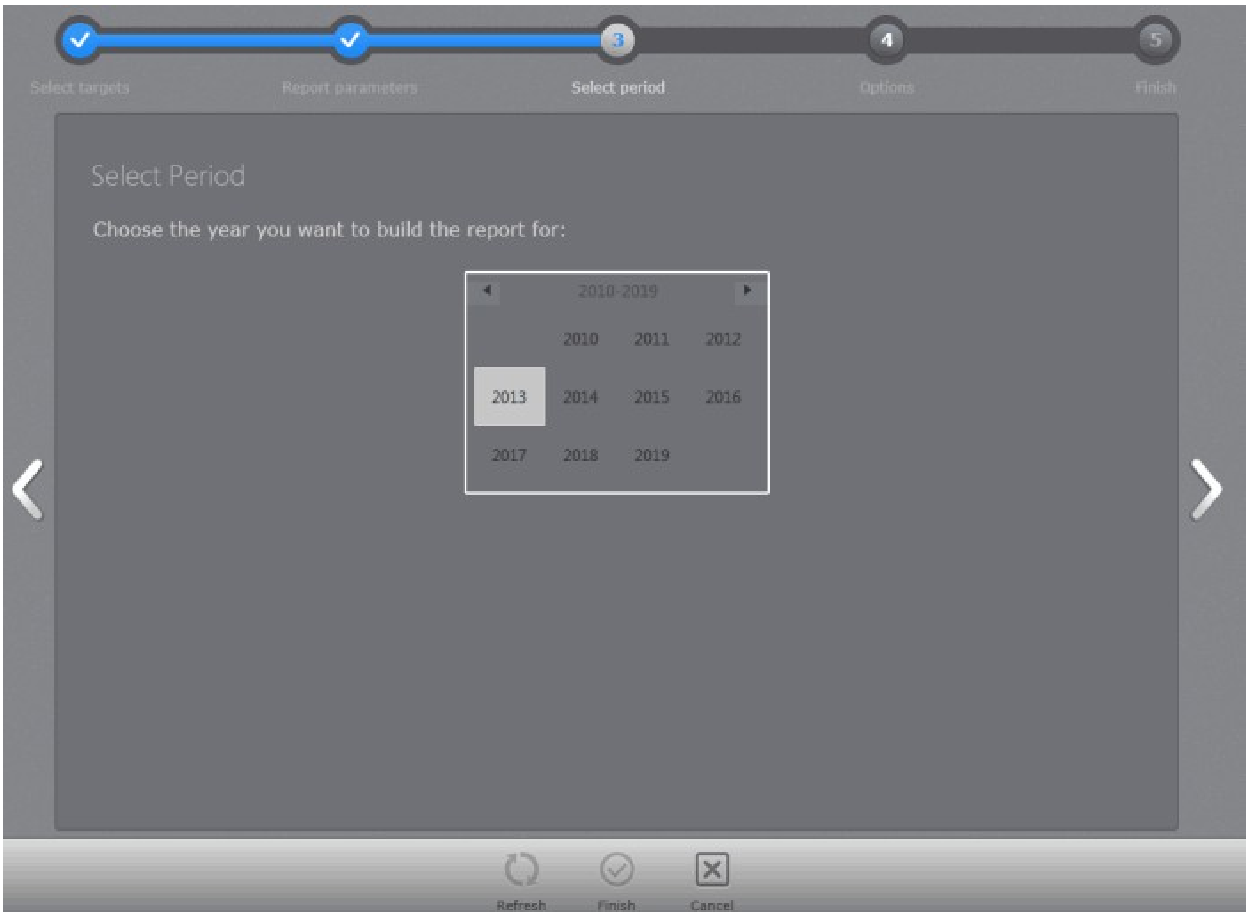
   - Day - Generates statistics for any one day. The day can be selected from a calendar in the next step 'Select Period'.

  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 CES 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.



Select Period

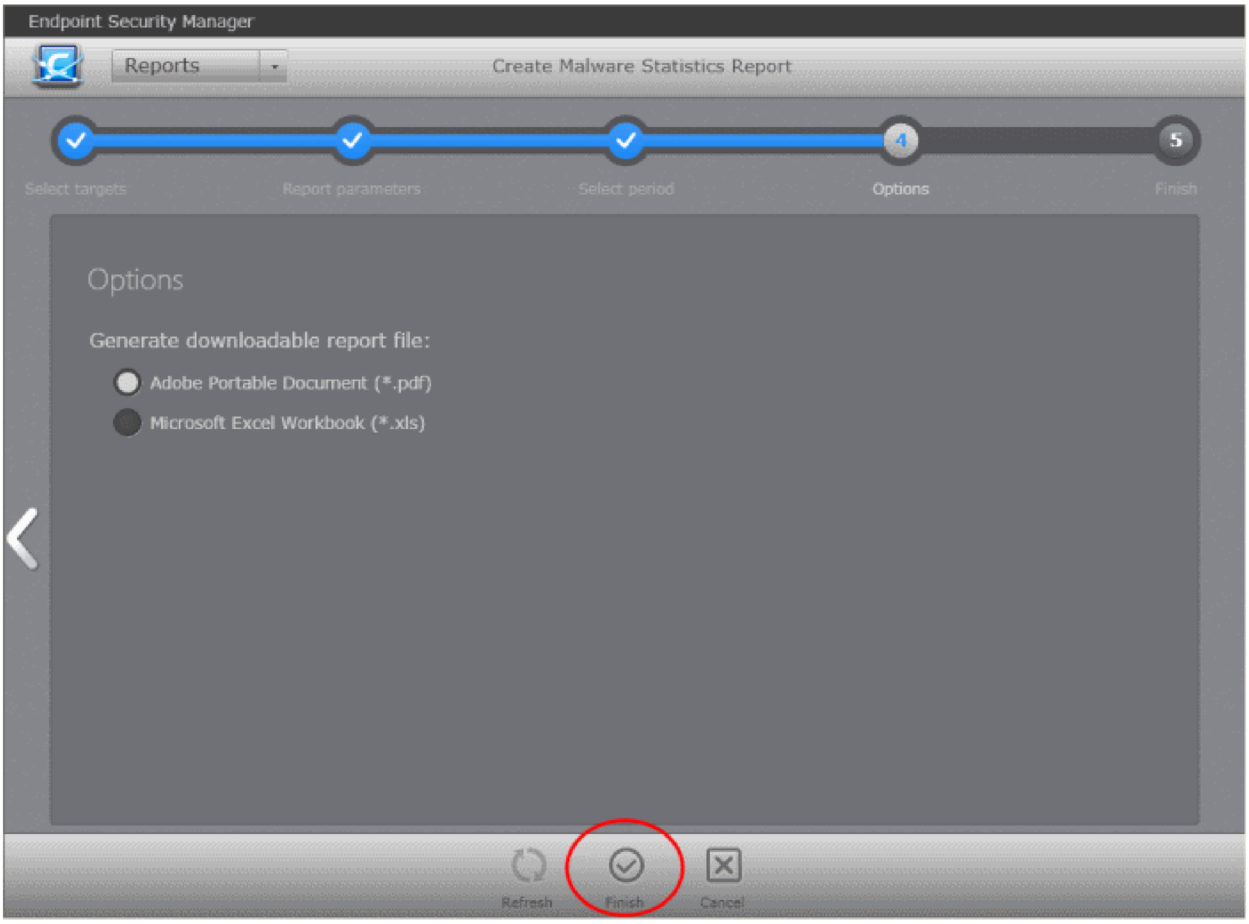
Choose the year you want to build the report for:

- 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.



Options

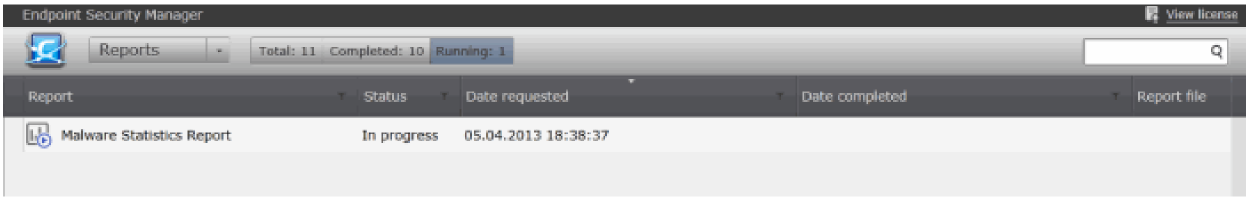
Generate downloadable report file:

○ Adobe Portable Document (*.pdf)

● Microsoft Excel Workbook (*.xls)

- 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.



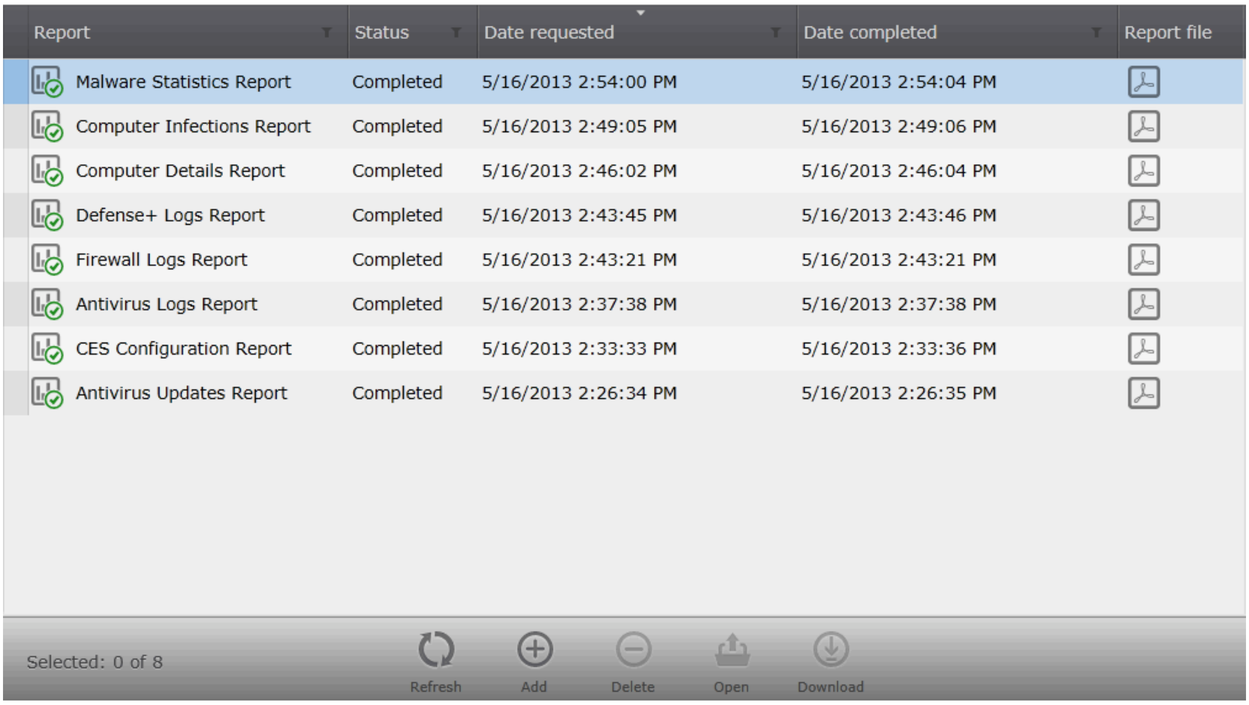
Report	Status	Date requested	Date completed	Report file
Malware Statistics Report	In progress	05.04.2013 18:38:37		

View the Report

The administrator can view the report at anytime after the completion.

To view the report

- Select the report and click Open or right click on the report and choose Open from the context sensitive menu.

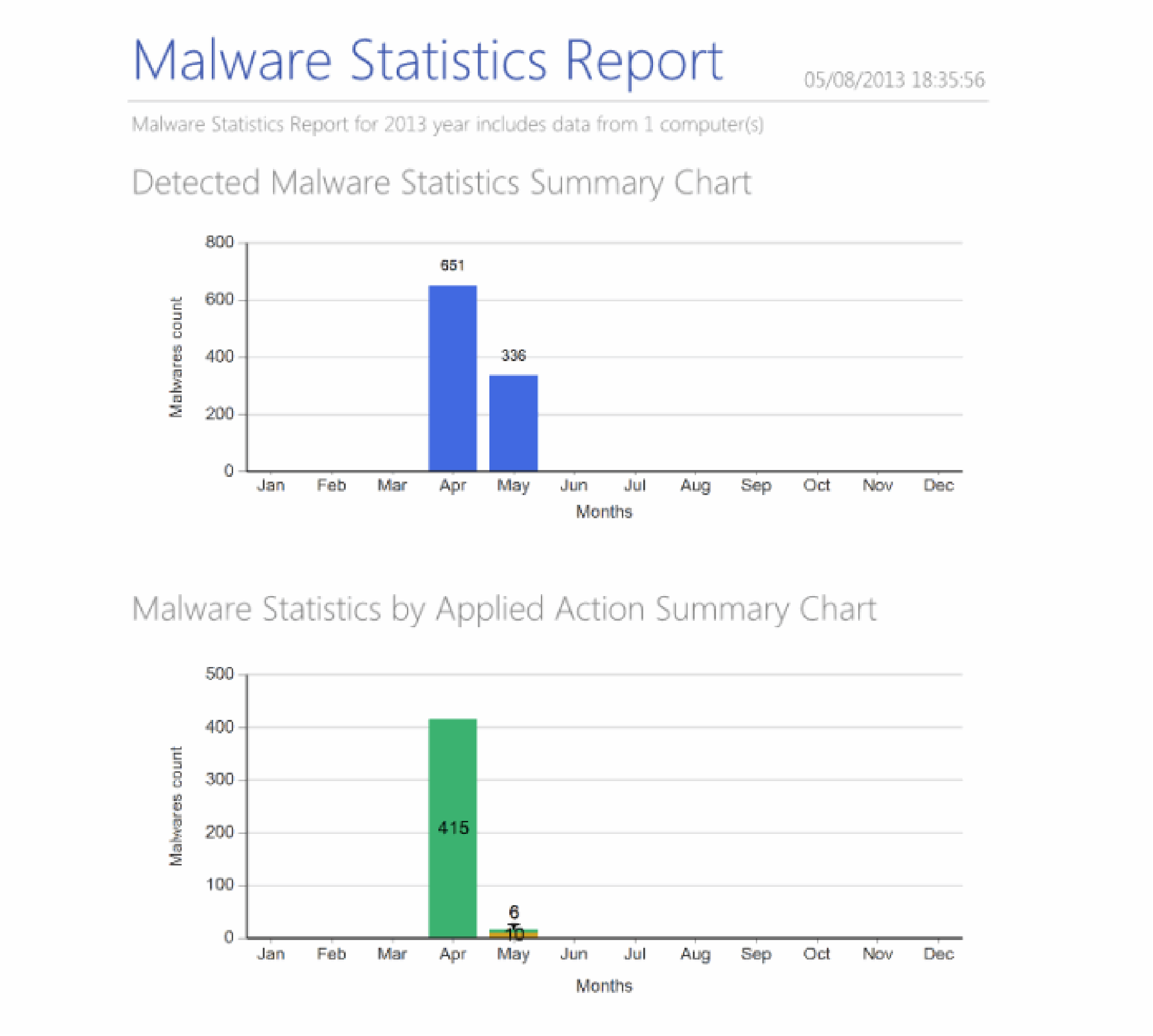


Report	Status	Date requested	Date completed	Report file
Malware Statistics Report	Completed	5/16/2013 2:54:00 PM	5/16/2013 2:54:04 PM	
Computer Infections Report	Completed	5/16/2013 2:49:05 PM	5/16/2013 2:49:06 PM	
Computer Details Report	Completed	5/16/2013 2:46:02 PM	5/16/2013 2:46:04 PM	
Defense+ Logs Report	Completed	5/16/2013 2:43:45 PM	5/16/2013 2:43:46 PM	
Firewall Logs Report	Completed	5/16/2013 2:43:21 PM	5/16/2013 2:43:21 PM	
Antivirus Logs Report	Completed	5/16/2013 2:37:38 PM	5/16/2013 2:37:38 PM	
CES Configuration Report	Completed	5/16/2013 2:33:33 PM	5/16/2013 2:33:36 PM	
Antivirus Updates Report	Completed	5/16/2013 2:26:34 PM	5/16/2013 2:26:35 PM	

Selected: 0 of 8

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:



Malware Statistics Report 05/08/2013 18:35:56

Malware Statistics Report for 2013 year includes data from 1 computer(s)

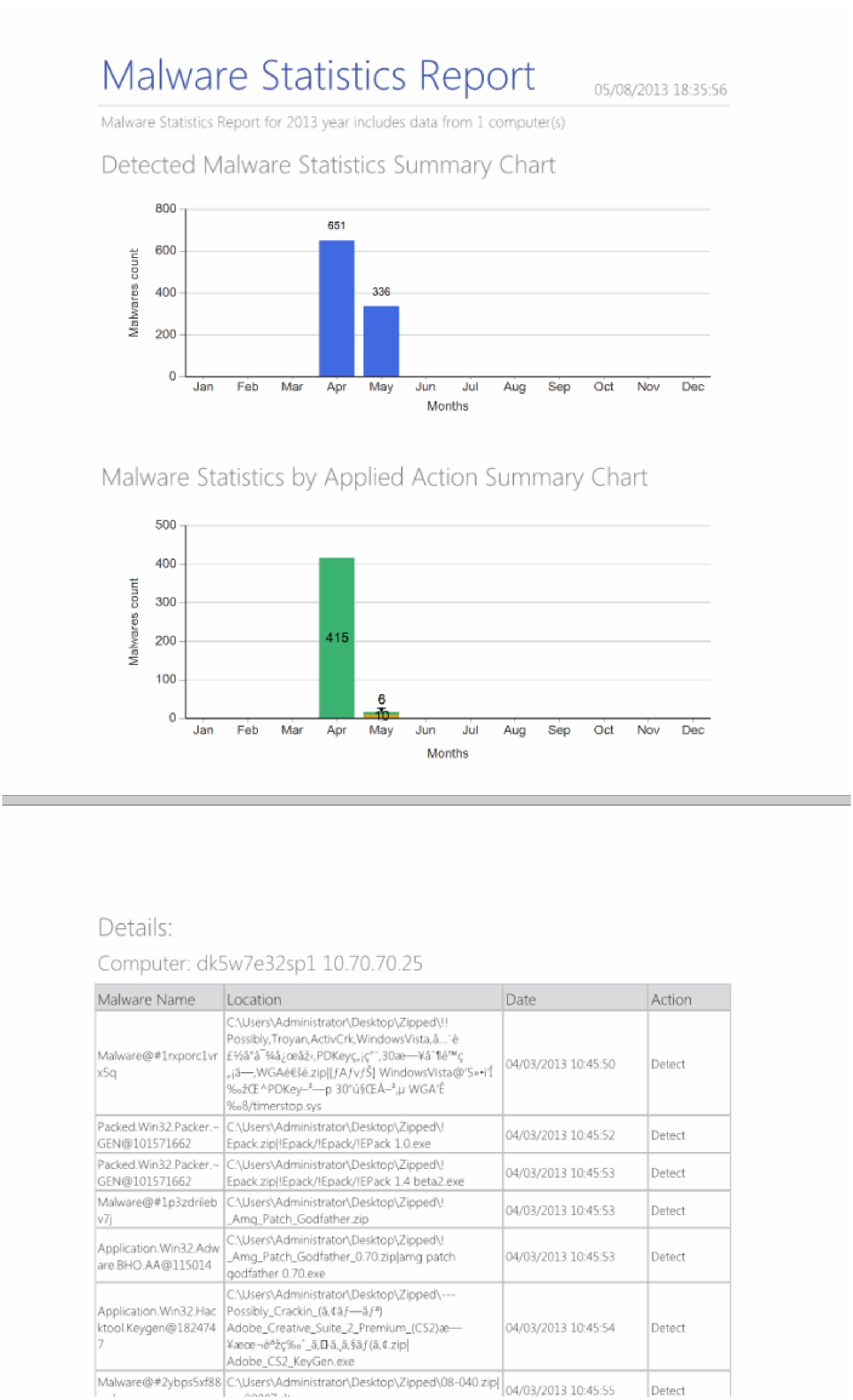
Detected Malware Statistics Summary Chart

Malware Statistics by Applied Action Summary Chart

'Deleted', 'Ignored' and 'Quarantined' are the decisions taken by CES 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 CES.

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.



Malware Statistics Report

05/08/2013 18:35:56

Malware Statistics Report for 2013 year includes data from 1 computer(s)

Detected Malware Statistics Summary Chart

Malware Statistics by Applied Action Summary Chart

Details:

Computer: dk5w7e32sp1 10.70.70.25

Malware Name	Location	Date	Action
Malware@#1rxporc1vrx5q	C:\Users\Administrator\Desktop\Zipped\!!Possibly,Troyan,ActivCrk,WindowsVista,å…¨è£½å"å¯¾å¿œå›‹,PDKeyç„¡ç"",30æ—¥å¨¶é™ç„¡å—,WGAé€šé.zip|[ƒAƒvƒŠ] WindowsVista@'S»•í'‰žŒ^PDKey–³—p 30"ú§ŒÀ–³,µ WGA'Ê‰ß/timerstop.sys	04/03/2013 10:45:50	Detect
Packed.Win32.Packer.~GEN@101571662	C:\Users\Administrator\Desktop\Zipped\!Epack.zip|!Epack/!Epack/!EPack 1.0.exe	04/03/2013 10:45:52	Detect
Packed.Win32.Packer.~GEN@101571662	C:\Users\Administrator\Desktop\Zipped\!Epack.zip|!Epack/!Epack/!EPack 1.4 beta2.exe	04/03/2013 10:45:53	Detect
Malware@#1p3zdrilebv7j	C:\Users\Administrator\Desktop\Zipped\!_Amg_Patch_Godfather.zip	04/03/2013 10:45:53	Detect
Application.Win32.Adware.BHO.AA@115014	C:\Users\Administrator\Desktop\Zipped\!_Amg_Patch_Godfather_0.70.zip|amg patch godfather 0.70.exe	04/03/2013 10:45:53	Detect
Application.Win32.Hacktool.Keygen@1824747	C:\Users\Administrator\Desktop\Zipped\---Possibly_Crackin_(ã‚¢ãƒ—ãƒª)Adobe_Creative_Suite_2_Premium_(CS2)æ—¥æœ¬èªžç‰ˆ_ã‚□ã‚‚ã‚§ãƒ(ã‚¢.zip|Adobe_CS2_KeyGen.exe	04/03/2013 10:45:54	Detect
Malware@#2ybps5xf88	C:\Users\Administrator\Desktop\Zipped\08-040.zip|	04/03/2013 10:45:55	Detect

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.

9.7. Policy Compliance Report

Each target computer in CESM can receive a security policy that dictates the security settings of each of the antivirus, firewall and Defense+ components of CES installed on it. The CES installation at the target endpoint will automatically be configured as per the applied policy when CES 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 by switching it to local administration mode, the computer becomes 'non-compliant' with its designated (or 'applied') policy. If the computer is switched back to remote management mode, its designated policy will be automatically reapplied at next polling time (as per the agent settings made to the policy) and the computer's status will return to 'compliant'.

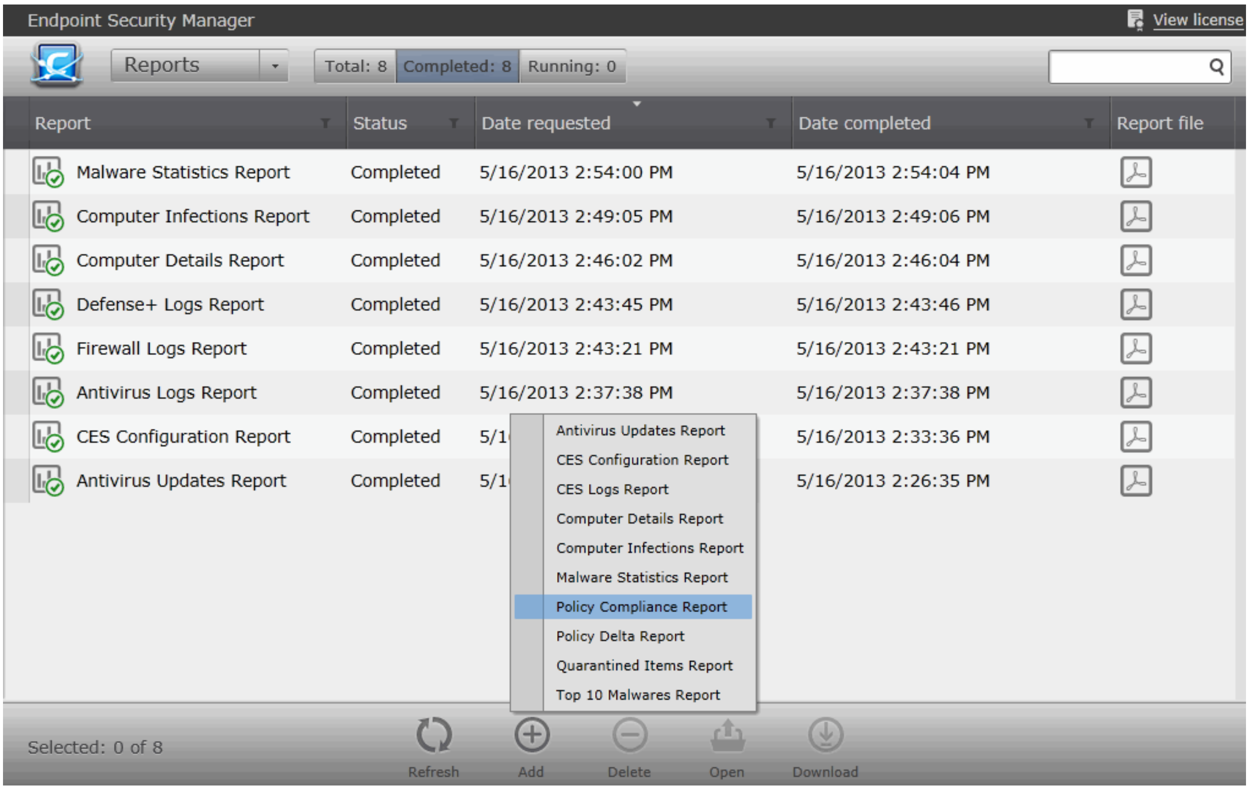
The target computers applied with the 'Locally Configured' policy will always be retained in 'Compliant' status as CESM does not enforce any policy compliance on to them. Also, 'Locally Configured' policy allows the user to change the CES configuration settings locally and stores the changes dynamically. 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 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 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.

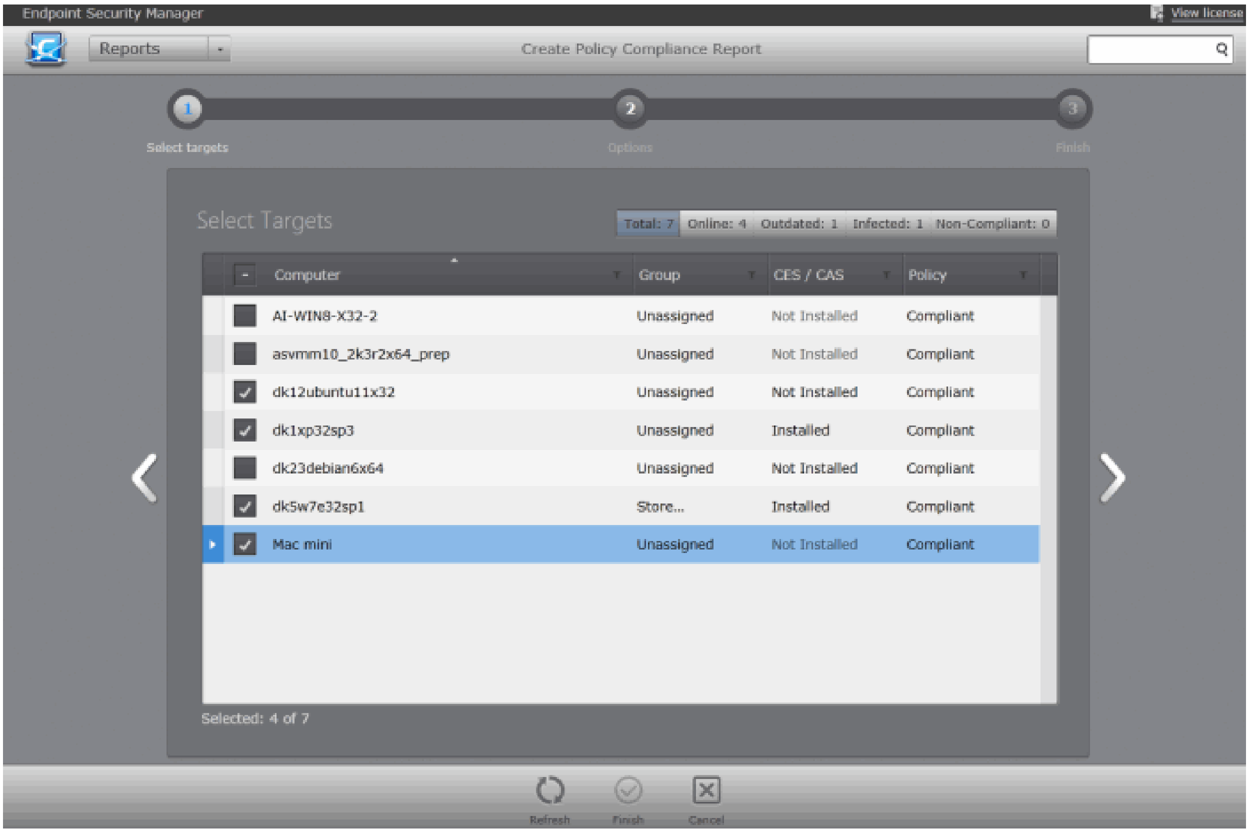


Report	Status	Date requested	Date completed	Report file
Malware Statistics Report	Completed	5/16/2013 2:54:00 PM	5/16/2013 2:54:04 PM	
Computer Infections Report	Completed	5/16/2013 2:49:05 PM	5/16/2013 2:49:06 PM	
Computer Details Report	Completed	5/16/2013 2:46:02 PM	5/16/2013 2:46:04 PM	
Defense+ Logs Report	Completed	5/16/2013 2:43:45 PM	5/16/2013 2:43:46 PM	
Firewall Logs Report	Completed	5/16/2013 2:43:21 PM	5/16/2013 2:43:21 PM	
Antivirus Logs Report	Completed	5/16/2013 2:37:38 PM	5/16/2013 2:37:38 PM	
CES Configuration Report	Completed	5/1	5/16/2013 2:33:36 PM	
Antivirus Updates Report	Completed	5/1	5/16/2013 2:26:35 PM	

- 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 Targets

Total: 7 Online: 4 Outdated: 1 Infected: 1 Non-Compliant: 0

	Computer	Group	CES / CAS	Policy
□	AI-WIN8-X32-2	Unassigned	Not Installed	Compliant
□	asvmm10_2k3r2x64_prep	Unassigned	Not Installed	Compliant
☑	dk12ubuntu11x32	Unassigned	Not Installed	Compliant
☑	dk1xp32sp3	Unassigned	Installed	Compliant
□	dk23debian6x64	Unassigned	Not Installed	Compliant
☑	dk5w7e32sp1	Store...	Installed	Compliant
☑	Mac mini	Unassigned	Not Installed	Compliant

Selected: 4 of 7

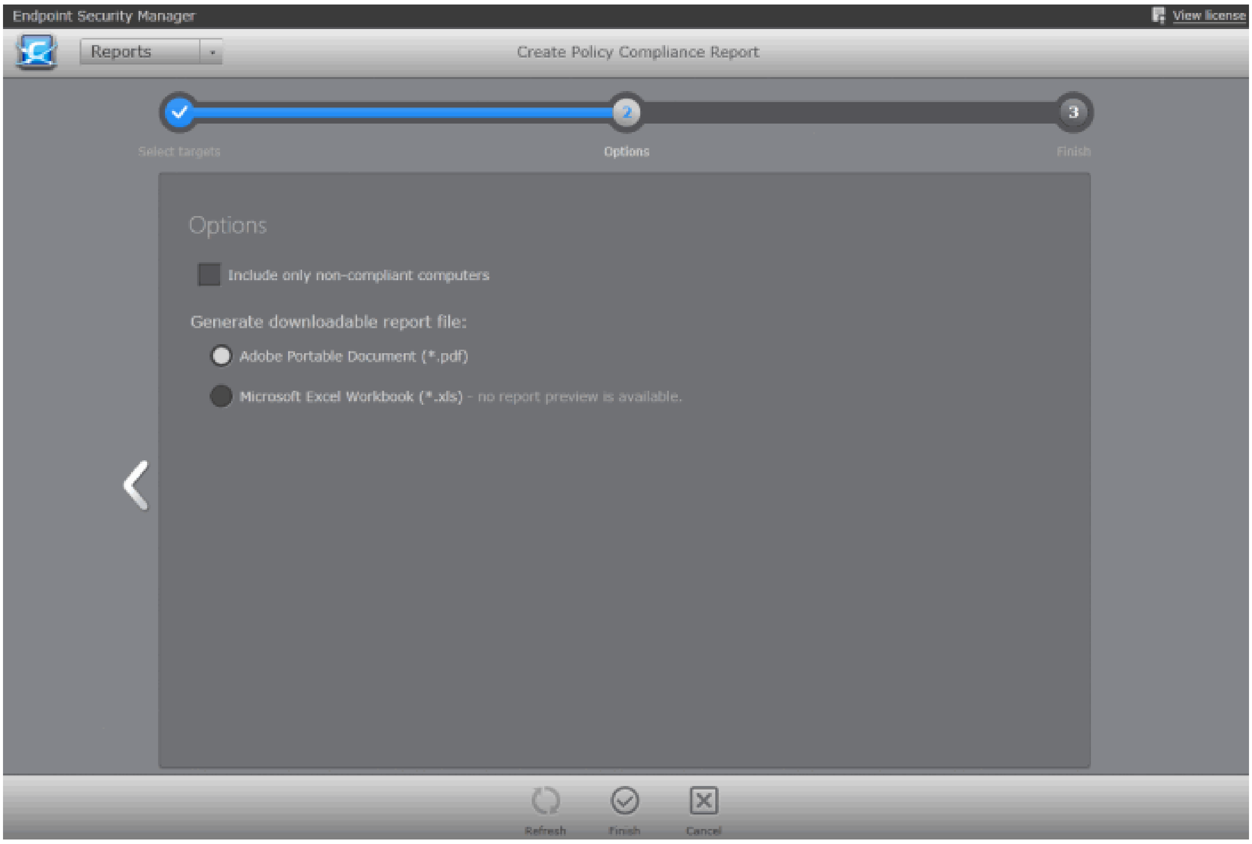
- Select the endpoint(s) for which you wish to generate the Policy Compliance report. The filter options in the header provides at-a-glance statistics of the computers in the network and allow the administrator to filter the computers based on the criteria. You can also filter the computers by clicking 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.



Options

□ Include only non-compliant computers

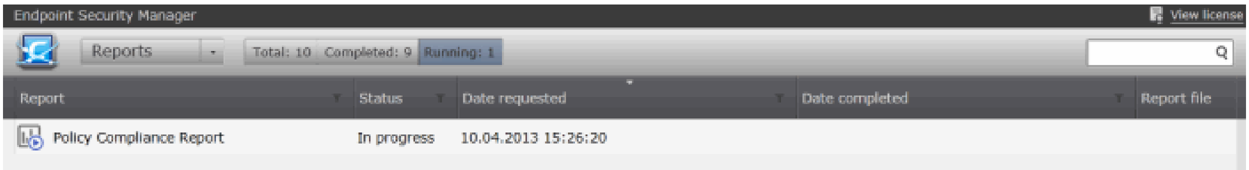
Generate downloadable report file:

○ Adobe Portable Document (*.pdf)

● Microsoft Excel Workbook (*.xls) - no report preview is available.

- 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.



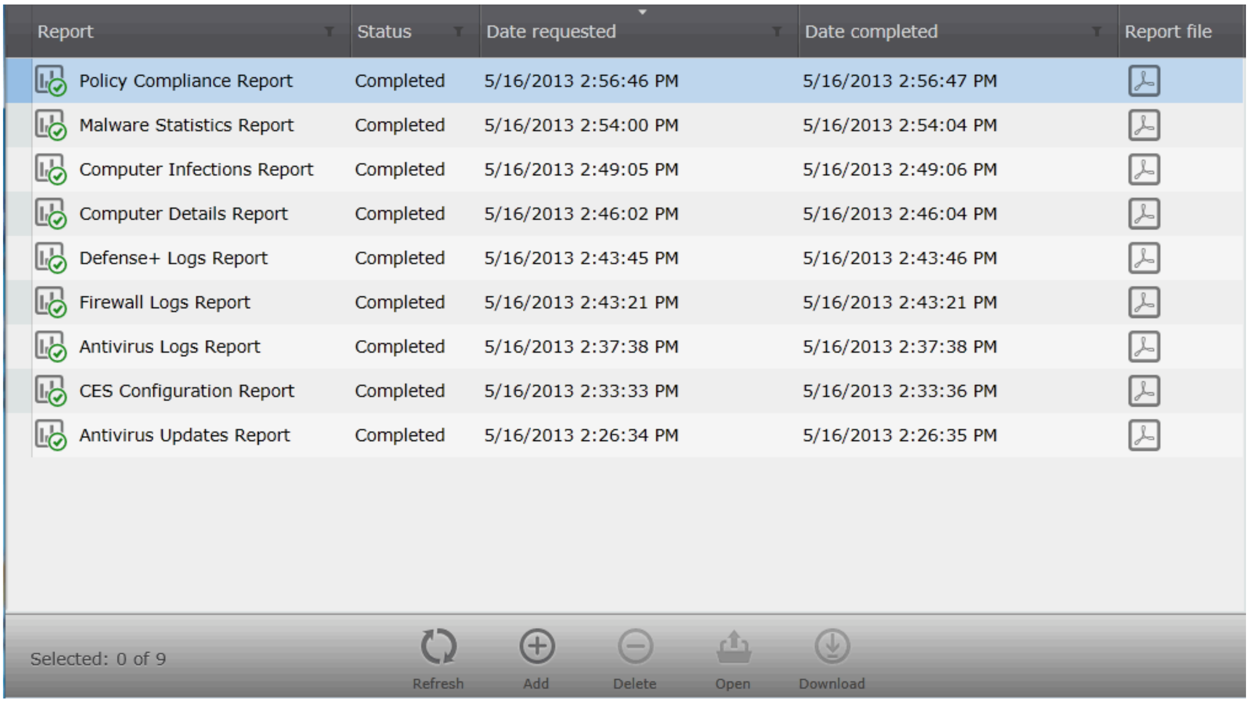
Report	Status	Date requested	Date completed	Report file
Policy Compliance Report	In progress	10.04.2013 15:26:20		

View the Report

The administrator can view the report at anytime after the completion.

To view the report

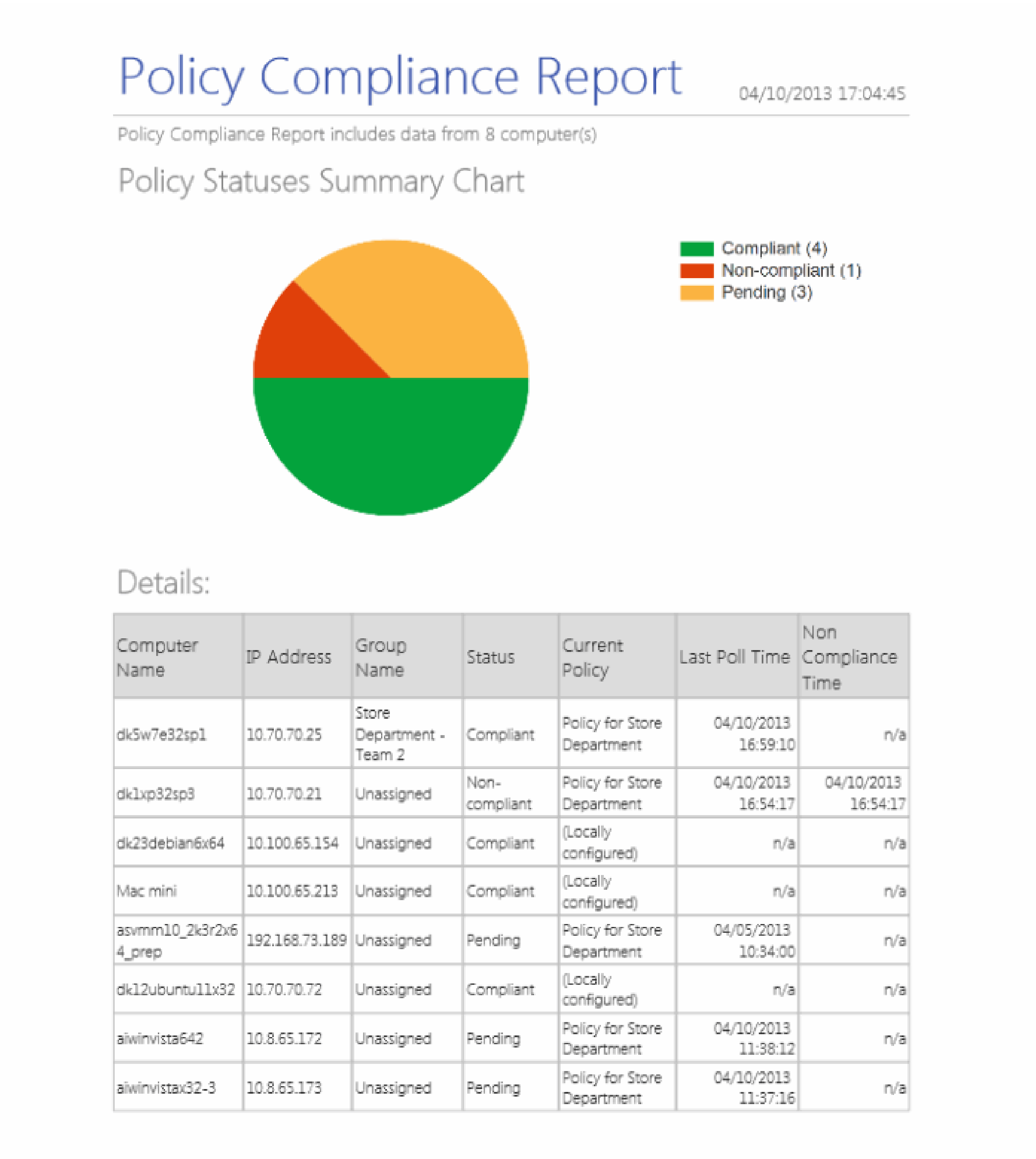
- Select the report and click Open or right click on the report and choose Open from the context sensitive menu.



Report	Status	Date requested	Date completed	Report file
Policy Compliance Report	Completed	5/16/2013 2:56:46 PM	5/16/2013 2:56:47 PM	
Malware Statistics Report	Completed	5/16/2013 2:54:00 PM	5/16/2013 2:54:04 PM	
Computer Infections Report	Completed	5/16/2013 2:49:05 PM	5/16/2013 2:49:06 PM	
Computer Details Report	Completed	5/16/2013 2:46:02 PM	5/16/2013 2:46:04 PM	
Defense+ Logs Report	Completed	5/16/2013 2:43:45 PM	5/16/2013 2:43:46 PM	
Firewall Logs Report	Completed	5/16/2013 2:43:21 PM	5/16/2013 2:43:21 PM	
Antivirus Logs Report	Completed	5/16/2013 2:37:38 PM	5/16/2013 2:37:38 PM	
CES Configuration Report	Completed	5/16/2013 2:33:33 PM	5/16/2013 2:33:36 PM	
Antivirus Updates Report	Completed	5/16/2013 2:26:34 PM	5/16/2013 2:26:35 PM	

Selected: 0 of 9

- 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.
- Following the summary, 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 are displayed.



Policy Compliance Report 04/10/2013 17:04:45

Policy Compliance Report includes data from 8 computer(s)

Policy Statuses Summary Chart

Details:

Computer Name	IP Address	Group Name	Status	Current Policy	Last Poll Time	Non Compliance Time
dk5w7e32sp1	10.70.70.25	Store Department - Team 2	Compliant	Policy for Store Department	04/10/2013 16:59:10	n/a
dk1xp32sp3	10.70.70.21	Unassigned	Non-compliant	Policy for Store Department	04/10/2013 16:54:17	04/10/2013 16:54:17
dk23debian6x64	10.100.65.154	Unassigned	Compliant	(Locally configured)	n/a	n/a
Mac mini	10.100.65.213	Unassigned	Compliant	(Locally configured)	n/a	n/a
asvmm10_2k3r2x64_prep	192.168.73.189	Unassigned	Pending	Policy for Store Department	04/05/2013 10:34:00	n/a
dk12ubuntu11x32	10.70.70.72	Unassigned	Compliant	(Locally configured)	n/a	n/a
aiwinvista642	10.8.65.172	Unassigned	Pending	Policy for Store Department	04/10/2013 11:38:12	n/a
aiwinvistax32-3	10.8.65.173	Unassigned	Pending	Policy for Store Department	04/10/2013 11:37:16	n/a

Downloading the Report

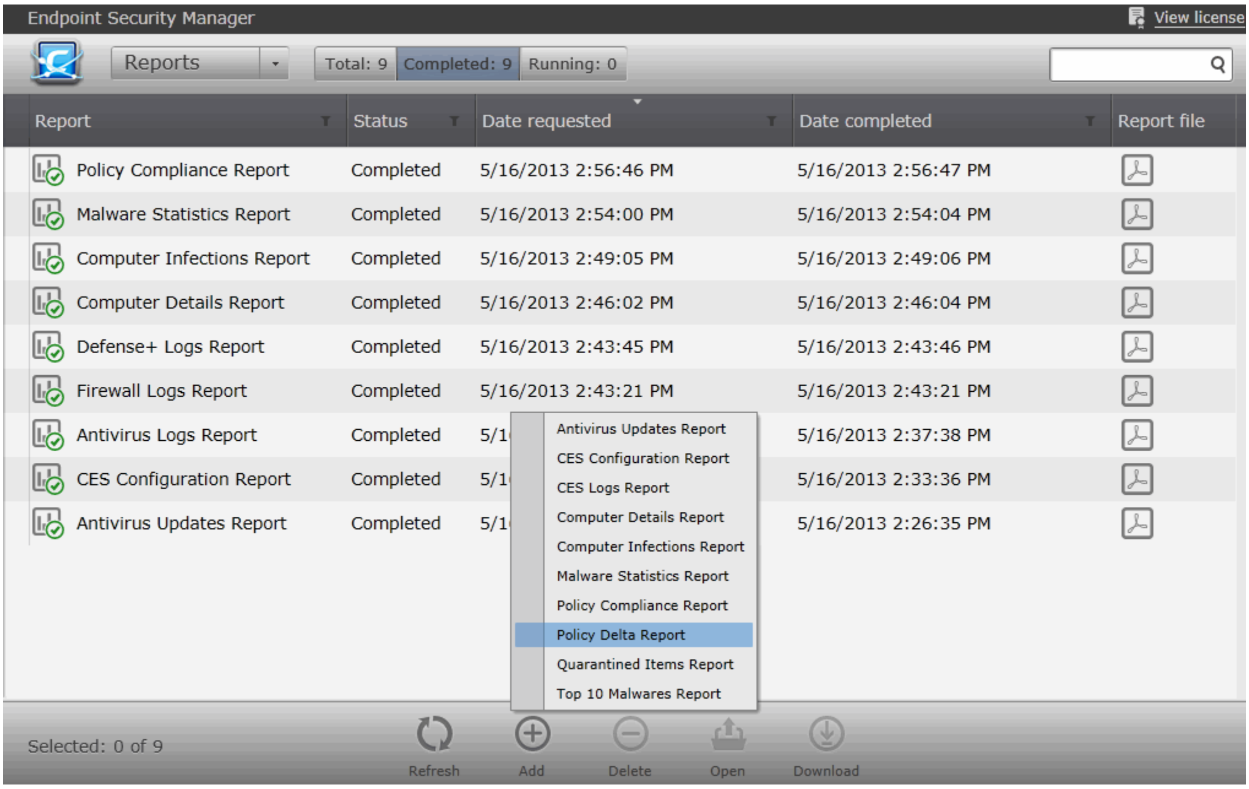
If the administrator had opted for generating a downloadable report, it can be downloaded by selecting the Report in the'Reports' area and clicking the download icon ⬇ at the bottom.

9.8. Policy Delta Report

The Policy Delta report provides a summary of the changes in the configuration of components of CES at the '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 components that are unchanged, changed or missing from the applied policy. The details in the report are helpful to the administrator for investigating the changes made to CES settings in the target computer and the reason(s) the computer received its non-compliant status.

To generate a Computer Infections report

- Open the 'Reports' area by choosing 'Reports' from the drop-down at the top left.

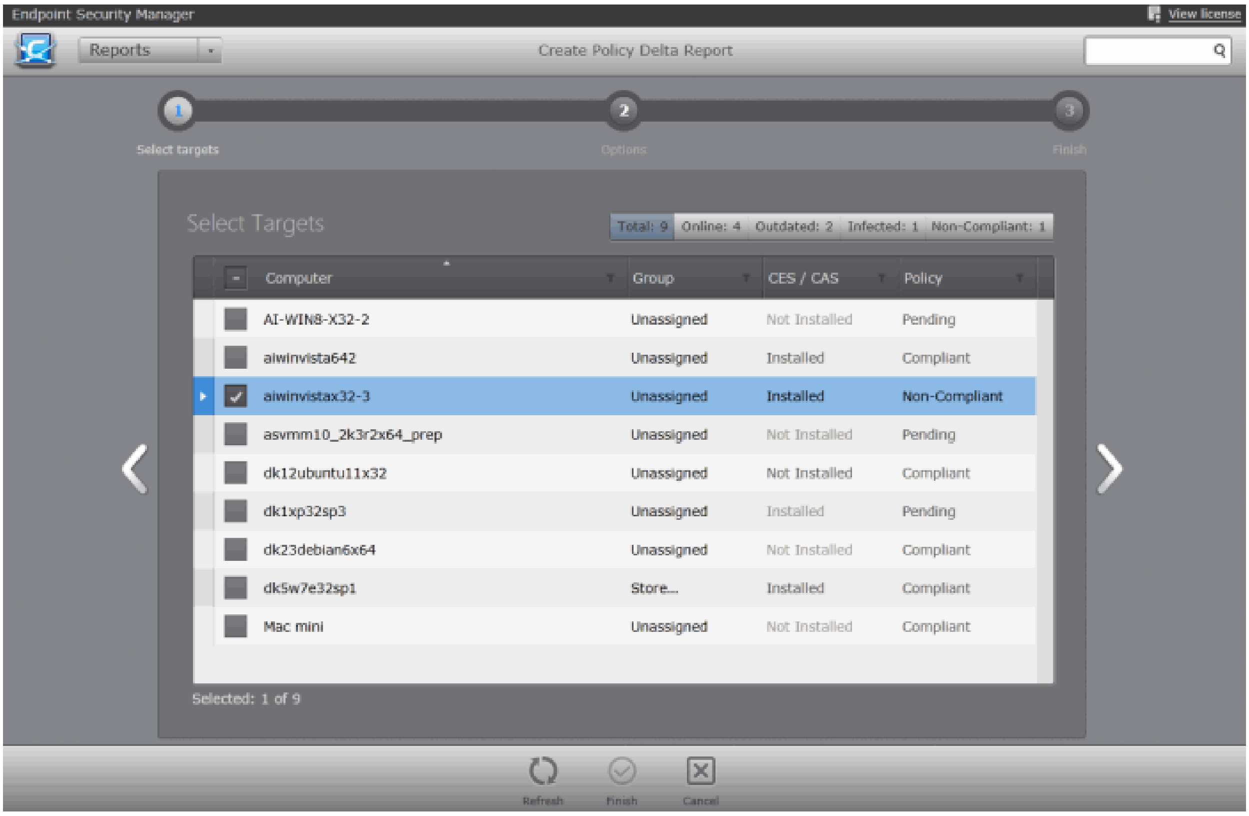


Report	Status	Date requested	Date completed	Report file
Policy Compliance Report	Completed	5/16/2013 2:56:46 PM	5/16/2013 2:56:47 PM	
Malware Statistics Report	Completed	5/16/2013 2:54:00 PM	5/16/2013 2:54:04 PM	
Computer Infections Report	Completed	5/16/2013 2:49:05 PM	5/16/2013 2:49:06 PM	
Computer Details Report	Completed	5/16/2013 2:46:02 PM	5/16/2013 2:46:04 PM	
Defense+ Logs Report	Completed	5/16/2013 2:43:45 PM	5/16/2013 2:43:46 PM	
Firewall Logs Report	Completed	5/16/2013 2:43:21 PM	5/16/2013 2:43:21 PM	
Antivirus Logs Report	Completed	5/1	5/16/2013 2:37:38 PM	
CES Configuration Report	Completed	5/1	5/16/2013 2:33:36 PM	
Antivirus Updates Report	Completed	5/1	5/16/2013 2:26:35 PM	

- 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.



	Computer	Group	CES / CAS	Policy
□	AI-WIN8-X32-2	Unassigned	Not Installed	Pending
□	aiwinvista642	Unassigned	Installed	Compliant
☑	aiwinvistax32-3	Unassigned	Installed	Non-Compliant
□	asvmm10_2k3r2x64_prep	Unassigned	Not Installed	Pending
□	dk12ubuntu11x32	Unassigned	Not Installed	Compliant
□	dk1xp32sp3	Unassigned	Installed	Pending
□	dk23debian6x64	Unassigned	Not Installed	Compliant
□	dk5w7e32sp1	Store...	Installed	Compliant
□	Mac mini	Unassigned	Not Installed	Compliant

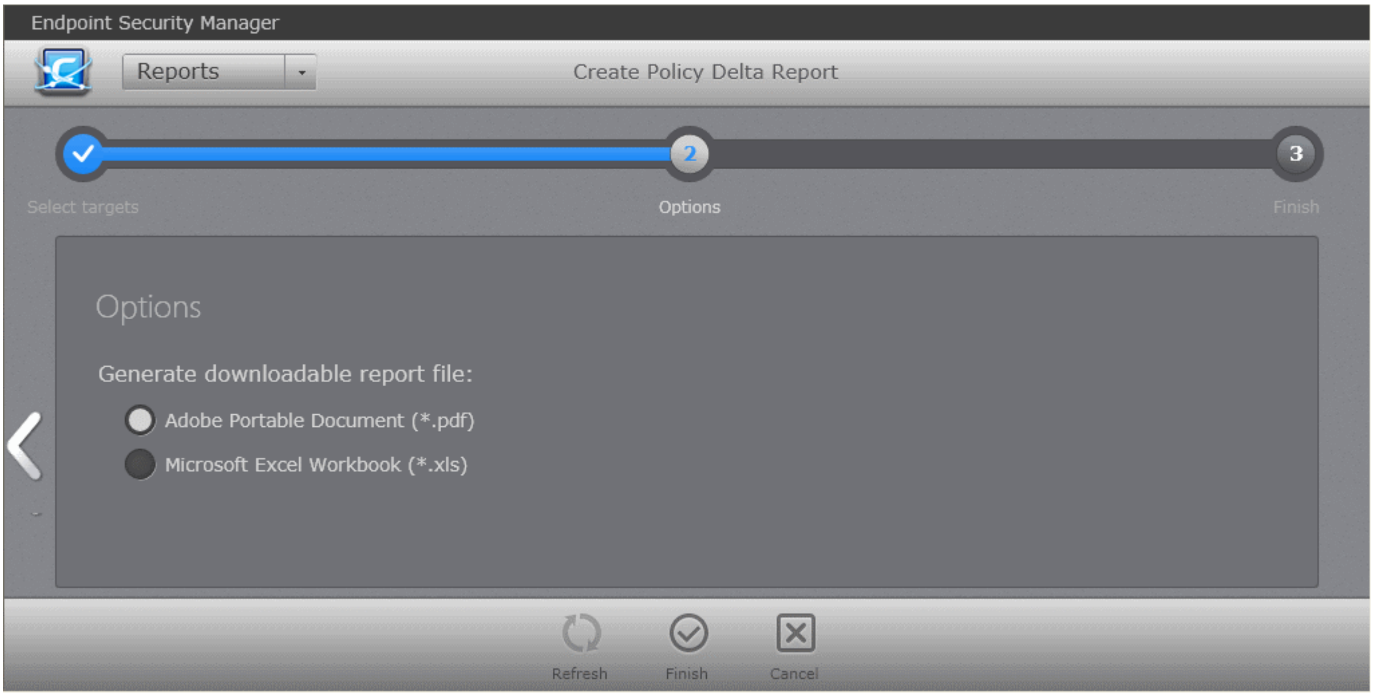
- Select the endpoint(s) for which you wish to generate the Policy Delta report. You can select only the endpoints with 'Non-Compliant' status. The filter options in the header provides at-a-glance statistics of the computers in the network and allow the administrator to filter the computers based on the criteria. You can also filter the computers by clicking the funnel icon on the column headers.
- Click the right arrow 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



Endpoint Security Manager

Reports

Create Policy Delta Report

Select targets — Options — Finish

Options

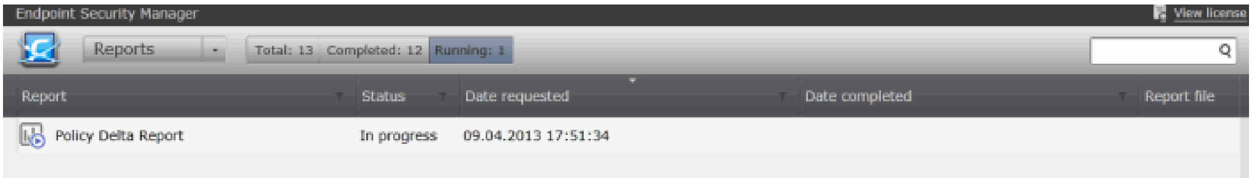
Generate downloadable report file:

○ Adobe Portable Document (*.pdf)

● Microsoft Excel Workbook (*.xls)

- 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.



Endpoint Security Manager

Reports — Total: 13 — Completed: 12 — Running: 1

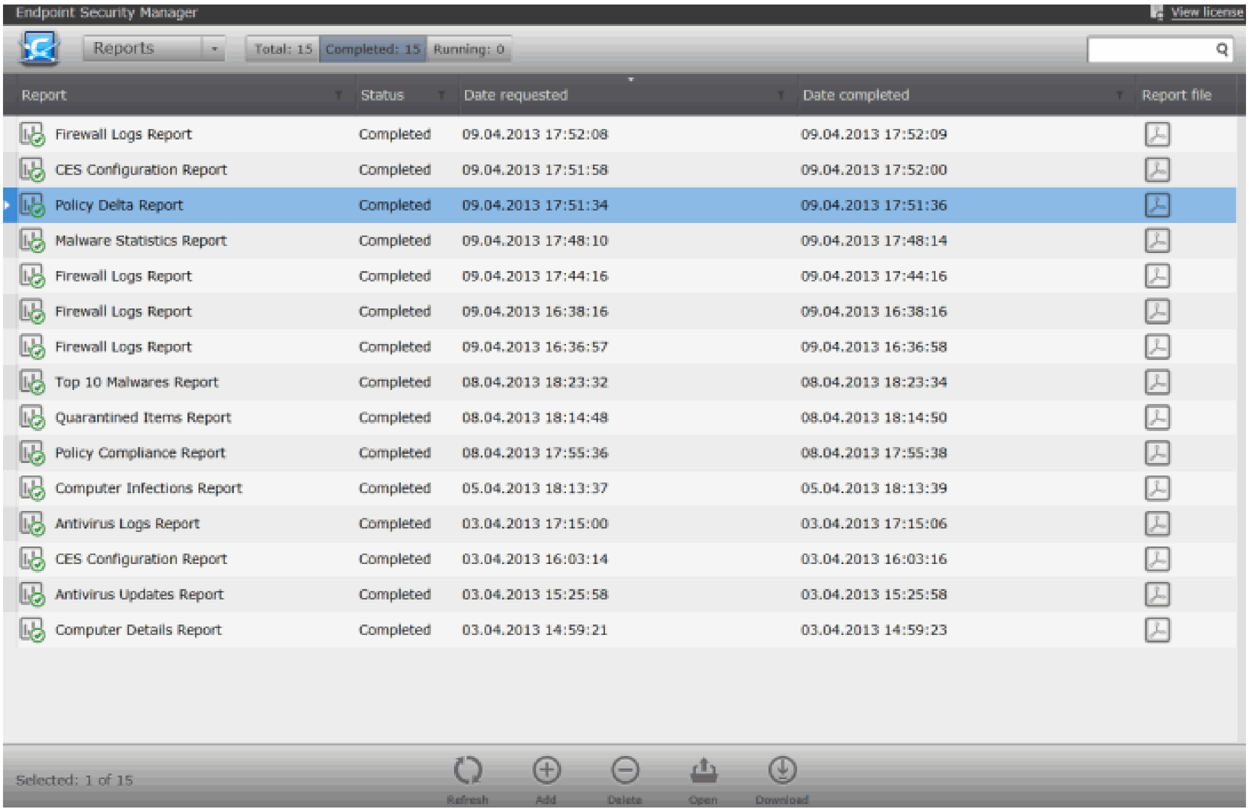
Report	Status	Date requested	Date completed	Report file
Policy Delta Report	In progress	09.04.2013 17:51:34		

View the Report

The administrator can view the report at anytime after the completion.

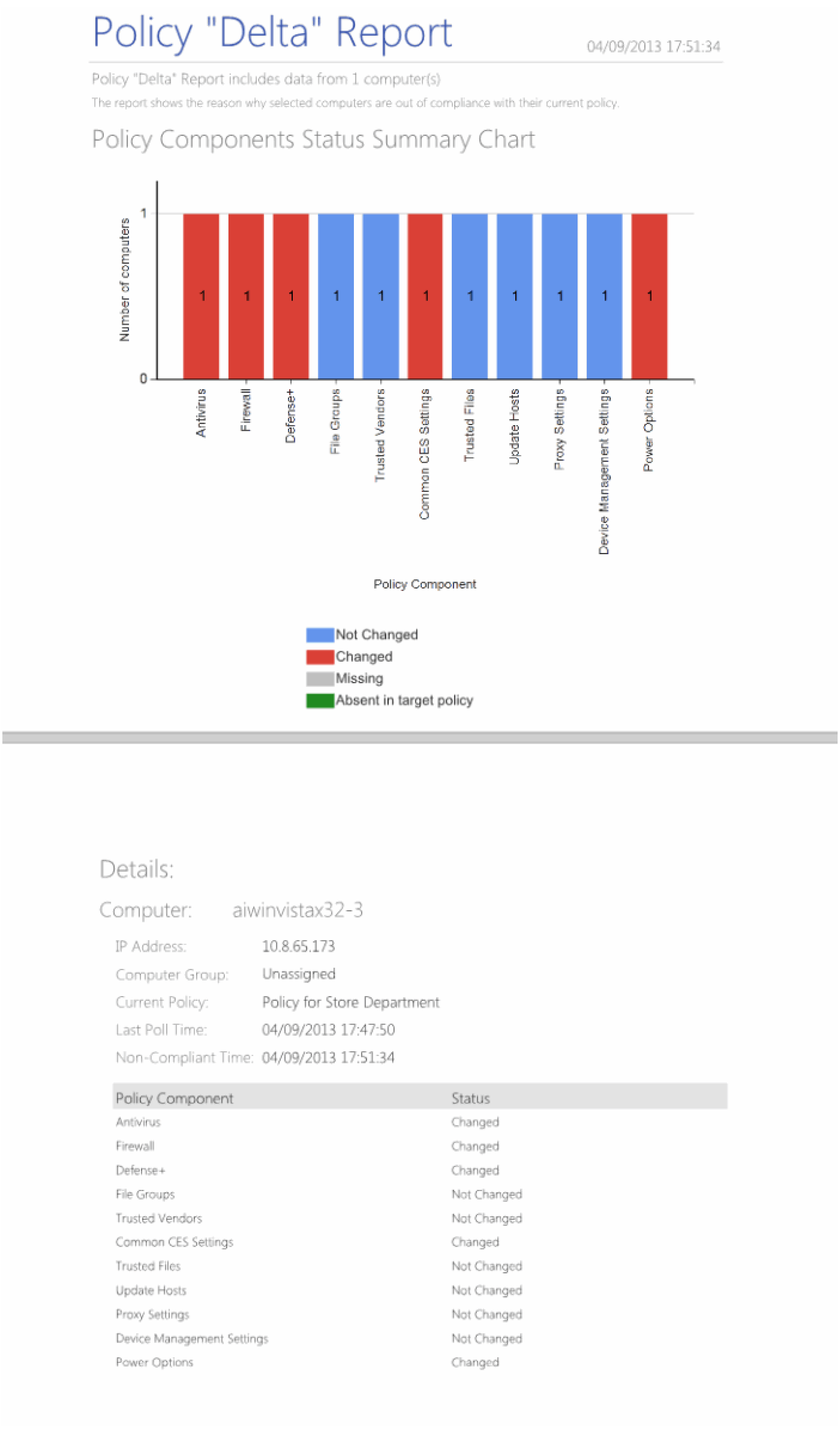
To view the report

- Select the report and click Open or right click on the report and choose Open from the context sensitive menu.



Report	Status	Date requested	Date completed	Report file
Firewall Logs Report	Completed	09.04.2013 17:52:08	09.04.2013 17:52:09	
CES Configuration Report	Completed	09.04.2013 17:51:58	09.04.2013 17:52:00	
Policy Delta Report	Completed	09.04.2013 17:51:34	09.04.2013 17:51:36	
Malware Statistics Report	Completed	09.04.2013 17:48:10	09.04.2013 17:48:14	
Firewall Logs Report	Completed	09.04.2013 17:44:16	09.04.2013 17:44:16	
Firewall Logs Report	Completed	09.04.2013 16:38:16	09.04.2013 16:38:16	
Firewall Logs Report	Completed	09.04.2013 16:36:57	09.04.2013 16:36:58	
Top 10 Malwares Report	Completed	08.04.2013 18:23:32	08.04.2013 18:23:34	
Quarantined Items Report	Completed	08.04.2013 18:14:48	08.04.2013 18:14:50	
Policy Compliance Report	Completed	08.04.2013 17:55:36	08.04.2013 17:55:38	
Computer Infections Report	Completed	05.04.2013 18:13:37	05.04.2013 18:13:39	
Antivirus Logs Report	Completed	03.04.2013 17:15:00	03.04.2013 17:15:06	
CES Configuration Report	Completed	03.04.2013 16:03:14	03.04.2013 16:03:16	
Antivirus Updates Report	Completed	03.04.2013 15:25:58	03.04.2013 15:25:58	
Computer Details Report	Completed	03.04.2013 14:59:21	03.04.2013 14:59:23	

The report will contain bar-graph summary of changes in components of CES in the selected computers followed by the list of selected computers with the status of each component of CES in them.



Policy "Delta" Report

04/09/2013 17:51:34

Policy "Delta" Report includes data from 1 computer(s)

The report shows the reason why selected computers are out of compliance with their current policy.

Policy Components Status Summary Chart

Details:

Computer: aiwinvistax32-3

IP Address:	10.8.65.173
Computer Group:	Unassigned
Current Policy:	Policy for Store Department
Last Poll Time:	04/09/2013 17:47:50
Non-Compliant Time:	04/09/2013 17:51:34

Policy Component	Status
Antivirus	Changed
Firewall	Changed
Defense+	Changed
File Groups	Not Changed
Trusted Vendors	Not Changed
Common CES Settings	Changed
Trusted Files	Not Changed
Update Hosts	Not Changed
Proxy Settings	Not Changed
Device Management Settings	Not Changed
Power Options	Changed

The status of each component indicates the difference in configuration of the component with respect to the actual setting as per the policy applied.

- **Absent** - means component is present on the endpoint, but the settings for it are not contained in the policy applied by CESM. The administrator can apply a different policy imported from a different source that contains settings for all the components.
- **Missing** - means either the component is absent on both the policy and the endpoint sides or on the endpoint side.
- **Changed** - means the configuration of the component in the endpoint side is different from the policy applied.
- **Not Changed** - means the configuration of the component is the same on both the policy and the endpoint sides.

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.

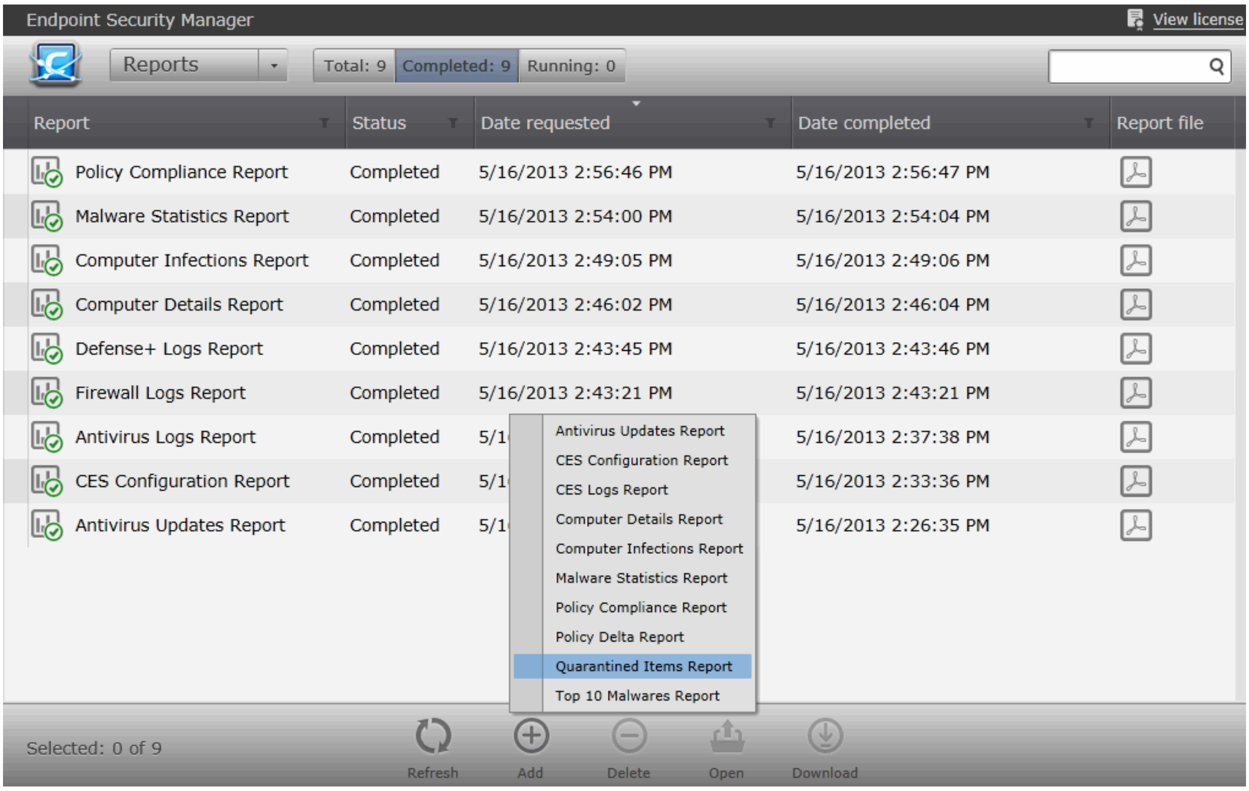
9.9. Quarantined Items Report

The 'Quarantined Items' report provides details on the malware detected and successfully quarantined at the target computers. The report also allows the administrator to remove the quarantined items or restore them to their original locations after analyzing the report.

Note: For the local CES 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 has been configured to automatically quarantine the threats identified from various scans. For more details on configuring CES 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.



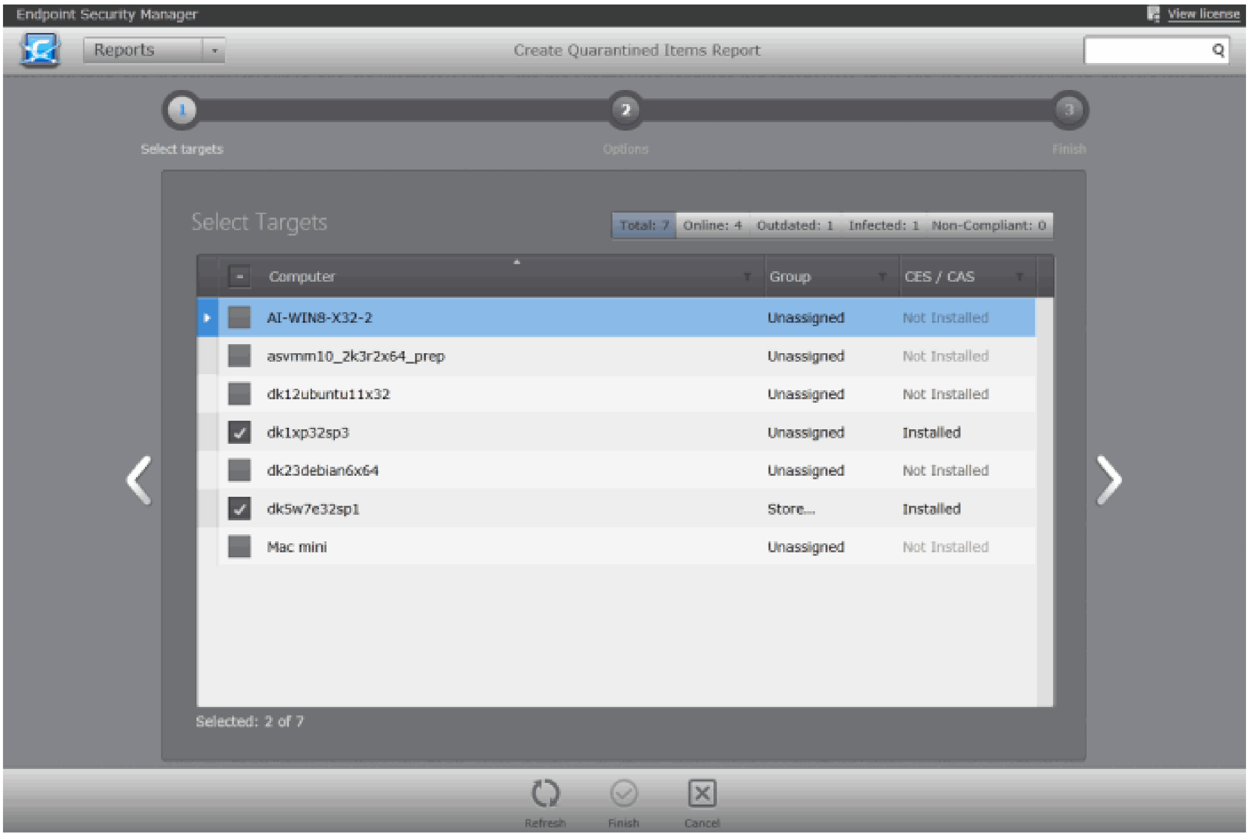
Report	Status	Date requested	Date completed	Report file
Policy Compliance Report	Completed	5/16/2013 2:56:46 PM	5/16/2013 2:56:47 PM	
Malware Statistics Report	Completed	5/16/2013 2:54:00 PM	5/16/2013 2:54:04 PM	
Computer Infections Report	Completed	5/16/2013 2:49:05 PM	5/16/2013 2:49:06 PM	
Computer Details Report	Completed	5/16/2013 2:46:02 PM	5/16/2013 2:46:04 PM	
Defense+ Logs Report	Completed	5/16/2013 2:43:45 PM	5/16/2013 2:43:46 PM	
Firewall Logs Report	Completed	5/16/2013 2:43:21 PM	5/16/2013 2:43:21 PM	
Antivirus Logs Report	Completed	5/1	5/16/2013 2:37:38 PM	
CES Configuration Report	Completed	5/1	5/16/2013 2:33:36 PM	
Antivirus Updates Report	Completed	5/1	5/16/2013 2:26:35 PM	

Selected: 0 of 9

- 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.


Endpoint Security Manager
View license
Reports
Create Quarantined Items Report
Select targets
Options
Finish
Select Targets
Total: 7 Online: 4 Outdated: 1 Infected: 1 Non-Compliant: 0
Refresh
Finish
Cancel

	Computer	Group	CES / CAS
□	AI-WIN8-X32-2	Unassigned	Not Installed
□	asvmm10_2k3r2x64_prep	Unassigned	Not Installed
□	dk12ubuntu11x32	Unassigned	Not Installed
☑	dk1xp32sp3	Unassigned	Installed
□	dk23debian6x64	Unassigned	Not Installed
☑	dk5w7e32sp1	Store...	Installed
□	Mac mini	Unassigned	Not Installed

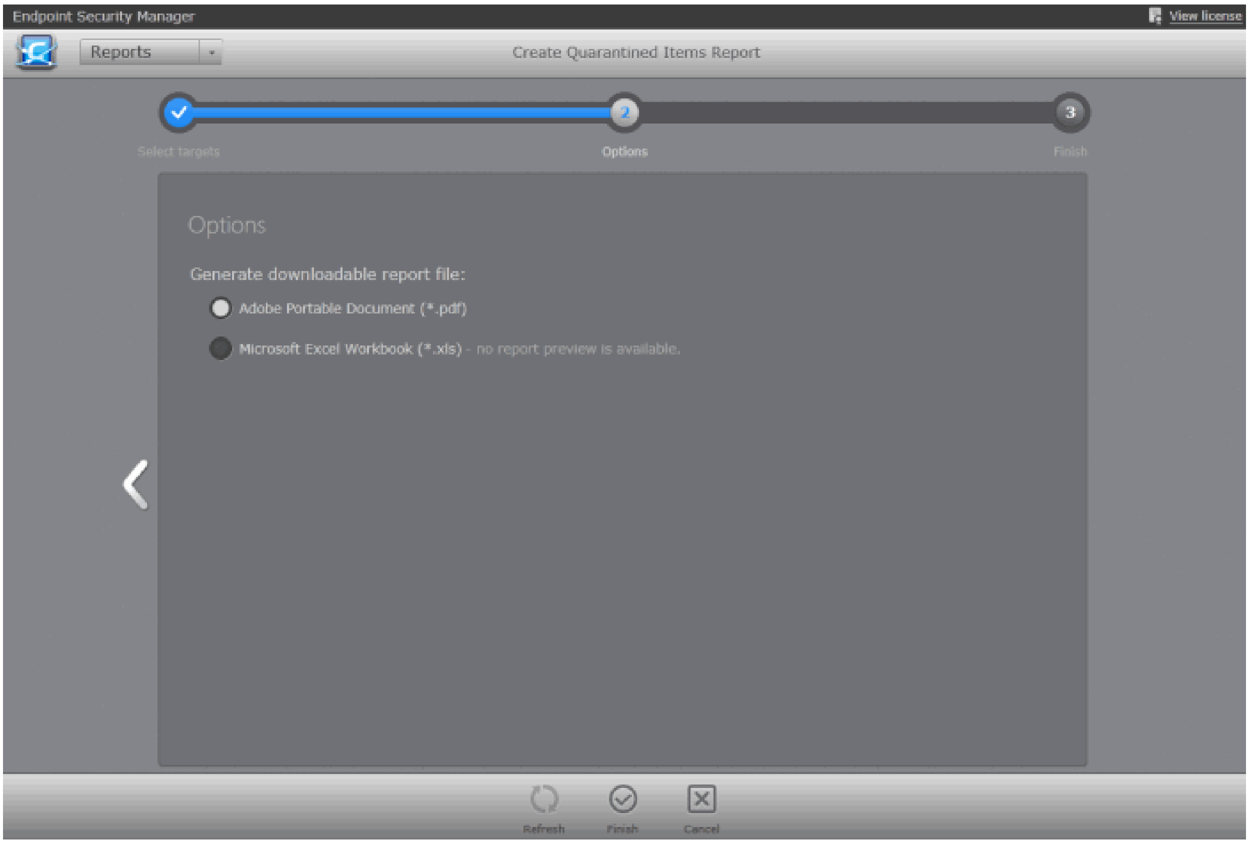
Selected: 2 of 7

- 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 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



Options

Generate downloadable report file:

○ Adobe Portable Document (*.pdf)

○ Microsoft Excel Workbook (*.xls) - no report preview is available.

- Click the 'Finish' icon to start generating the report.

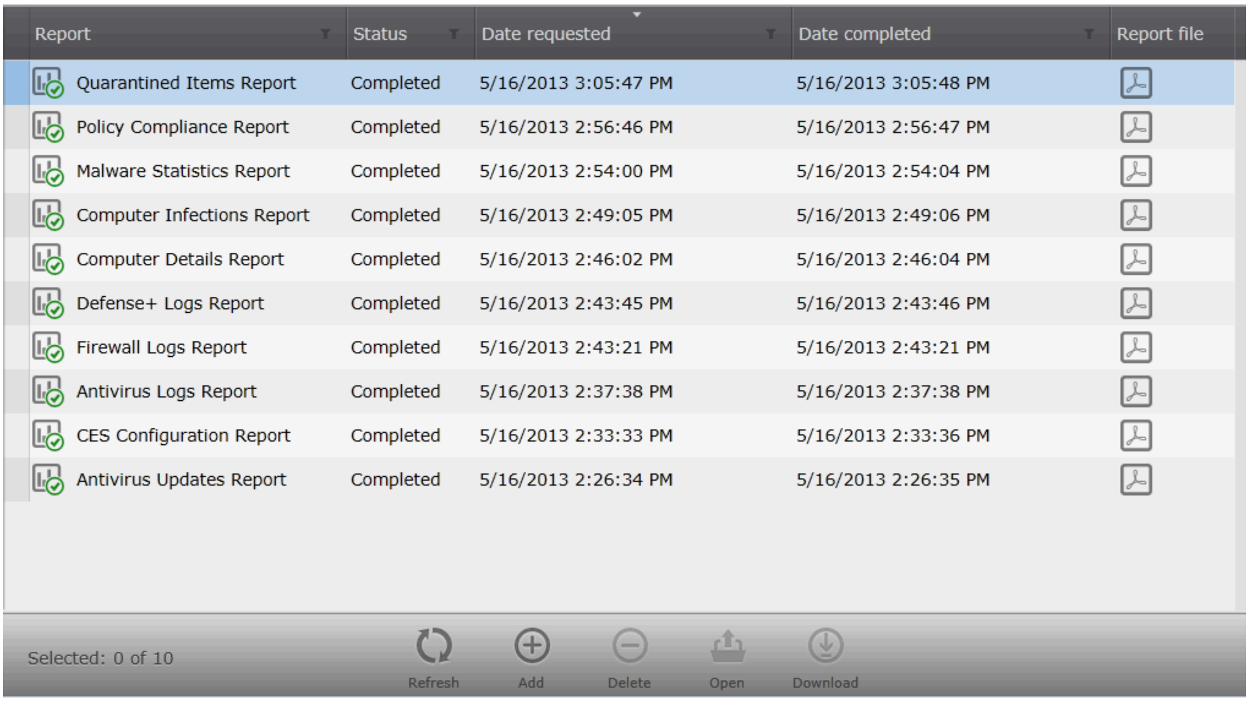
The report generation will be started or added to the queue. The progress will be displayed in the 'Reports' area.

View the Report

The administrator can view the report at anytime after the completion.

To view the report

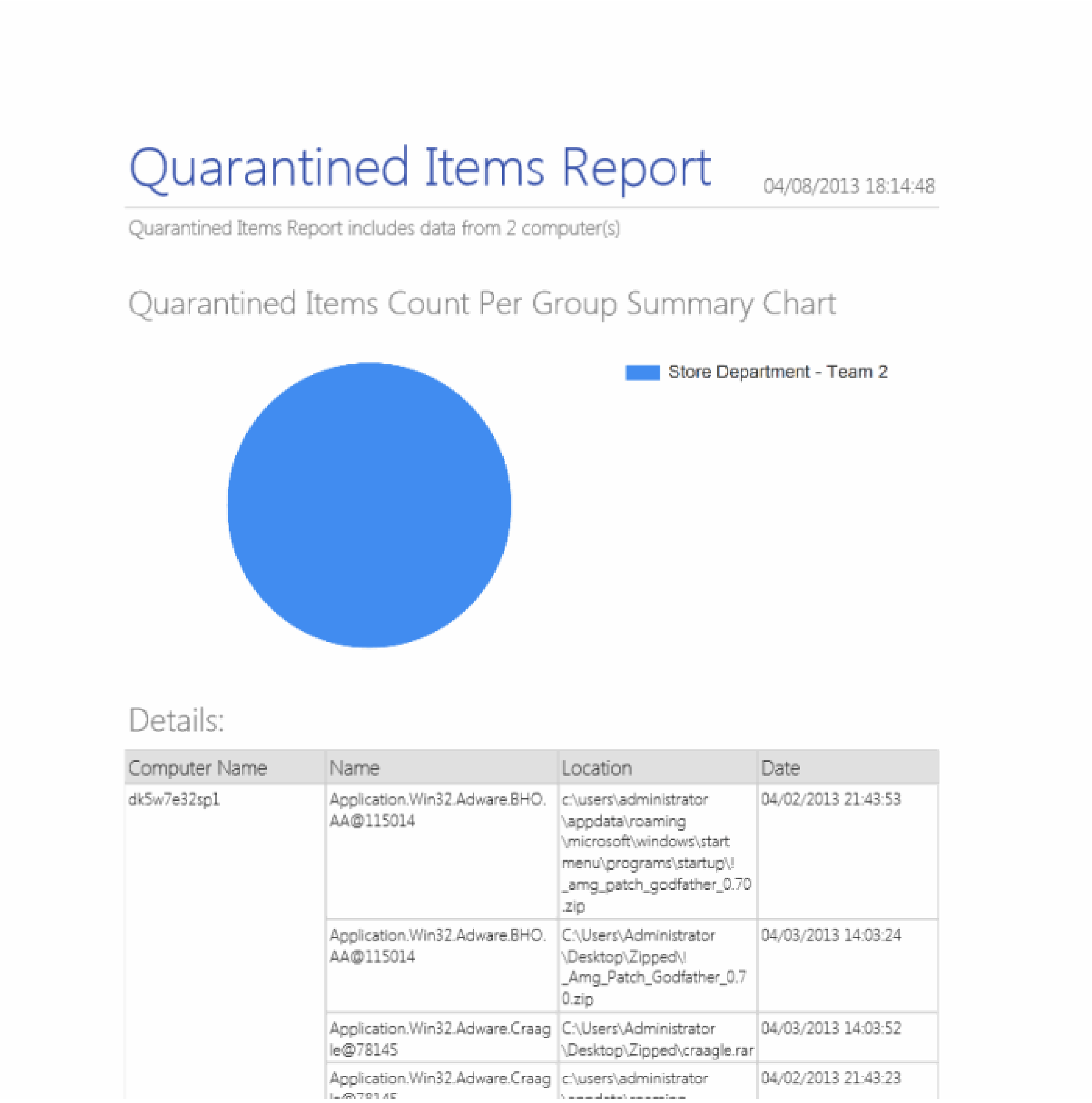
- Select the report and click 'Open' or right click on the report and choose 'Open' from the context sensitive menu.



Report	Status	Date requested	Date completed	Report file
Quarantined Items Report	Completed	5/16/2013 3:05:47 PM	5/16/2013 3:05:48 PM	
Policy Compliance Report	Completed	5/16/2013 2:56:46 PM	5/16/2013 2:56:47 PM	
Malware Statistics Report	Completed	5/16/2013 2:54:00 PM	5/16/2013 2:54:04 PM	
Computer Infections Report	Completed	5/16/2013 2:49:05 PM	5/16/2013 2:49:06 PM	
Computer Details Report	Completed	5/16/2013 2:46:02 PM	5/16/2013 2:46:04 PM	
Defense+ Logs Report	Completed	5/16/2013 2:43:45 PM	5/16/2013 2:43:46 PM	
Firewall Logs Report	Completed	5/16/2013 2:43:21 PM	5/16/2013 2:43:21 PM	
Antivirus Logs Report	Completed	5/16/2013 2:37:38 PM	5/16/2013 2:37:38 PM	
CES Configuration Report	Completed	5/16/2013 2:33:33 PM	5/16/2013 2:33:36 PM	
Antivirus Updates Report	Completed	5/16/2013 2:26:34 PM	5/16/2013 2:26:35 PM	

Selected: 0 of 10

The report will contain 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.



Quarantined Items Report 04/08/2013 18:14:48

Quarantined Items Report includes data from 2 computer(s)

Quarantined Items Count Per Group Summary Chart

Details:

Computer Name	Name	Location	Date
dk5w7e32sp1	Application.Win32.Adware.BHO.AA@115014	c:\users\administrator\appdata\roaming\microsoft\windows\start menu\programs\startup\!_amg_patch_godfather_0.70.zip	04/02/2013 21:43:53
	Application.Win32.Adware.BHO.AA@115014	C:\Users\Administrator\Desktop\Zipped\!_Amg_Patch_Godfather_0.70.zip	04/03/2013 14:03:24
	Application.Win32.Adware.Craagle@78145	C:\Users\Administrator\Desktop\Zipped\craagle.rar	04/03/2013 14:03:52
	Application.Win32.Adware.Craag	c:\users\administrator	04/02/2013 21:43:23

Downloading the Report

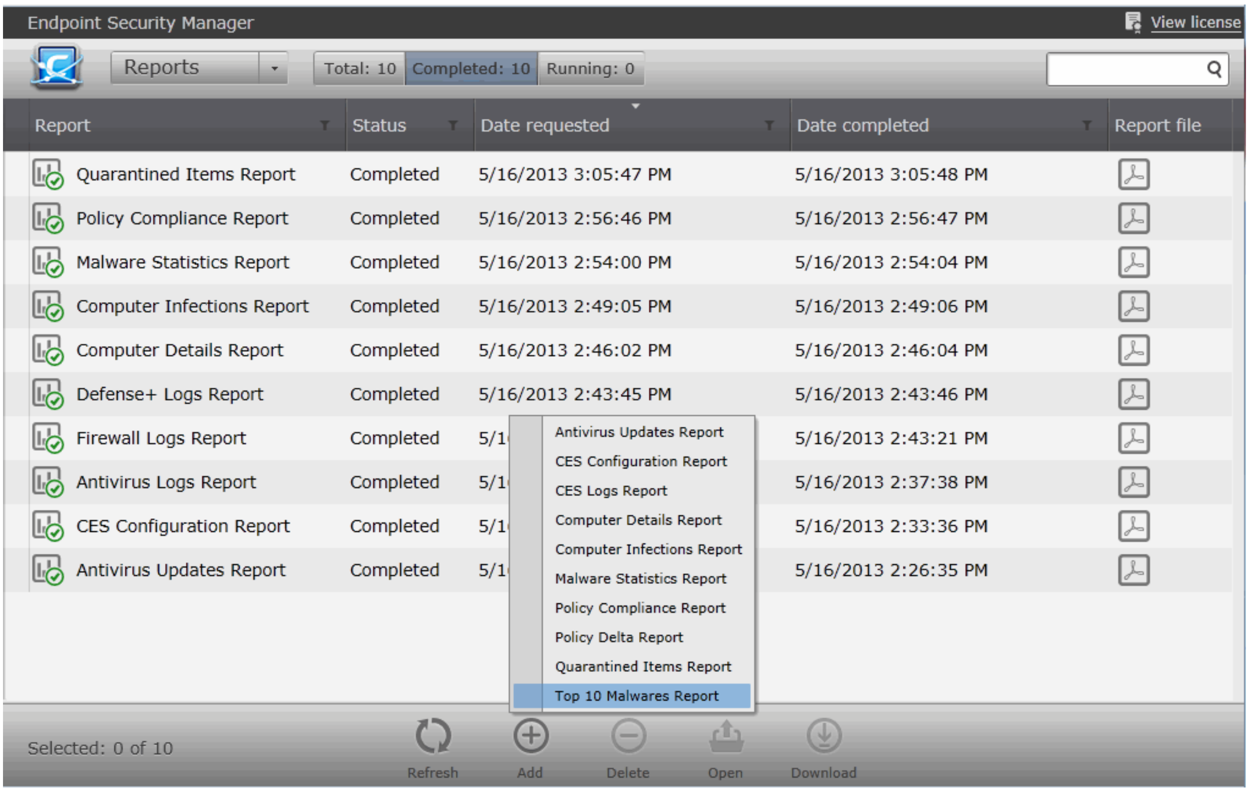
If the administrator had opted for generating a downloadable report, it can be downloaded by selecting the Report in the 'Reports' area and clicking the download icon ⬇ at the bottom.

9.10. Top 10 Malwares Report

The 'Top 10 Malwares' report provides information on the malware that has most affected the selected endpoints in 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.

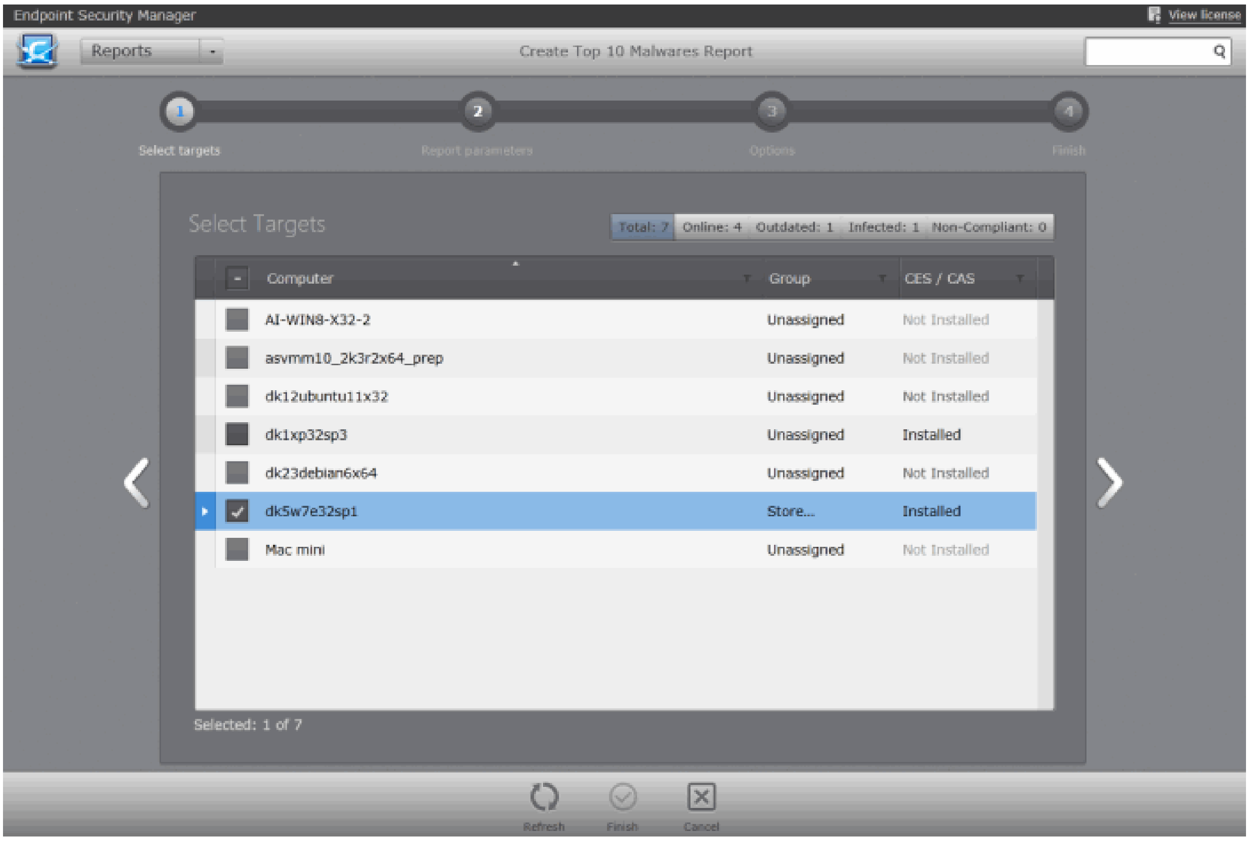


Report	Status	Date requested	Date completed	Report file
Quarantined Items Report	Completed	5/16/2013 3:05:47 PM	5/16/2013 3:05:48 PM	
Policy Compliance Report	Completed	5/16/2013 2:56:46 PM	5/16/2013 2:56:47 PM	
Malware Statistics Report	Completed	5/16/2013 2:54:00 PM	5/16/2013 2:54:04 PM	
Computer Infections Report	Completed	5/16/2013 2:49:05 PM	5/16/2013 2:49:06 PM	
Computer Details Report	Completed	5/16/2013 2:46:02 PM	5/16/2013 2:46:04 PM	
Defense+ Logs Report	Completed	5/16/2013 2:43:45 PM	5/16/2013 2:43:46 PM	
Firewall Logs Report	Completed	5/1	5/16/2013 2:43:21 PM	
Antivirus Logs Report	Completed	5/1	5/16/2013 2:37:38 PM	
CES Configuration Report	Completed	5/1	5/16/2013 2:33:36 PM	
Antivirus Updates Report	Completed	5/1	5/16/2013 2:26:35 PM	

- 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 Targets

Total: 7 | Online: 4 | Outdated: 1 | Infected: 1 | Non-Compliant: 0

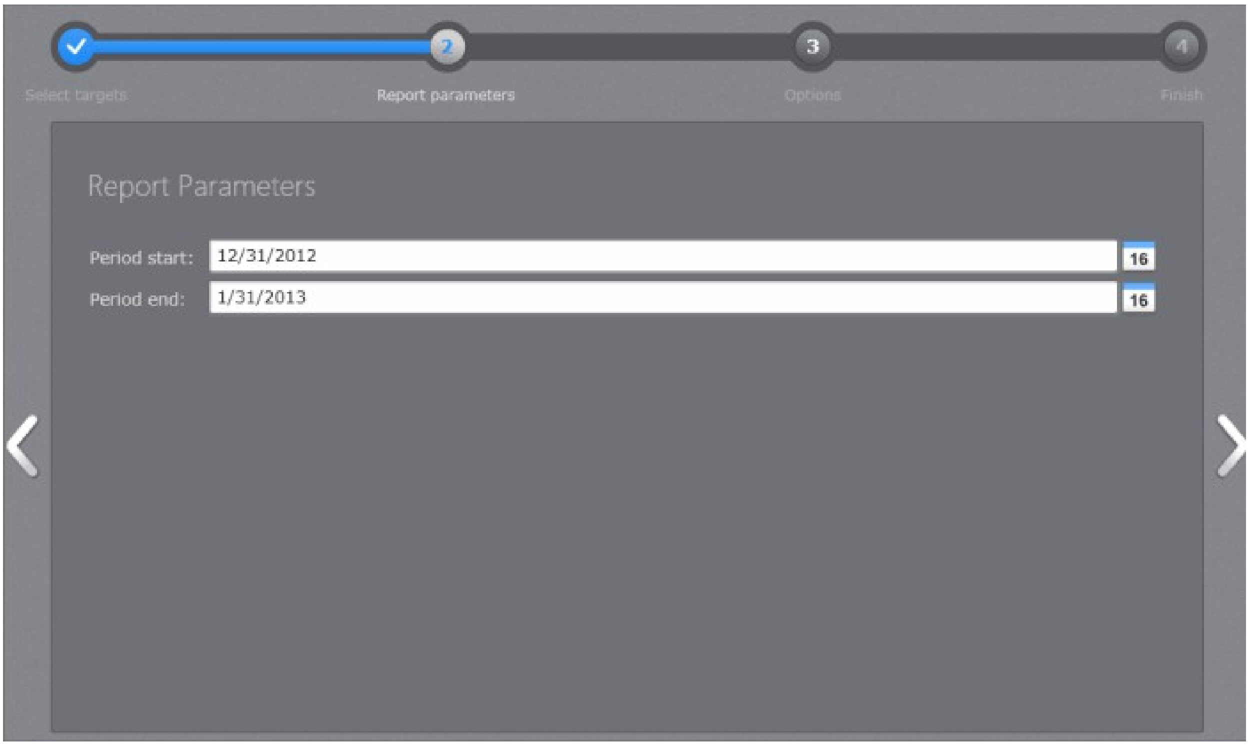
	Computer	Group	CES / CAS
□	AI-WIN8-X32-2	Unassigned	Not Installed
□	asvmm10_2k3r2x64_prep	Unassigned	Not Installed
□	dk12ubuntu11x32	Unassigned	Not Installed
□	dk1xp32sp3	Unassigned	Installed
□	dk23debian6x64	Unassigned	Not Installed
☑	dk5w7e32sp1	Store...	Installed
□	Mac mini	Unassigned	Not Installed

Selected: 1 of 7

- 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.



Report Parameters

Period start: 12/31/2012

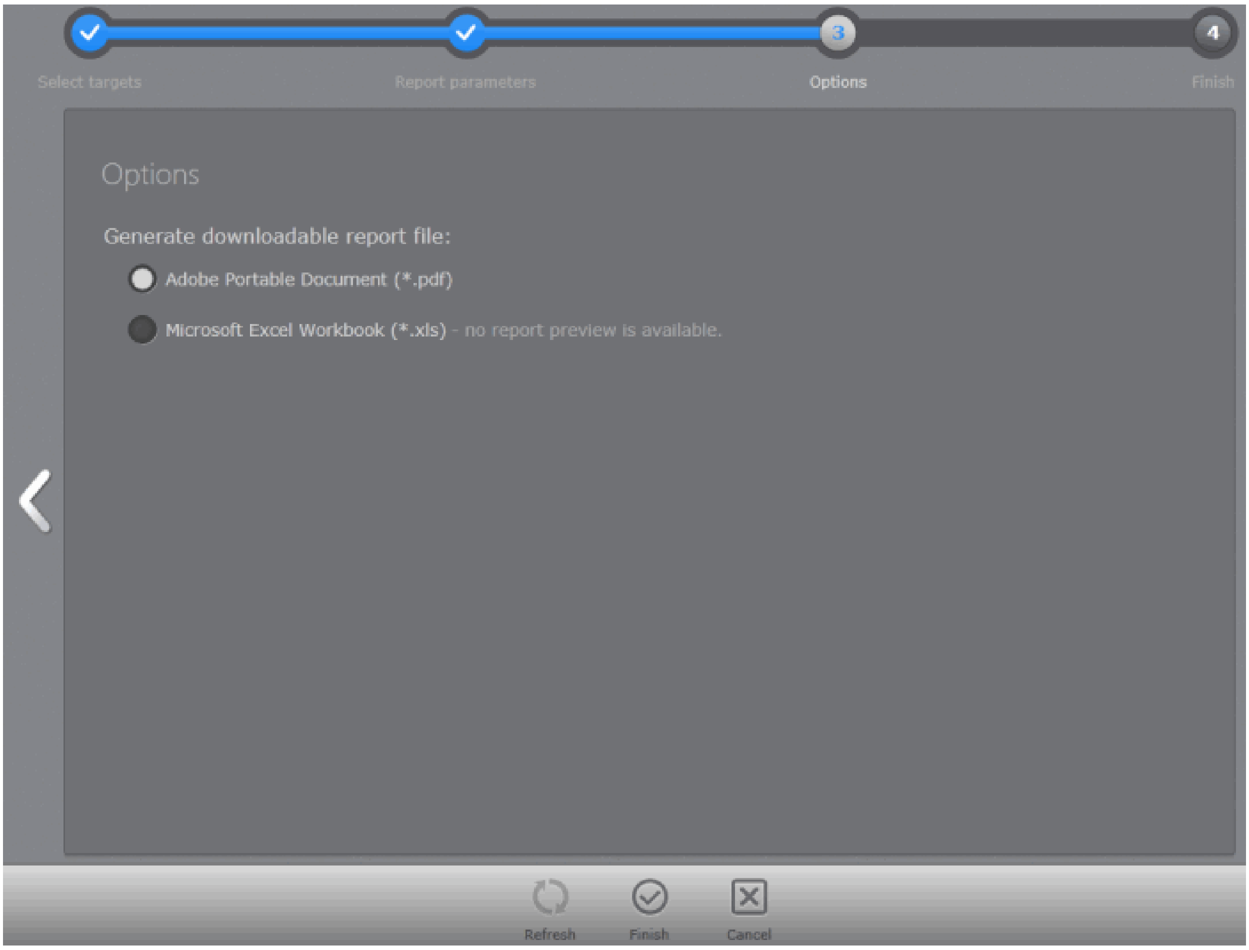
Period end: 1/31/2013

- 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 downloaded to the administrator's computer.
- Select required options



Options

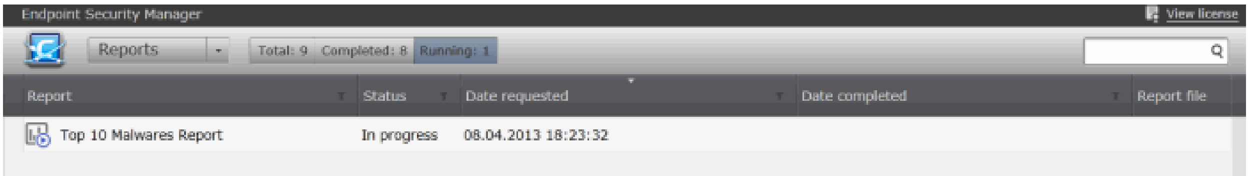
Generate downloadable report file:

○ Adobe Portable Document (*.pdf)

● Microsoft Excel Workbook (*.xls) - no report preview is available.

- 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.



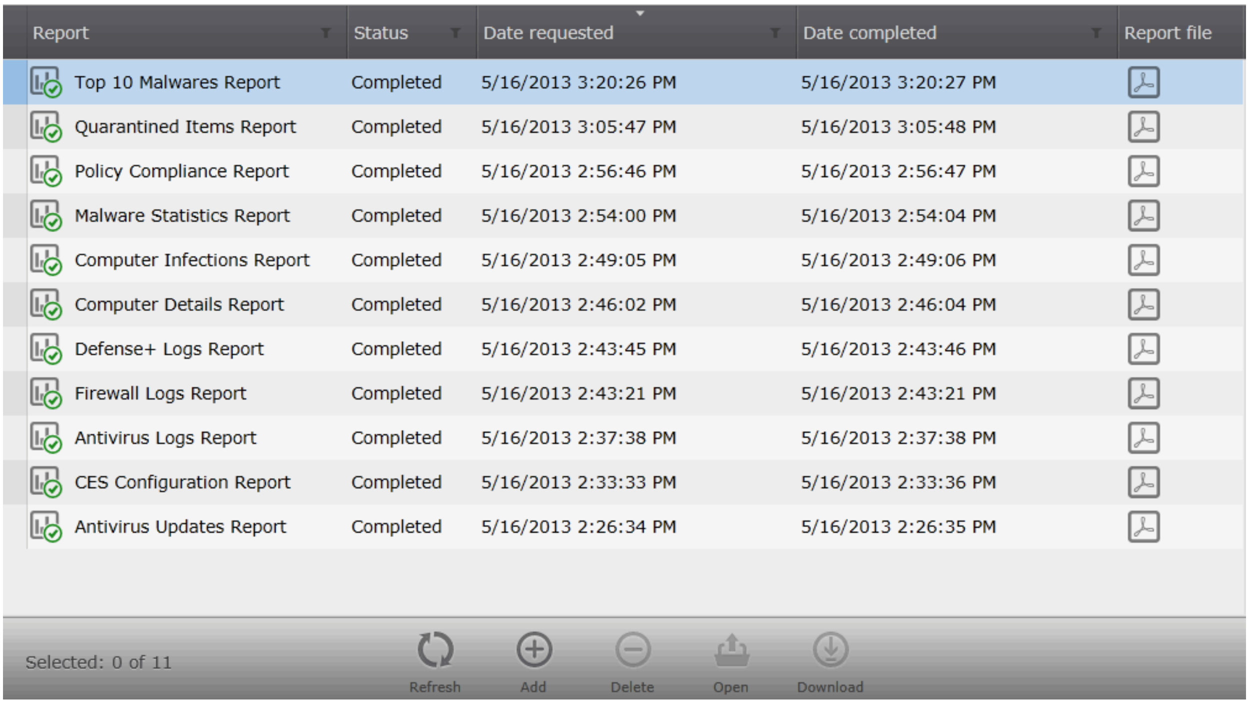
Report	Status	Date requested	Date completed	Report file
Top 10 Malwares Report	In progress	08.04.2013 18:23:32		

View the Report

The administrator can view the report at anytime after the completion.

To view the report

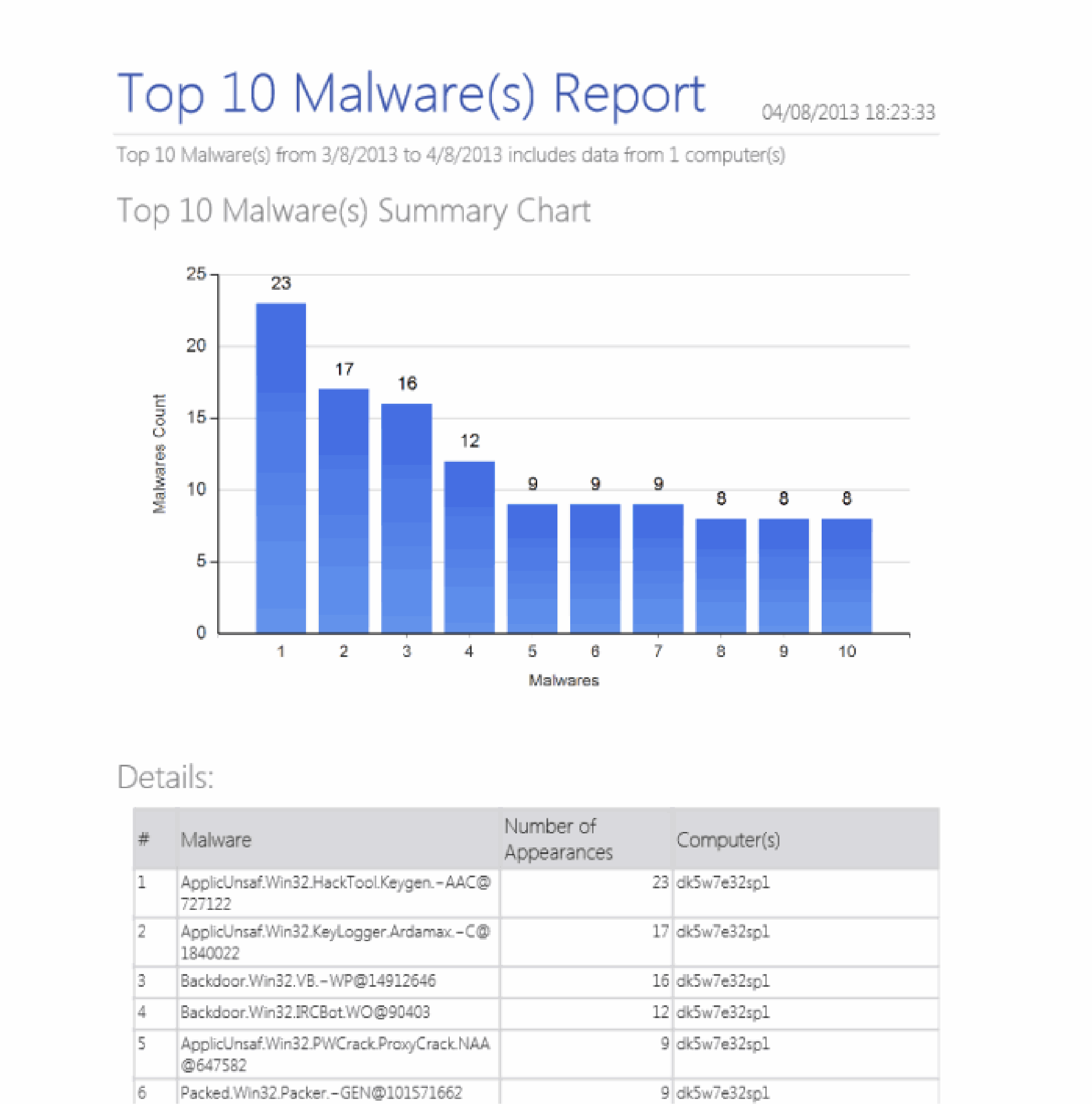
Select the report and click Open or right click on the report and choose Open from the context sensitive menu.



Report	Status	Date requested	Date completed	Report file
Top 10 Malwares Report	Completed	5/16/2013 3:20:26 PM	5/16/2013 3:20:27 PM	
Quarantined Items Report	Completed	5/16/2013 3:05:47 PM	5/16/2013 3:05:48 PM	
Policy Compliance Report	Completed	5/16/2013 2:56:46 PM	5/16/2013 2:56:47 PM	
Malware Statistics Report	Completed	5/16/2013 2:54:00 PM	5/16/2013 2:54:04 PM	
Computer Infections Report	Completed	5/16/2013 2:49:05 PM	5/16/2013 2:49:06 PM	
Computer Details Report	Completed	5/16/2013 2:46:02 PM	5/16/2013 2:46:04 PM	
Defense+ Logs Report	Completed	5/16/2013 2:43:45 PM	5/16/2013 2:43:46 PM	
Firewall Logs Report	Completed	5/16/2013 2:43:21 PM	5/16/2013 2:43:21 PM	
Antivirus Logs Report	Completed	5/16/2013 2:37:38 PM	5/16/2013 2:37:38 PM	
CES Configuration Report	Completed	5/16/2013 2:33:33 PM	5/16/2013 2:33:36 PM	
Antivirus Updates Report	Completed	5/16/2013 2:26:34 PM	5/16/2013 2:26:35 PM	

Selected: 0 of 11

The report will 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.



Top 10 Malware(s) Report 04/08/2013 18:23:33

Top 10 Malware(s) from 3/8/2013 to 4/8/2013 includes data from 1 computer(s)

Top 10 Malware(s) Summary Chart

Details:

#	Malware	Number of Appearances	Computer(s)
1	ApplicUnsaf.Win32.HackTool.Keygen.~AAC@727122	23	dk5w7e32sp1
2	ApplicUnsaf.Win32.KeyLogger.Ardamax.~C@1840022	17	dk5w7e32sp1
3	Backdoor.Win32.VB.~WP@14912646	16	dk5w7e32sp1
4	Backdoor.Win32.IRCBot.WO@90403	12	dk5w7e32sp1
5	ApplicUnsaf.Win32.PWCrack.ProxyCrack.NAA@647582	9	dk5w7e32sp1
6	Packed.Win32.Packer.~GEN@101571662	9	dk5w7e32sp1

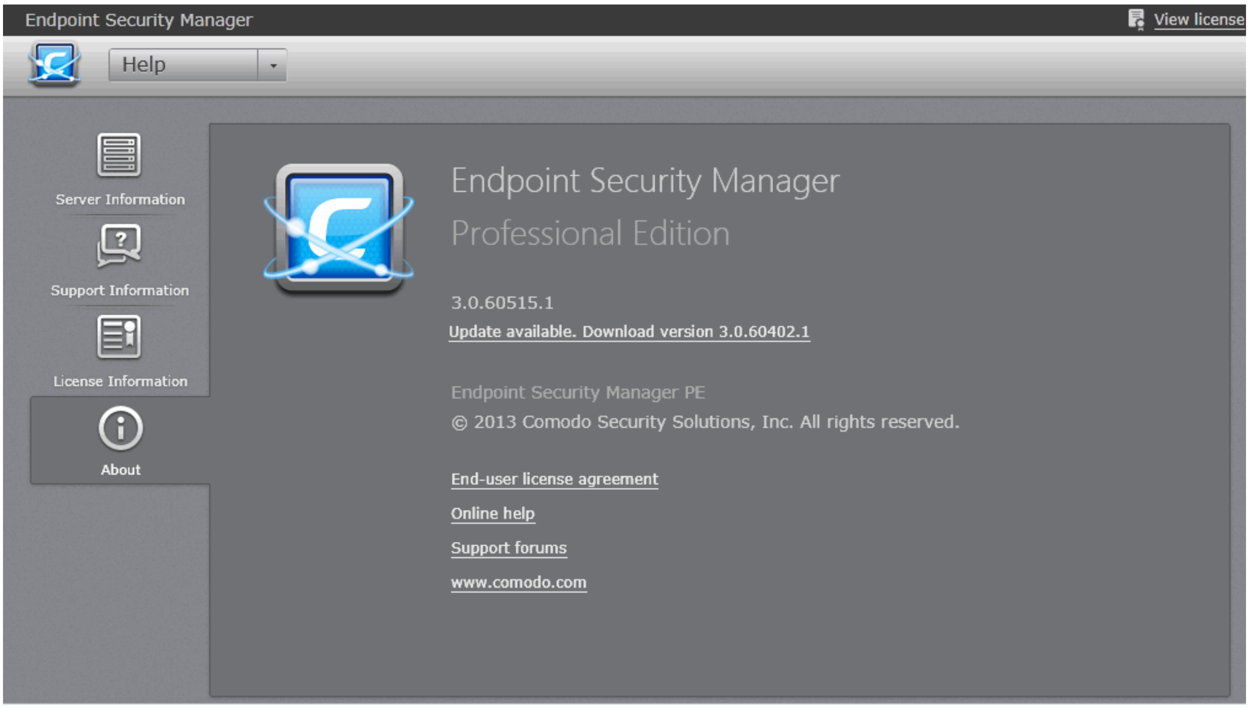
Downloading the Report

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.

10. 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.



Endpoint Security Manager

Professional Edition

3.0.60515.1

Update available. Download version 3.0.60402.1

Endpoint Security Manager PE

© 2013 Comodo Security Solutions, Inc. All rights reserved.

End-user license agreement

Online help

Support forums

www.comodo.com

- **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.

10.1. Viewing Server Information

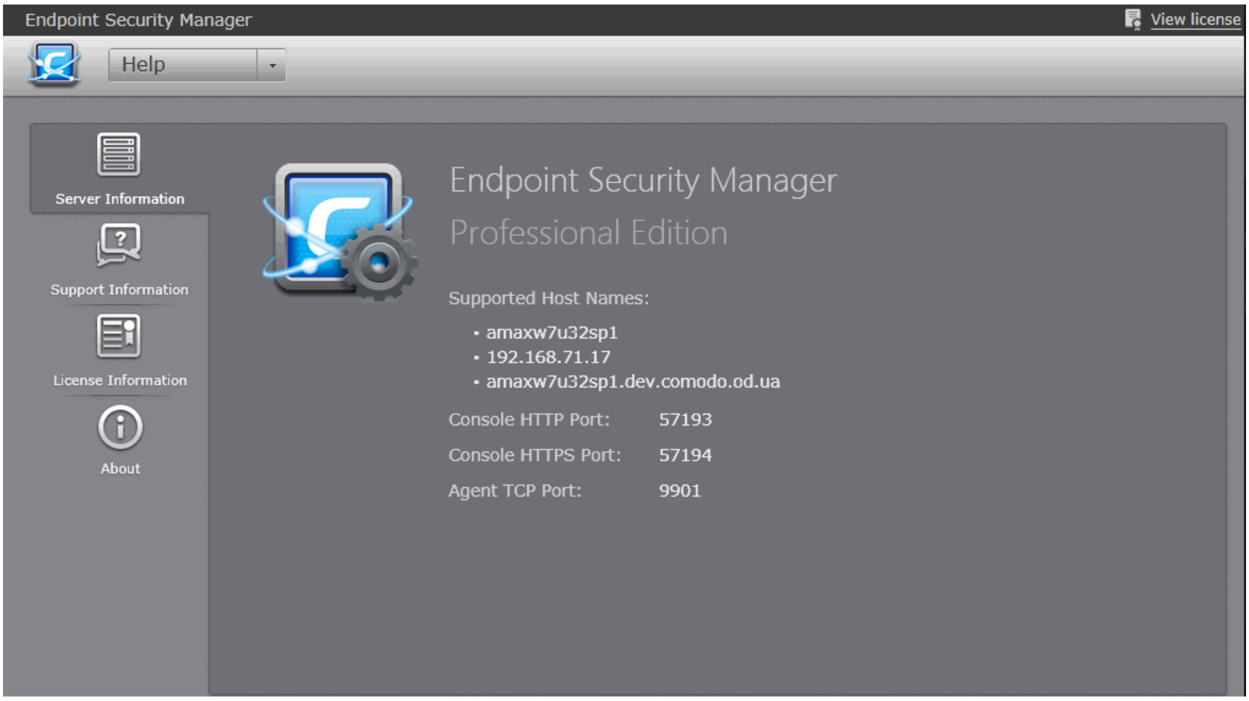
The 'Server Information' screen displays details of the server computer(s) on which CESM console is installed.

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:

- amaxw7u32sp1
- 192.168.71.17
- amaxw7u32sp1.dev.comodo.od.ua

Console HTTP Port: 57193

Console HTTPS Port: 57194

Agent TCP Port: 9901

- **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.

Refer to **Appendix 1** for more information on the configuration of the host names and connection ports of CESM service through the configuration tool.

10.2. Viewing Support Information

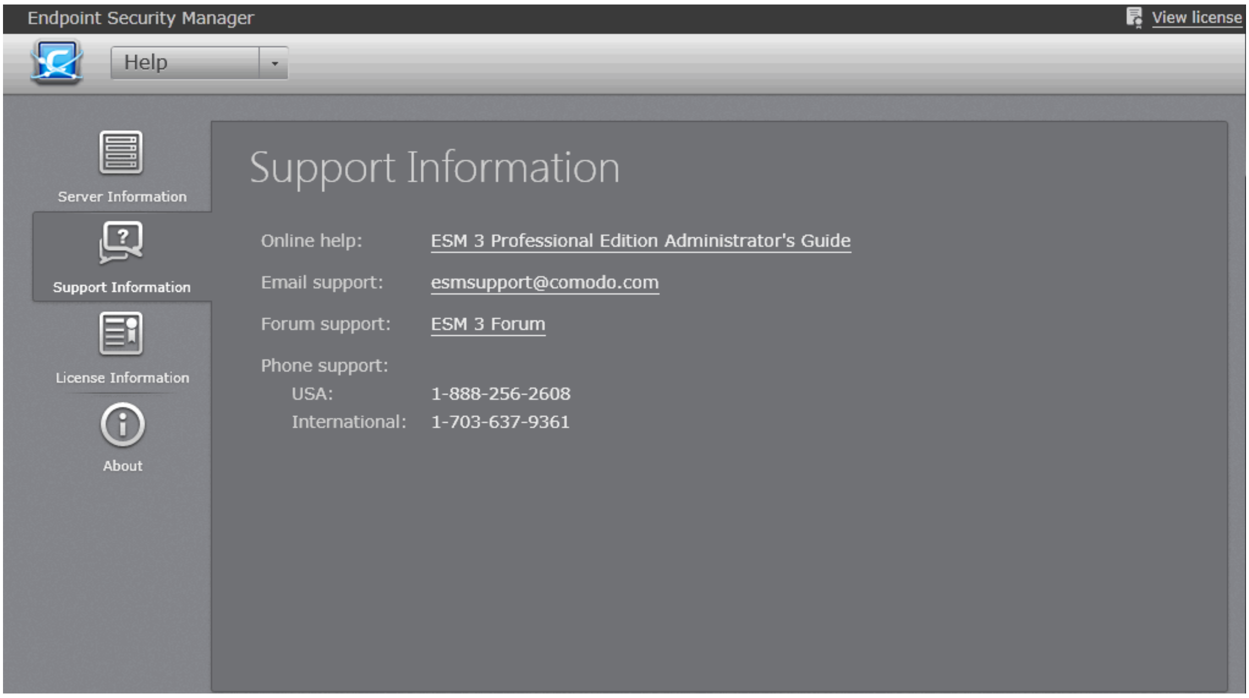
The 'Support Information' screen displays details on getting support in different ways for CESM.

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.



Support Information

Online help: ESM 3 Professional Edition Administrator's Guide

Email support: esmsupport@comodo.com

Forum support: ESM 3 Forum

Phone support:

USA: 1-888-256-2608

International: 1-703-637-9361

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.

Chat Support:

Comodo LivePCSupport is a personalized computer support service provided by friendly computer experts at Comodo, available 24/7. To get LivePCSupport, click 'LivePCSupport' link from the **License Information screen**. If you are accessing the service for the first time, the LPCS client will be downloaded and installed on your computer. A chat session will be started enabling you to explain your problem to the support technician.

After requesting your permission, they'll establish a remote connection to your computer and fix the problems right in front of your eyes.

Refer to Live PCsupport help guide at **http://help.comodo.com/topic-86-1-416-4616-Introduction-to-Comodo-GeekBuddy.html**.

10.3. Viewing License Information

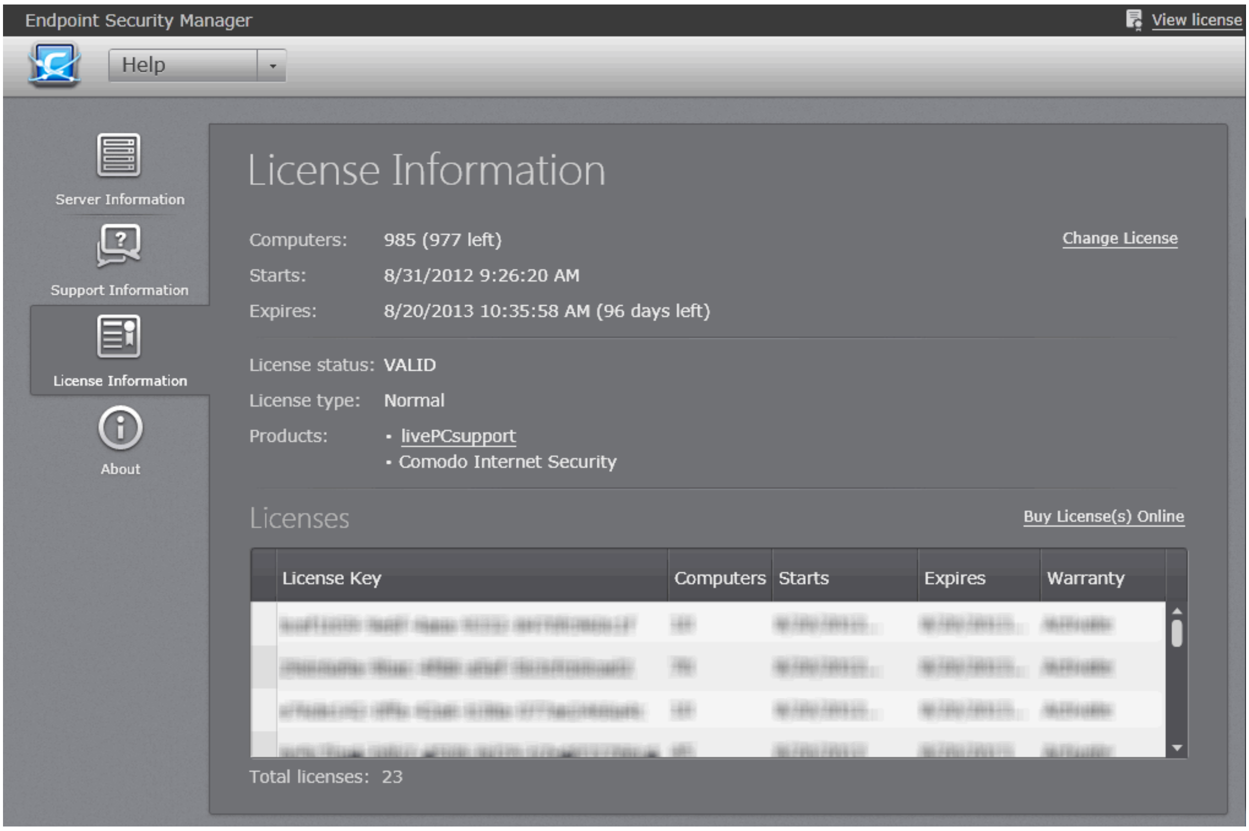
The 'License Information' screen displays details on the number of licenses purchased, their type and validity status. The 'License Information' screen also allows the administrator to purchase additional licenses, upgrade licenses, renew licenses and to get live chat support.

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.



License Information

Computers: 985 (977 left)

Starts: 8/31/2012 9:26:20 AM

Expires: 8/20/2013 10:35:58 AM (96 days left)

Change License

License status: VALID

License type: Normal

Products:
- livePCsupport
- Comodo Internet Security

Licenses

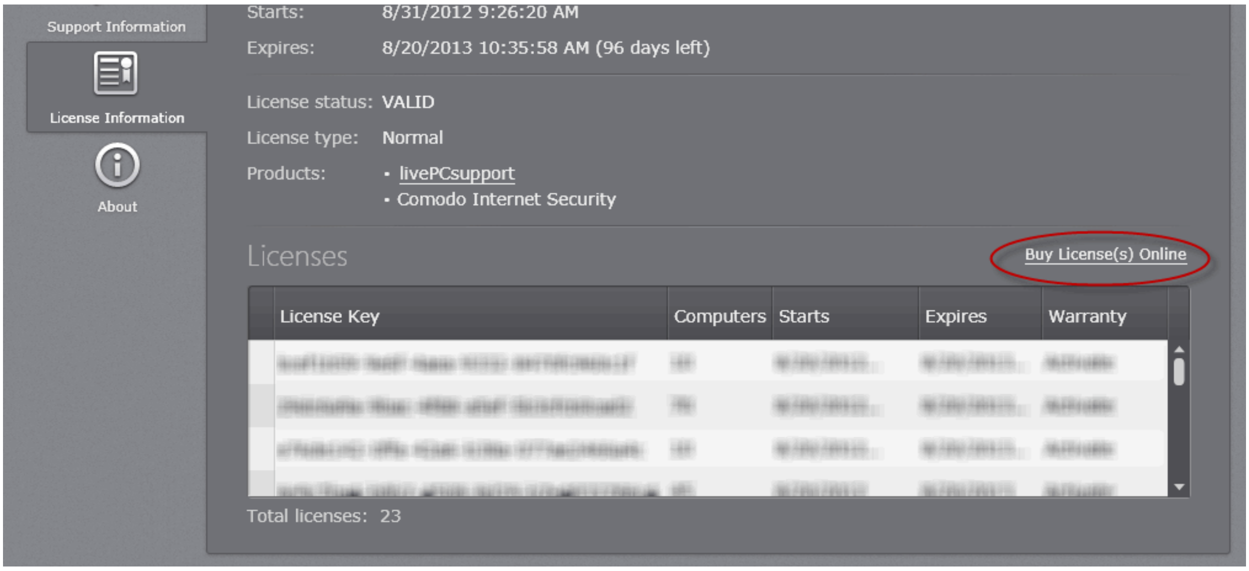
Buy License(s) Online

License Key	Computers	Starts	Expires	Warranty
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Total licenses: 23

To purchase new licenses

- Click 'Buy License(s) Online':



Starts: 8/31/2012 9:26:20 AM

Expires: 8/20/2013 10:35:58 AM (96 days left)

License status: VALID

License type: Normal

Products:
- livePCsupport
- Comodo Internet Security

Licenses

Buy License(s) Online

License Key	Computers	Starts	Expires	Warranty
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Total licenses: 23

You will be taken to the Comodo website to purchase the new licenses. After payment is complete, you will receive the license activation key through email.

10.3.1. Upgrading Your License

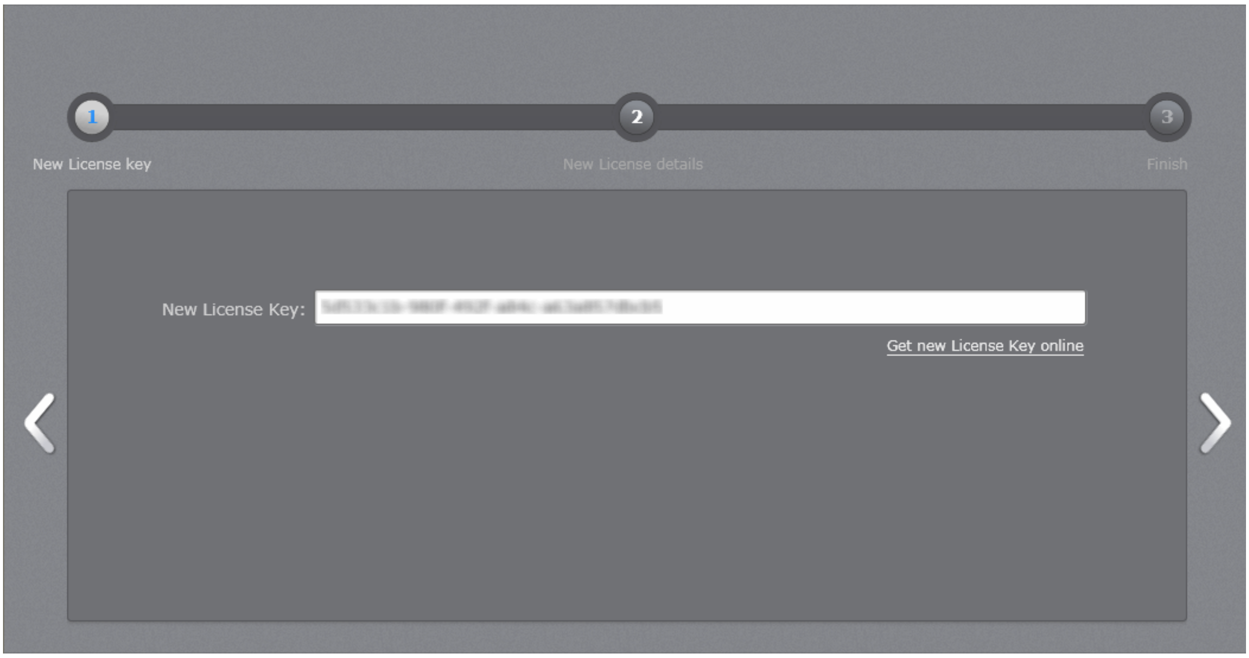
If you have purchased new licenses to add more endpoints, you need to upgrade your license by entering the new license key obtained via email.

To upgrade your license

- Click **Change License** beside 'Computers' from the 'License Information' screen.

The Change License wizard will be started.

- Enter the new license activation key you received via email.

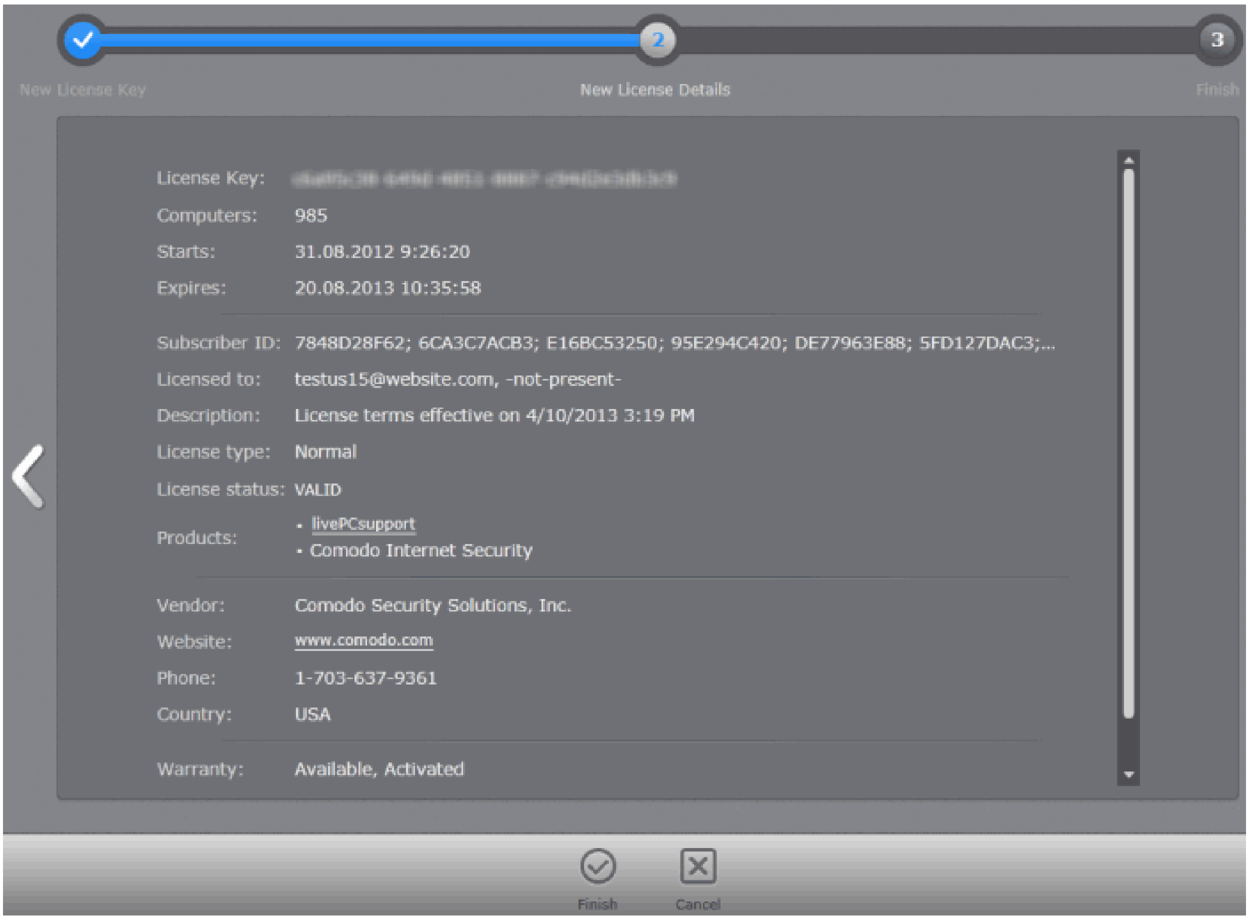


New License Key:

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.



License Key: [redacted]

Computers: 985

Starts: 31.08.2012 9:26:20

Expires: 20.08.2013 10:35:58

Subscriber ID: 7848D28F62; 6CA3C7ACB3; E16BC53250; 95E294C420; DE77963E88; 5FD127DAC3;...

Licensed to: testus15@website.com, -not-present-

Description: License terms effective on 4/10/2013 3:19 PM

License type: Normal

License status: VALID

Products:
- livePCsupport
- Comodo Internet Security

Vendor: Comodo Security Solutions, Inc.

Website: www.comodo.com

Phone: 1-703-637-9361

Country: USA

Warranty: Available, Activated

- Click 'Finish' to exit the wizard. Your license will be upgraded.

10.4. Viewing the About Screen

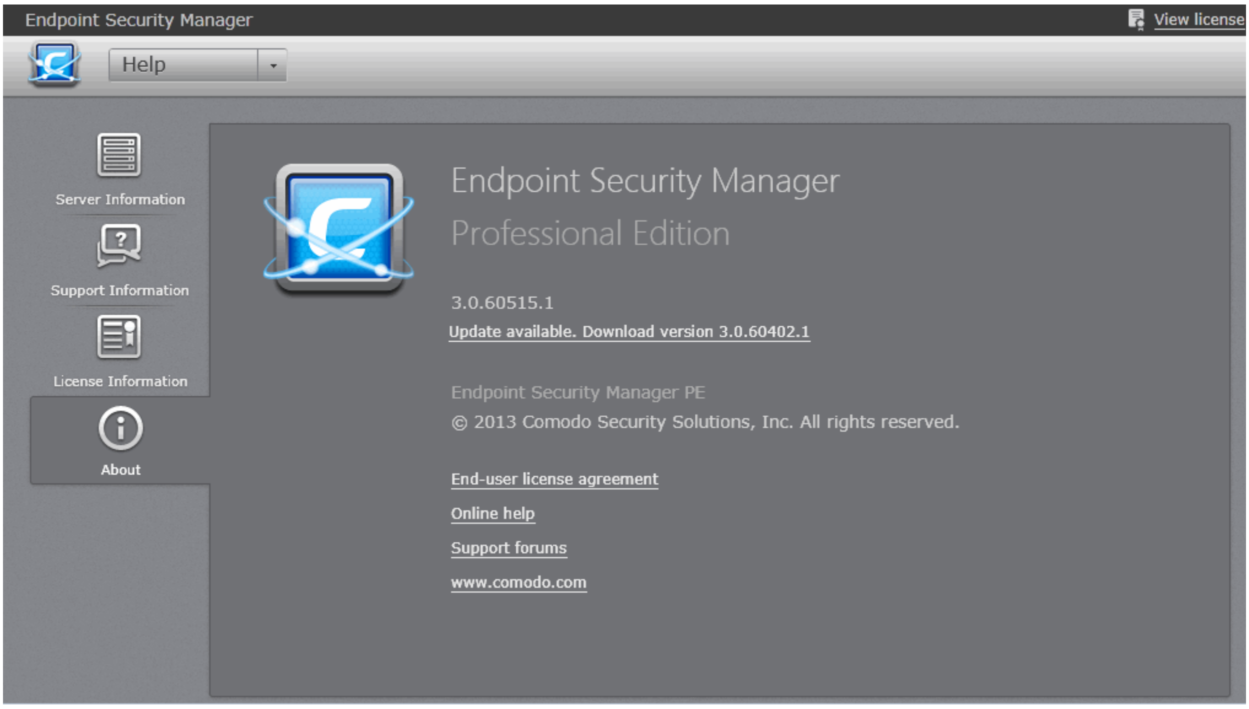
- The 'About' screen displays the version information of CESM currently installed on your server and copyright information. The screen also informs you if an updated version is available and, if so, enables you to download and install it. The screen contains links to get support on CESM from the online 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.



Endpoint Security Manager
Professional Edition

3.0.60515.1
Update available. Download version 3.0.60402.1

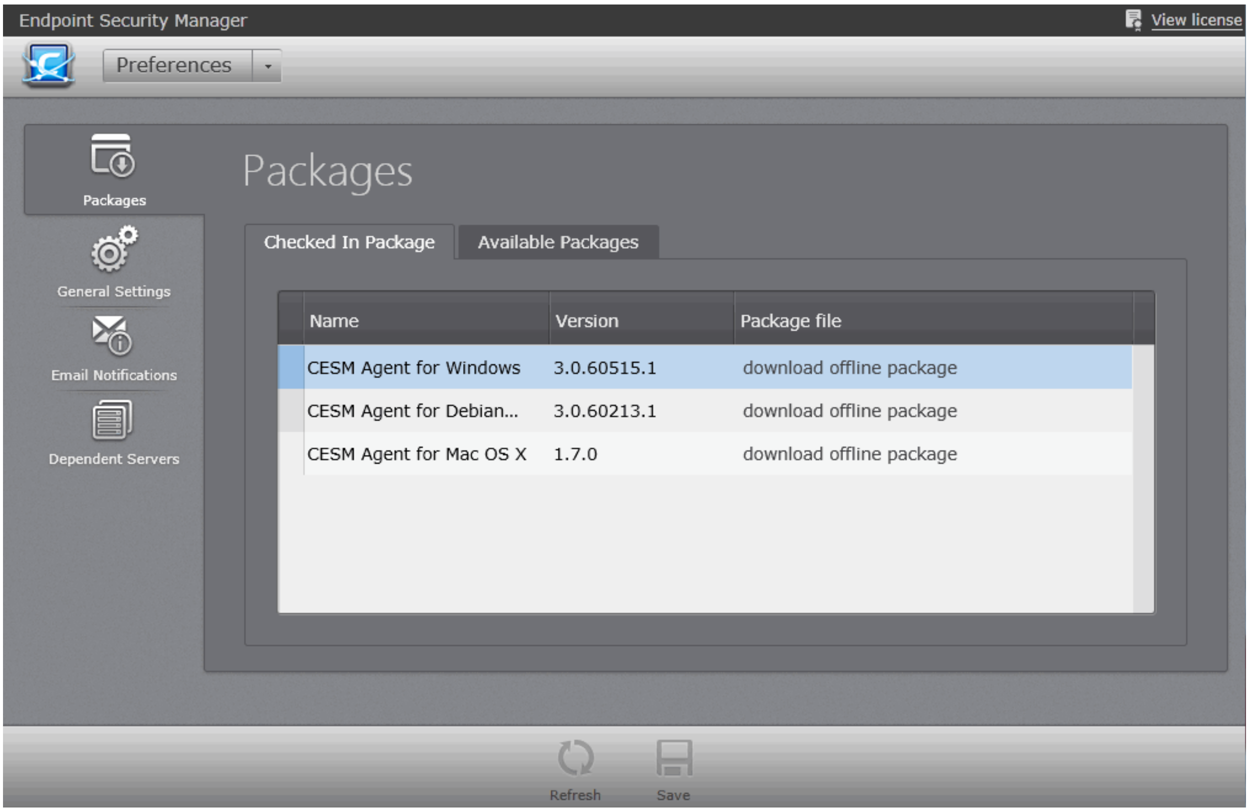
Endpoint Security Manager PE
© 2013 Comodo Security Solutions, Inc. All rights reserved.

End-user license agreement
Online help
Support forums
www.comodo.com

- Clicking **Update available. Download version** 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.

11. Viewing and Managing Preferences

The 'Preferences' area 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.



Name	Version	Package file
CESM Agent for Windows	3.0.60515.1	download offline package
CESM Agent for Debian...	3.0.60213.1	download offline package
CESM Agent for Mac OS X	1.7.0	download offline package

- **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.
- **General Settings** - Enables administrators to configure lifetime of archived reports. Refer to **Configuring General Settings** 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.

11.1. 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.

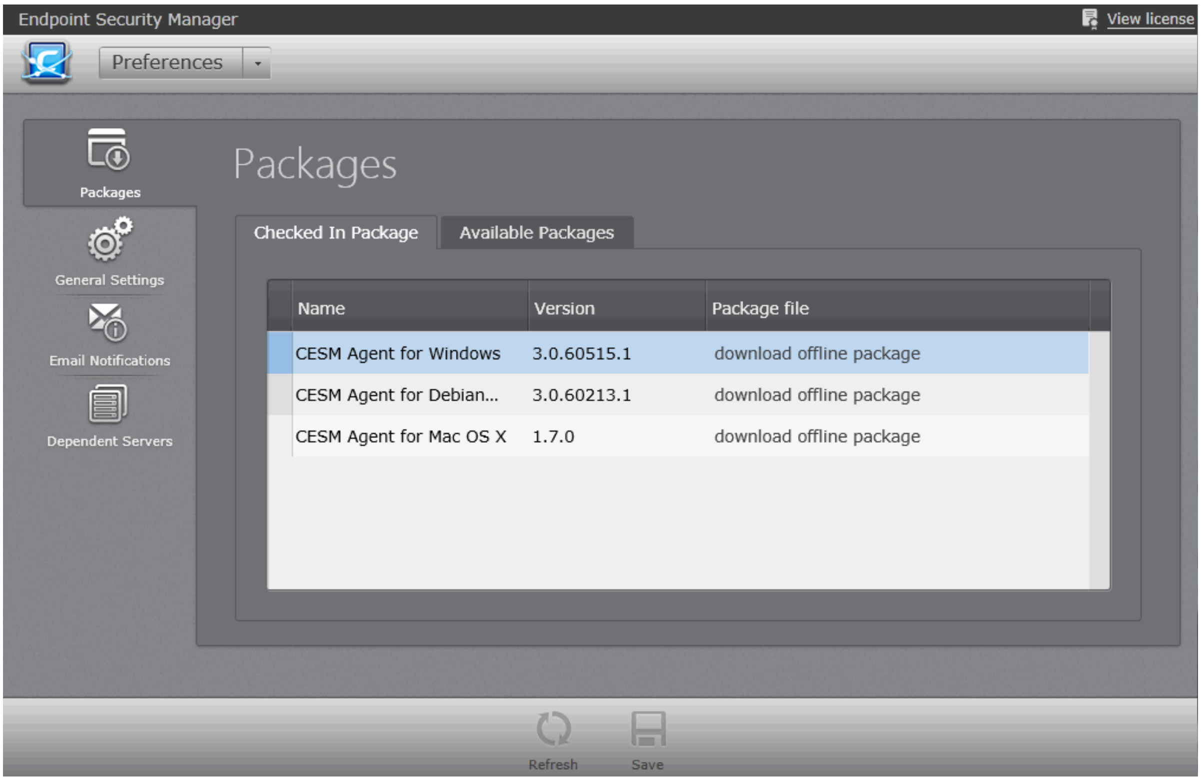
The Administrator can download CESM Agent setup for different Operating Systems from the 'Preferences' > Packages screen.

To access the Agent Packages screen

- Click 'Preferences' > 'Packages' area from the drop-down at the top left.

The interface contains two areas:

- Changed In Package displays the all downloaded and registered packages in the system.
- Available Packages tab displays all available packages for downloading, allows administrator to check for updates and download them.



Name	Version	Package file
CESM Agent for Windows	3.0.60515.1	download offline package
CESM Agent for Debian...	3.0.60213.1	download offline package
CESM Agent for Mac OS X	1.7.0	download offline package

- To download CESM agent setup file for Windows as .exe file, select the package file and click **download offline package.**
- To download CESM agent setup file for Linux as .deb file, **select the package file and click download offline package.**
- To download CESM agent setup file for Mac OS as .dmg file, **select the package file and click download offline package.**

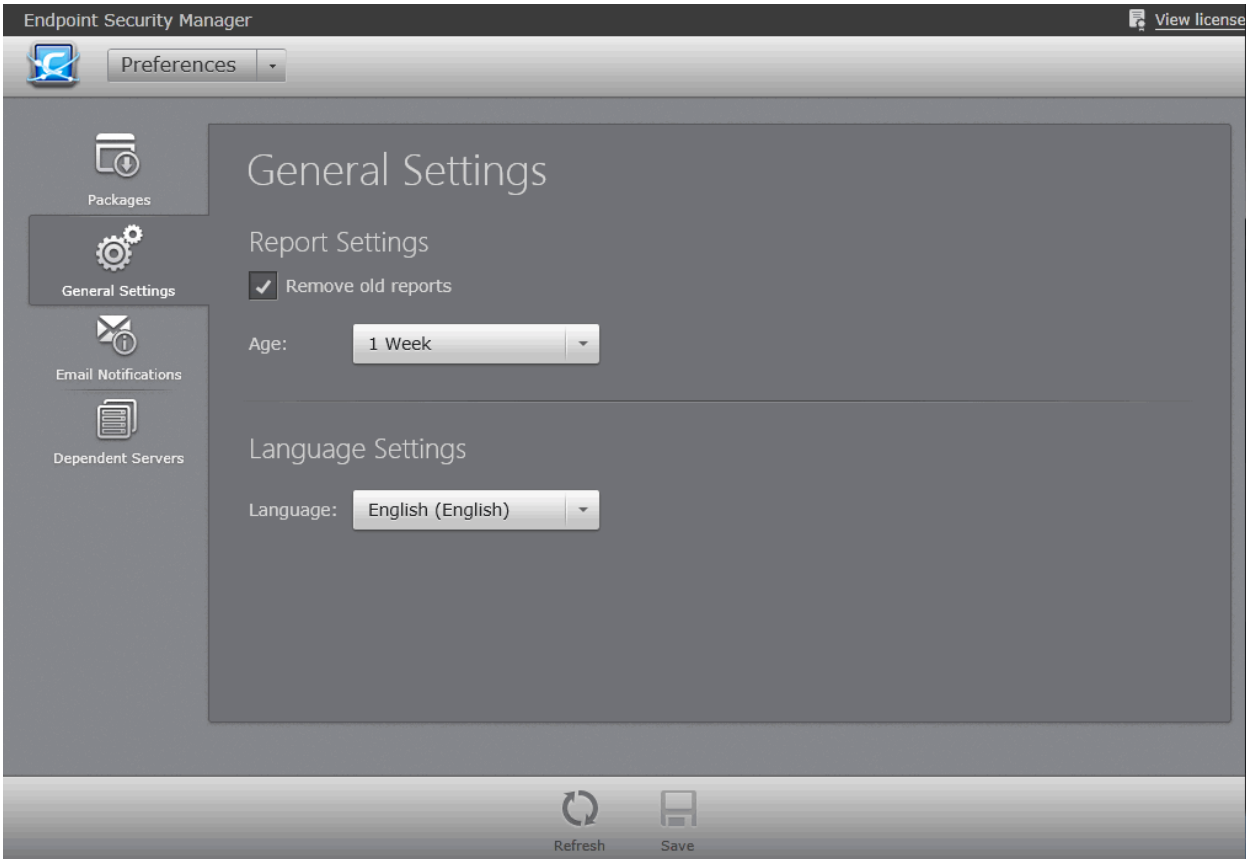
Refer to **Adding Computers by Manual Installation of Agent** for more details on installing the agent on to target endpoints.

11.2. Configuring General Settings

The 'Report Settings' screen allows administrators to configure the length of time that reports should be stored on the CESM server and the language of the report.

To access the Report Settings screen

- Click 'Preferences' > 'General Settings' area from the drop-down at the top left.



General Settings

Report Settings

☑ Remove old reports

Age: 1 Week

Language Settings

Language: English (English)

- 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

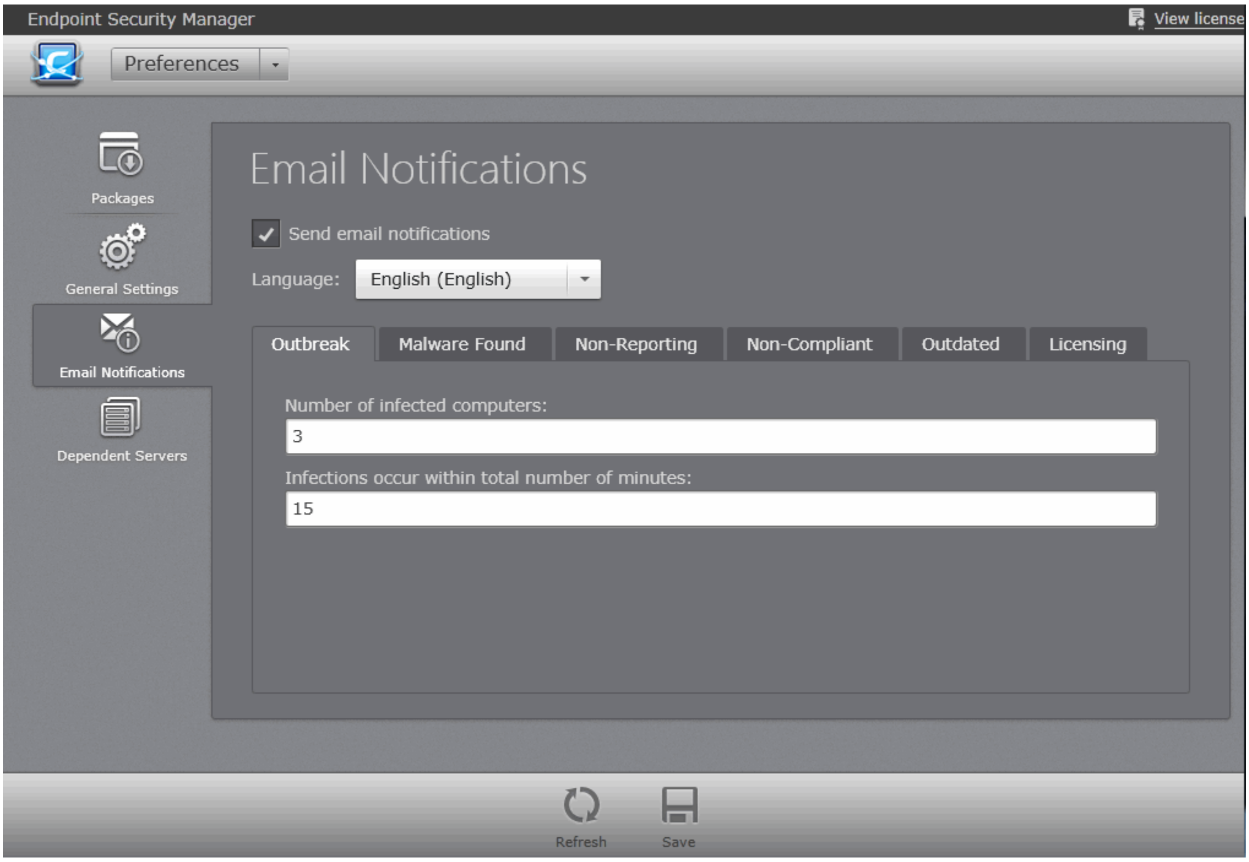
11.3. Managing Email Notifications

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.

Important Note: In order to send automated emails, the STMP server settings and email addresses are to be configured under the 'Internet and Mail Settings' tab in the CESM Configuration Tool. The server will have to be restarted for the configuration to take effect. Refer to the section **Internet and Mail Settings** in **Appendix 1 -The Service Configuration Tool** for more details.

To access the Email Notifications screen

- Click 'Preferences' > 'Email Notifications' area from the drop-down at the top left.



Email Notifications

☑ Send email notifications

Language: English (English)

Outbreak | Malware Found | Non-Reporting | Non-Compliant | Outdated | Licensing

Number of infected computers: 3

Infections occur within total number of minutes: 15

- To enable automated email notifications select the 'Send email Notifications' check box.
- Configure the email notification parameters 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** - A notification will be sent when the number of endpoints infected by malware equals to or exceeds this Value. *Default = 1.* **Infections occur within total 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** - A notification will be sent 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.* **Minutes idle** - Specify the period of time that CESM should wait after the endpoint first fails to report before sending the notification. *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 computers** - Specify the number of non-compliant endpoints before CESM will send a notification email. *Default = 1*
Outdated	Send a notification mail when the	**Number of AV outdated** - CESM will send an notification

	number of endpoints using an outdated virus database reaches a set threshold.	email when it detects this number of endpoints are using outdated databases. *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*.

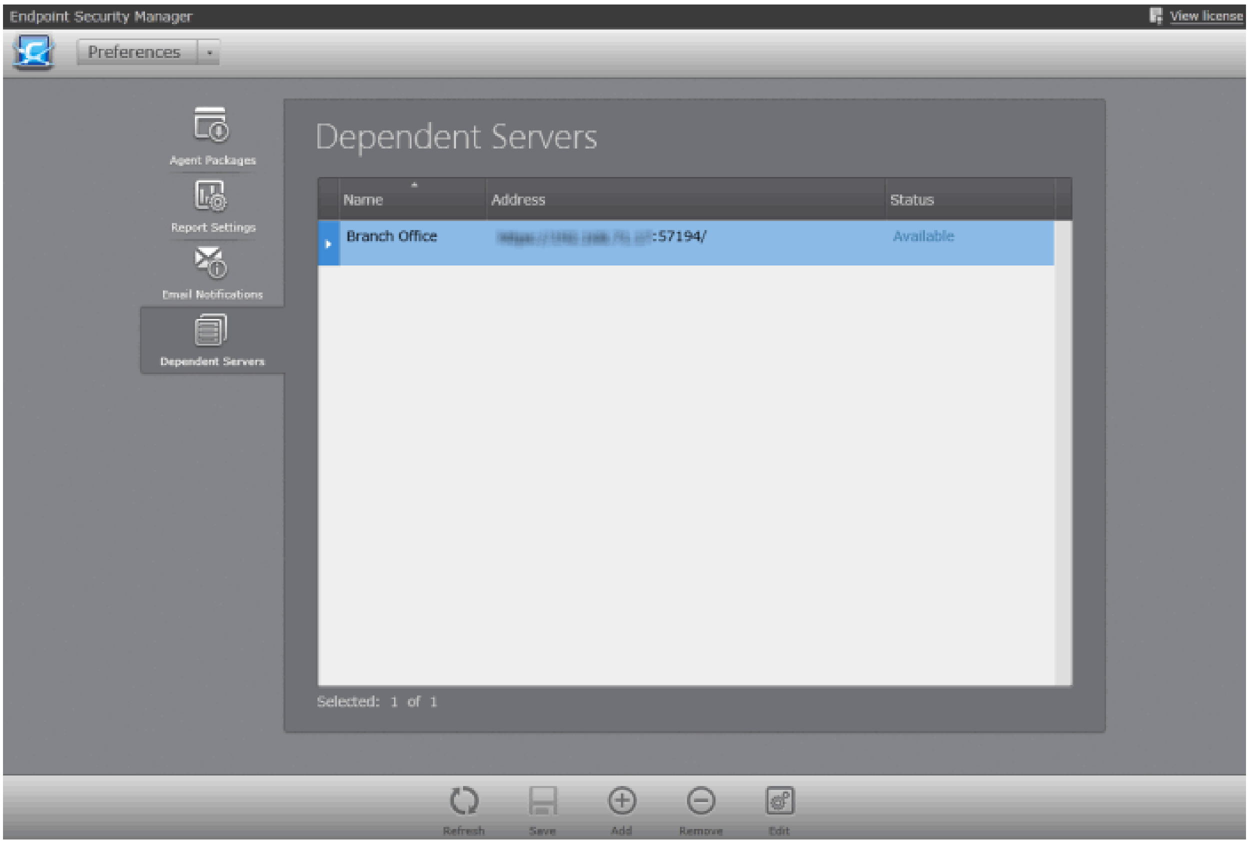
11.4. Viewing and Managing Dependent Servers

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.



Dependent Servers

Name	Address	Status
Branch Office	[redacted]:57194/	Available

Selected: 1 of 1

From here, administrators can add, edit and remove dependent servers.

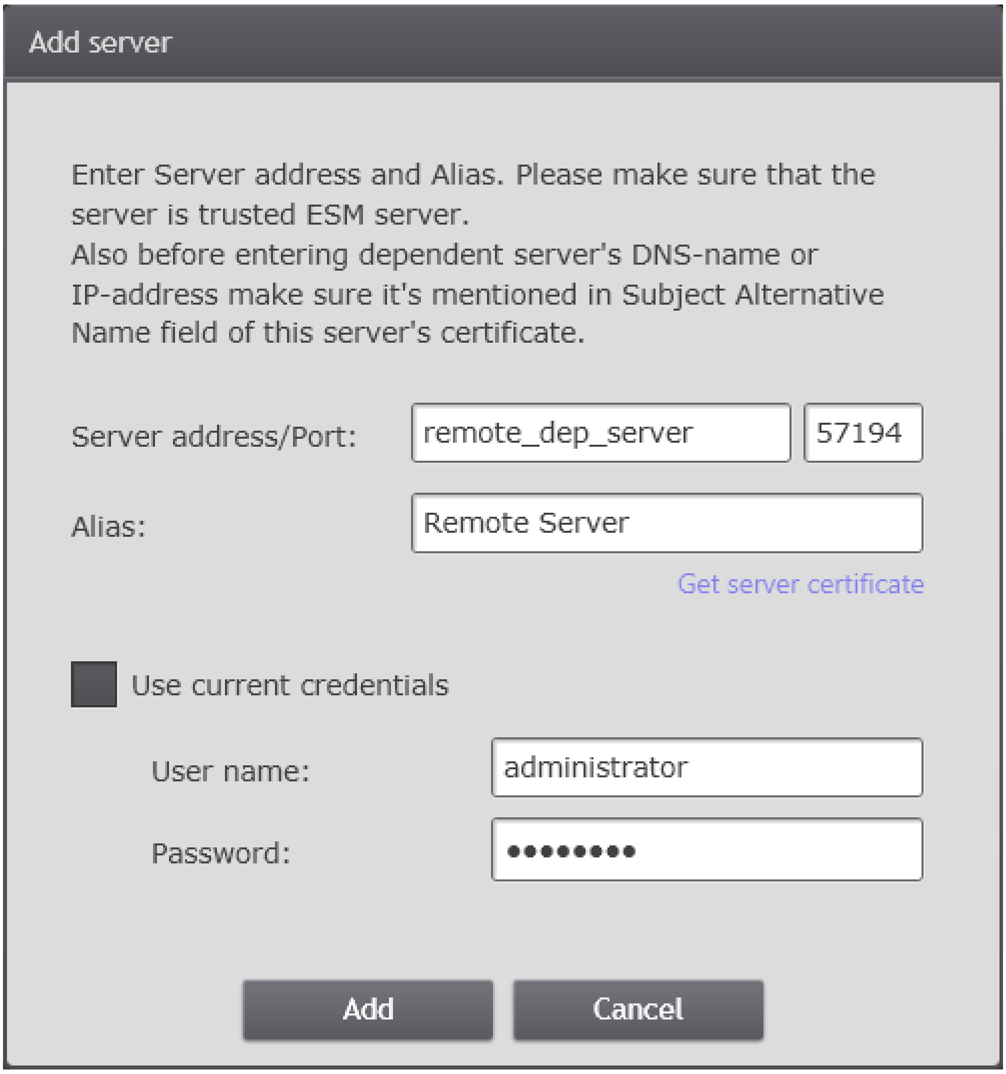
11.4.1. Adding a Dependent Server

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

Enter Server address and Alias. Please make sure that the server is trusted ESM server.
Also before entering dependent server's DNS-name or IP-address make sure it's mentioned in Subject Alternative Name field of this server's certificate.

Server address/Port: remote_dep_server 57194

Alias: Remote Server

□ Use current credentials

User name: administrator

Password: ●●●●●●●●●

Reminder: The server certificate of the central CESM server needs to be installed in the remote server. If not installed previously, click 'Get server certificate' in the dialog shown above and install It on the remote server.

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.
Current User Credentials (Selected by default)	Selecting this option will add the server using the credentials of the current CESM administrator. Deselecting this box will allow you specify an alternative administrative account on the remote server.

After clicking 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.

11.4.2. 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, 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.

11.4.3. 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**.

11.4.4. 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.

The Applications area - View all applications installed on endpoints connected to remote CESM sever and uninstall unwanted applications.

Refer to **The 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.

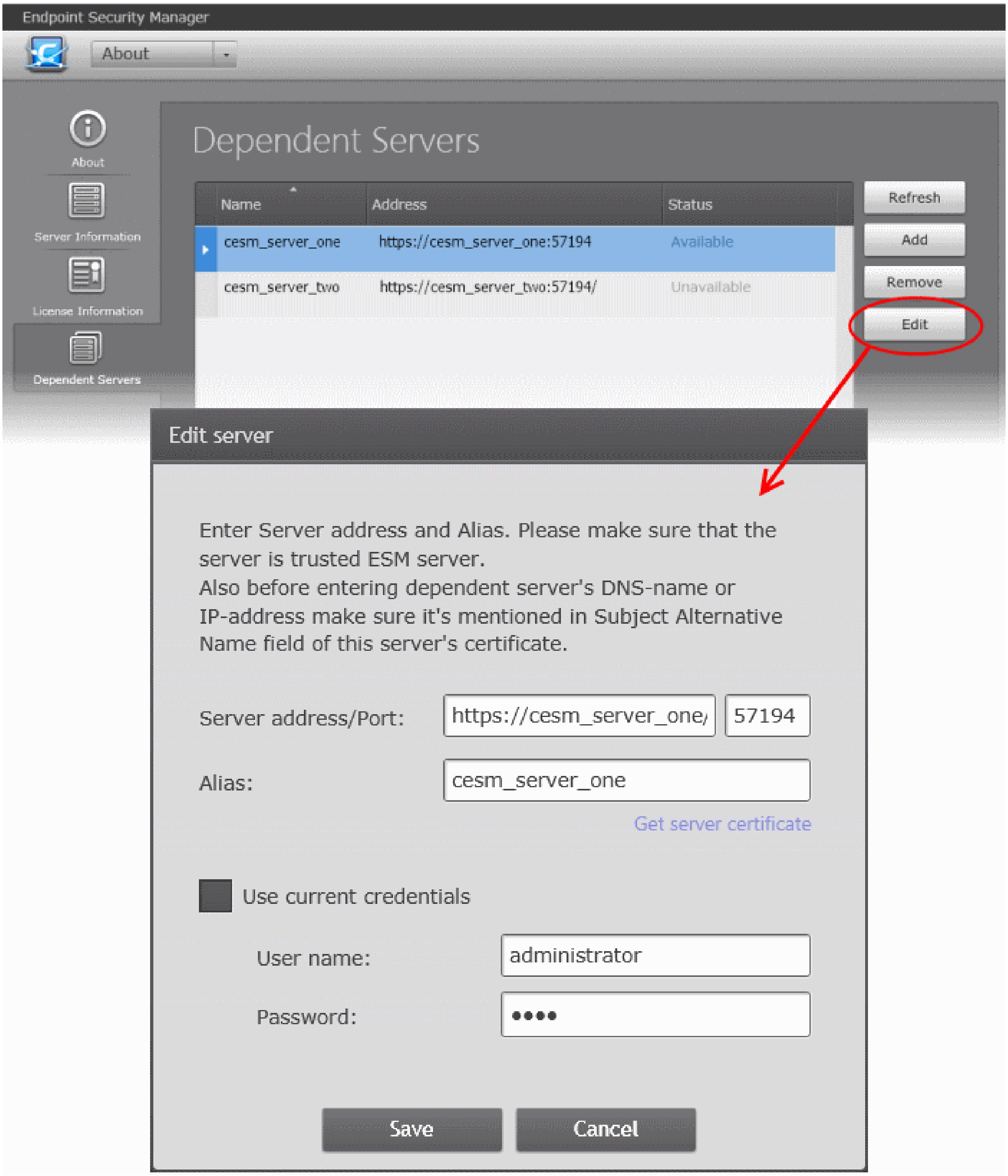
11.4.5. Editing Dependent Servers

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' button, alternatively double click on the dependent server 'Name' or 'Status'.

The 'Edit Server' dialog will open.



Name	Address	Status
cesm_server_one	https://cesm_server_one:57194	Available
cesm_server_two	https://cesm_server_two:57194/	Unavailable

Edit server

Enter Server address and Alias. Please make sure that the server is trusted ESM server.
Also before entering dependent server's DNS-name or IP-address make sure it's mentioned in Subject Alternative Name field of this server's certificate.

Server address/Port: https://cesm_server_one/ 57194

Alias: cesm_server_one

Get server certificate

□ Use current credentials

User name: administrator

Password: ●●●●

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 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. Leaving this option unselected 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 dedicated network administrator. Password: Enter the password of the dedicated network administrator.

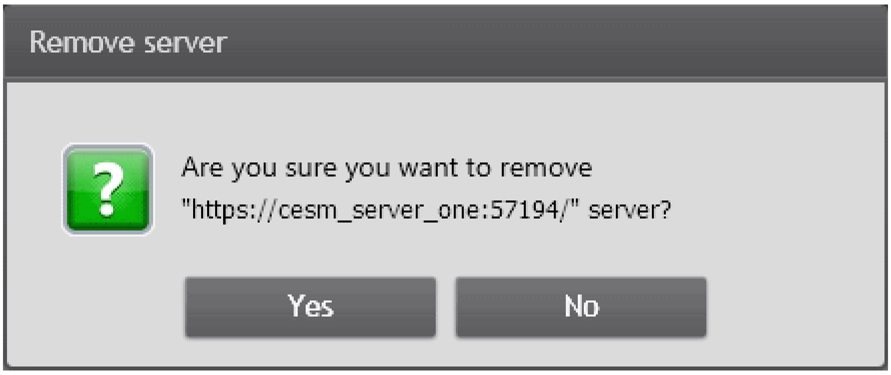
- Click 'Save' for your changes to take effect.

11.4.6. 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.



Remove server

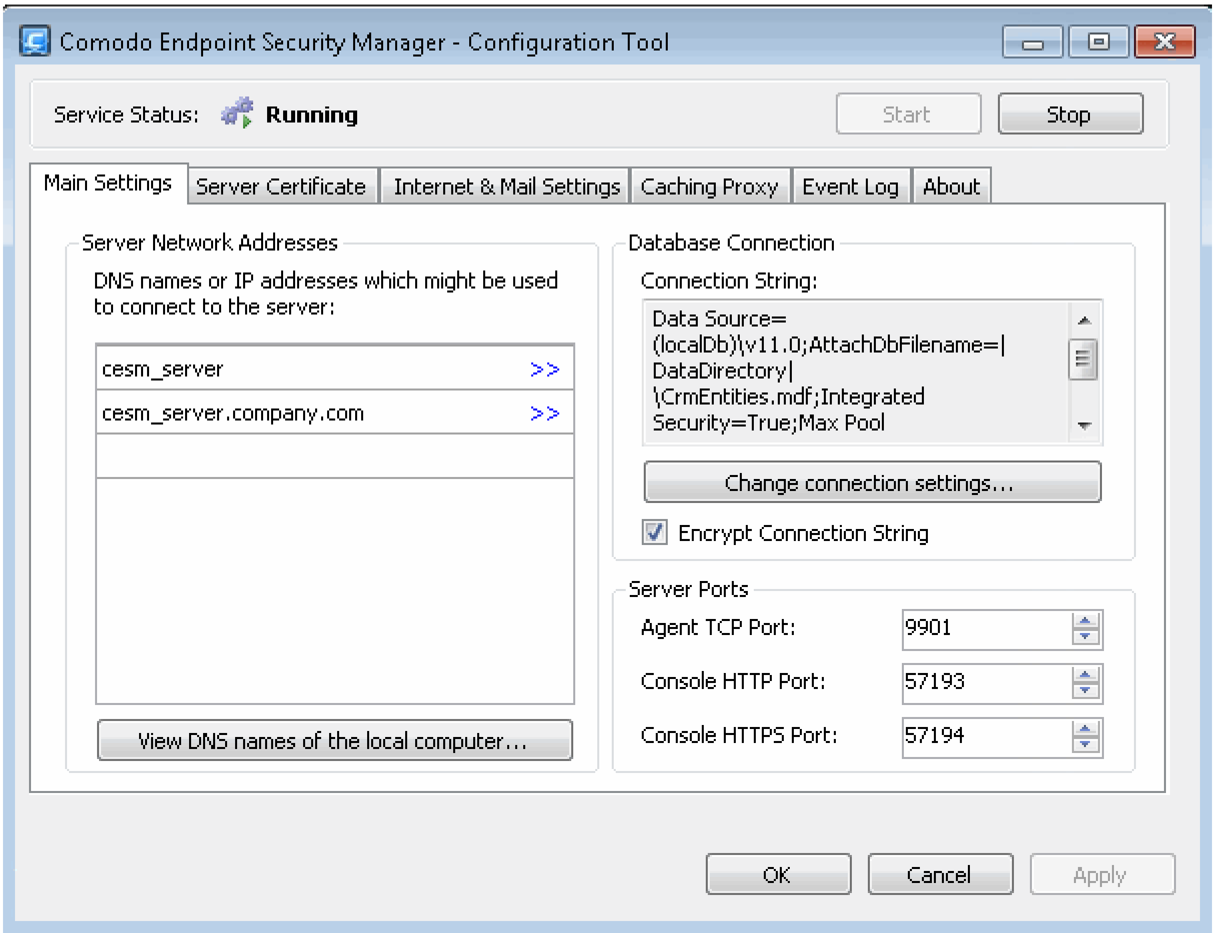
Are you sure you want to remove "https://cesm_server_one:57194/" server?

- Click 'Yes'.

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 in the CESM server and can be accessed from the Windows Start Menu.



Comodo Endpoint Security Manager - Configuration Tool

Service Status: **Running**

Server Network Addresses

DNS names or IP addresses which might be used to connect to the server:

cesm_server >>
cesm_server.company.com >>

Database Connection

Connection String:

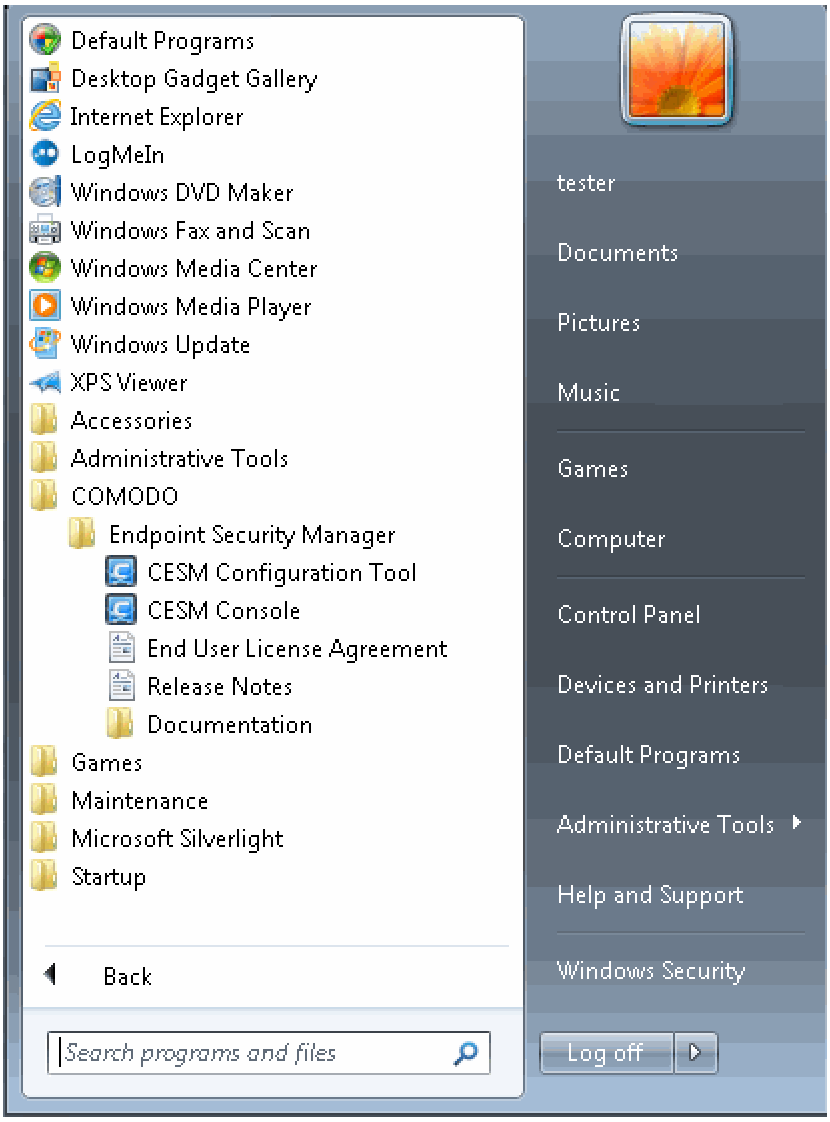
Data Source=(localDb)\v11.0;AttachDbFilename=|DataDirectory|\CrmEntities.mdf;Integrated Security=True;Max Pool

☑ Encrypt Connection String

Server Ports

Agent TCP Port: 9901
Console HTTP Port: 57193
Console HTTPS Port: 57194

To open the Service Configuration Tool, Click Start > All Programs > COMODO > Endpoint Security Manager > CESM Configuration Tool.

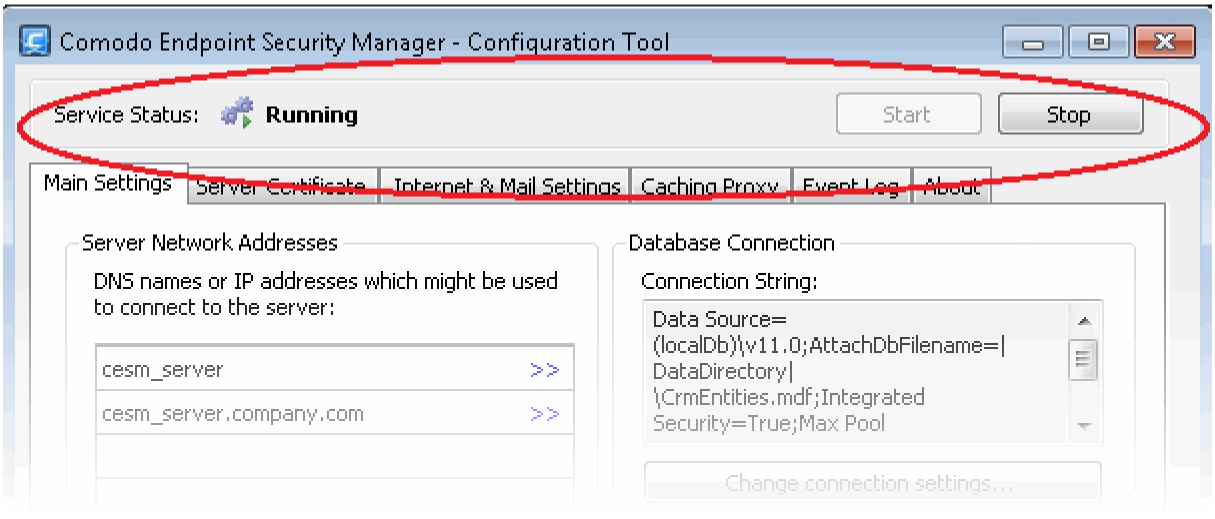


The main interface of the tool will be opened. It contains four areas:

- 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 and Mail Settings - Enables the administrator to view and modify proxy server and outgoing mail settings.
- Caching Proxy Settings - Enables administrators to manage access to resources.
- Event Log - Enables the administrator to view the log of database events.
- About - Indicates the current service ESM version.

Start and Stop the ESM Service

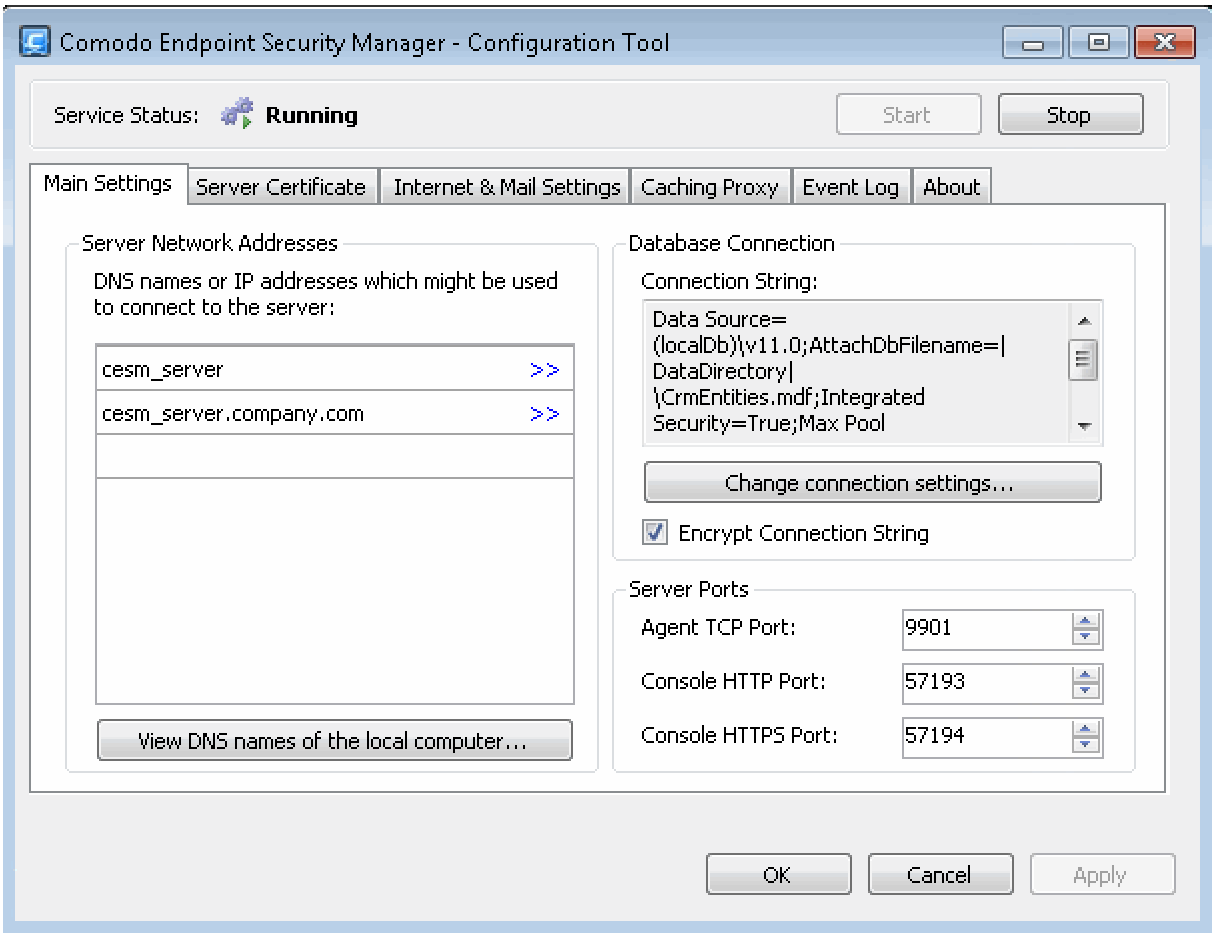
The Service Status area at the top of the interface displays the current running status of the ESM Service as 'Running' or 'Stopped'.


Comodo Endpoint Security Manager - Configuration Tool
Service Status: Running
Start
Stop
Main Settings
Server Certificate
Internet & Mail Settings
Caching Proxy
Event Log
About
Server Network Addresses
DNS names or IP addresses which might be used to connect to the server:
cesm_server >>
cesm_server.company.com >>
Database Connection
Connection String:
Data Source=(localDb)\v11.0;AttachDbFilename=|DataDirectory|\CrmEntities.mdf;Integrated Security=True;Max Pool
Change connection settings...

- To stop the running service, simply click the 'Stop' button.
- To start the service, simply click the 'Start' button.

Main Settings

The Main Settings page displays the ESM server IP addresses and/or hostnames in the 'Server Network Addresses' field and Database connection settings, Console Port, Secure Console Port and Agent Ports at the right.


Comodo Endpoint Security Manager - Configuration Tool
Service Status: Running
Start
Stop
Main Settings
Server Certificate
Internet & Mail Settings
Caching Proxy
Event Log
About
Server Network Addresses
DNS names or IP addresses which might be used to connect to the server:
View DNS names of the local computer...
Database Connection
Change connection settings...
Server Ports
OK
Cancel
Apply

cesm_server >>
cesm_server.company.com >>

Connection String:
Data Source=(localDb)\v11.0;AttachDbFilename=|DataDirectory|\CrmEntities.mdf;Integrated Security=True;Max Pool

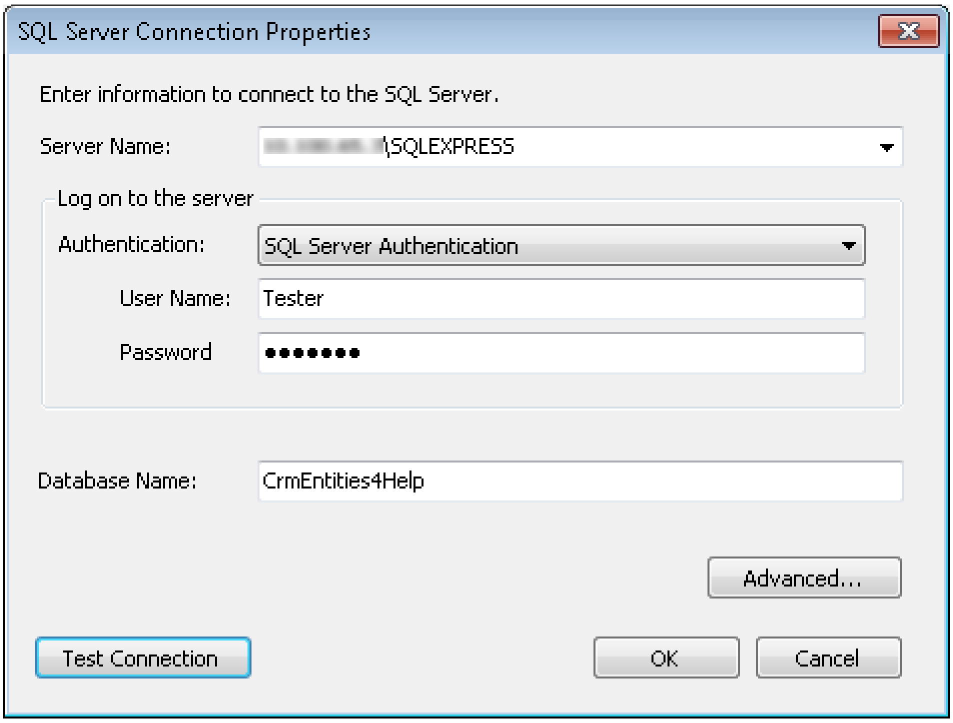
☑ Encrypt Connection String

Agent TCP Port: 9901
Console HTTP Port: 57193
Console HTTPS Port: 57194

- To add an IP or Hostname, simply begin typing in the blank row beneath those already listed. Click 'OK' to confirm.
- To change port numbers, simply type the new port number in the appropriate field.

- 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.



SQL Server Connection Properties

Enter information to connect to the SQL Server.

Server Name: [redacted]\SQLEXPRESS

Log on to the server

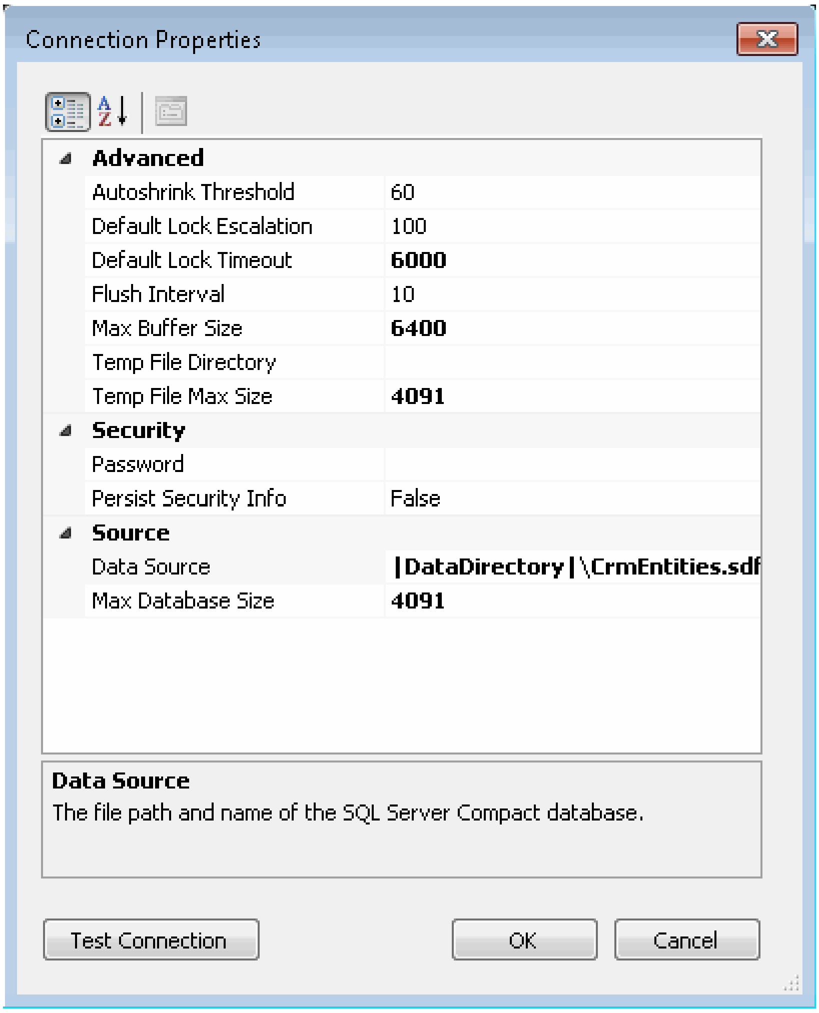
Authentication: SQL Server Authentication

User Name: Tester

Password ●●●●●●●

Database Name: CrmEntities4Help

- You can configure the SQL server connection settings from this dialog. For configuring advanced connection properties, click the 'Advanced' button.



Advanced	
Autoshrink Threshold	60
Default Lock Escalation	100
Default Lock Timeout	**6000**
Flush Interval	10
Max Buffer Size	**6400**
Temp File Directory	
Temp File Max Size	**4091**
Security	
Password	
Persist Security Info	False
Source	
Data Source	**|DataDirectory|\CrmEntities.sdf**
Max Database Size	**4091**

Data Source

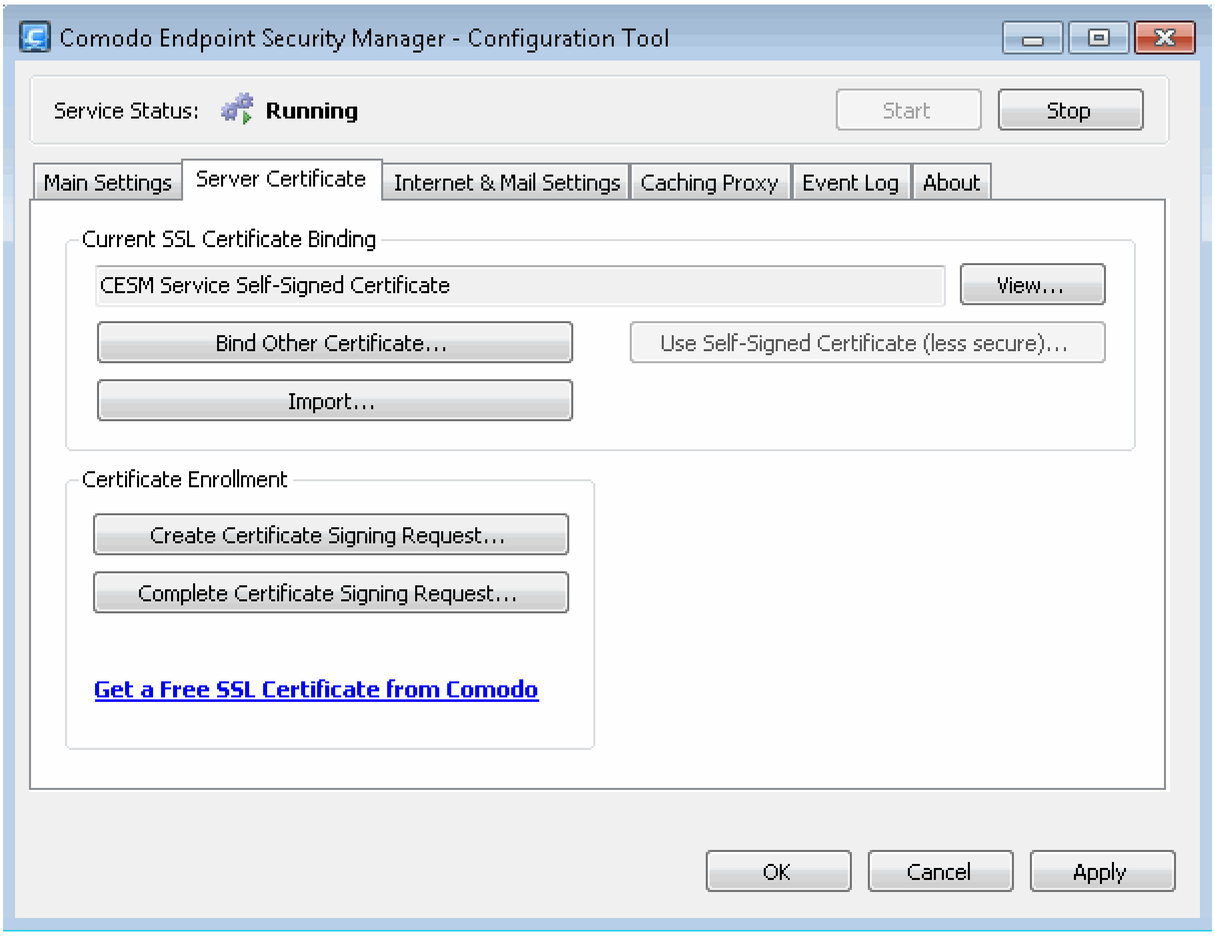
The file path and name of the SQL Server Compact database.

- 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 manage server certificate such as to view the details of current certificate installed on the server, import new certificate, create certificate signing request and install new SSL certificate.



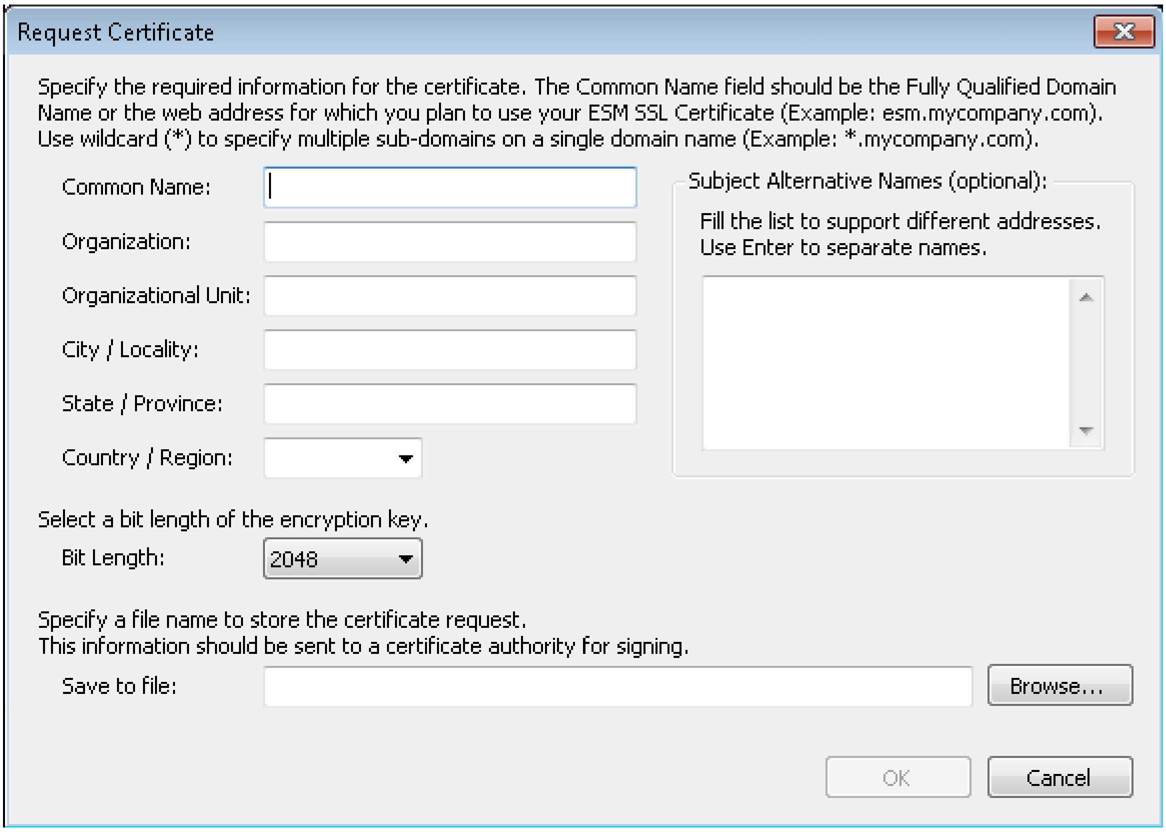
Comodo Endpoint Security Manager - Configuration Tool
Service Status: Running
Start
Stop
Main Settings
Server Certificate
Internet & Mail Settings
Caching Proxy
Event Log
About
Current SSL Certificate Binding
CESM Service Self-Signed Certificate
View...
Bind Other Certificate...
Use Self-Signed Certificate (less secure)...
Import...
Certificate Enrollment
Create Certificate Signing Request...
Complete Certificate Signing Request...
Get a Free SSL Certificate from Comodo
OK
Cancel
Apply

- 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.



Request Certificate

Specify the required information for the certificate. The Common Name field should be the Fully Qualified Domain Name or the web address for which you plan to use your ESM SSL Certificate (Example: esm.mycompany.com). Use wildcard (*) to specify multiple sub-domains on a single domain name (Example: *.mycompany.com).

Common Name:

Organization:

Organizational Unit:

City / Locality:

State / Province:

Country / Region:

Subject Alternative Names (optional):

Fill the list to support different addresses. Use Enter to separate names.

Select a bit length of the encryption key.

Bit Length: 2048

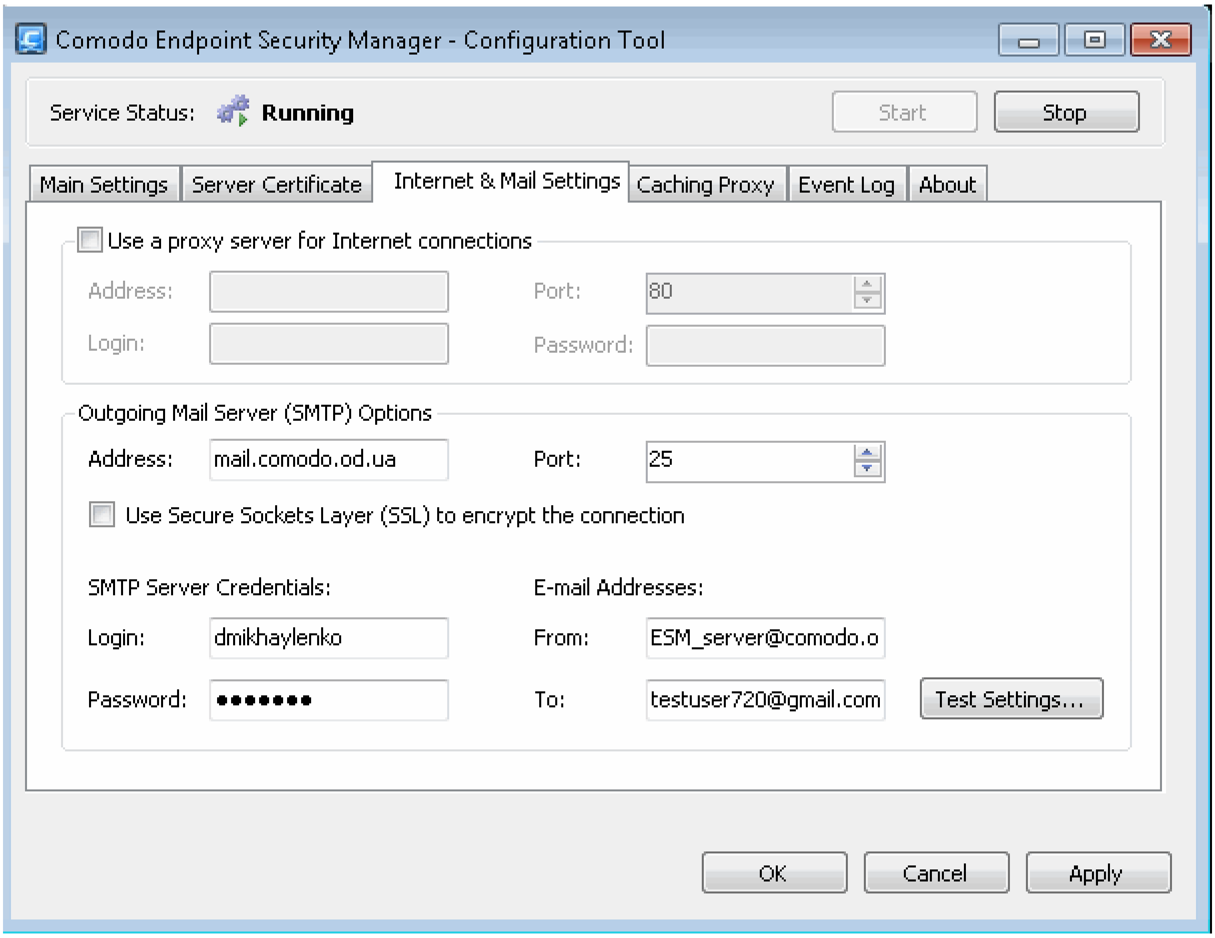
Specify a file name to store the certificate request. This information should be sent to a certificate authority for signing.

Save to file:

- 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 and Mail Settings

The Internet and Mail Settings tab allows administrators to specify mail settings for receiving alerts from ESM and to specify any Internet proxy connection settings.



Service Status: Running

□ Use a proxy server for Internet connections

Address:

Port: 80

Login:

Password:

Outgoing Mail Server (SMTP) Options

Address: mail.comodo.od.ua

Port: 25

□ Use Secure Sockets Layer (SSL) to encrypt the connection

SMTP Server Credentials:

Login: dmikhaylenko

Password: ●●●●●●●●

E-mail Addresses:

From: ESM_server@comodo.o

To: testuser720@gmail.com

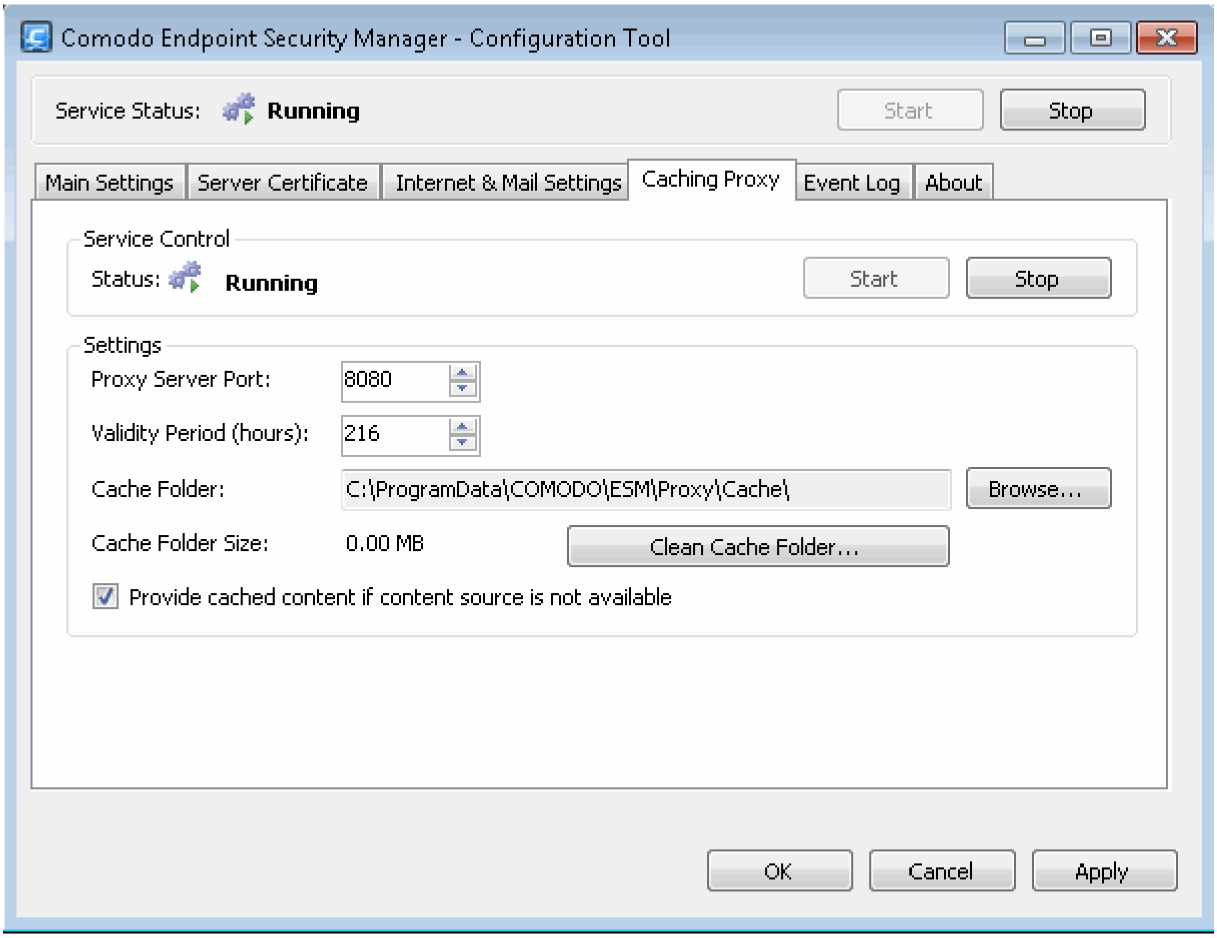
The email alerts will appear to come from ESM Server by default if the 'From' field contains a simple email address. Your personal mail configuration may be useful in completing the mail server section.

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...

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.



Service Status: Running

Service Control

Status: Running

Settings

Proxy Server Port: 8080

Validity Period (hours): 216

Cache Folder: C:\ProgramData\COMODO\ESM\Proxy\Cache\

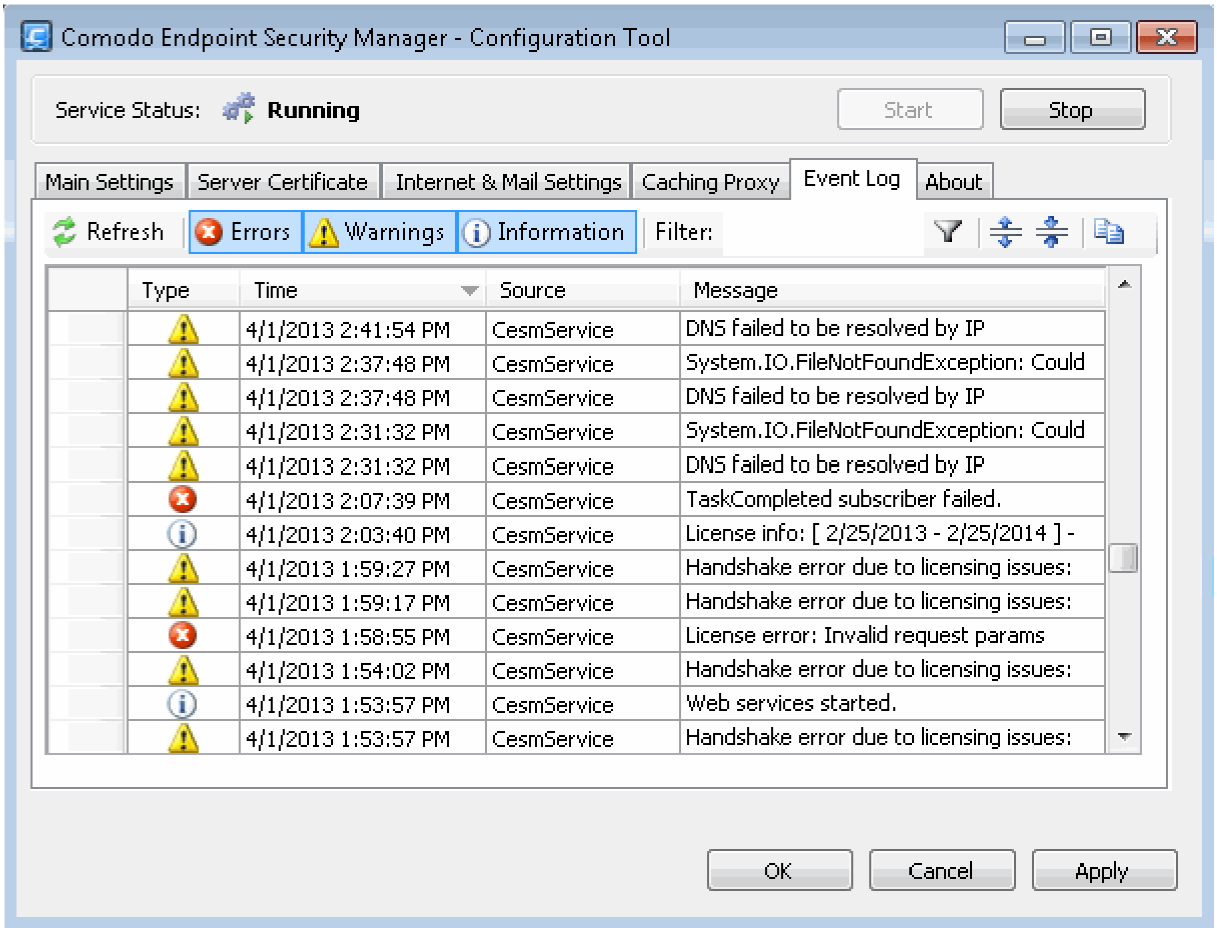
Cache Folder Size: 0.00 MB

☑ Provide cached content if content source is not available

- 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.

Viewing Database Event Log

The 'Event Log' contains a list of notifications from ESM central service that may assist administrators to troubleshoot problems.

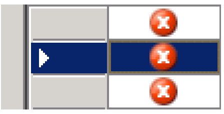


Type	Time	Source	Message
⚠	4/1/2013 2:41:54 PM	CesmService	DNS failed to be resolved by IP
⚠	4/1/2013 2:37:48 PM	CesmService	System.IO.FileNotFoundException: Could
⚠	4/1/2013 2:37:48 PM	CesmService	DNS failed to be resolved by IP
⚠	4/1/2013 2:31:32 PM	CesmService	System.IO.FileNotFoundException: Could
⚠	4/1/2013 2:31:32 PM	CesmService	DNS failed to be resolved by IP
✖	4/1/2013 2:07:39 PM	CesmService	TaskCompleted subscriber failed.
ℹ	4/1/2013 2:03:40 PM	CesmService	License info: [2/25/2013 - 2/25/2014] -
⚠	4/1/2013 1:59:27 PM	CesmService	Handshake error due to licensing issues:
⚠	4/1/2013 1:59:17 PM	CesmService	Handshake error due to licensing issues:
✖	4/1/2013 1:58:55 PM	CesmService	License error: Invalid request params
⚠	4/1/2013 1:54:02 PM	CesmService	Handshake error due to licensing issues:
ℹ	4/1/2013 1:53:57 PM	CesmService	Web services started.
⚠	4/1/2013 1:53:57 PM	CesmService	Handshake error due to licensing issues:

- 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.

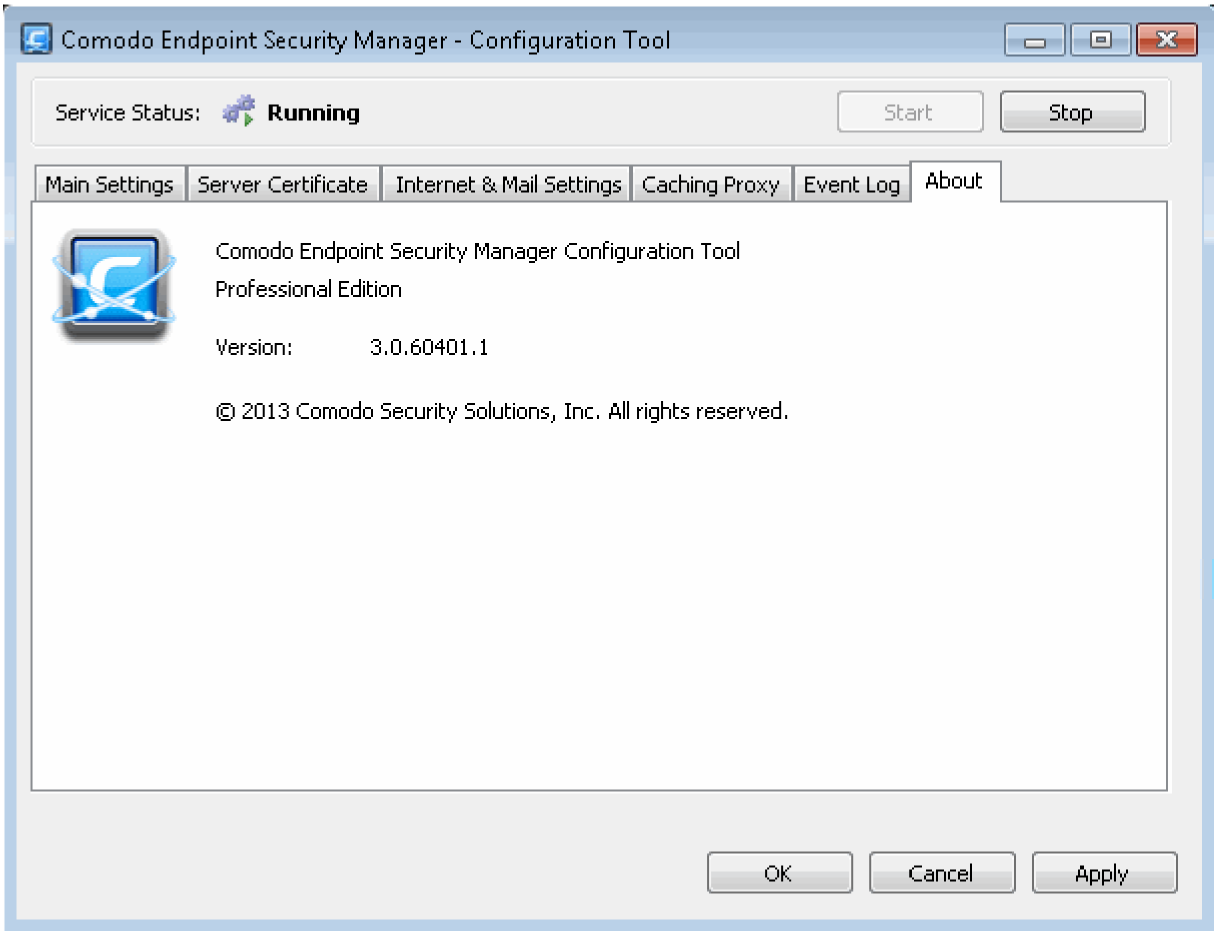
Column	Types/Format	Definition / Description
Type (of event)	✖	Error - 'Errors' are those events whereby the ESM Central Service failed to execute a command.
	⚠	Warning - High severity errors that may (or already have) prevented the ESM service from connecting to the data source. For example, a critical application crash.
	ℹ	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 ÷ control to view a condensed version of the message (this is the default view). - Use the ⎘ 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.
▽	*Apply Filter*	Implements the filter typed into the text field.
	*Select Event*	Selects a particular event row. Once selected, clicking the 'Expand Rows' control will highlight the information pertaining to this event.
⇕	*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.
÷	*Contract Rows*	Displays the condensed 'Message' (all events). This is the default view.
⎘	*Copy*	Copies the contents of the selected cells to the clipboard.

About

The 'About' tab provides the copyright information and the current ESM version number and license information.



Comodo Endpoint Security Manager Configuration Tool

Professional Edition

Version: 3.0.60401.1

© 2013 Comodo Security Solutions, Inc. All rights reserved.

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 CES policies - an introduction**
- **How to Setup External Access from Internet**
- **How to Install CES on Endpoints Added by Manually Installing the Agent**

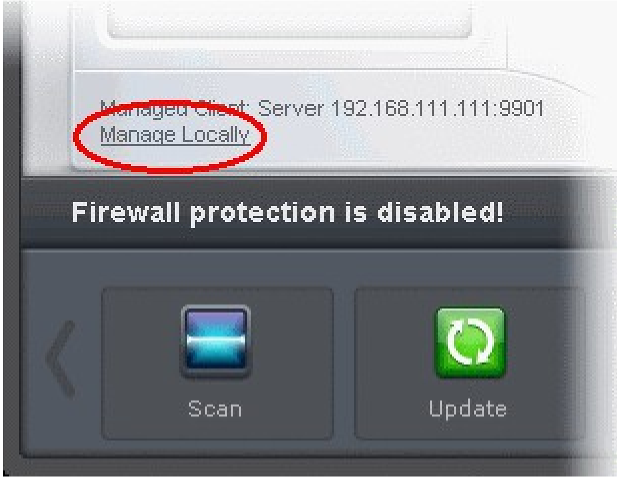
How to Configure CES policies - An Introduction

A CESM policy is the security configuration of Comodo Endpoint Security (CES) 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.

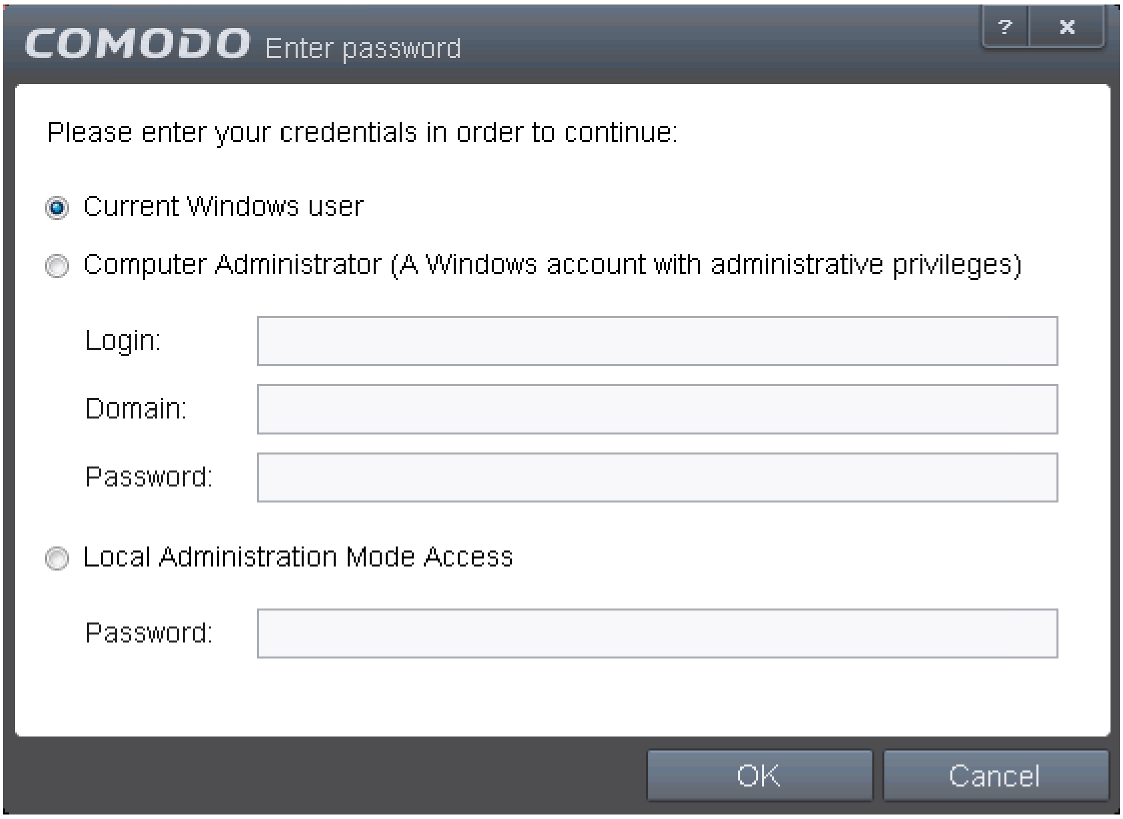
The CESM Policy can be derived from the configuration of Antivirus, Firewall and Defense+ components of CES on an endpoint and can be rolled out to any number of endpoints or endpoint groups.

In order to configure Antivirus, Firewall and Defense+ settings in CES on an endpoint computer, the administrator has to ensure that the endpoint computer is either 'Locally Configured' (it has no policy) or it is in local mode (or CESM will remotely re-apply the endpoint's security policy and override any changes made by the administrator).

Click 'Manage Locally' at the lower left of the CES interface to enable local administration mode:


Managed Client: Server 192.168.111.111:9901
Manage Locally
Firewall protection is disabled!
Scan
Update

- Select user account for CES to access your computer


COMODO Enter password

Please enter your credentials in order to continue:

● Current Windows user

○ Computer Administrator (A Windows account with administrative privileges)

Login:

Domain:

Password:

○ Local Administration Mode Access

Password:

CES requires administrative privileges in order to change the configuration.

- If you have logged in as administrator, leave 'Current Windows User' selected.
- If you have logged in as a user with limited privileges, select Computer Administrator or Local Administration Mode Access and enter the credentials accordingly.
- Click OK.

The administrator can now configure the settings for Antivirus, Firewall and Defense+ components of CES 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.

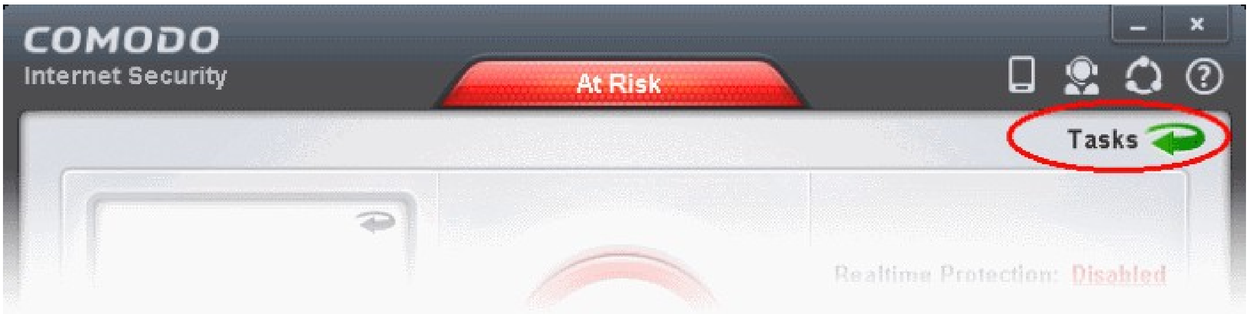
The remainder of this page is a quick primer to key areas within CES for modifying Antivirus, Firewall and Defense+ settings along with links to the appropriate section in the dedicated CES user-guide should further help be required.

Antivirus Settings

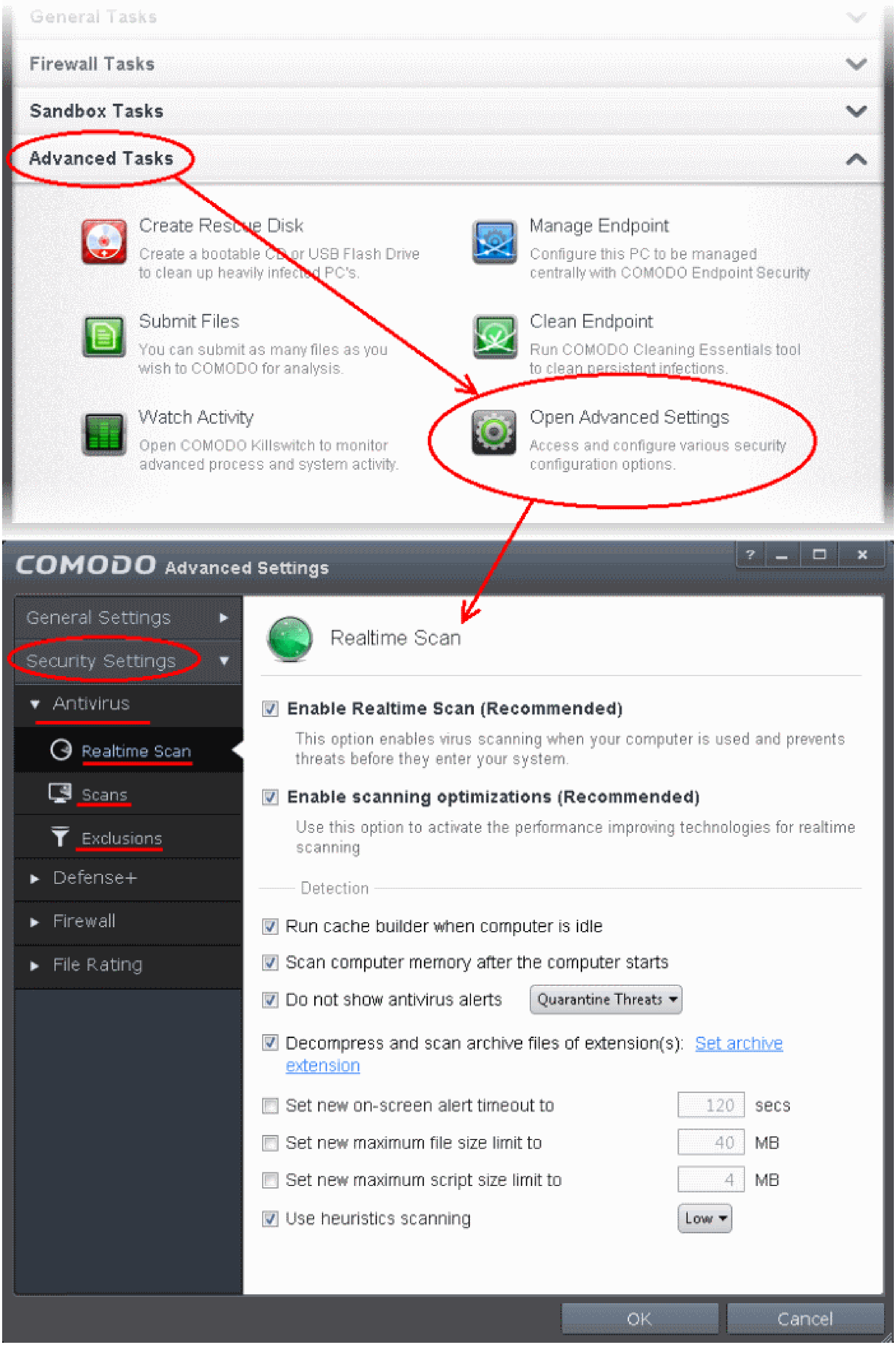
Comodo Antivirus leverages multiple technologies, including Real-time/On-Access Scanning, On Demand Scanning and a fully featured Scan Scheduler to immediately start cleaning or quarantining suspicious files from your hard drives, shared disks, emails, downloads and system memory.

To configure Antivirus Behavior Settings

- Click the 'Tasks' arrow from the CES 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. The Antivirus Behavior Settings interface will open.



General Tasks

Firewall Tasks

Sandbox Tasks

Advanced Tasks

Create Rescue Disk
Create a bootable CD or USB Flash Drive to clean up heavily infected PC's.

Manage Endpoint
Configure this PC to be managed centrally with COMODO Endpoint Security

Submit Files
You can submit as many files as you wish to COMODO for analysis.

Clean Endpoint
Run COMODO Cleaning Essentials tool to clean persistent infections.

Watch Activity
Open COMODO Killswitch to monitor advanced process and system activity.

Open Advanced Settings
Access and configure various security configuration options.

COMODO Advanced Settings

Realtime Scan

☑ **Enable Realtime Scan (Recommended)**

This option enables virus scanning when your computer is used and prevents threats before they enter your system.

☑ **Enable scanning optimizations (Recommended)**

Use this option to activate the performance improving technologies for realtime scanning

Detection

☑ Run cache builder when computer is idle

☑ Scan computer memory after the computer starts

☑ Do not show antivirus alerts Quarantine Threats

☑ Decompress and scan archive files of extension(s): Set archive extension

□ Set new on-screen alert timeout to 120 secs

□ Set new maximum file size limit to 40 MB

□ Set new maximum script size limit to 4 MB

☑ Use heuristics scanning Low

- 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 excludes scanning.

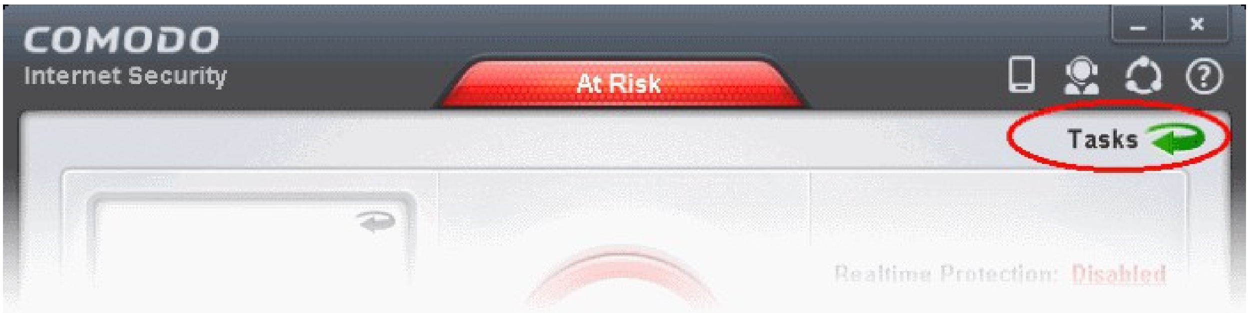
If more details are required for these settings, see **http://help.comodo.com/** for Comodo Endpoint Security.

Firewall Settings

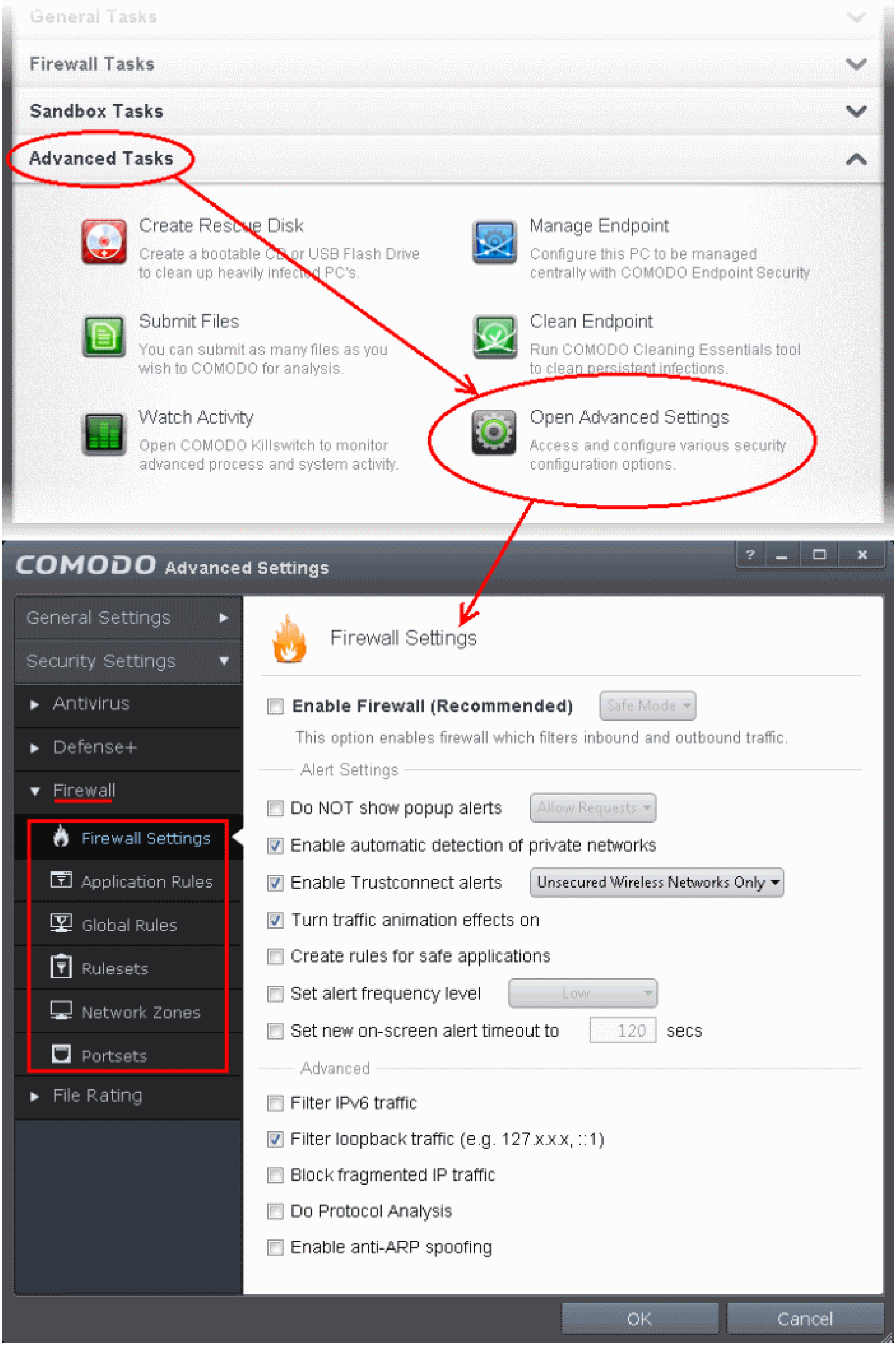
The firewall component of Comodo Endpoint Security offers the highest levels of security against inbound and outbound threats, can stealth endpoint ports against hackers and can prevent malicious software from transmitting confidential data over the Internet.

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.



Create Rescue Disk
Create a bootable CD or USB Flash Drive to clean up heavily infected PC's.

Manage Endpoint
Configure this PC to be managed centrally with COMODO Endpoint Security

Submit Files
You can submit as many files as you wish to COMODO for analysis.

Clean Endpoint
Run COMODO Cleaning Essentials tool to clean persistent infections.

Watch Activity
Open COMODO Killswitch to monitor advanced process and system activity.

Open Advanced Settings
Access and configure various security configuration options.

Firewall Settings

□ **Enable Firewall (Recommended)** Safe Mode
This option enables firewall which filters inbound and outbound traffic.

Alert Settings

□ Do NOT show popup alerts Allow Requests
☑ Enable automatic detection of private networks
☑ Enable Trustconnect alerts Unsecured Wireless Networks Only
☑ Turn traffic animation effects on
□ Create rules for safe applications
□ Set alert frequency level Low
□ Set new on-screen alert timeout to 120 secs

Advanced

□ Filter IPv6 traffic
☑ Filter loopback traffic (e.g. 127.x.x.x, ::1)
□ Block fragmented IP traffic
□ Do Protocol Analysis
□ Enable anti-ARP spoofing

- 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.

If more details are required for these settings, see **http://help.comodo.com/** for Comodo Endpoint Security.

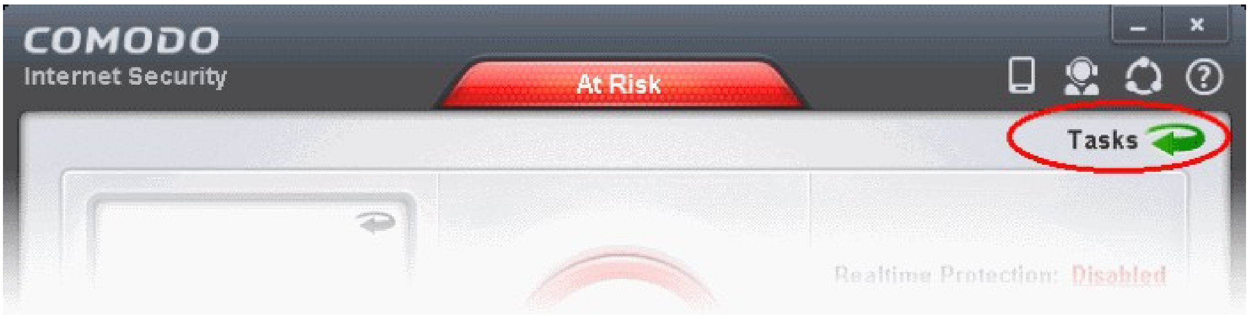
Defense+ Settings

The Defense+ component of Comodo Endpoint Security is a collection of prevention based security technologies designed to preserve the integrity, security and privacy of your operating system and user data.

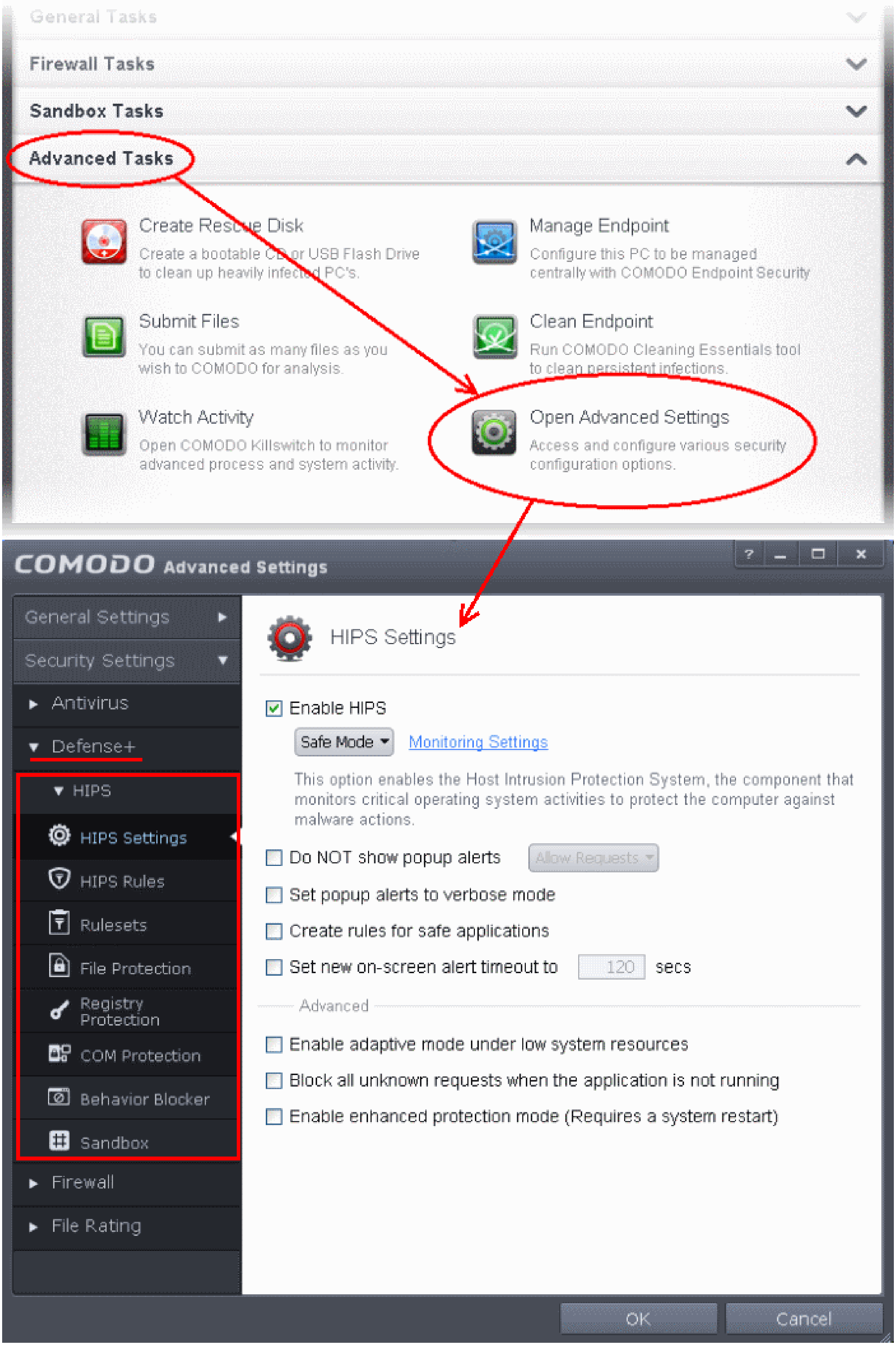
- **Behavior Blocker** – Authenticates every executable and process running on your computer and prevents them from taking actions that could harm your computer. Unrecognized processes and applications will be auto-sandboxed and run under a set of restrictions so they cannot harm your computer. This gives untrusted (but harmless) applications the freedom to operate whilst untrusted (and potentially malicious) applications are prevented from damaging your PC or data.
- **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.

To configure Defense+ 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' > 'Defense+' from the left hand side navigation of 'Advanced Settings' interface.



General Tasks

Firewall Tasks

Sandbox Tasks

Advanced Tasks

Create Rescue Disk
Create a bootable CD or USB Flash Drive to clean up heavily infected PC's.

Manage Endpoint
Configure this PC to be managed centrally with COMODO Endpoint Security

Submit Files
You can submit as many files as you wish to COMODO for analysis.

Clean Endpoint
Run COMODO Cleaning Essentials tool to clean persistent infections.

Watch Activity
Open COMODO Killswitch to monitor advanced process and system activity.

Open Advanced Settings
Access and configure various security configuration options.

COMODO Advanced Settings

HIPS Settings

☑ Enable HIPS

Safe Mode ▾ Monitoring Settings

This option enables the Host Intrusion Protection System, the component that monitors critical operating system activities to protect the computer against malware actions.

☐ Do NOT show popup alerts Allow Requests ▾

☐ Set popup alerts to verbose mode

☐ Create rules for safe applications

☐ Set new on-screen alert timeout to 120 secs

Advanced

☐ Enable adaptive mode under low system resources

☐ Block all unknown requests when the application is not running

☐ Enable enhanced protection mode (Requires a system restart)

- Click 'Hips' and then the options below it from the LHS navigation to configure the overall behavior of host intrusion prevention system.
- Click 'Behavior Blocker' from the LHS navigation to define how proactive the Behavior Blocker should be and which types of files it should check.
- Click 'Sandbox' from the LHS navigation to add applications to be run in sandbox always and to configure the sandbox.

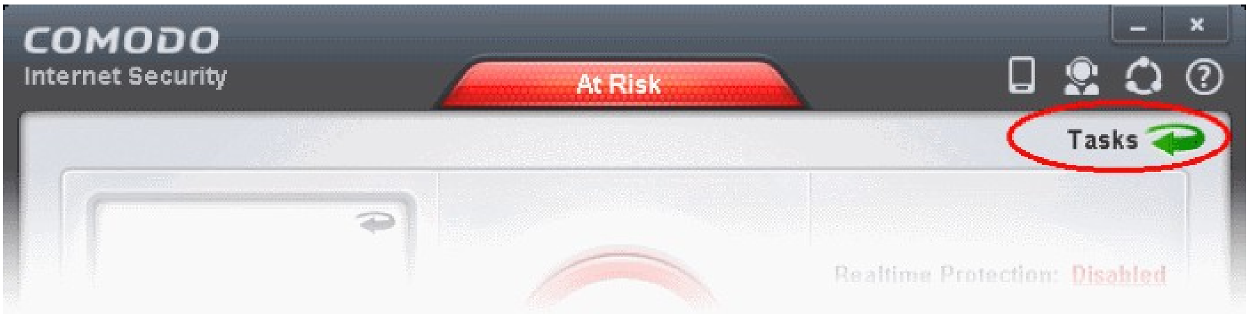
If more details are required for these settings, see **http://help.comodo.com/** for Comodo Endpoint Security.

File Rating Settings

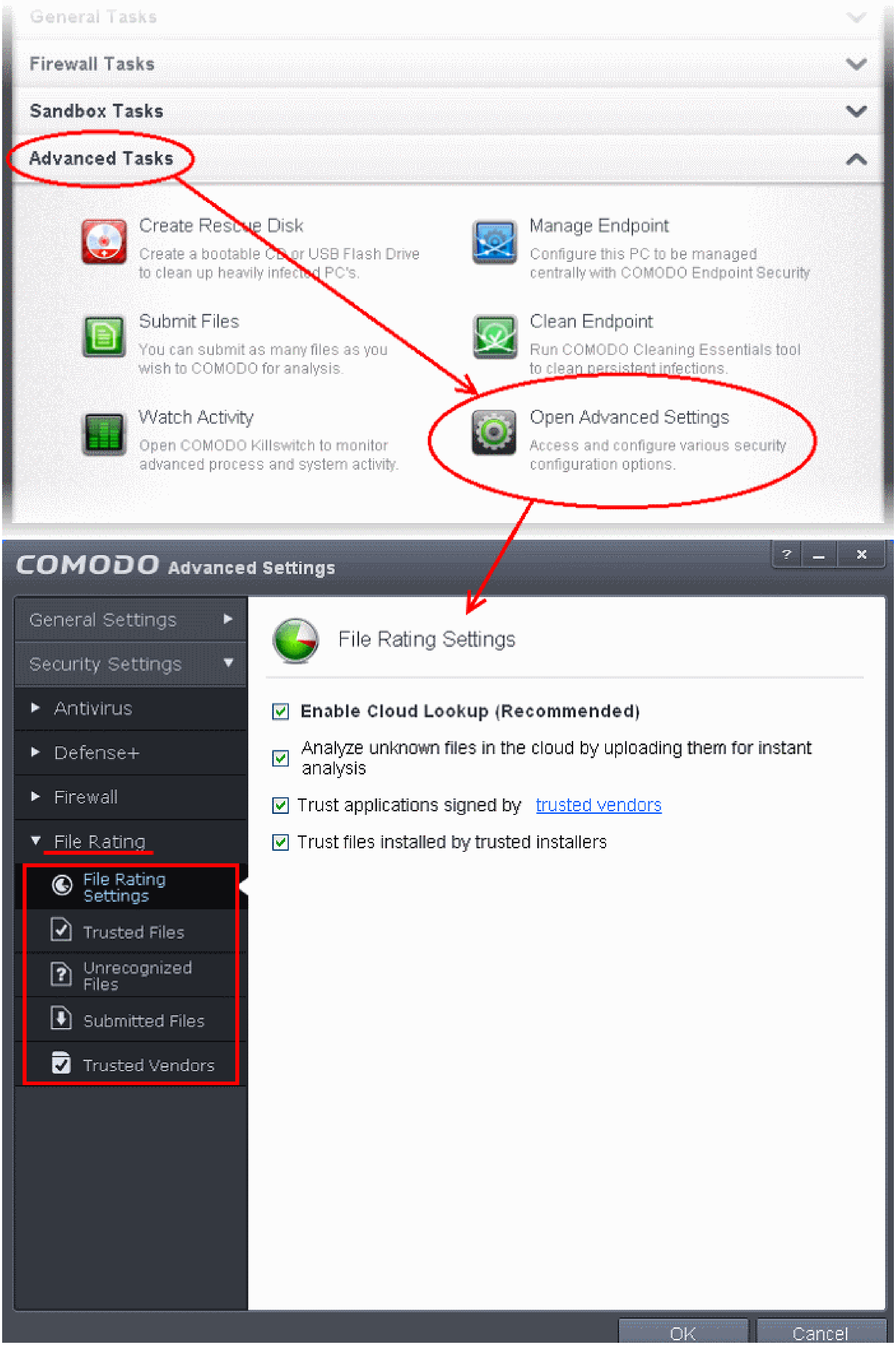
CES allows the administrators to add trusted files that should be excluded from monitoring by HIPS, Unrecognized files that should be blocked and add trusted software vendors to Trusted Vendors list so that the applications from trusted vendors will not be monitored by HIPS.

To configure File Rating Settings

- Click the 'Tasks' arrow from the CES 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.



Create Rescue Disk
Create a bootable CD or USB Flash Drive to clean up heavily infected PC's.

Manage Endpoint
Configure this PC to be managed centrally with COMODO Endpoint Security

Submit Files
You can submit as many files as you wish to COMODO for analysis.

Clean Endpoint
Run COMODO Cleaning Essentials tool to clean persistent infections.

Watch Activity
Open COMODO Killswitch to monitor advanced process and system activity.

Open Advanced Settings
Access and configure various security configuration options.

File Rating Settings

☑ **Enable Cloud Lookup (Recommended)**

☑ Analyze unknown files in the cloud by uploading them for instant analysis

☑ Trust applications signed by trusted vendors

☑ Trust files installed by trusted installers

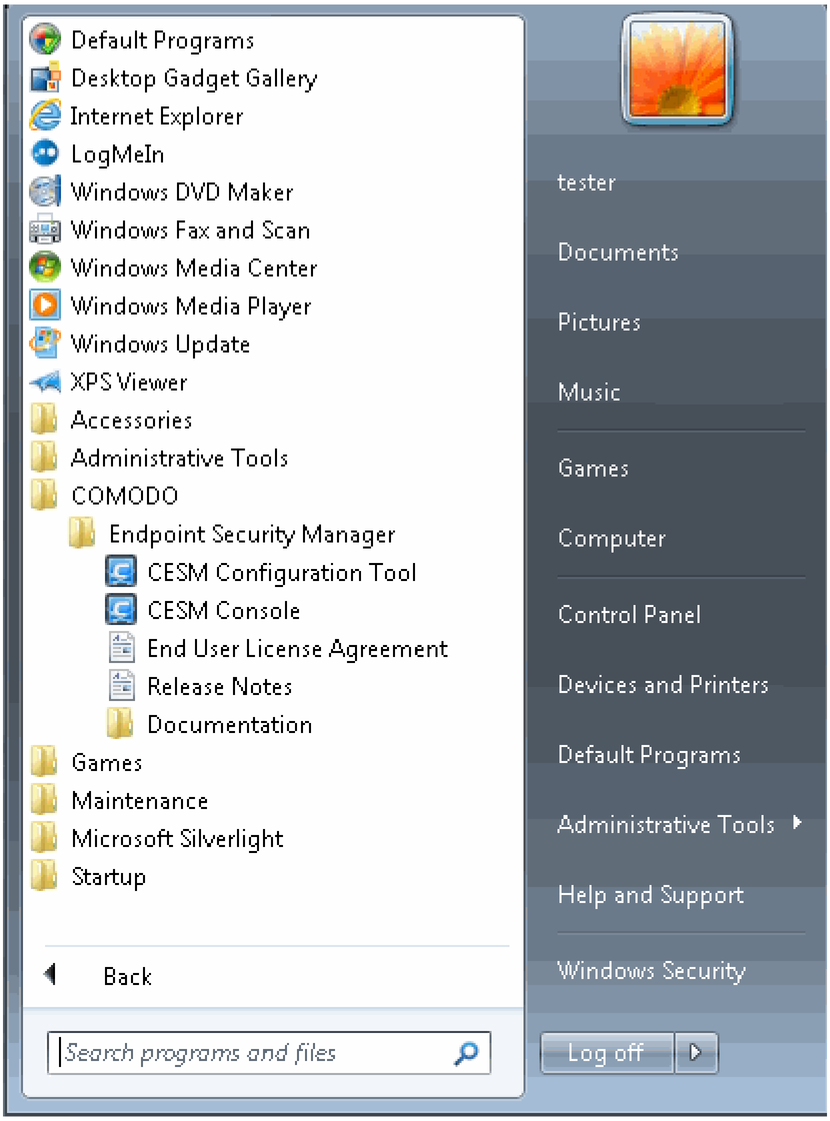
- Click 'File Rating Settings' from the LHS navigation to configure settings that govern the overall behavior of file rating.
- Click 'Trusted Files' from the LHS navigation to view the list of trusted files and manually add files to it.
- Click 'Unrecognized Files' from the LHS navigation to view and manage unrecognized items.
- 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 **http://help.comodo.com/** for Comodo Endpoint Security.

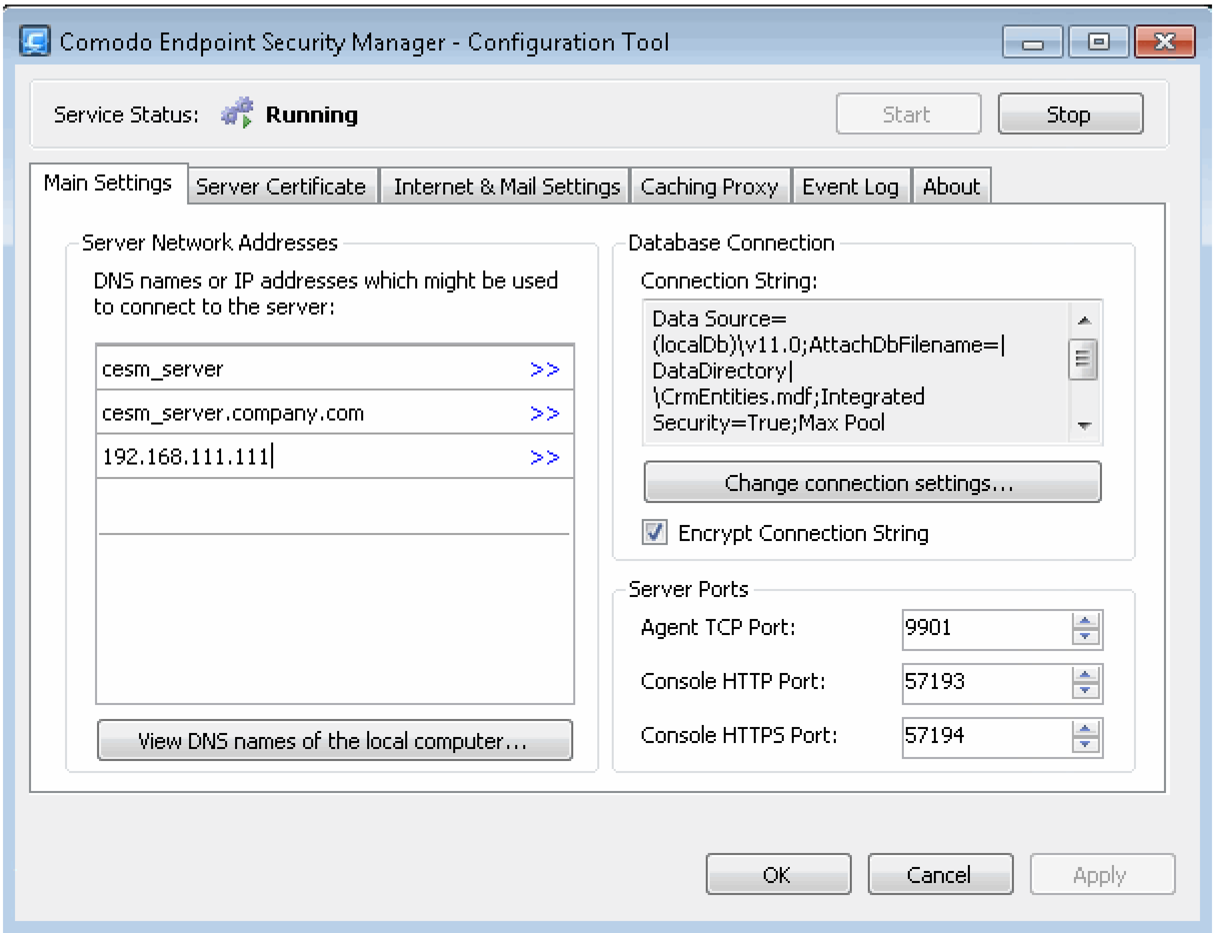
How to Setup External Access from Internet

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).



Comodo Endpoint Security Manager - Configuration Tool

Service Status: **Running**

Server Network Addresses

DNS names or IP addresses which might be used to connect to the server:

- cesm_server
- cesm_server.company.com
- 192.168.111.111

Database Connection

Connection String:

```
Data Source=
(localDb)\v11.0;AttachDbFilename=|
DataDirectory|
\CrmEntities.mdf;Integrated
Security=True;Max Pool
```

☑ Encrypt Connection String

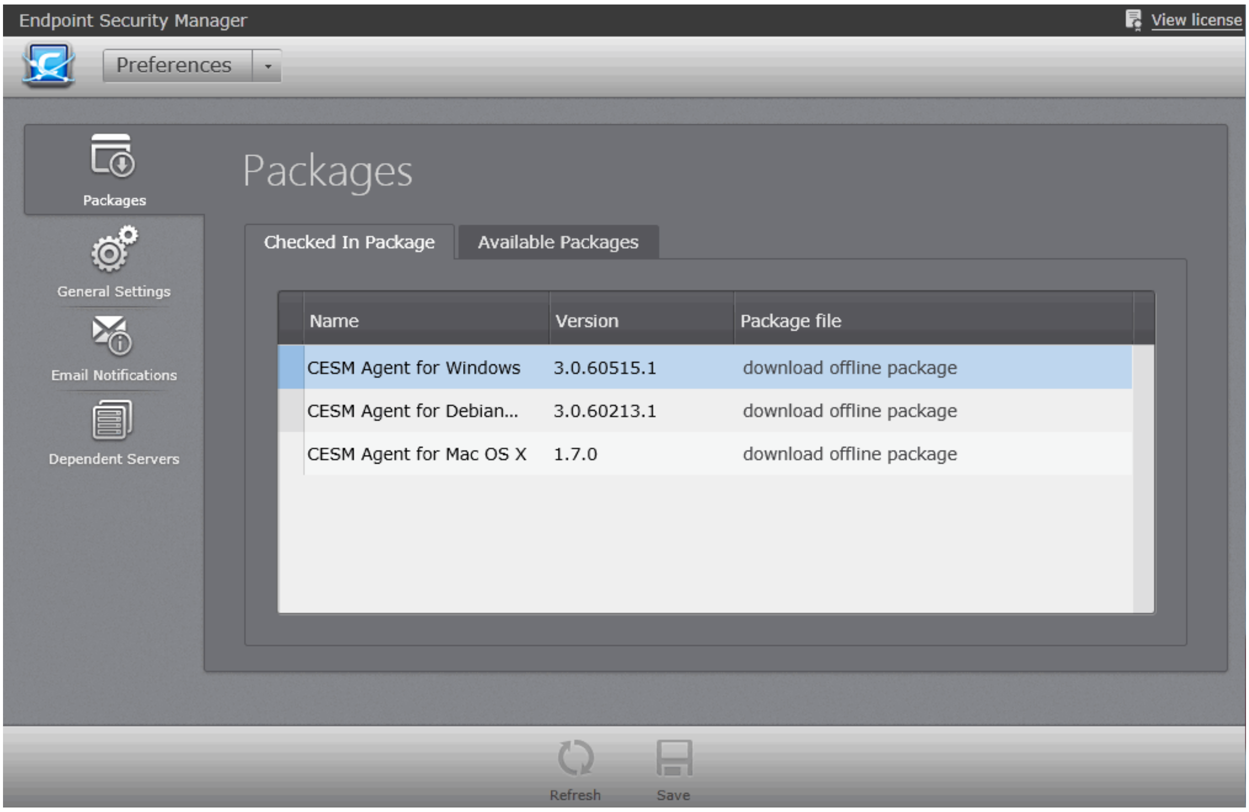
Server Ports

Agent TCP Port:	9901
Console HTTP Port:	57193
Console HTTPS Port:	57194

- 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) 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.



Name	Version	Package file
CESM Agent for Windows	3.0.60515.1	download offline package
CESM Agent for Debian...	3.0.60213.1	download offline package
CESM Agent for Mac OS X	1.7.0	download offline package

  - To download CESM agent setup file for Windows as .exe file, click **download offline package**
  - To download CESM agent setup file for Linux as .deb file, click **download offline package**
  - To download CESM agent setup file for Mac OS as .dmg file, click **download offline package**
- Click 'Save' in the 'File Download' dialog and save the file in the location of your choice.
- 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'.

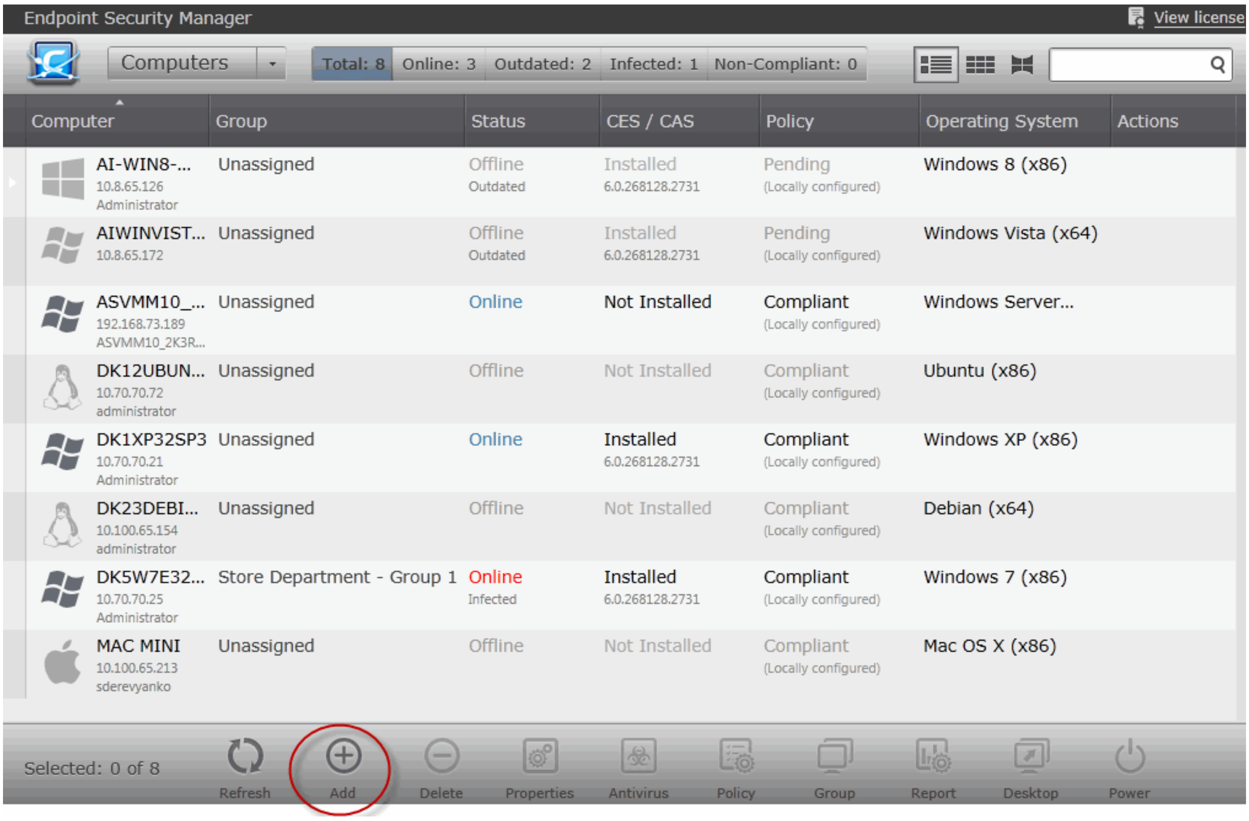
- See section **Creating New Endpoint Groups and importing Exising Endpoints** for more details on creating endpoint groups.
- See section **Creating a New Security Policy** for more details on creating a new policy.
- See section **Key Concepts** to know about CESM Key Concepts.
- See section '**Best Practices**' to know how to use CESM effectively.

How to Install CES on Endpoints Added by Manually Installing the Agent

The endpoint security software Comodo Endpoint Security can be remotely installed on to endpoints added to CESM by manually installing the agent and connected through external networks from the CESM administrative console.

To install CES

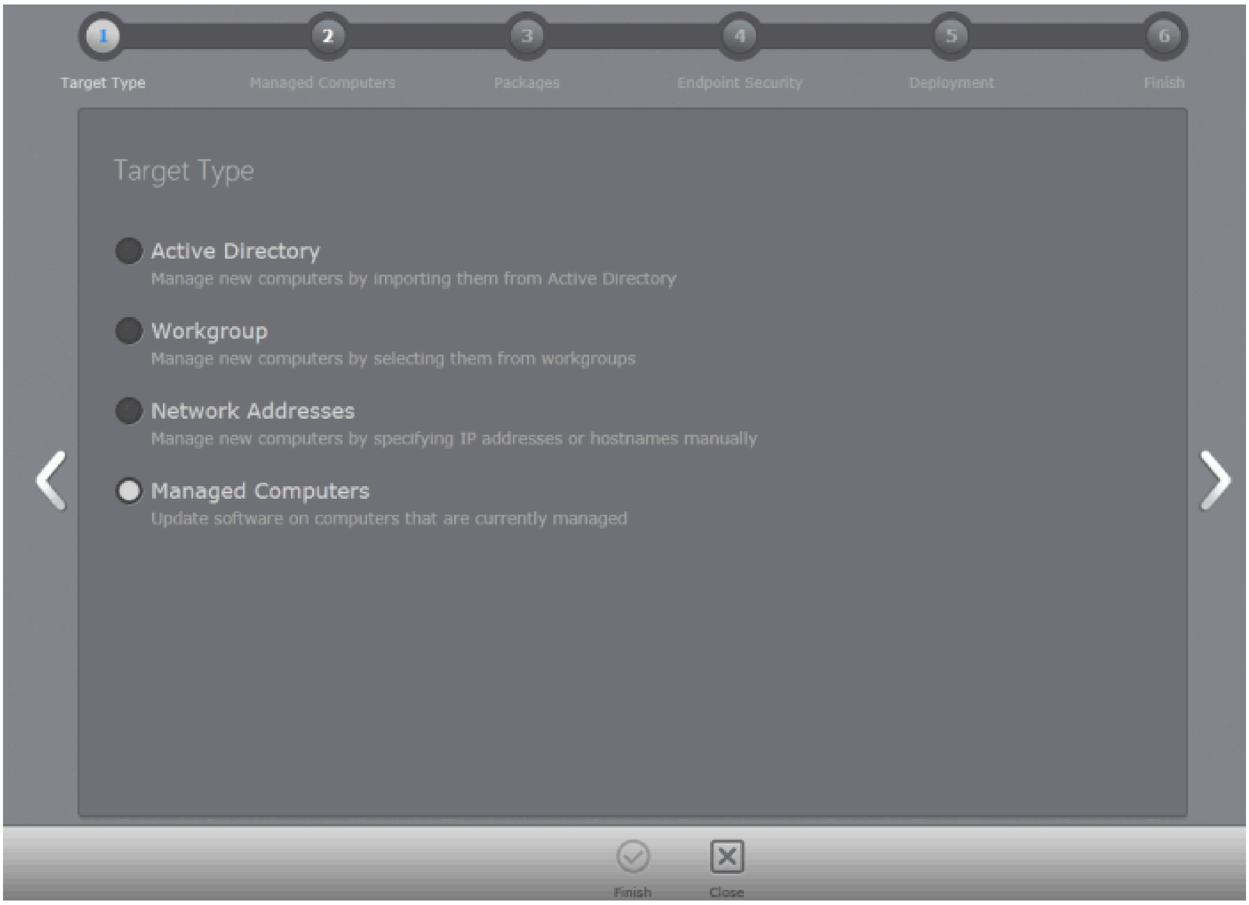
1. Open the 'Computers' area by selecting Computers from the drop-down at the top left.
2. Click 'Add' from the 'Computers' area to start the wizard.



Computer	Group	Status	CES / CAS	Policy	Operating System	Actions
AI-WIN8-... 10.8.65.126 Administrator	Unassigned	Offline Outdated	Installed 6.0.268128.2731	Pending (Locally configured)	Windows 8 (x86)	
AIWINVIST... 10.8.65.172	Unassigned	Offline Outdated	Installed 6.0.268128.2731	Pending (Locally configured)	Windows Vista (x64)	
ASVMM10_... 192.168.73.189 ASVMM10_2K3R...	Unassigned	Online	Not Installed	Compliant (Locally configured)	Windows Server...	
DK12UBUN... 10.70.70.72 administrator	Unassigned	Offline	Not Installed	Compliant (Locally configured)	Ubuntu (x86)	
DK1XP32SP3 10.70.70.21 Administrator	Unassigned	Online	Installed 6.0.268128.2731	Compliant (Locally configured)	Windows XP (x86)	
DK23DEBI... 10.100.65.154 administrator	Unassigned	Offline	Not Installed	Compliant (Locally configured)	Debian (x64)	
DK5W7E32... 10.70.70.25 Administrator	Store Department - Group 1	Online Infected	Installed 6.0.268128.2731	Compliant (Locally configured)	Windows 7 (x86)	
MAC MINI 10.100.65.213 sderevyanko	Unassigned	Offline	Not Installed	Compliant (Locally configured)	Mac OS X (x86)	

Selected: 0 of 8

3. Select 'Managed Computers' and click the right arrow button to proceed to the next step.



Target Type

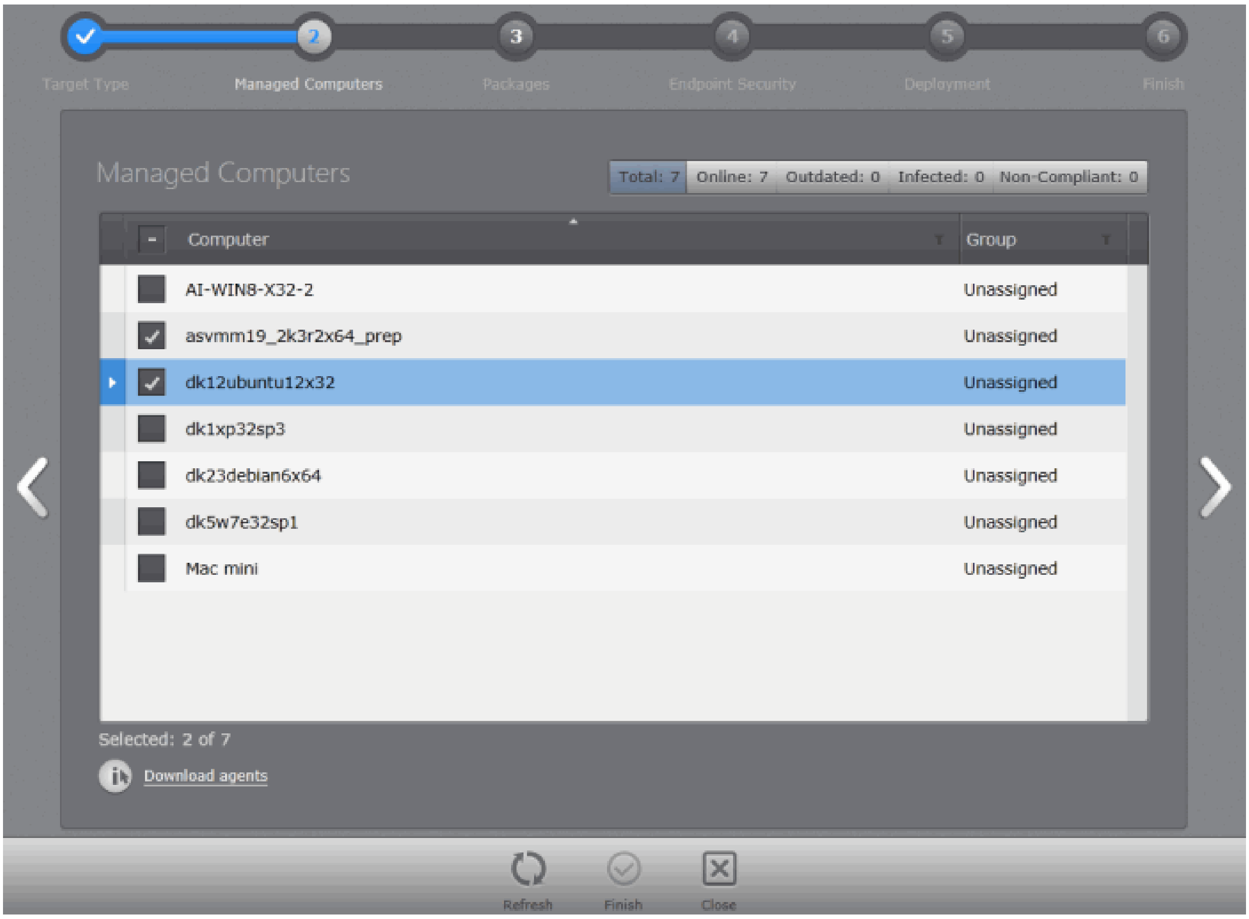
○ Active Directory
Manage new computers by importing them from Active Directory

○ Workgroup
Manage new computers by selecting them from workgroups

○ Network Addresses
Manage new computers by specifying IP addresses or hostnames manually

● Managed Computers
Update software on computers that are currently managed

All the managed computers will be listed.



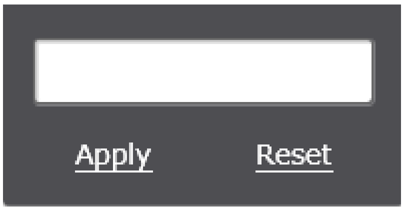
Managed Computers

Total: 7 | Online: 7 | Outdated: 0 | Infected: 0 | Non-Compliant: 0

▣	Computer	Group
□	AI-WIN8-X32-2	Unassigned
☑	asvmm19_2k3r2x64_prep	Unassigned
☑	dk12ubuntu12x32	Unassigned
□	dk1xp32sp3	Unassigned
□	dk23debian6x64	Unassigned
□	dk5w7e32sp1	Unassigned
□	Mac mini	Unassigned

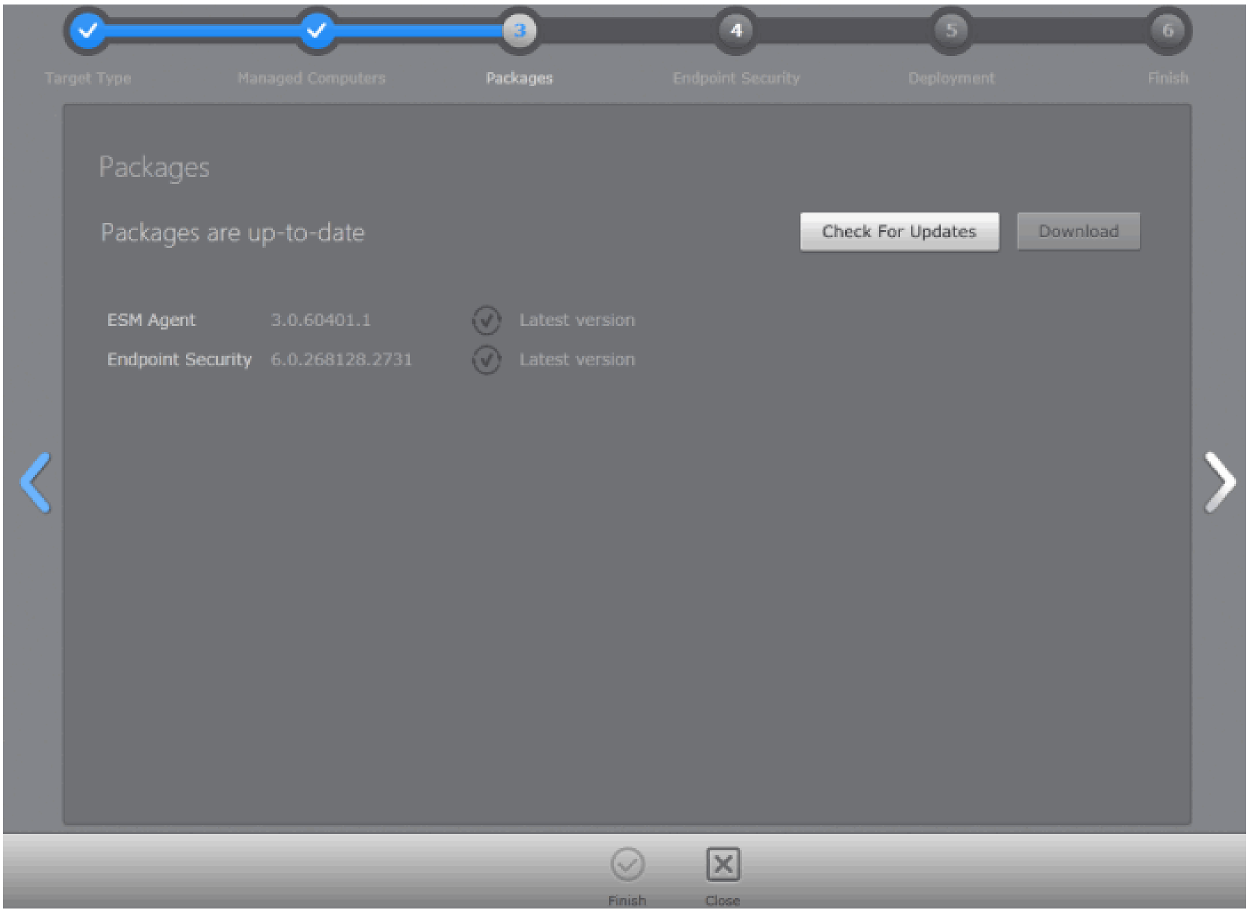
Selected: 2 of 7

4. Select the endpoints on which you want to install CES application from the list.



- Click the filter icon T in the 'Name' 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 stage 'Packages' displays the version details of ESM Agent and CES. You can also check for updates of these applications and download it in your server for deployment on to the selected endpoints.



Packages

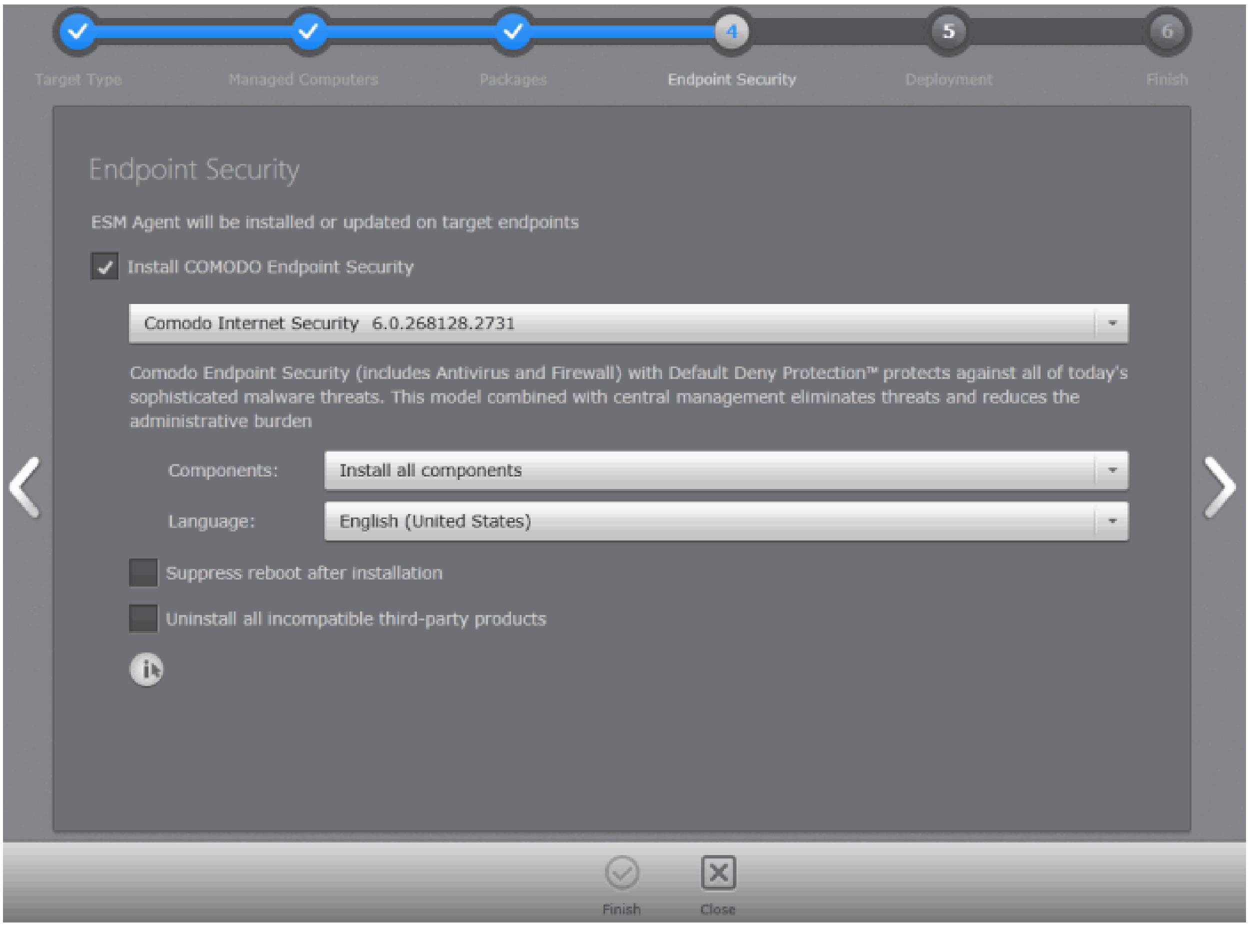
Packages are up-to-date

ESM Agent 3.0.60401.1 ✓ Latest version

Endpoint Security 6.0.268128.2731 ✓ Latest version

5. Click 'Check for Updates' to find out if any newer version of CESM Agent and CES are available.
   - If any newer versions are available, you can choose to download them to the CESM server by clicking 'Download'
6. 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):



Endpoint Security

ESM Agent will be installed or updated on target endpoints

☑ Install COMODO Endpoint Security

Comodo Internet Security 6.0.268128.2731

Comodo Endpoint Security (includes Antivirus and Firewall) with Default Deny Protection™ protects against all of today's sophisticated malware threats. This model combined with central management eliminates threats and reduces the administrative burden

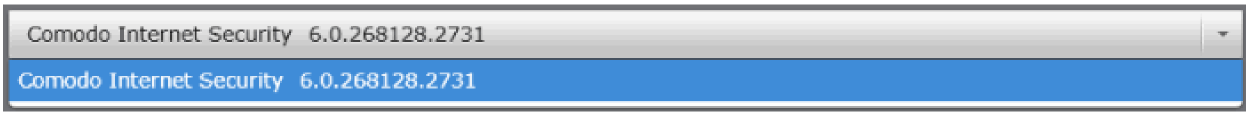
Components: Install all components

Language: English (United States)

□ Suppress reboot after installation

□ Uninstall all incompatible third-party products

7. Select 'Install Comodo Endpoint Security' check box.
8. Select the version of CES you wish to install on the selected endpoints from the drop-down.



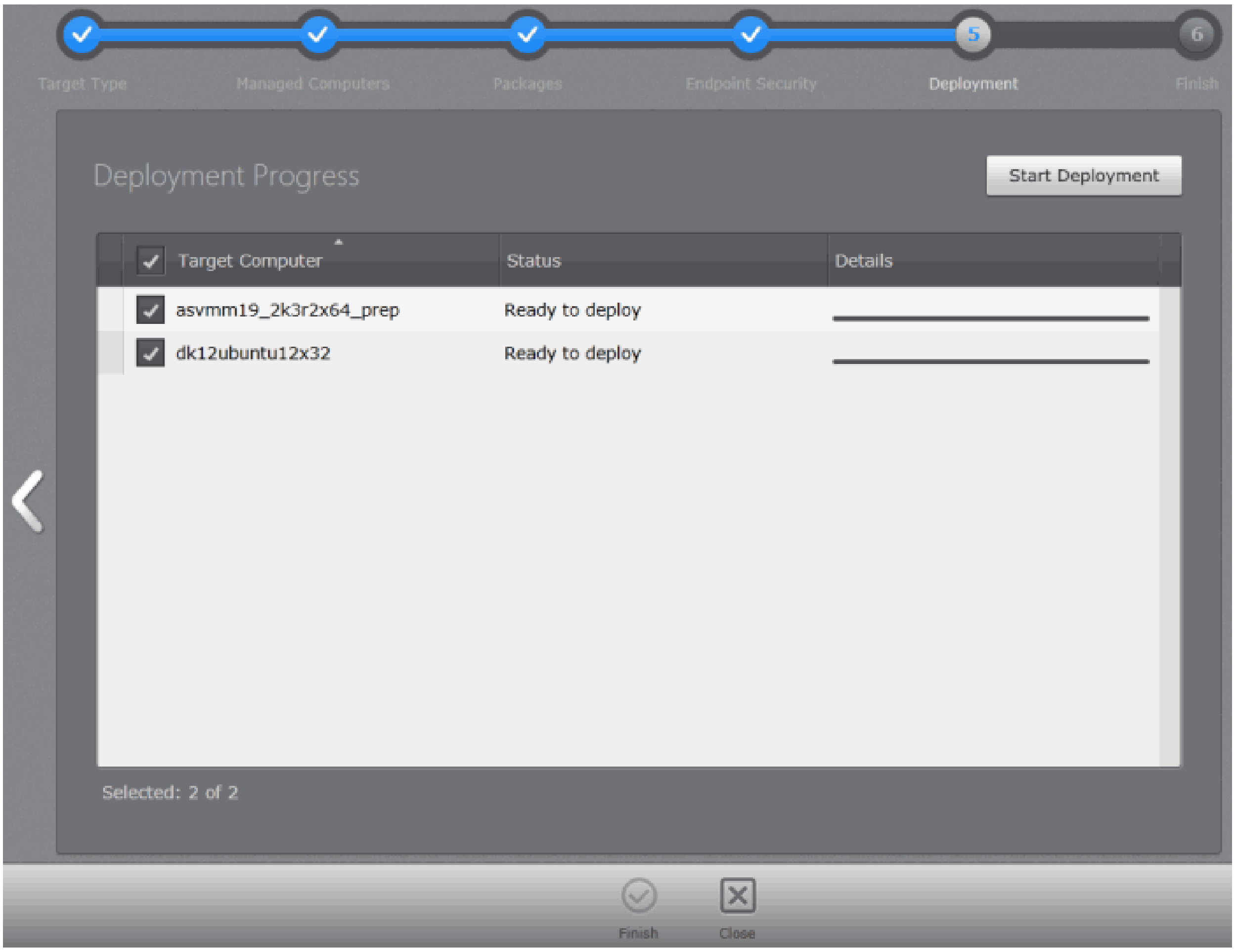
Comodo Internet Security 6.0.268128.2731

Comodo Internet Security 6.0.268128.2731

- Select whether you want to include all the components (Firewall and Antivirus), Antivirus only or Firewall only from the Components 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 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.

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

The next step is the deployment process.

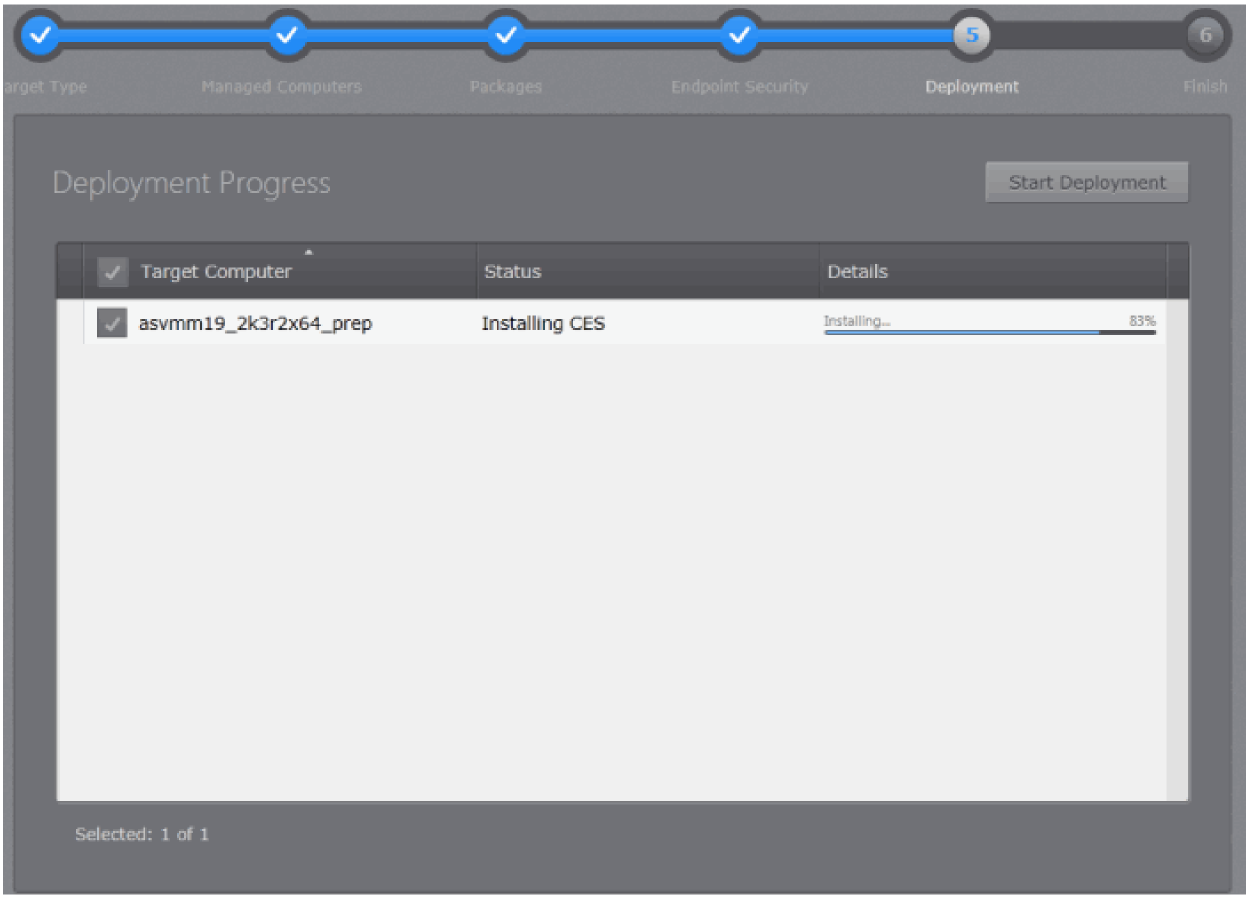


☑ Target Computer	Status	Details
☑ asvmm19_2k3r2x64_prep	Ready to deploy	
☑ dk12ubuntu12x32	Ready to deploy	

Selected: 2 of 2

10. Click 'Start Deployment'.

The deployment progress will be displayed.

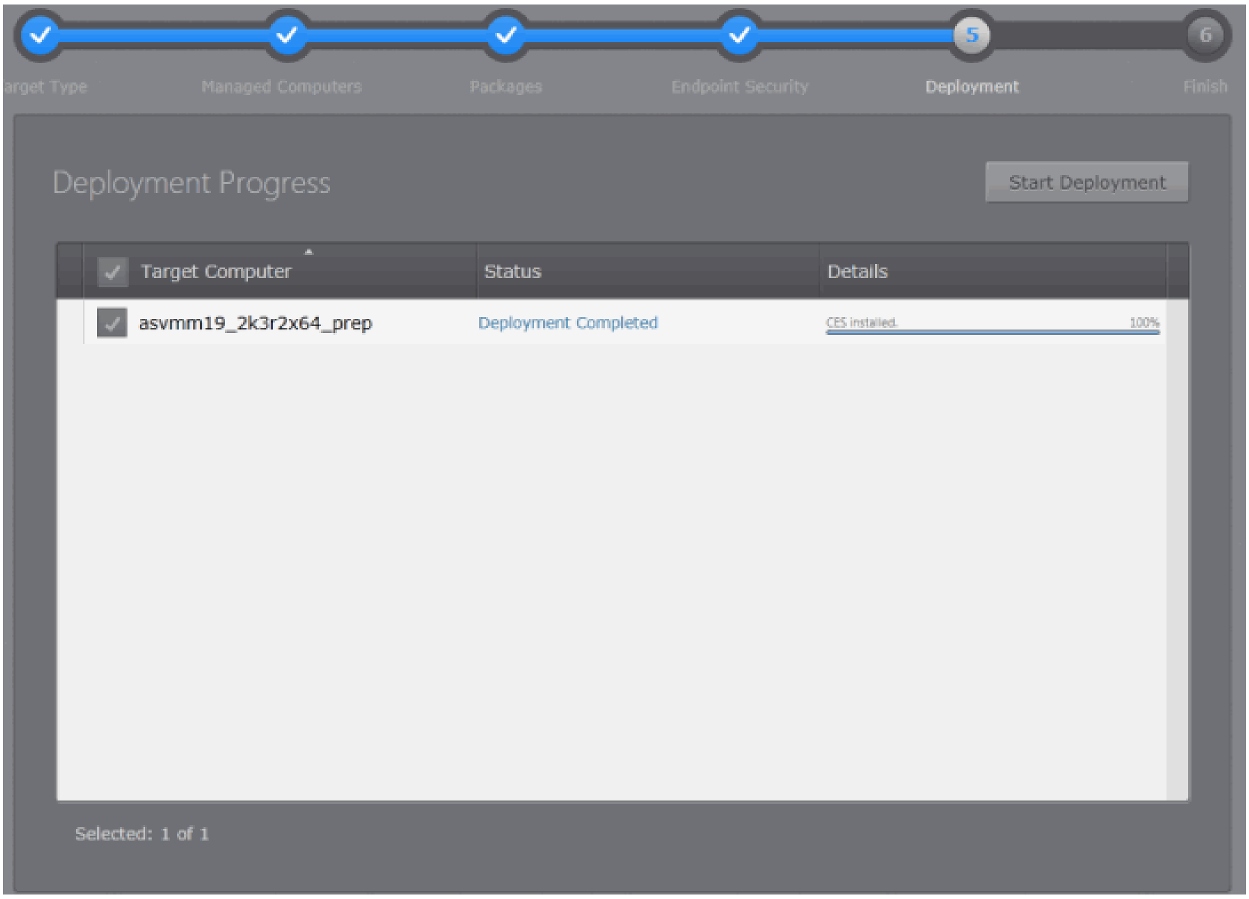


Deployment Progress

☑ Target Computer	Status	Details
☑ asvmm19_2k3r2x64_prep	Installing CES	Installing... 83%

Selected: 1 of 1

On completion of installation, the results screen will appear.



Deployment Progress

☑ Target Computer	Status	Details
☑ asvmm19_2k3r2x64_prep	Deployment Completed	CES installed. 100%

Selected: 1 of 1

11. 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

STE 100

Clifton, NJ 07013

United States

Tel : +1.877.712.1309

Email: **EnterpriseSolutions@Comodo.com**

For additional information on Comodo - visit **http://www.comodo.com**.