COMODO
Creating Trust Online®

Comodo
Endpoint Security Manager
Business Edition

Software Version 2.0

Administrator Guide

Guide Version 2.0.031312

Comodo Security Solutions
525 Washington Blvd.
Jersey City, NJ 07310

Table of Contents

1. Introduction to Comodo Endpoint Security Manager - Business Edition

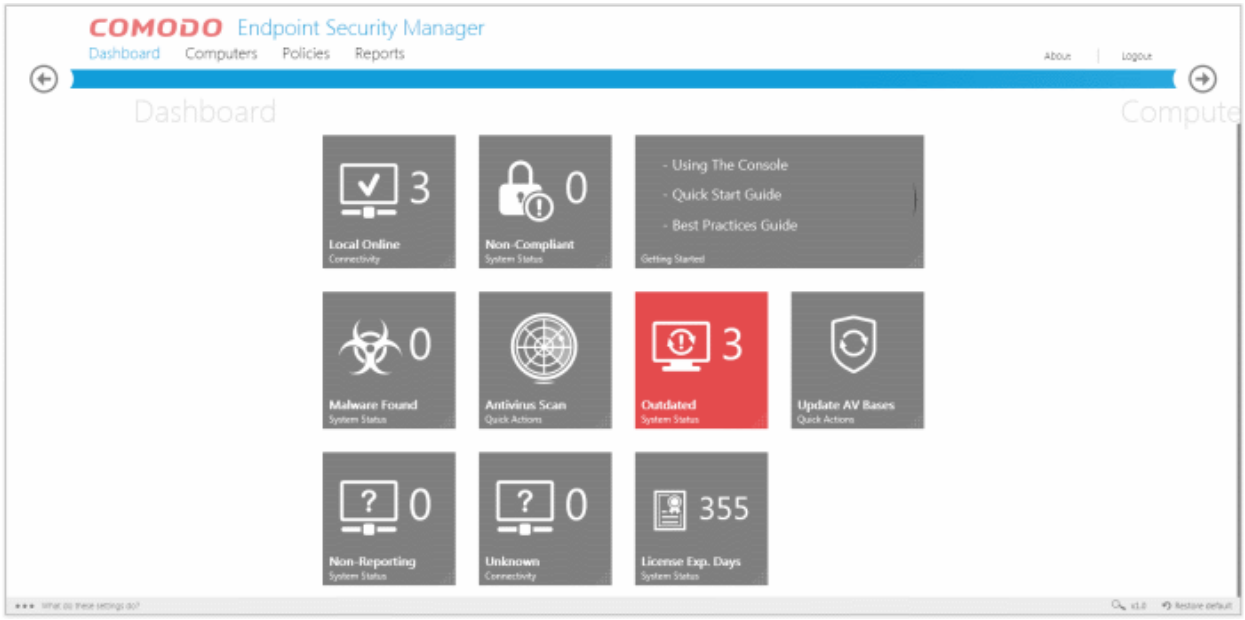
Comodo Endpoint Security Manager (CESM) Business Edition is designed to help administrators of corporate networks deploy, manage and monitor Comodo endpoint security software on managed networked computers.

Total Protection for networked computers

CESM allows administrators to leverage and maximize the protection offered by Comodo's endpoint security solutions. These products can now be centrally managed and administered to ensure a workforce that is protected by best-of-breed solutions such as Comodo Internet Security (including Firewall and Anti-virus). If installed individually, each product delivers superior protection against its specific threat vector. If installed as a full suite of packages, they provide a level of total endpoint security that is unrivaled in the industry.

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. Furthermore, CESM's dashboard provides fingertip access to tasks wizards, important network and task related data and support resources. The Administrator can add endpoint computers, install agents, create new policies and do much more quickly by using the wizards via the web interface.



Features:

- New web browser-based panorama- style user interface compatible with touch-screen computers
- New Dashboard interface with Active Tiles™ and configurable email alerts
- New policy-based Comodo Internet Security configuration management
- New Internet policy supports different CIS configuration for laptops
- Integration with the latest Comodo Internet Security
- New Active 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 Business Edition and is broken down into the following main sections.

Dashboard Area - Features a set of highly configurable, dynamic tiles that let system administrators create the control panel of their choice.

- Dashboard area gives an immediate heads-up on network, virus and policy status
- Serves as a launchpad for common tasks such as antivirus scans or database updates
- Highly customizable - tiles can be dragged, dropped and re-arranged as admin sees fit
- Dynamic - admins can change the type of information that is shown on any particular tile
- Additional Active Tiles™ with extra functionality can be dragged onto the dashboard by clicking the ellipsis button on the settings bar at the lower left of the interface

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.

- View complete details of the endpoints that are managed by CESM
- Add/Import computers to CESM for centralized management
- Create computer Groups for easy administration
- Apply security policies to computers and groups
- Download the latest version of the agent and deploy agents to target computers

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

- View a list of all policies along with their descriptions and the CIS component covered by the policy
- View and modify the details of any policy - including name, description, CIS components, target computers and whether the policy should allow local configuration
- Add or remove policies as per requirements
- Export any policy to .xml file
- Create a new policy by importing settings from another computer, using another pre-existing policy or from a saved xml file

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

- 'In-report remediation' allows admins to launch any corrective actions directly from the report itself
- 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 CIS configuration, policy compliance, malware statistics, policy delta, CIS logs, quarantined items and more

1.1. Software Components and System Requirements

Software Components

CESM Business Edition consist of three interdependent software components:

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

Administrative Console

The Administrative Console provides access to all functionality of Comodo Endpoint Security Manager through a friendly and

highly configurable interface. Administrators can use the console to deploy, manage and monitor Comodo Endpoint security software on networked computers.

- Click here to go to the Admin console help pages
- Click here for system requirements for endpoint machines that run the administrative console
- Click here to read about logging into the console

Central Service

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

- Click here for a guide that explains how to install Central Service
- Click here for system requirements for machines that run the central service
- Click here to read about the central service configuration tool

Remote Agents

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

- Click here for system requirements for endpoint machines that run the 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
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: **Windows Server 2003** - SP1 or higher Small Business Server Small Business Server R2 **Windows Server 2008 -** SP2 or higher Small Business Server Server R2 **Microsoft Windows Client Family:**	The following operating systems are supported: **Windows Server 2003** - SP 1 or higher Small Business Server Small Business Server R2 **Windows Server 2008 -** SP2 or higher Small Business Server Server R2 **Microsoft Windows Client Family:**

CENTRAL SERVICE COMPUTER - SYSTEM REQUIREMENTS		
	Windows 7	**Windows 7**
Software Environment	Microsoft .NET Framework 4.0 Microsoft ReportViewer 2010 SP1 (**Note** - The above components will be installed automatically if not present)	Microsoft .NET Framework 4.0 Microsoft ReportViewer 2010 SP1 (**Note** - The above components will be installed automatically if not present)
Database	Microsoft SQL Server Compact 4.0 (**Note** - The above component will be installed automatically if not present)	Microsoft SQL Server Compact 4.0 (**Note** - The above component will be installed automatically if not present)
Other Requirements	The CESM program modules (Console, Service and Agent) may require Windows Firewall and/or personal firewall configuration changes in order to operate successfully. By default, the CESM Central Service is assigned: • TCP Port 9901 open to the Internet for inbound connections from Agents on portable computers • TCP Ports 57193, 57194 open to the Internet for inbound http: and https: console connections 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 1024x600 Netbook display with browser set to full-screen at this resolution Minimum 1024x768 display with windowed browser Touch capable display interface and operating system (optional)	Minimum 1024x600 Netbook display with browser set to full-screen at this resolution Minimum 1024x768 display with windowed browser Touch capable display interface and operating system (optional)
Software		
Browsers and software	Microsoft Silverlight 4.0 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 4.0 Microsoft Internet Explorer 7.0 or higher Mozilla Firefox 3.0 or higher Google Chrome 4.0 or higher
Other Requirements	• TCP Ports 57193,57194 will be used for http: and https: connections	

Endpoint Computer - (a managed PC that will run Comodo Internet 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: **Windows XP** - SP2 or later **Windows Vista** - SP1 or later **Windows 7**	The following operating systems are supported: **Windows XP** - SP2 or later **Windows Vista** - SP1 or later **Windows 7**
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.	

1.2. Removing Incompatible Products

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

- During the installation process, CESM BE can detect and automatically remove some brands of incompatible software
- However, certain software can be detected by CESM BE, but must be removed manually
- The following table contains a list of incompatible software and states whether CESM BE can detect and remove it or only detect it

Vendor	Product Name	Uninstall Type	Components
AVAST Software	avast! Free Antivirus	Detect only	avast! Free Antivirus
Symantec Corporation	Symantec Endpoint Protection	Automatic	Symantec Endpoint Protection
Agnitum	Outpost Security Suite Pro 7.1	Detect only	Outpost Security Suite Pro 7.1
Sophos Limited	Sophos Endpoint Security and Control	Automatic	Sophos AutoUpdate Sophos Anti-Virus Sophos Client Firewall
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
ESET	ESET Smart Security	Automatic	ESET Smart 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)
Avira GmbH	Avira AntiVir Premium	Detect only	Avira AntiVir Desktop
AVG Technologies	AVG Internet Security	Detect only	AVG 2011
Kaspersky Lab.	Kaspersky Antivirus	Detect only	Kaspersky Antivirus
Comodo Group	COMODO Internet Security 4.1, 5.8	Automatic	COMODO Internet Security

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 livePCSupport.

You have a choice of two installation files, 'CESM_BE_Setup_2.0.<version>.exe' or 'CESM_BE_Setup_2.0.<version>_Full.exe'

The '..._FULL.exe' file is a larger file that also contains additional, required software (.net Framework 4, SQL Server Compact 4.0 and Microsoft Report Viewer 10.0).

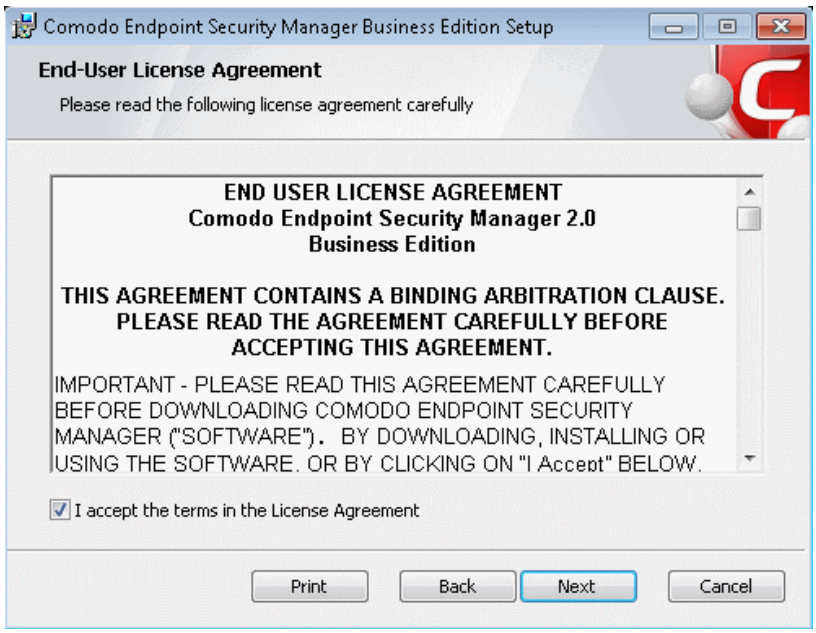
The other file does not contain this additional software but will download it from the Internet if it is not detected on your server.

To start the installation, double click on the setup file. The installer welcome screen will be displayed.

Click 'Next'.

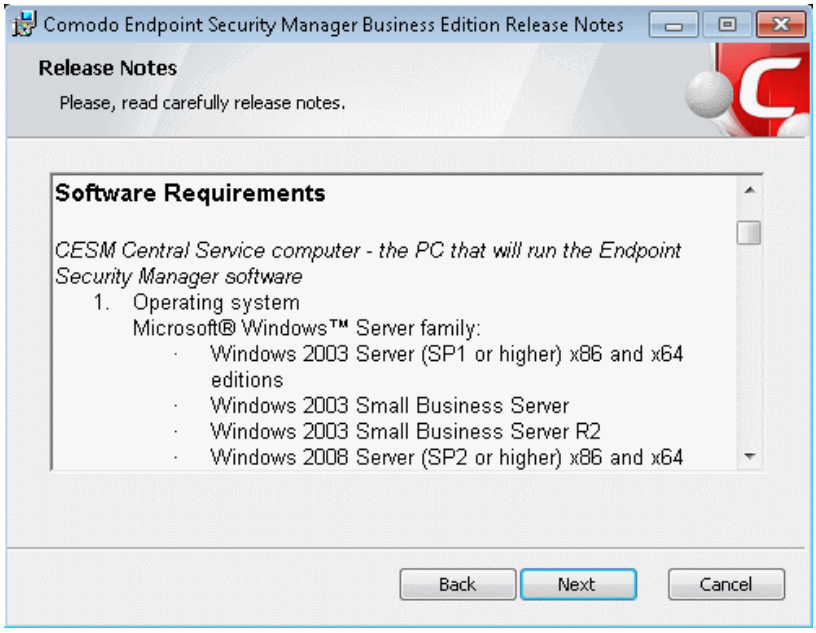
2. License Agreement

The End-User License Agreement will be displayed:



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

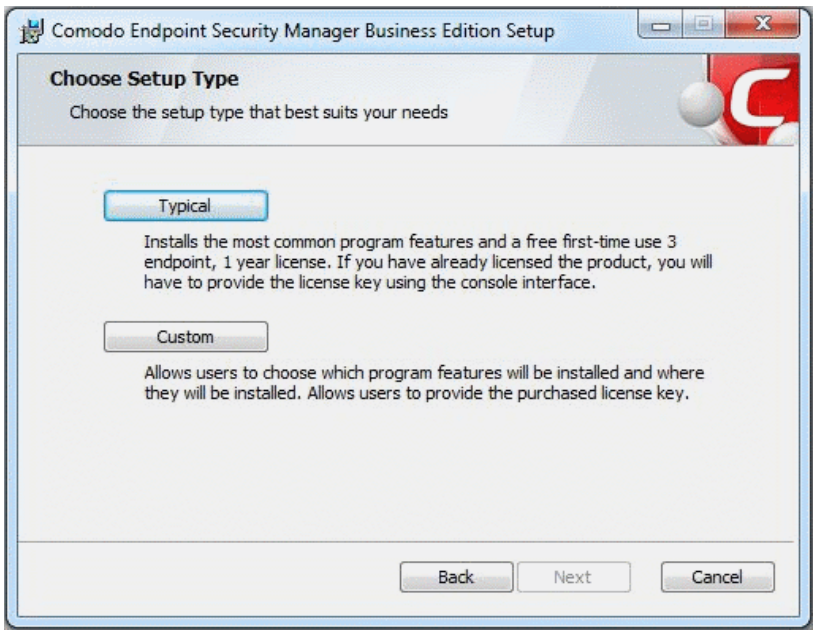
The release notes for the current version of CESM will be displayed.



Read the notes and click 'Next'.

3. Choosing Installation Preferences

The next stage is to choose the setup type:



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

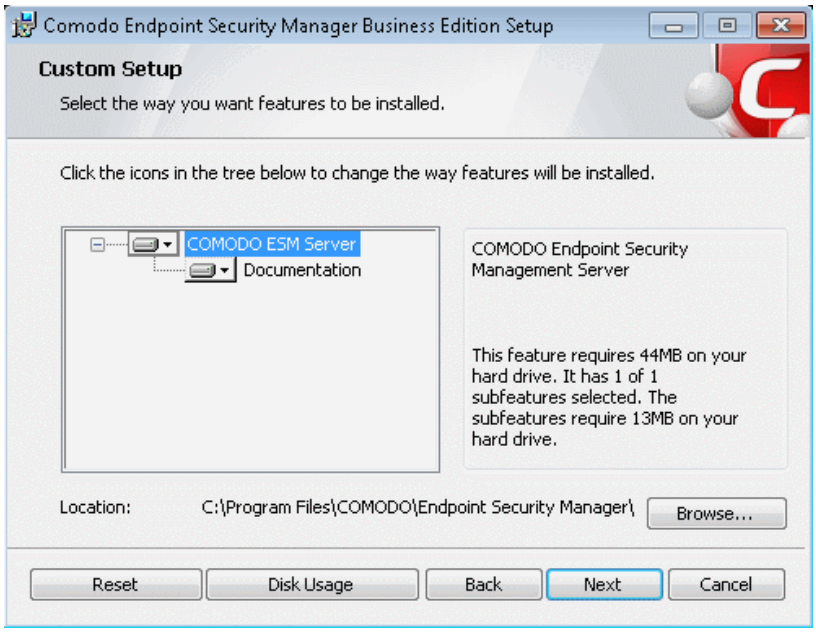
  On selecting 'Typical' and clicking 'Next', the setup progress will move to finalization.

Note: If you choose to install CESM BE in Typical mode, after installation the CESM server will automatically apply a free 3-endpoint/1 year first-time-use license. If you have already obtained a license key, it is best to use the Custom option; otherwise

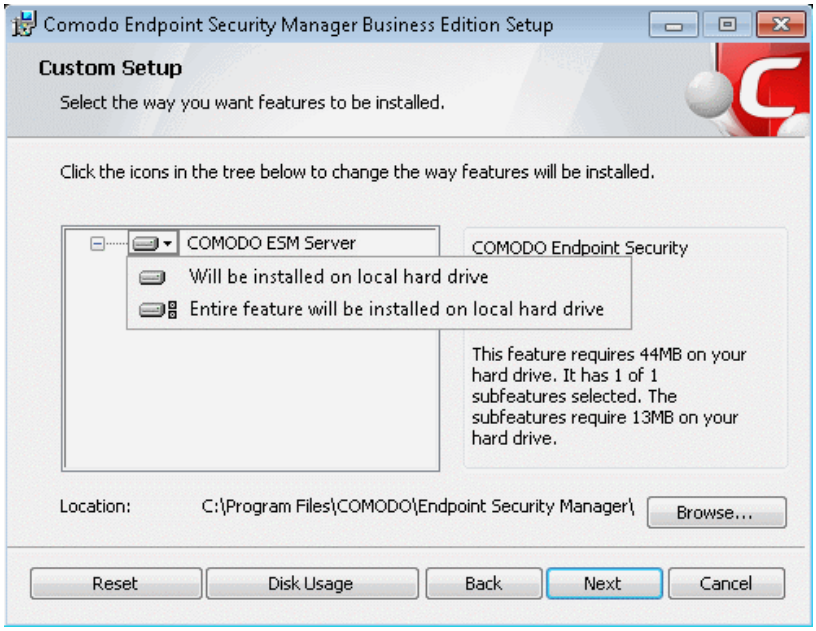
you will need to replace it and provide your license key by clicking the License tile in the Console interface.

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

Note: If you choose to install CESM BE in Custom mode, you will be prompted to provide a valid license key during setup. If you do not provide a key, the CESM server will automatically apply a free 3-endpoint/1 year first-time-use license.



Choose the components that you want to install.

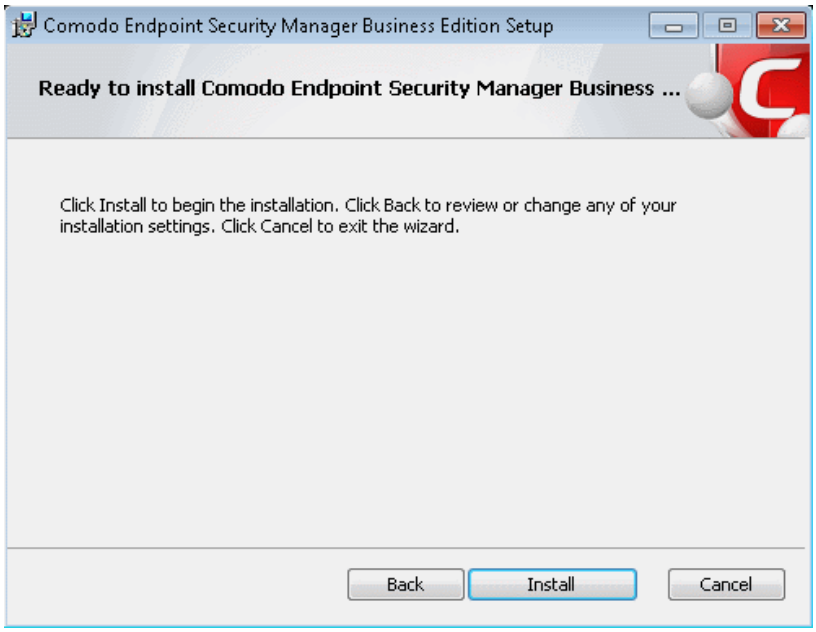


Custom Setup - Key	
Control	**Description**
	Icons with the ▼ symbol to the right are the currently selected installation option. Clicking this icon will open a menu allowing the user to select alternative installation options. These alternative installation options are explained in the next four rows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

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

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

Click 'Next' then 'Install' to begin the installation process.



4. Finalizing the Installation

Once installation is complete the finish dialog is displayed - offering admins the opportunity to either finish and exit the installer or finish and start the configuration tool.

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

  Click here for more details on CESM Configuration Tool.

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

Further reading:

Key Concepts - Definitions of key terms in CESM.

Quick Start Guide - Importing endpoints to central management.

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

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

1.4. Key Concepts

Endpoint - 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 Internet Security (CIS) 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 CIS, managed by the CESM central service.

Agent - A CESM agent is a client program to be installed on each and every managed endpoint for connection and communication to the CESM server. The agent is responsible for receiving tasks like applying security policy to CIS 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.

Policy - A policy is the security configuration of Comodo Internet Security (CIS) deployed on an endpoint or a group of endpoints. Each policy determines the antivirus settings, Internet access rights, firewall traffic filtering rules, sandbox configuration and Defense+ application control settings for an endpoint. For creating new policies, the administrator has to configure CIS at an endpoint in local mode and then import it as a policy into CESM. The imported policy can be applied to computer groups or individual endpoints as required. Although CESM cannot apply policy or run tasks like AV scans on an endpoint that is in 'local administration' mode, it can still fetch data from such machines for generating real time reports.

Local Mode - When an endpoint is in 'Local Mode', CIS settings are considered as being locally administered and CESM will not enforce (although it will continue to report on) policy compliance (the endpoint will continue to use the security configuration already in effect on that machine). Administrators should enable 'Local Mode' (or apply the 'Locally Configured' policy) and leave it in this mode while editing policy on the local machine using the endpoint's CIS interface. If returned to 'Remote Mode', CESM will automatically re-apply assigned policy overwriting administrator's change. While in 'Local Mode', the endpoint will continue to report connectivity and virus outbreak details.

Remote Mode - CESM can apply a security policy and can run tasks like AV scans and database updates only if CIS 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 CIS 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 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 CIS 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 CIS 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 CIS are installed automatically from the administrative console or manually at the endpoints using the 'Manage this Endpoint' feature of CIS 2012 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 Business Edition (CESM BE) then install and monitor installations of Comodo Internet Security (CIS) 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 Comodo Endpoint Security Manager Business Edition *(see* **Installing and Configuring the Service** *if you need more help with this)*

1. Download and run the CESM BE 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 and Windows Server 2003/2008.

   There is a choice of two setup files. The '..._FULL.exe' file contains all additional, required software (.net Framework 4, SQL Server compact 4.0 and Microsoft Report Viewer 10.0). 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 compact and Microsoft report viewer).
3. Select 'Typical' as the installation type for fastest setup experience; after installation you will need to provide a valid license key by clicking the License tile using the Console interface. 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.
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.

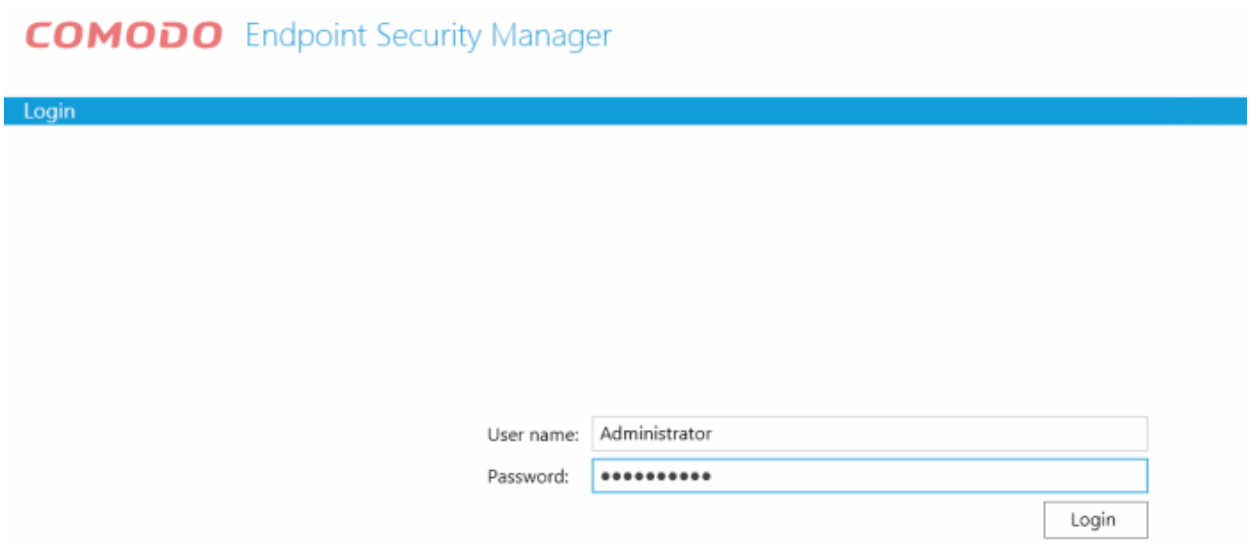
Step 2 - Login to the Admin Console *(see* **logging into the console** *if you need more help with this)*

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 user ID and password of the system that CESM was installed on to begin using your software.



3. To log out of the console, close the browser window or tab containing the console, or press the 'Refresh' button or click the 'Logout' link at the top right of the interface next to 'About' link.

Note on using the interface

The recommended navigational technique in the administrative console is to swipe the screen in the direction you wish to move as if you are 'dragging' the screen (for example, when you want to move onto the next step in a wizard, you can just drag the screen to the left).

'Swiping' is done by holding down the left mouse button in white space and dragging the mouse in the required direction. For example, if you wish to move onto the next step of a wizard, you would left click + hold then drag the mouse the left. If you wanted to move back to the previous step, left click + hold then drag the mouse to the right.

If you have a touch-sensitive screen then you can swipe between screens with your finger.

A third alternative is to click the circled black arrows at the top or plain arrows in the middle on the left and right of the interface.

For the best experience, use the browser in full-screen mode (click 'F11' on Internet Explorer).

Step 3 - Install Agents (and optionally Comodo Internet Security) on Target Machines

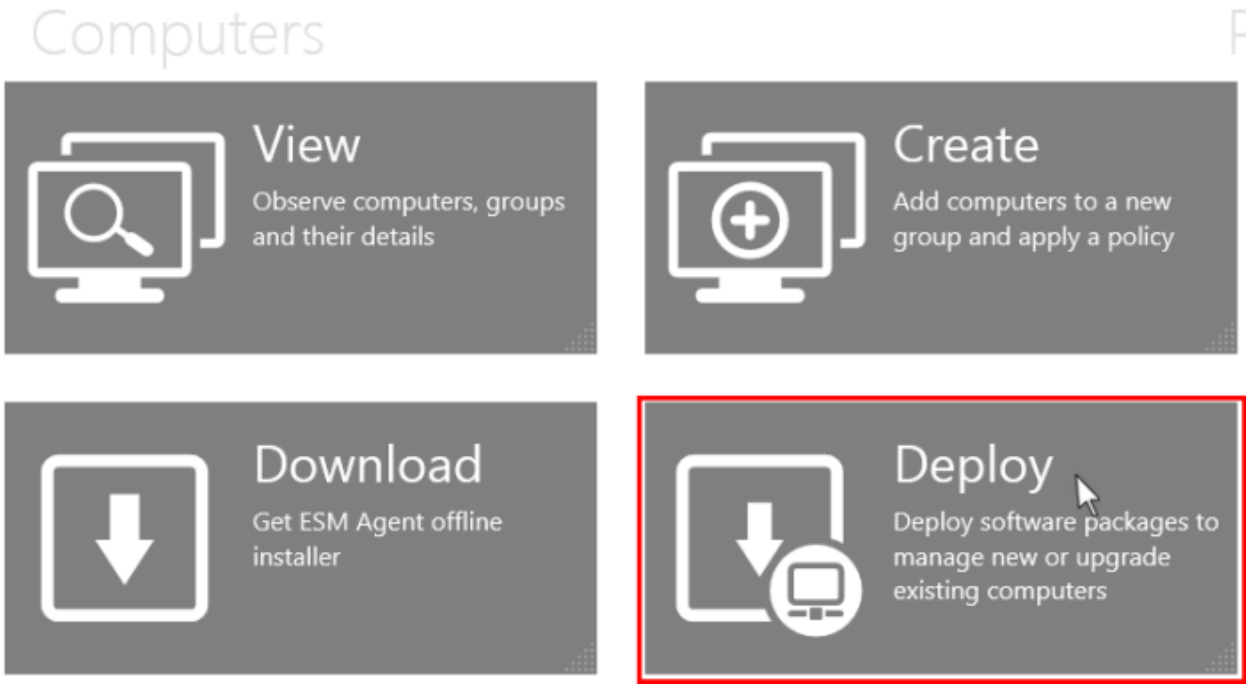
In order for CESM to centrally manage an endpoint, the endpoint must have two elements installed - (i) Comodo Internet Security software (ii) The CESM agent. The agent is a small piece of software that facilitates communication between the endpoint and the CESM server. The next stage of setup is to install this agent.

There are three methods to accomplish this:

- Remotely, using a console wizard to automatically push the agent and (optionally) CIS onto target machines. This wizard is started by clicking the 'Deploy' tile in the 'Computers' section of the console.
- Locally. You can install the agent and bring endpoints under central management by clicking the 'Manage this endpoint' link in the CIS interface. A walk-through using this method can be found at **How to Connect CIS to CESM at the Local Endpoint**.
- 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 CIS**.

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

1. Click 'Computers' in the top navigation (2nd link from the left) to open the 'Computers' area.
2. Click the 'Deploy' tile from the 'Computers' area to start the wizard (by default, the tile is positioned bottom right).



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 white 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 circled black arrows at the top or plain 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 '+' button to confirm your choice. Repeat until you have added all IP addresses or ranges that you wish to scan.

    Swipe left 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 Internet 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 CIS. 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 or19 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, machinename\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 CIS. You can also check for updates of these applications and download it in your server for deployment on to the end-points.

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

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

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

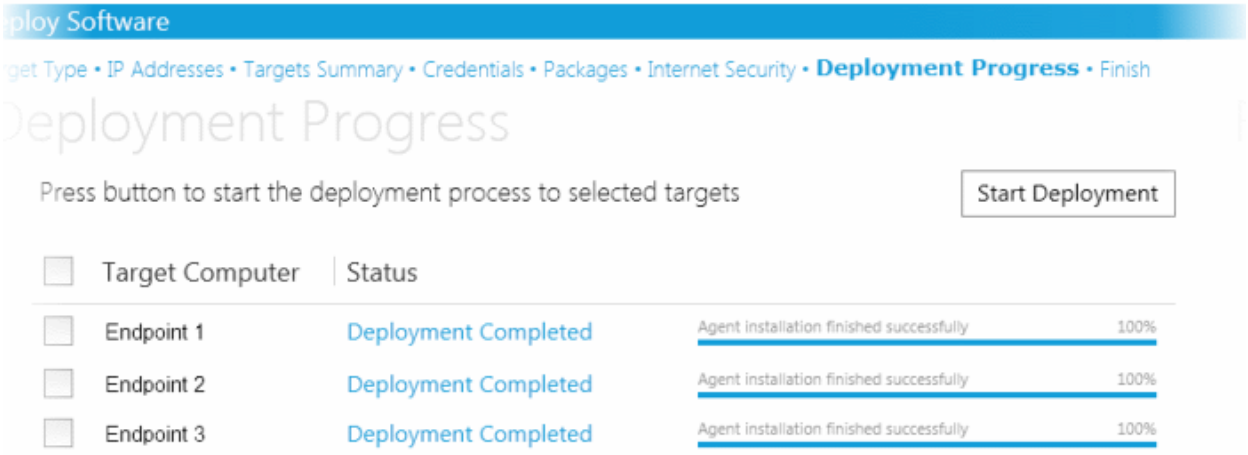
      (2) Choose components to install - Firewall, Antivirus or All Components.

      (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.

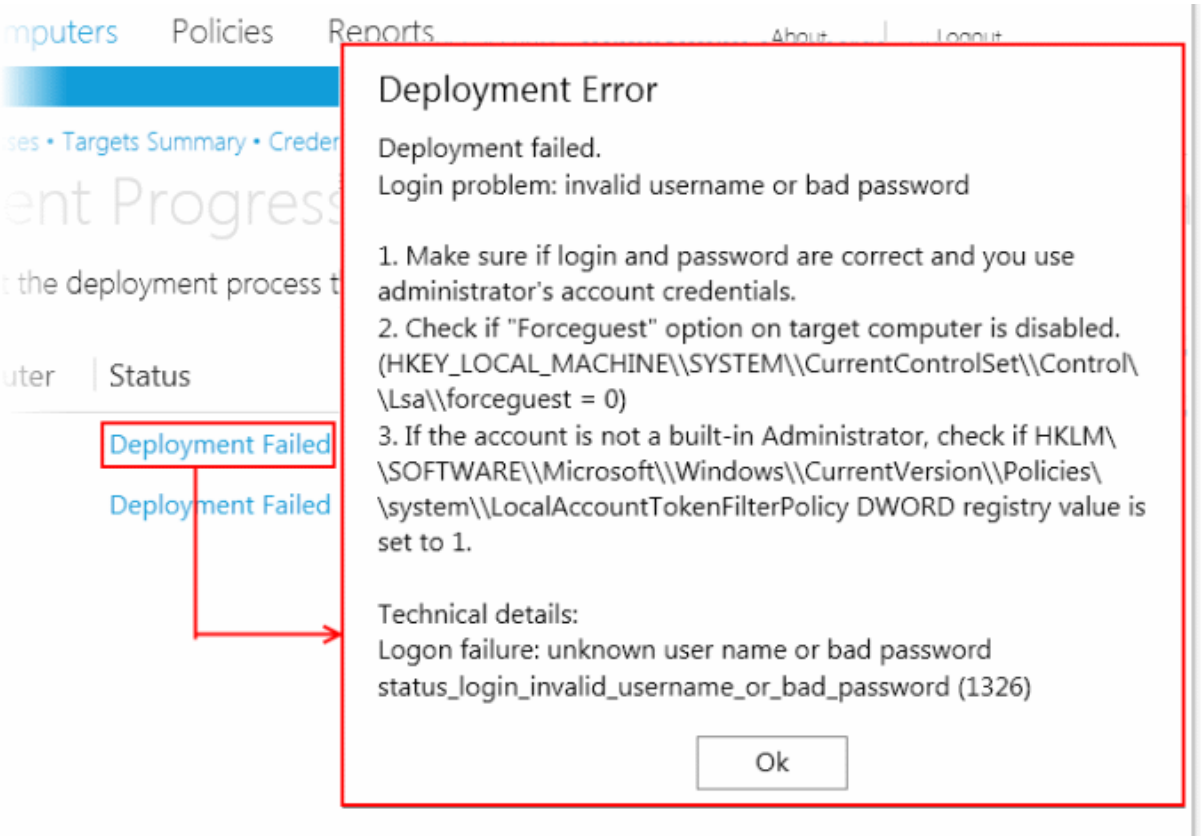
      (4) 'Uninstall all incompatible products' - Check this option to uninstall select third party antivirus, firewall and other desktop security software from the endpoints, prior to the installation of CIS. Performing this step will remove potentially incompatible products and thus enable CIS to operate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

    - To move onto the deployment stage, 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.



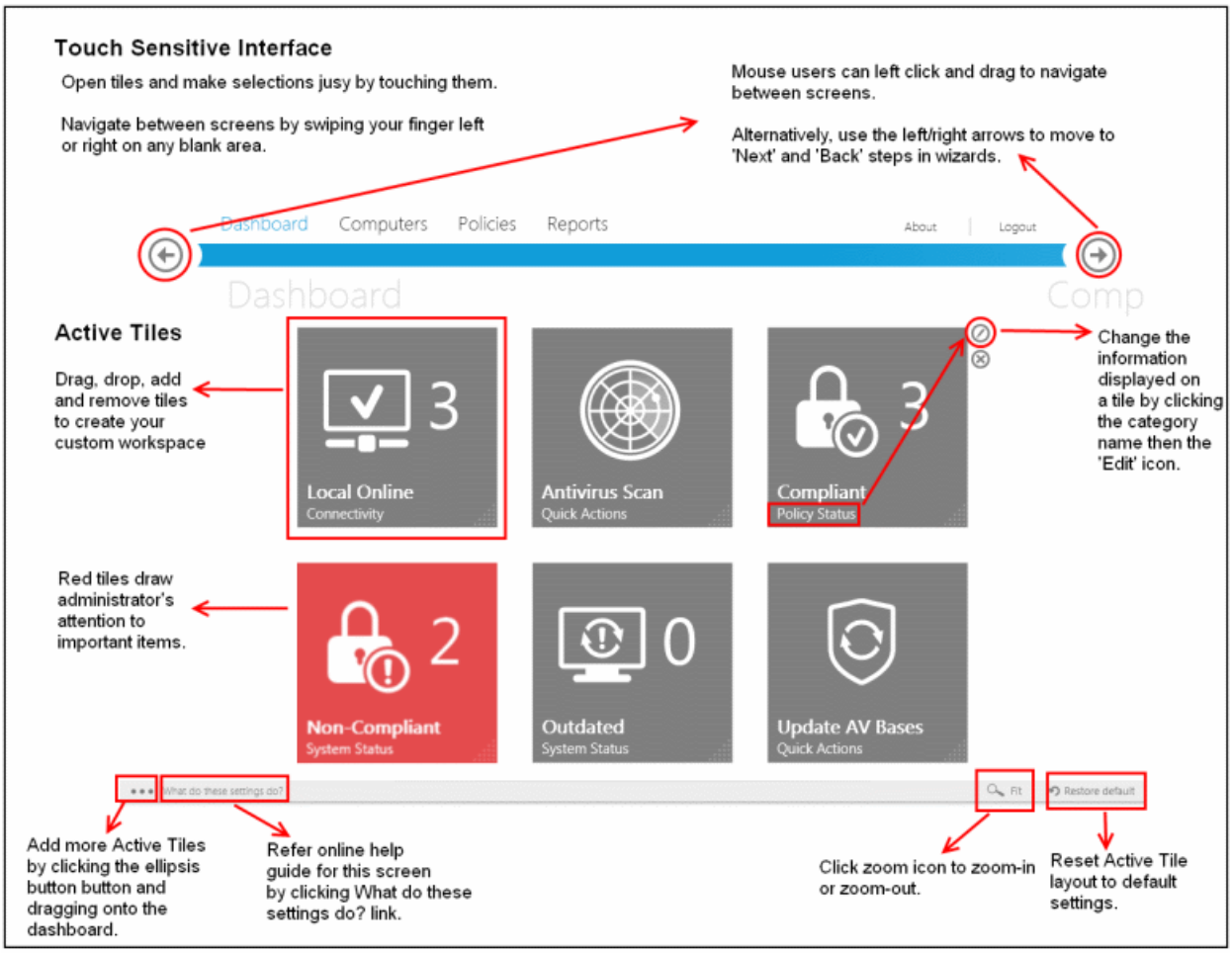
    - If deployment fails, click on the words 'Deployment Failed' to discover the reason. The info box also contains advice that may remediate the issue.



- 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 & CIS then those endpoints should now be reporting to CESM.

Step 4 - Check that target endpoints are reporting correctly

1. Click 'Dashboard' from the top navigation.
2. This will open CESM's dynamic control panel:



3. Tiles on the dashboard display real-time information regarding connectivity, virus outbreaks and security policy compliance. Other tiles allow you to quickly launch common tasks such as updating virus databases and running anti-virus scans. In this first instance, click the 'Local Online' and 'Non-reporting' tiles to check that the import process went according to plan.

    - After checking that all computers are reporting correctly, it is a good idea to make sure the latest virus databases are installed. Click the 'Update AV Bases' tile to begin this process.
    - After updating, we advise running a virus scan on all computers. Click the 'Antivirus Scan' tile 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 via the 'Malware Found' tile.
    - A full description of the dashboard interface. The meaning of each tile and how to add more tiles can be found in **The Dashboard Area**.
    - 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 CIS 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, click the 'Computers' link from the top navigation followed by the 'Create' tile. 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 Endpoint Groups' if you need help with this wizard. See 'The Computers 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 Internet Security (CIS) deployed on a group of endpoints. Each policy determines the antivirus settings, Internet access rights, firewall traffic filtering rules, sandbox configuration 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 CIS 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 CIS settings on the endpoint itself - either by physically sitting at the machine or by a remote connection. See How to Configure CIS Policies - An Introduction for general advice with this.
- 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, click 'Policies' then the 'Create' tile to start the policy import and deployment wizard. Select 'A computer' as source type then 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 Active Reports™

The reports area contains a wealth of valuable information for administrators. Each report is an 'Active Report' that allows admins to launch relevant tasks from within the report itself. Admins can also drill-down to individual endpoints from any report. Reports can be exported, printed and cover the following categories:

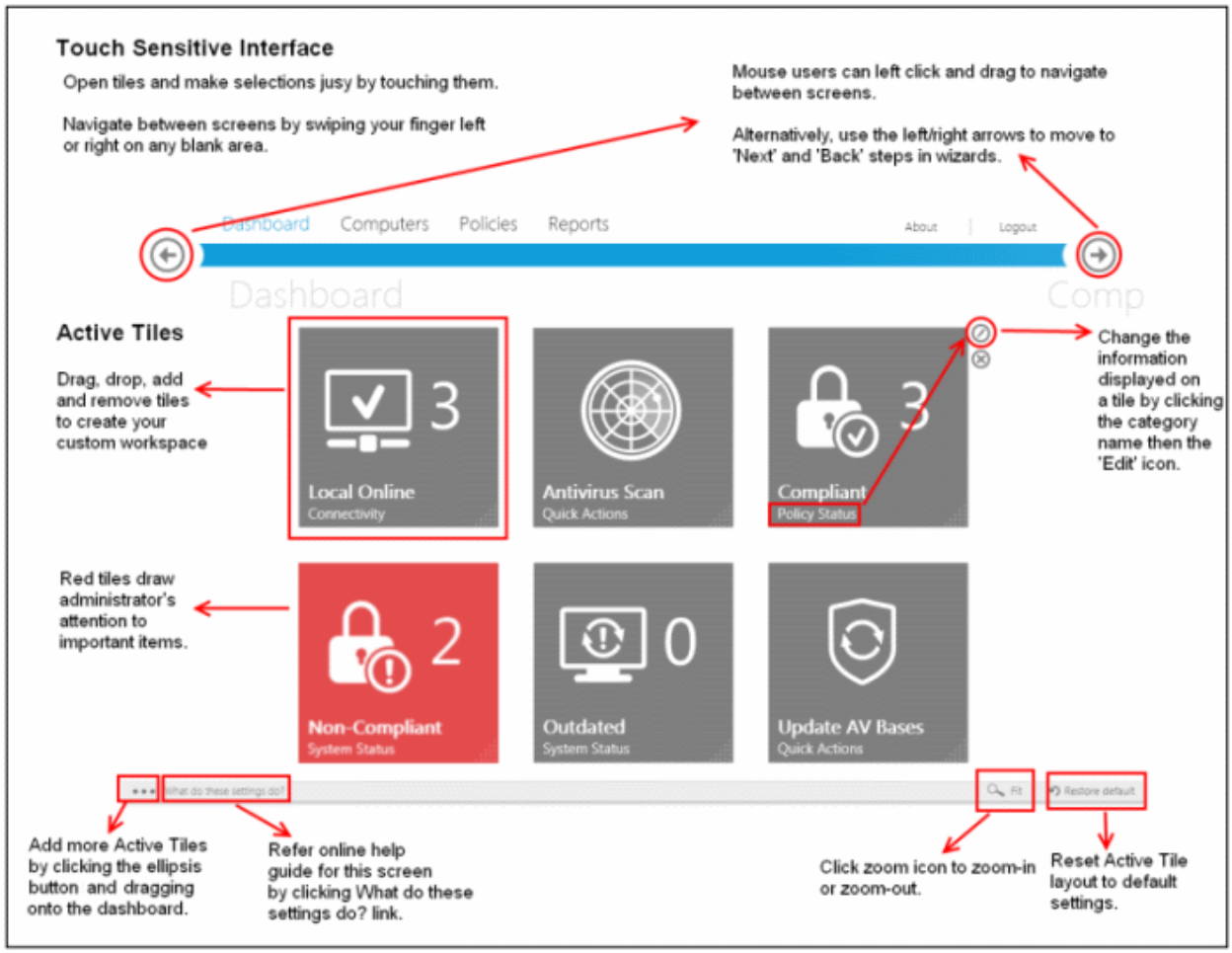
- Computer Details
- CIS Configuration
- Computer Infections
- Quarantined Items
- Antivirus Updates
- CIS Log
- Policy Compliance
- Policy Delta
- Malware Statistics
- Top 10 Malwares

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 main interface consists of four main areas that you navigate by clicking the title, swiping or clicking the left/right arrows - 'Dashboard', 'Computers', 'Policies' and 'Reports'- as well as additional functions in About and Logout and on the settings bar at the bottom of the interface. Within each area is a set of task-specific 'tiles' which provide fast access to the main functionality of the software. The following image shows the admin interface open at the 'Dashboard' area:



Main Functional Areas

- **Dashboard** - Provides a snapshot of the status of managed computers and serves as a launchpad for common tasks such as running antivirus scans and updates. Tiles on the dashboard can be reconfigured to display precisely the information an administrator finds most effective for their environment. Some tiles can also generate alerts for the administrator. See **The Dashboard Area** for more details.
- **Computers** - View, manage and add groups of computers. Specify policies on a per-computer or group basis. Download and deploy the CESM agent onto target computers 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 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.
- **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. Most reports are 'Active Reports™' and

allow administrators to initiate various tasks. See **The Reports Area** for more details.

- **About** - Allows administrators to view the current CESM version and a download link if any newer version of the application is available. It also provides the server information and license information. You can also upgrade the license in this screen. See '**About**' section for more details.
- **Logout** - Allows administrators to logout of the CESM Console.
- Settings Bar - Allows administrators to add Active Tiles™ to the dashboard area by clicking the ellipsis button and dragging to the dashboard. Refer to the section **Adding and Reconfiguring Tiles** for more details. The settings bar also allows the administrators to zoom-in or zoom-out and reset the Active Tile layout to default settings.

Note: Apart from swiping or dragging, you can also use the arrow keys at the right and left of the blue title bar to navigate through the areas. Reports and wizards having multiple pages or screens often display navigation arrows to the left and/or right of the main screen area that can be used in the same manner.

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 **machine**

  Use the following address convention to access the console

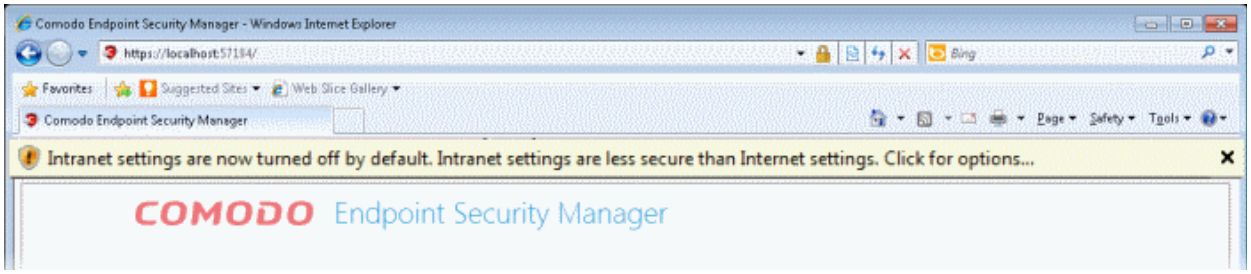
  https://<server hostname or IP address>:57194

  - 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

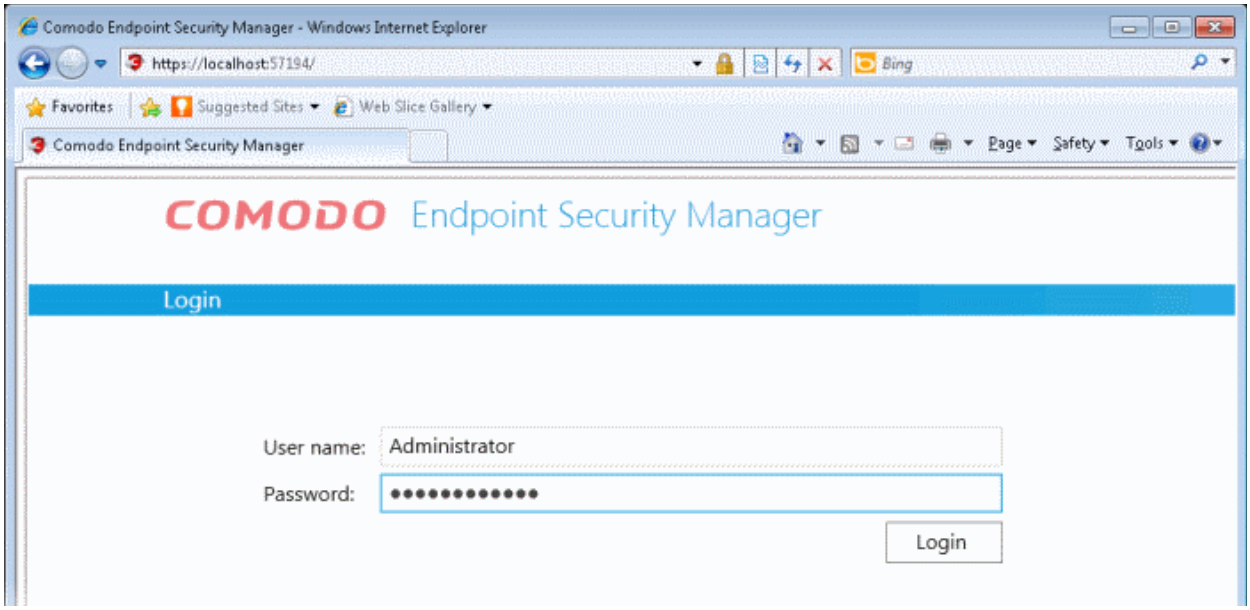
Note: If you receive a browser security error, you have not **installed an SSL certificate** from a Certification Authority. If you will not be installing a custom certificate, you can download the self-signed certificate in your browser by clicking 'Get server certificate' at the bottom of the login 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.

- If the console is opened for the first time from the server in which it is installed or any machine in the local network, Internet Explorer displays a warning message indicating that the Intranet Settings are disabled.



  - Performance-wise, CESM works fine with either Intranet or Internet settings. 'Internet settings' provide a more secure connection to the CESM server than 'Intranet settings' but, if the connection is within your internal network anyway, this may not be necessary. Click the alert bar if you wish to switch on 'Intranet settings'. Close the alert bar to keep 'Internet settings'.

- Login to the console using the Windows administrator user ID 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).



Next - **The Dashboard Area.**

2.2. The Dashboard Area

Active Tiles™ are classified according to category, with each category of tile capable of displaying multiple information types. **Tiles can be added or removed** according to your preference. See '**Default Tiles**' section below if you would like to see quick explanations of the tiles on the default layout.

Tile Categories:

- **Quick Actions** - Tiles that launch specific tasks. A 'Quick Action' tile can be configured to launch 'Antivirus Scan Action' or 'Update AV Bases' Action. Refer to '**Quick Actions Tile**' for more details.
- **Policy Status** - Tiles that display the compliance status of endpoints with their assigned CIS security policy. The specifics of each policy are set in the Comodo Internet Security software installed on a endpoint machine. Display options include 'Compliant', 'Non-compliant', 'Pending' or 'Show All'. Refer to **Policy Status Tile** for more details.
- **Updates** - Tiles that inform the admin how many endpoints are using the latest version of the antivirus database and how many need to be updated. Display options are 'Show Up to Date Endpoints Only', 'Show Outdated Endpoints Only', 'Show Unknown Endpoints Only' and 'Show All'. Refer to **Endpoint Updates Tile** for more details.
- **Infections** - Tiles that display the number of managed endpoints with a specific malware infection status. Infection statuses that can be shown on these tiles are 'Infected Endpoints', 'Not Infected Endpoints', 'Infection Status Unknown' or 'Show All'. Refer to **Endpoint Infections Tile** for more details.
- **Connectivity** - Tiles that display the number of managed endpoints with a specific connectivity status. Display options are 'Local Online Only' (managed computers on the local network), 'Internet Online Only' (managed computers connected to CESM over the Internet), 'Unknown Endpoints' (managed endpoints that have not checked in and have an unknown state) or 'Show All'. Refer to **Connectivity Tile** for more details.
- **Getting Started** - Tiles that display shortcuts to online help for common tasks and questions. Examples include 'How to Install CIS' and 'How to configure CIS policies. Refer to **Getting Started Tile** for more details.
- **System Status** - Tiles that display important network, virus and system information. System Status tiles can be configured to display:
  - # Malware Outbreaks - Informs you of a potential virus outbreak on your network by turning red and indicating the number of endpoints on which virus or malware was found within the defined threshold. See **Outbreak** configurable parameters on System Status Tile page for more details.
  - # Malware found - Displays the number of malware identified and not handled by the local CIS installation in the endpoint(s). See **Malware Found** configurable parameters on System Status Tile page for more details.
  - # Non-reporting endpoints - Displays the number of connected endpoints that do not report to the CESM console. See **Non-reporting** configurable parameters on System Status Tile page for more details.
  - # Non-compliant endpoints - Displays the number of connected endpoints that are not compliant with the CIS

policy applied to them. See Non-Complaint configurable parameters on System Status Tile page for more details.

- # Outdated Endpoints - Displays the number of connected endpoints which are currently using an outdated antivirus (AV) database. See Outdated configurable parameters on System Status Tile page for more details.
- License Information - Displays the number of days remaining for the license to expire. See Licensing details on System Status Tile page for more details.
- All of the above - Creates a tile that displays all possible 'System Status' information explained above. See System Status Tile Configurable Parameters table on System Status Tile page for more details. This tile will indicate by turning red and highlighting in bold the monitored settings have an active warning.

The administrator can add any number of System Status tiles to display information as required. Alternatively, a single tile can be set to display all information. Admins can configure any tile in this category to indicate a warning by turning red, which will also generate an email notification when configured. (for example, send a notification if malware is found on computer or send a notification when there is only 30 days remaining on the license). Refer to System Status Tile for more details.

- License Status - Displays a summary of license information (the number of endpoints covered and the expiry date). Refer to for more License Status Tile details.

Default Tiles: By default, ten tiles are displayed in the dashboard area. The following descriptions are for those default tiles. Administrators should note that each tile is capable of displaying multiple information types and that more tiles can be added as per requirements.

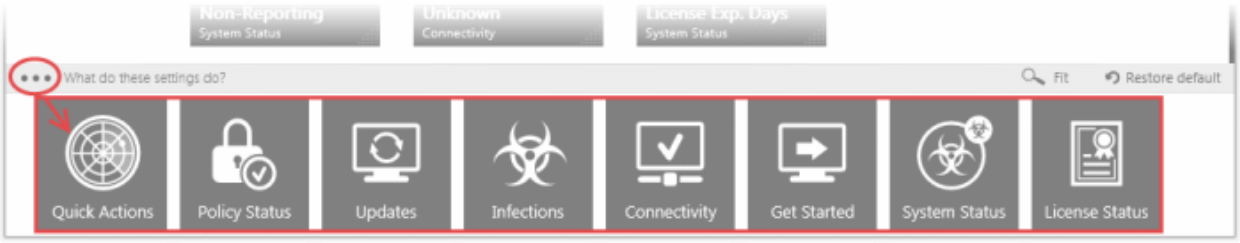
- **Local Online -** *('Connectivity' tile category)* Displays a summary of local network endpoints that are currently online and connected to CESM. Administrators can re-configure this tile to show only computers connected via the Internet, only show 'unknown' endpoints connected to CESM or elect to show all connected endpoints on a single tile. Admins can add more 'Connectivity' tiles if they wish to see, for example, 'Local', 'Internet' and 'All' connected machines on separate tiles.
- **Non-Compliant** - *('System Status' tile category)* Displays a summary of endpoints that are not compliant with their assigned security policy. The specifics of each policy are set in the Comodo Internet Security software and can be imported from one machine and applied to other machines. If the endpoint is in 'Remote Mode' then non-compliance is 'auto-corrected' by CESM as soon as it is detected (it will push the correct policy back onto the machine). If the endpoint is in 'Local Mode' then it will retain non-compliant status until the administrator switches back to remote mode. The endpoints applied with 'Locally Configured' policy will always be retained in Compliant status as CESM does not enforce any policy compliance on to them.
- **Getting Started -** *('Getting Started ' tile category)* Display shortcuts to online help for common tasks and questions. Examples include 'How to Install CIS' and 'How to configure CIS policies.
- **Malware Found** - *('System Status' tile category)* Displays the total number of viruses identified on all managed endpoints. 'Malware Found' shows number of malware discovered during the scans and not handled successfully (deleted, disinfected or quarantined) locally by CIS. The number will remain until next scan and clean on the affected computer(s). Clicking this tile will open a summary screen that lists the names of the malware found, the endpoints and the endpoints that were affected.
- **Antivirus Scan** – *('Quick Actions' tile category)* Launch an on-demand antivirus scan on selected computers or groups of computers. After clicking this tile the admin will be asked to choose target endpoints, choose a scan profile ('My Computer' or 'Critical Areas') before launching the scan.
- **Outdated** – *('System Status' tile category)* Displays the number of endpoints using an outdated virus signature database. Clicking this tile will open the antivirus updates report from which administrators can remotely update the relevant machines (the 'Update' button is along the bottom of the screen and will automatically update any and all outdated machines).
- **Update AV Bases** – *('Quick Actions' tile category)* Launches the update virus database wizard. After clicking the tile, admins will need to select which computers to update before initiating the update process.
- **Non-Reporting –** *('System Status' tile category)* Lists any managed endpoints that are failing to report to CESM. This may be because they are currently offline, because they no longer have CIS and/or the agent installed or because of a network error. CESM can only manage machines that report to it. Clicking this link will jump to the 'View All Computers' screen where offline computers can be reviewed.
- **Unknown -** *('Connectivity' tile category)* Lists the *number of* Unknown Endpoints' (managed endpoints that have not checked in and have an unknown state). Clicking this link will jump to the 'View All Computers' screen where unknown endpoints can be reviewed.
- **License Exp. Days –** *('License Status' tile category)* Displays the number of days remaining on the current license. Clicking this tile will display current license details. Swipe this screen to the right (or click the right hand navigation

arrow) to enter a new license key. Please see **How to Upgrade Your License** for more details.

Next - **Adding and Re-configuring Tiles**

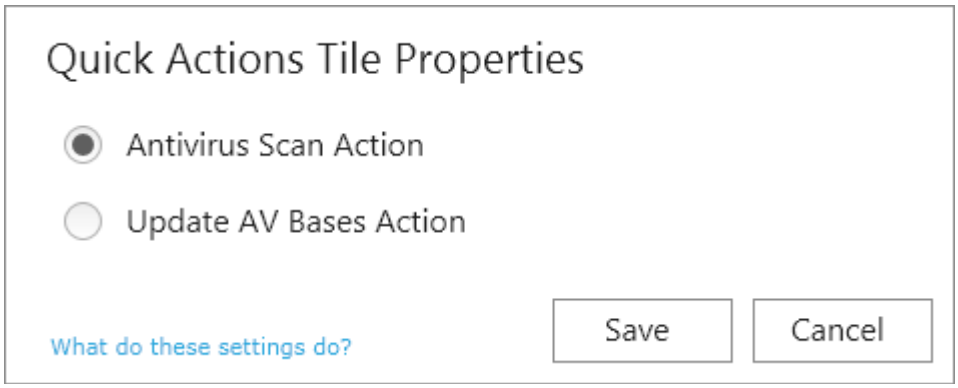
2.2.1. Adding and Re-configuring Tiles

Active Tiles™ can be added to your dashboard by clicking the ellipsis button at the left of the settings bar then dragging the required category tile up into the main workspace. The new tile will then display the properties dialog, allowing the administrator to choose its information and behavior. See the sections that follow for available settings for each category tile.



Once added to the interface, any tile can be reconfigured to display specific information by clicking or tapping the lower edge of the tile below the category name at the bottom of the tile then clicking the 'Edit' icon. The following image shows the 'Quick Actions' tile.

- Clicking will open a dialog that allows the admin to choose the type of information that should be displayed. In this case, a 'Quick Actions' tile is capable of launching antivirus scans or updating virus databases. If the admin wants both capabilities to be available, then they should drag two 'Quick Actions' tiles onto the dashboard and configure each for different actions.



- Clicking will remove the tile from the dashboard.

2.2.1.1. Quick Actions Tiles

The Quick Action category of tiles enables administrators to launch common and important tasks on managed endpoints.

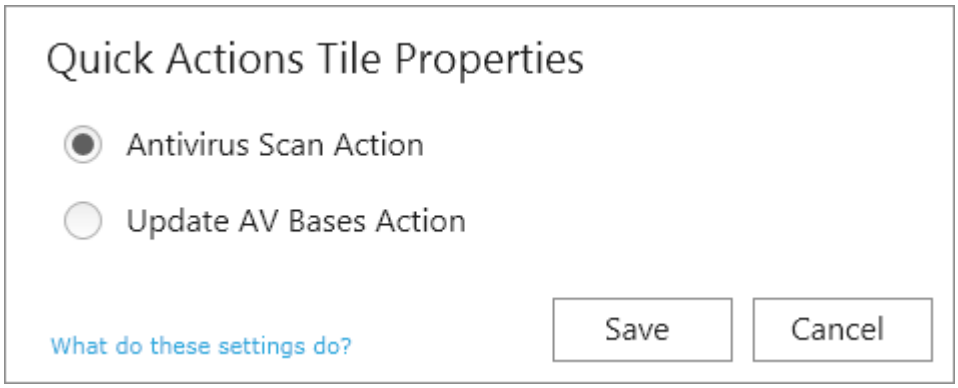
Tasks that can be assigned to a Quick Action tile are:

- **Antivirus Scan Action** - Launches the 'Run a Scan Wizard' when clicked. After clicking this tile, admins should select the target machines and scan profile ('My Computer' or 'Critical Areas'). The results of the scan can be viewed by clicking the 'Computer Infections' tile from the 'Reports' area and selecting the endpoints. See **Running An Antivirus Scan on Muliple Endpoints** for a quick tutorial.
- **Update AV Bases Action** - Updates the AV database on selected computers. Clicking this tile will open the Update Bases Wizard where the admin can select which machines should be updated before clicking 'Finish' to launch the update process. Refer to the section **Updating AV databases** if more details are required.

Adding a Quick Action tile

1. Click the ellipsis button at the bottom left of the settings bar.
2. Drag the Quick Action tile into the dashboard.

The 'Quick Actions Tile Properties' dialog will appear.



3. Choose the type of action you want to see on the tile at the properties dialog.

You can add as many Quick Action tiles as as you wish for different actions.

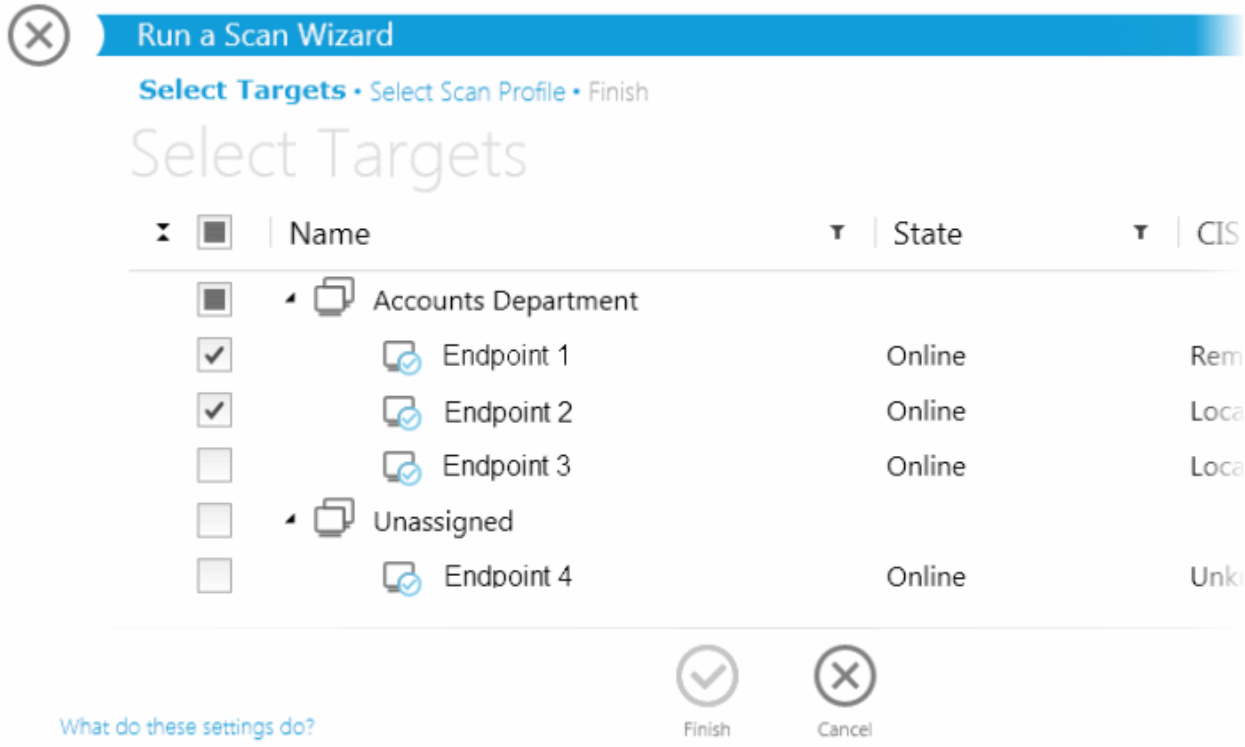
To change the type of information displayed in the Quick Actions tile, click the words 'Quick Actions' at the bottom of the tile then the icon: . To remove the tile, click the icon :

Running An Antivirus Scan on Multiple Endpoints

Clicking the Antivirus Scan tile will open step 1 of the scanning wizard. The remaining steps are displayed below the blue title bar with the current step highlighted in blue. To move backwards or forwards between steps, use the arrows on either side of the title bar (or left click and drag to swipe the screens left or right).

Step 1 - Select Targets

- Choose the endpoints on which you wish to run the antivirus scan by selecting the check boxes beside them. Selecting a group name selects all the endpoints in the group.



- Clicking the icon displays only the groups. Click it once again to display all the endpoints in the groups.
- Click the filter icon in the 'Name; column header to search for a particular endpoint.
- Click the filter icon in the 'State' column header to search for endpoints that are in online mode.
- Click the right arrow to confirm your selection and move to the next step.

Step 2 - Select Scan Profile

The 'Scan Profile' defines the areas and folders to be scanned in the endpoints.

- **My Computer** - All drives on the endpoint will be scanned.
- **Critical Areas** - Only "Windows", "Program Files" and "Document and Settings" folders on the endpoints operating system drive will be scanned.

Click the profile you wish to execute then click the right arrow to move to the next step.

Step 3 - Run the Scan

If the selections made in the previous steps need to be re-checked or modified, the administrator can go back by clicking the left arrow.

- Once satisfied with your settings, click the Finish icon (or swipe left) to begin the scanning process.

The wizard will then move to the 'View All Computers' screen which will display scan progress beneath the name of the target computers. This screen can be accessed at any time by clicking 'Computers' then the 'View All Computers' tile.

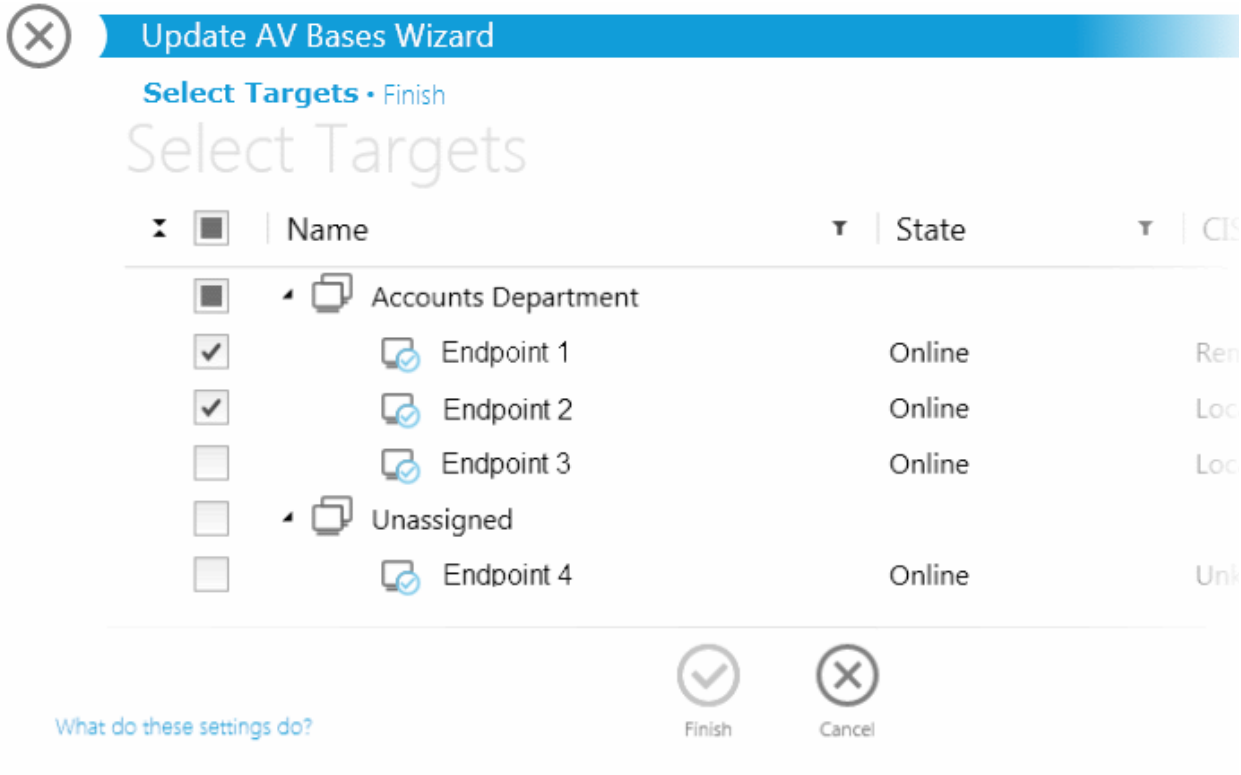
- If malware is discovered during the scan that is not handled (deleted, disinfected or quarantined) then the 'Malware Found' and/or 'Infections' tiles on the dashboard will turn red (as appropriate) and display the number of samples and/or affected endpoints. Malware that is successfully dealt with will not show on the 'Malware Found' tile.
- Admins can elect to receive email notifications upon malware discovery. Email notifications are set up by editing the"Malware Found' tile:
  - Click 'Dashboard' and locate the 'Malware Found' tile. Click the words 'System Status' at the bottom of the tile.
  - Click the 'Edit' icon to open the properties dialog. Enable the 'Send Email Notifications' checkbox (make sure 'Malware Found' is displayed in the drop down box).
- The results of the scan can be viewed as an 'Infection report' from the 'Reports' area - click 'Reports' then the 'Computer Infections' tile. 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.

Updating AV databases

Clicking the Update AV Bases tile will start the 'Update AV Bases' wizard.

- Choose the endpoints on which the antivirus signature database has to be updated by selecting the check boxes beside them. Selecting the checkbox beside a group name selects all the endpoints in the group.



- Click the Finish icon to start the update process in the endpoints.

The administrator can confirm the update process by clicking the "View All Computers' tile (click 'Computers' then 'View All Computers').

2.2.1.2. Policy Status Tile

The 'Policy Status' tile displays the status of endpoint compliance with their assigned CIS security policy.

Policy Status Tile with all the information

Policy Status Tile with selected information

The specifics of each policy manage the settings in the Comodo Internet Security software installed on an endpoint. Policies can be created in a number of ways - including importing directly from an existing configuration of CIS on a specific endpoint. Once imported, policies can be quickly rolled out to other endpoints or groups of endpoints. A policy can be applied to a machine that is in either 'Remote Mode' or 'Local Mode'. If the endpoint is in 'Remote Mode' then policy non-compliance is 'auto-corrected' by CESM as soon as it is detected (it will push the correct policy back onto the machine). If the endpoint is in 'Local Mode' then it

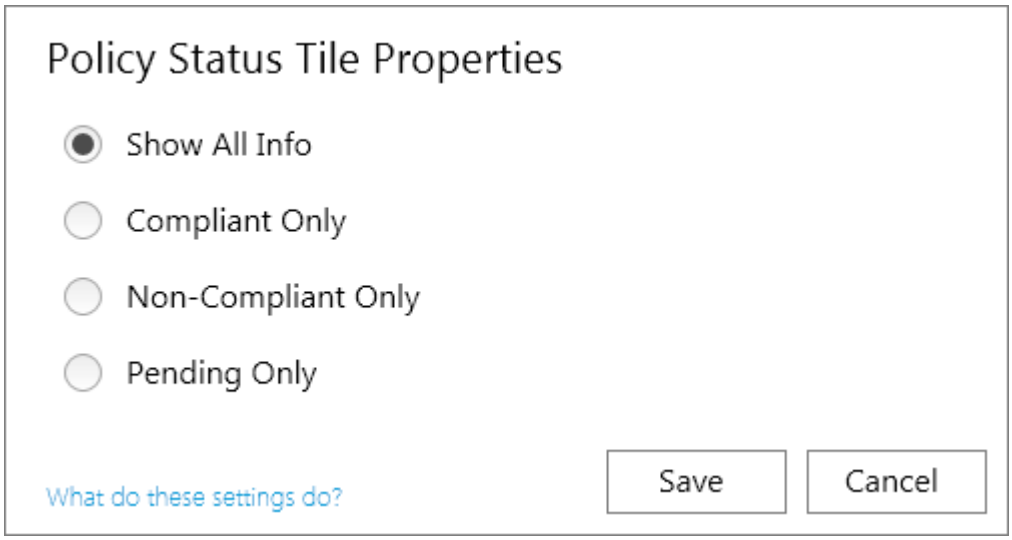
will retain non-compliant status until the administrator switches to remote mode.

The Policy Status tile can be configured to display the number of endpoints that are 'Compliant', 'Non-compliant', 'Pending (analysis)' or can show all types.

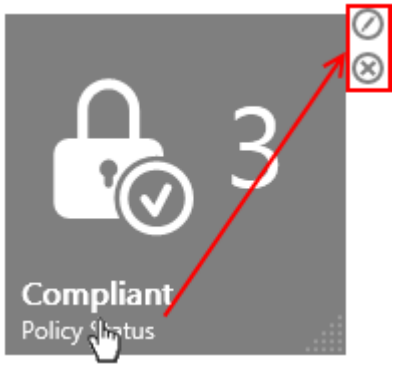
- Clicking the 'Policy Status' tile will open a detailed Policy Compliance report. This provides an overview of compliance status of selected endpoints. See **Policy Compliance Report** for more details.
- If you wish to view the specific reasons that an endpoint fell out of compliance, please run a '**Policy Delta**' report.
- Policies are discussed in more detail in the '**Policies**' chapter. Click the following links to go to the section you would like help with:
  - **Policy Overview and Key concepts**
  - **How to create and deploy a policy**
  - **How to view and modify policies**

Adding a Policy Status Tile

1. Click the ellipsis button at the bottom left of the interface.
2. Drag the 'Policy Status' tile into the dashboard. The 'Policy Status Tile Properties' dialog will appear.



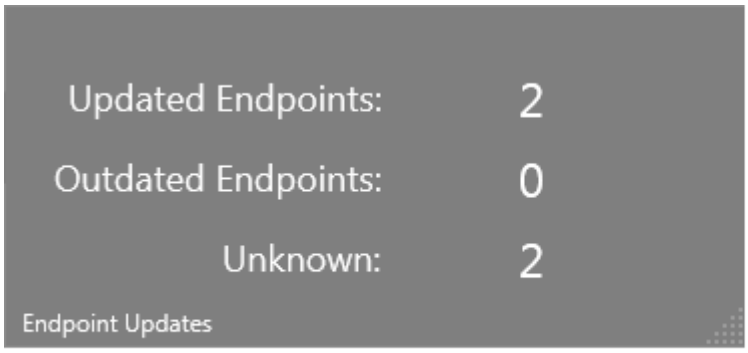
3. Choose the type of information you want to be displayed in the tile from the Properties dialog and click 'Save' The new tile will be added to the dashboard area. You can add as many Policy Action tiles as as you wish for the information you wish to see in the dashboard.
4. To change the type of information displayed in the Policy Status tile, click the words 'Policy Status' at the bottom of the tile then the icon: . To remove the tile, click the icon:



2.2.1.3. Endpoint Updates Tile

Displays a summary of endpoints that are updated, outdated or unknown. The tile can configured to display:

- **Updated Endpoints Only** - Displays number of endpoints that have up-to-date AV database
- **Outdated Endpoints Only** - Displays number of endpoints whose AV database is outdated and needs to be updated
- **Unknown Endpoints Only** - Displays the number of endpoints for which database information is not available
- **Show All Info** - Displays all of the above on a single tile



Endpoint Updates Tile with all information

Endpoint Updates Tile with selected information

Tiles will turn red if CESM detects endpoints that are using old databases. The administrator can add any number of Updates tiles, each showing different information as required.

- Clicking the 'Outdated' Endpoint Updates tile opens the Antivirus Updates Report which shows the update status of all endpoints. The Antivirus Updates Report can also be generated by clicking the '**Antivirus Updates**' tile in the '**Reports**' area. Refer to **Antivirus Updates Report** for more details.

- To update outdated computers, please use one of the following methods:
  - Click the 'Endpoint Updates' tile on the dashboard to open the AV Update Report'
  - Click the 'Update' icon at the bottom of this report to initiate an update task on all outdated computer

    OR

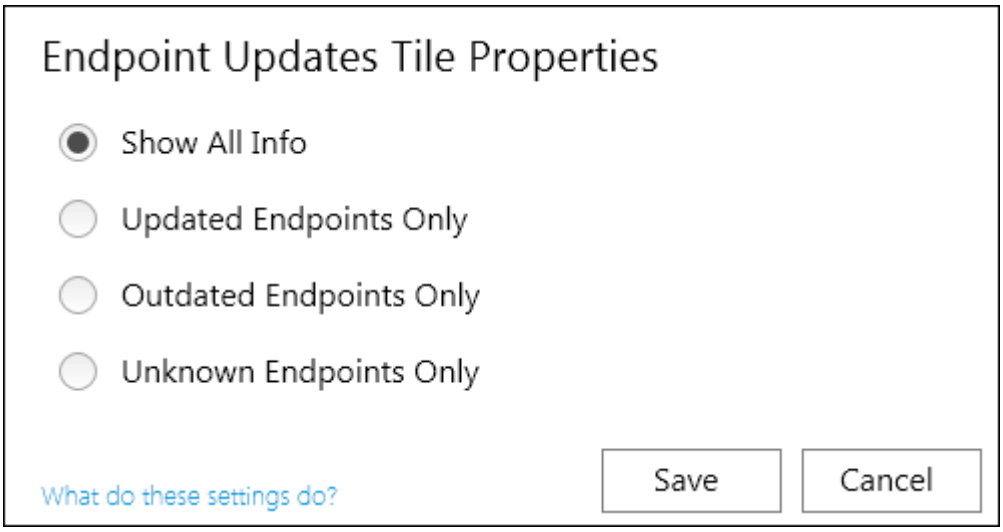
  - Click 'Computers' > 'View ' tile
  - Select the required computers and click 'Update AV' at the bottom of the interface to initiate an update task on the selected computers

    OR

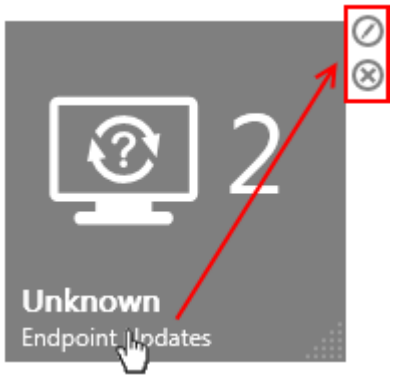
  - Click 'Reports' > 'Updates' tile
  - Choose target computers and click 'Finish' to launch the report
  - Click the 'Update' icon at the bottom of this report to initiate an update task on all outdated computers

Adding an Endpoint Updates Tile

1. Click the ellipsis button at the bottom left of the settings bar.
2. Drag the 'Updates' tile into the dashboard. The 'Endpoint Updates Tile Properties' dialog will appear.



3. Select the information to be displayed as per your requirement in the properties tile and click 'Save'. The new tile will be added to the dashboard area. You can add as many 'Updates' tiles as as you wish for the information you wish to see in the dashboard.
4. To change the type of information for a particular tile, click the words 'Endpoint Updates' at the bottom of the tile then the icon: . To remove the tile, click the icon: .



2.2.1.4. Endpoint Infections Tile

Displays the number of endpoints on which malware was detected to be present. If no malware is detected then the tile is gray colored but will turn red if malware is found. The tile can be configured to display the number of 'Infected Endpoints', 'Not Infected Endpoints', 'Infection Status Unknown' and all data.

Endpoint Infections Tile with all information

Endpoint Infections Tile with selected information

- 'Infections' refers to malware that has been detected but not 'handled' by Comodo Internet Security (it has not been

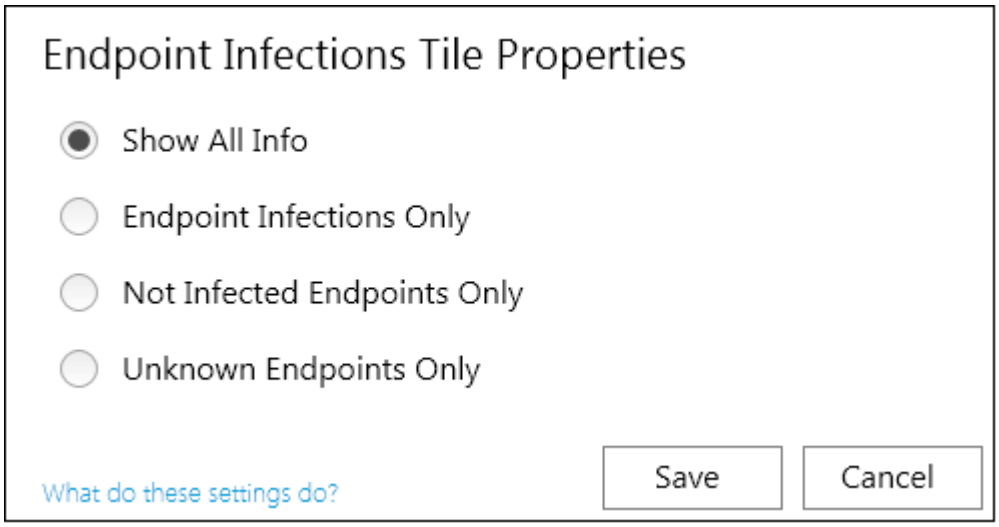
deleted, disinfected or quarantined and is still located on the endpoint). If the malware was handled successfully by CIS then it will *not* show on this tile.

- Administrators are advised to immediately investigate machines currently shown as hosting malware. Comodo Internet Security can be used to manually quarantine suspicious files if automatic quarantine is not enabled.

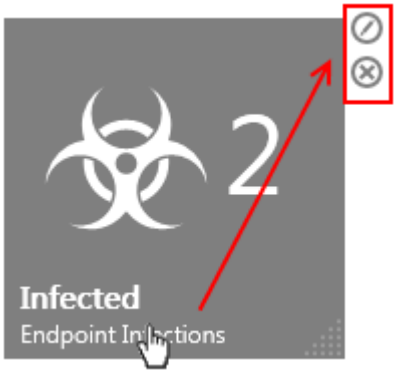
  Alternatively, the application can be used to clean and disinfect the malware at the affected machine.
- Clicking the 'Endpoint Infections' tile will open the 'Computer Infections Report' which lists the endpoints affected along with the name and location of the malware. From here, admins can run an on-demand AV scan on selected computers. Refer to **Computer Infections Report** for more details.

Adding an Endpoint Infections Tile

1. Click the ellipsis button on the settings bar at the bottom left of the interface.
2. Drag the 'Infections' tile into the dashboard. The 'Endpoint Infections Tile Properties' dialog will appear.



3. Select the information to be displayed as per your requirement in the properties tile and click 'Save'. The new tile will be added to the dashboard area. You can add as many 'Endpoint Infections' tiles as as you wish for the information you wish to see in the dashboard.
4. To change the type of displayed information for a particular tile, click the words 'Endpoint Infections' at the bottom of the tile then the icon: . To remove the tile, click the icon: .



2.2.1.5. Connectivity Tile

The Connectivity tile displays of the number of endpoints that are currently online and can be controlled through the CESM console.

The tile can be configured to display:

- 'Local Online' - endpoints connected through the local network
- 'Internet Online' - endpoints connected through the Internet
- 'Unknown' - managed endpoints that are not currently in a known policy state that can be determined by CESM
- All of the above on a single tile

Connectivity Tile with all information

Connectivity Tile with selected information

As with all dashboard tiles, administrators can add as many connectivity tiles as they wish.

Clicking a connectivity tile will open the 'View All Computers' interface. From this screen, admins can:

- View an overall summary of details pertaining to computers on the network - including security policy, online/offline status and CIS mode (locally administrated or Remote administrated)

  See Viewing Endpoints for an overview of the information available from the 'View All Computers' interface.

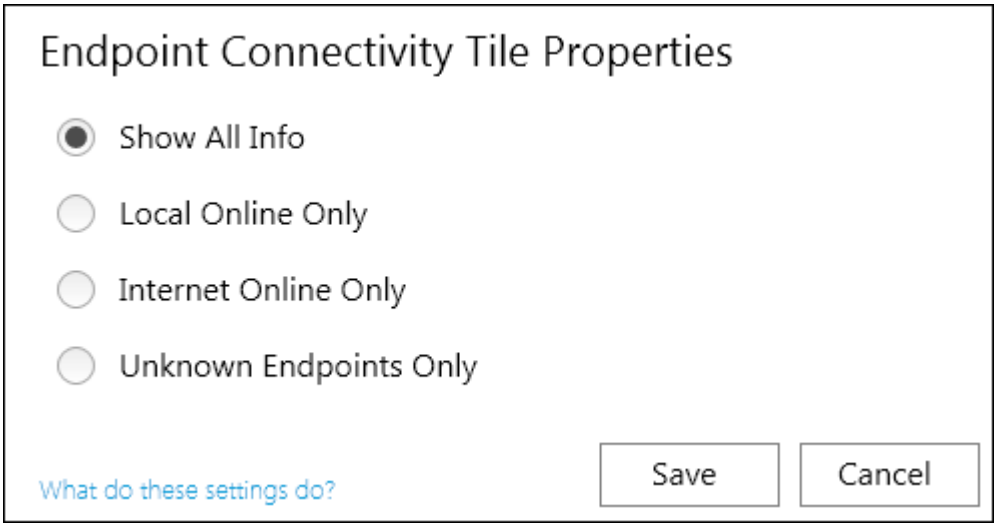
- Launch various tasks such as creating a new computer group and running AV scans or database updates on selected computers

  Click Here for a list and explanation of the tasks that can be launched from the 'View All Computers' interface.

Tip: The View All Computers interface can also be opened by clicking the 'View ' tile in the 'Computers' area.

Adding a Connectivity Tile

1. Click the ellipsis button on the settings bar at the lower left of the interface.
2. Drag the 'Connectivity' tile into the dashboard. The 'Endpoint Connectivity Tile Properties' dialog will appear.



3. Select the information to be displayed as per your requirement in the properties tile and click 'Save'. The new tile will

be added to the dashboard area. You can add as many 'Connectivity' tiles as as you wish for the information you wish to see in the dashboard.

4. To change the type of displayed information for a particular tile, click the words 'Connectivity' at the bottom of the tile then the icon: . To remove the tile, click the icon: .

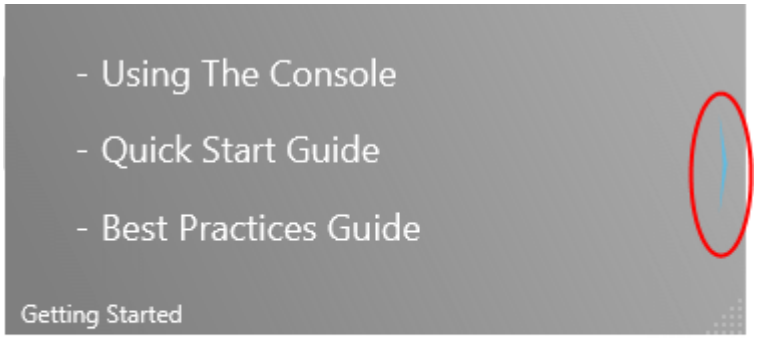
2.2.1.6. Getting Started Tile

The 'Getting Started' tile provides handy links for new CESM Business Edition administrators to Help Guide pages which contain guidance on common tasks.

- Using the administrative console
- Quick start guide
- Best practices guide
- How to connect Comodo Internet Security (CIS) to CESM at the local endpoint
- How to setup external access from the Internet
- How to Install CIS
- How to configure CIS policies

Adding Getting Started Tile

1. Click the ellipsis button on the settings bar at the lower left of the interface.
2. Drag the 'Getting Started' tile into the dashboard.



Getting Started Tile with all the links
Clicking a link opens the respective help page in the online help guide

3. Click the right or left arrows to navigate for more help links. The arrow will turn blue in color when the mouse cursor is placed over it.

2.2.1.7. System Status Tile

The 'System Status' tiles provide real time updates on critical network security data.

There are six types of 'System Status' tile:

- 'Outbreaks'- # of endpoints affected by malware within a threshold that indicates a potential virus outbreak
- 'Malware Found' - # managed computers with unhandled malware detections
- 'Non - reporting' - # of computers not reporting to CESM
- 'Non- compliant' - # computers that are not compliant with their assigned security policy
- 'Outdated' - # computers whose antivirus (AV) database is outdated
- 'Licensing' - # Number of days remaining on current license

System Status Tile (Normal)

System Status Tile (Alerting)

System Status Tile with all information

System Status Tile with selected information

Each tile will turn red as a warning if certain thresholds are exceeded. For example, if the number of non-compliant computers is greater than the defined values (default = 1).

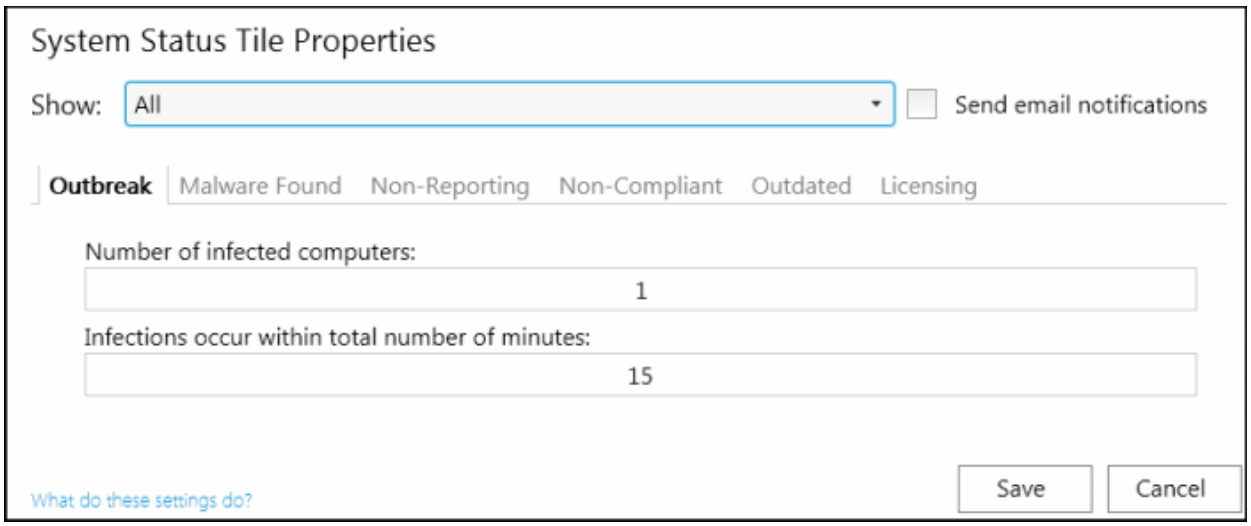
When you drag a system status tile onto the dashboard (See '**Adding a System Status** Tile') you will be asked to:

- Choose the type of tile (select from the list of six types described above. Alternatively, select 'All').
- Specify an alert threshold number. The parameters of the threshold will vary depending on the type of tile. If the threshold is exceeded then the tile will turn red.
- Optional - specify that an email notification is sent **should** the threshold be reached.

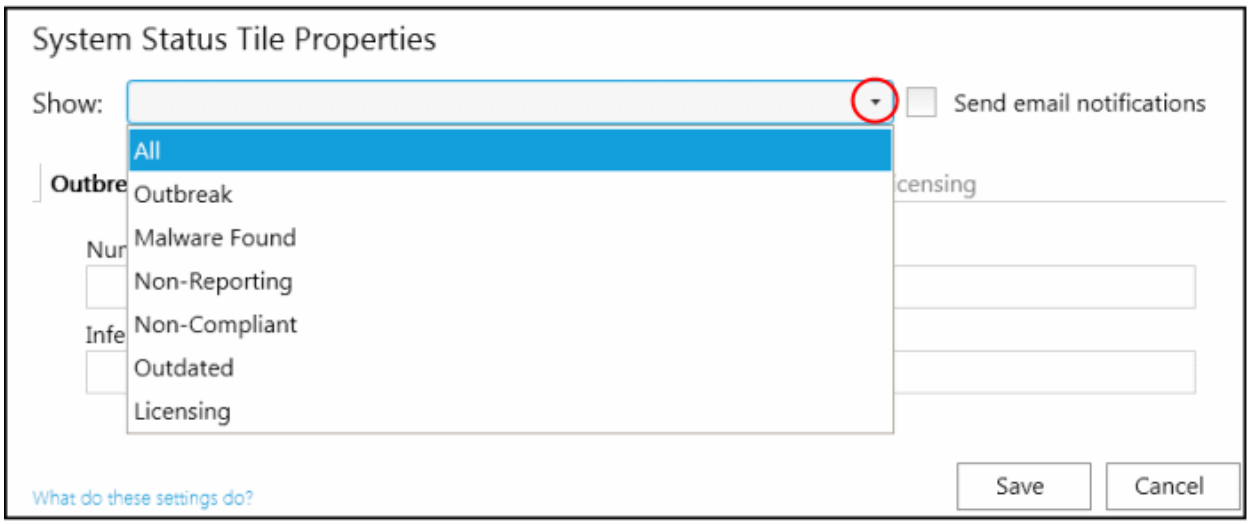
The next section explains how to add a system status tile; contains a **table that describes each tile and what happens when you click each tile** and concludes with a quick example showing how to configure a system status tile.

Adding a System Status Tile

1. Click the ellipsis button on the settings bar at the lower left of the interface.
2. Drag the 'System Status' tile into the dashboard. The 'System Status Tile Properties' dialog will appear.



3. Select the information to be displayed in the new tile from the 'Show:' drop-down.



Since the System Status tile also serves as an alert to indicate the occurrence of events that require immediate attention of the administrator, the administrator should configure the maximum permissible values for the parameters while adding the tile. See the **System Status Tile - Table of Information Displayed and Configurable Parameters**.

The administrator can also configure for CESM to send automated emails on occurrence of such events. If the check box 'Send email notifications' is selected, CESM will automatically send an alert email to the administrator on the occurrence of the events as specified.

Note – if you select 'All' from the drop-down list you will need to go into each tab and specify thresholds.

System Status Tile - Table of Information Displayed and Configurable Parameters

Information	Description	Configurable Parameters	Shortcut to...
All	Creates a tile that displays all possible 'System Status' information. The tile turns red to alert the administrator if one or more monitored settings (indicates as bold) exceeded the set permissible value.	The administrator has to configure the maximum permissible values for all the items. Refer to the rows below for more details.	NA
Outbreak	Displays the number	**Number of PC's have to be infected** - The	Clicking the 'Outbreak' tile will open the

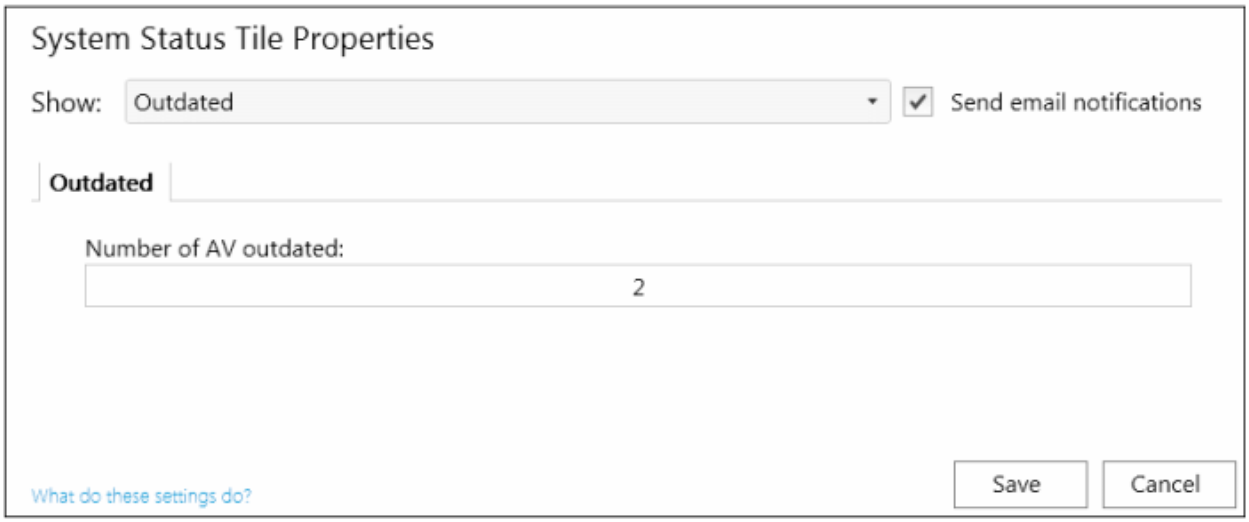
	of endpoints infected by virus or other malware.	administrator can specify the number of endpoints so that if the number of endpoints infected by malware equals to or exceeds this value, the tile alerts the administrator. *Default = 1* **Infections occur within total number of hours** - The administrator can specify the period (in hours) for generating the alert after the first infection. *Default = 0*	'Computer Infections Report' which lists the endpoints affected along with the name and location of the malware. Refer to **Computer Infections Report** for more explanation of these reports.
Malware Found	Displays the number of malware identified and not handled by the local CIS installation in the endpoint(s).	**Number of infected computers** - The administrator can specify the number of endpoints so that if the number of endpoints infected by malware equals to or exceeds this value, the tile alerts the administrator. *Default = 1*	Clicking the 'Malware Found' tile will open the 'Computer Infections Report' which lists the endpoints affected along with the name and location of the malware. Refer to **Computer Infections Report** for more explanation of these reports.
Non-Reporting	Displays the number of connected endpoints that do not report to the CESM console.	**Number of non-reporting computers** - The administrator can specify the number of endpoints so that if the number of non-reporting endpoints equals to or exceeds this value, the tile alerts the administrator. *Default = 1* **Hours idle** - The administrator can specify the period (in hours) for which CESM can wait after the endpoint has gone non-reporting, before the tile alerts the administrator. *Default = 0.*	Clicking the 'Non-Reporting' tile opens the 'View All Computers' interface which displays a list of all endpoints and endpoint groups along with their security policy, state and CIS mode (locally administrated or Remote administrated). Refer to **Viewing Endpoints** for more details.
Non-Compliant	Displays the number of connected endpoints that are not compliant with the CIS policy applied to them.	**Number of non-compliant computers** - The administrator can specify the number of endpoints so that if the number of non-compliant endpoints equals to or exceeds this value, the tile alerts the administrator. *Default = 1*	Clicking this tile will open a Policy Compliance report which displays a list of all non-compliant endpoints and endpoint groups. Refer to **Policy Compliance Report** for more details.
Outdated	Displays the number of connected endpoints which are currently using an outdated antivirus (AV) database	**Number of AV outdated** – The administrator can specify the number of endpoints so that if the number of outdated endpoints equals to or exceeds this value, the tile alerts the administrator. *Default = 1*	Clicking the 'Outdated' tile opens Antivirus Updates Report that shows the AV signature database update status of all the endpoints. Refer to **Antivirus Updates Report** for more details.
Licensing	Displays the number of days remaining for the license to expire.	**License expiration days** - The administrator can specify the number of days before the expiration day for the tile to alert. *Default = 30.*	Clicking the 'Licensing' tile will start the License Upgrade Wizard that allows you to view and change you license. See **How to Upgrade Your License** for more details.

4. Select the check box 'Send email notification' if you wish to generate email notification when certain conditions are met (for example, if a virus is detected or if a machine does not report for a certain period of time).
5. Click 'Save'. The new tile will be added to the dashboard area. You can add as many 'System Status' tiles as as you wish for the information you wish to have, to the dashboard.
6. To change the type of information for a particular tile, click the words 'System Status' at the bottom of the tile then the icon: . To remove the tile, click the icon: .

Example:
If the administrator wishes to add a 'System Status' tile to (1) display the number of endpoints whose AV database is outdated, (2) for the tile to turn red when the number of outdated systems is equal to or exceeds two, (3) Receive an email notification

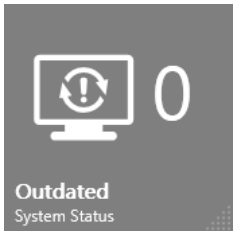
when the number equals to or exceeds two, then:

1. Click the ellipsis button on the settings bar at the lower left of the interface.
2. Drag the System Status tile to the dashboard. The 'System Status Tile Properties' dialog will appear.
3. Select 'Outdated' from the 'Show:' drop-down. The 'Outdated' tab will appear beneath the 'Show:' drop-down.
4. Enter 2 in the Number of 'AV outdated:' text field.
5. Select 'Send email notifications' checkbox.

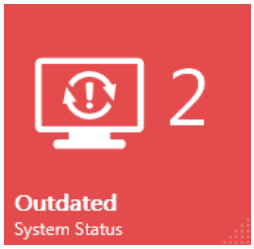


6. Click 'Save'.

A new 'System Status' tile will be added to the Dashboard which will display the number of endpoints whose AV database is outdated in real time. The example to the left shows a gray tile with zero outdated endpoints (everything's fine).



If the number of outdated endpoints equals or exceeds two, the tile will turn red to alert the administrator and an email notification will also be sent out.



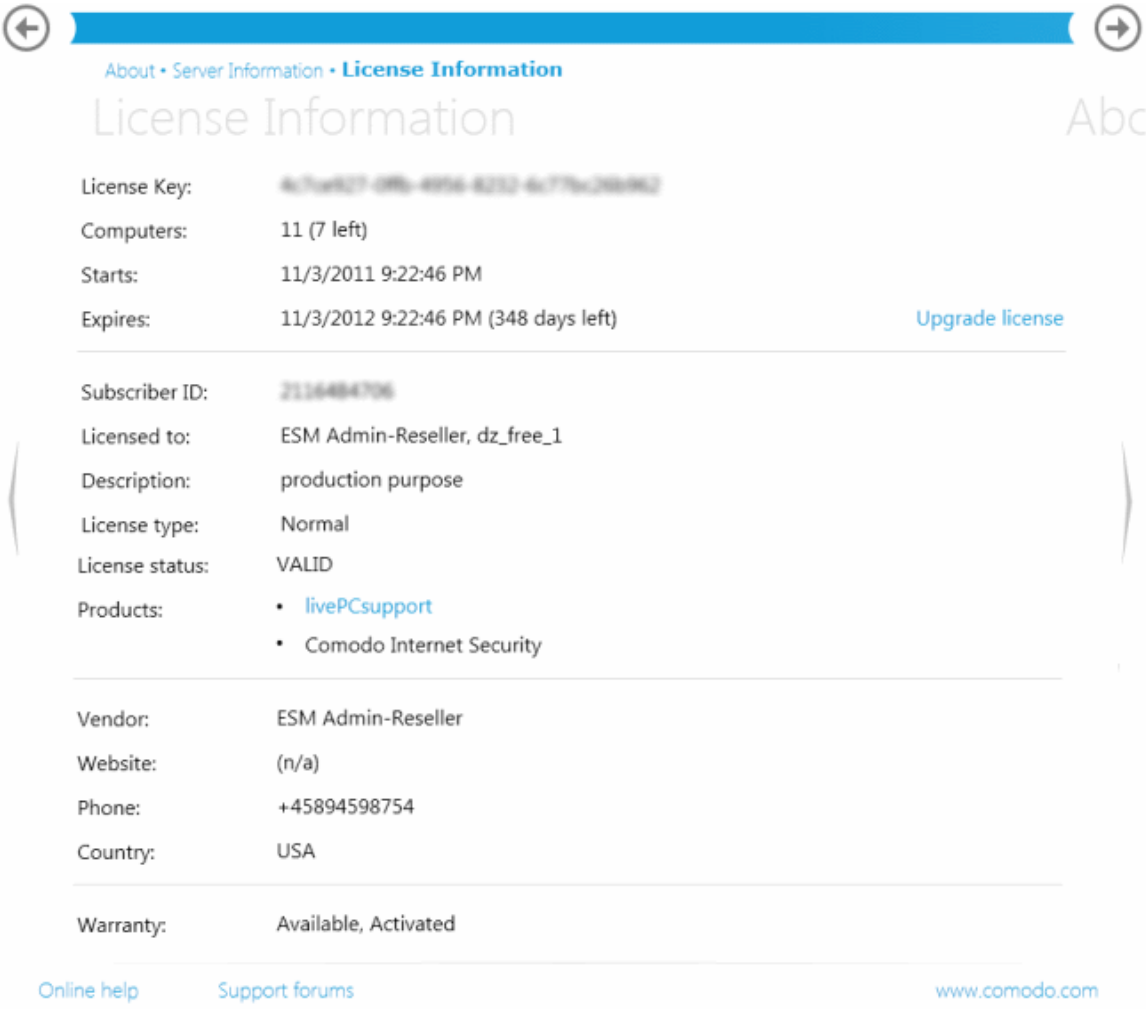
2.2.1.8. License Status Tile

The 'License Status' tile displays a summary of the number of endpoints permitted by your license and the license expiry date.

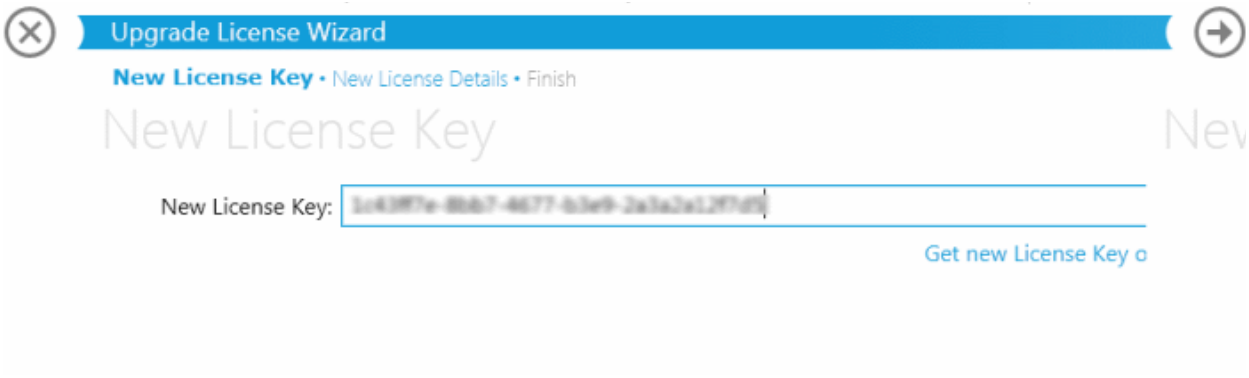
- This tile will turn red if the total number of detected endpoints exceeds the licensed number. Admins can use the 'Connectivity' tile to present to the total number of networked computers.
- This tile will turn red if the license has expired.
- Related to this tile is the 'Licensing' Tile which provides a highly visual reminder of the number of *days remaining* on a license.
- Click anywhere on the tile to open the license details and upgrade wizard.

Upgrading Your License

1. Navigate to Dashboard area. The License Status tile will display the number of endpoint covered by and the validity period of your current license.
2. Click the 'License Status' tile. The details of your current license are displayed.



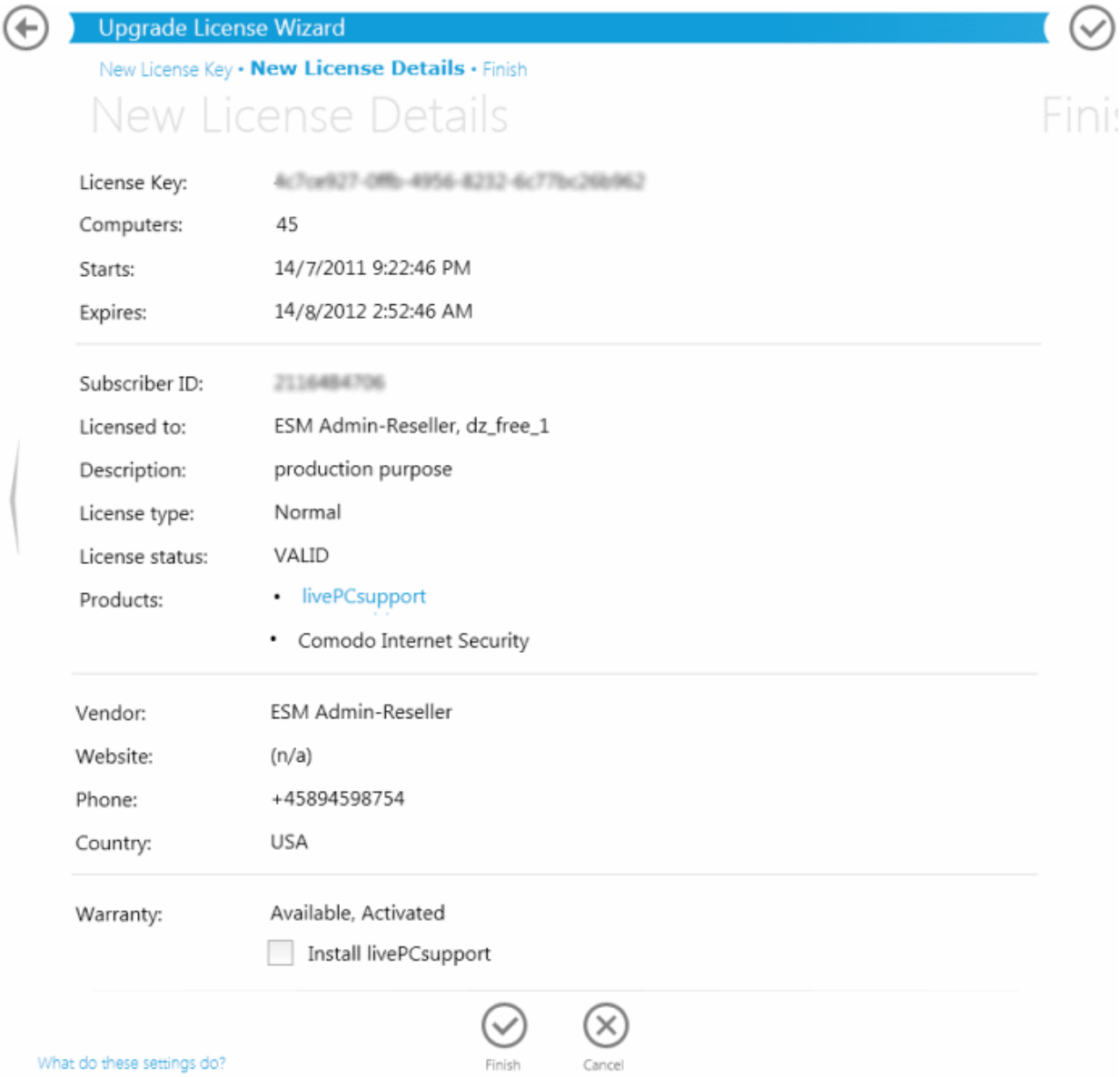
3. Click the 'Upgrade license' link to move to the next step - Entering the new license key.



4. Enter the license activation key you received via email.

Note: If you do not have a new license key, click the 'Get new License Key online' link to purchase it online from Comodo website.

5. Swipe the screen to the left or click the right arrow to move to the next step - New License. The details of your new license will be displayed.



6. Swipe the screen to left or click 'Finish' to activate the new license and exit the wizard.

Adding a License Status Tile

1. Click the ellipsis button on the settings bar at the lower left of the interface.
2. Drag the 'License Status' tile into the dashboard.

2.3. 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.

The 'Computers' area allows the administrator to:

- View the list of endpoints that are managed by CESM
- Add/Import computers to CESM for centralized management
- Create computer Groups for easy administration
- Apply security policies to computers and groups
- Download the latest version of the agent and deploy agents to target computers

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.

There are four tiles:

- **View** - Enables administrators to view all the endpoints/endpoint groups added to CESM. Also allows to view the details of individual computers or groups.
- **Create** - Enables administrator to create new endpoint groups, add endpoints into them, and apply security policies for the endpoint security software as per the administration requirements.
- **Download** - Enables administrator to download the agent for installation on the endpoints.
- **Deploy** - Enables the administrator to import/add computers from the local network into the CESM console by installing the CESM agent onto discovered endpoints. Computers can be imported from Active Directory, Workgroup or by entering IP addresses. Once imported/added by installing the agent, the endpoint computer is ready to be managed through CESM.

Adding an endpoint to CESM requires an agent to be installed in it. The agent can be installed in two ways:

- **Install agent while importing computers**
- **Download and Install agent 'manually' on endpoint computers**

Once the agent is installed, the endpoints can communicate with and be managed by CESM.

2.3.1. Adding Endpoint Computers to CESM

Each managed endpoint requires a small software agent to be installed to facilitate communication between it and 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 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.

Alternatively, Comodo Internet Security (CIS) can be installed in endpoint computers separately and from the CIS interface the endpoints can be connected to CESM. For more details refer the sections, **How to Install CIS** and **How to Connect CIS to CESM at the Local Endpoint**.

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 CIS, running AV scans, deploying agents, updating AV databases and more).** Refer to **Creating Endpoint Groups** for more details.

2.3.1.1. Importing Computers by Automatic Installation of Agent

The 'Deploy' wizard will install the CESM agent 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 'Deploy' tile from the 'Computers' area to start the wizard:

Step 1 - Select the Target Type

Computers can be imported into CESM in the following ways:

- **Active Directory** - imports computers from an Active Directory Domain.
- **Workgroup** - imports computers from a Workgroup.
- **IP Address** - 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.

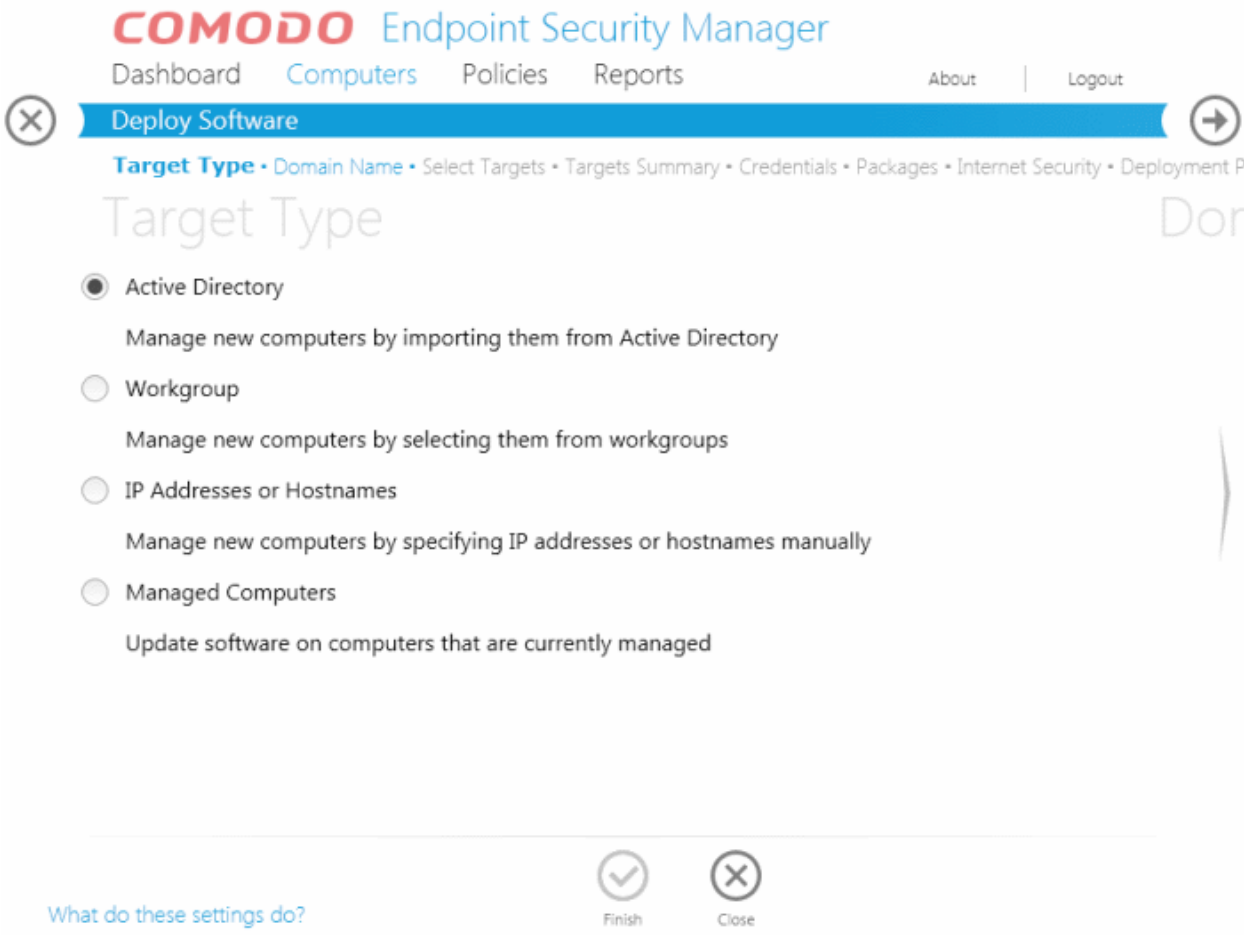
Note: Targets are contacted by the CESM service computer and its network connection, not the computer running the management console.

CESM Business 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 IP Addresses if you want to import computers by specifying their IP addresses or DNS names.

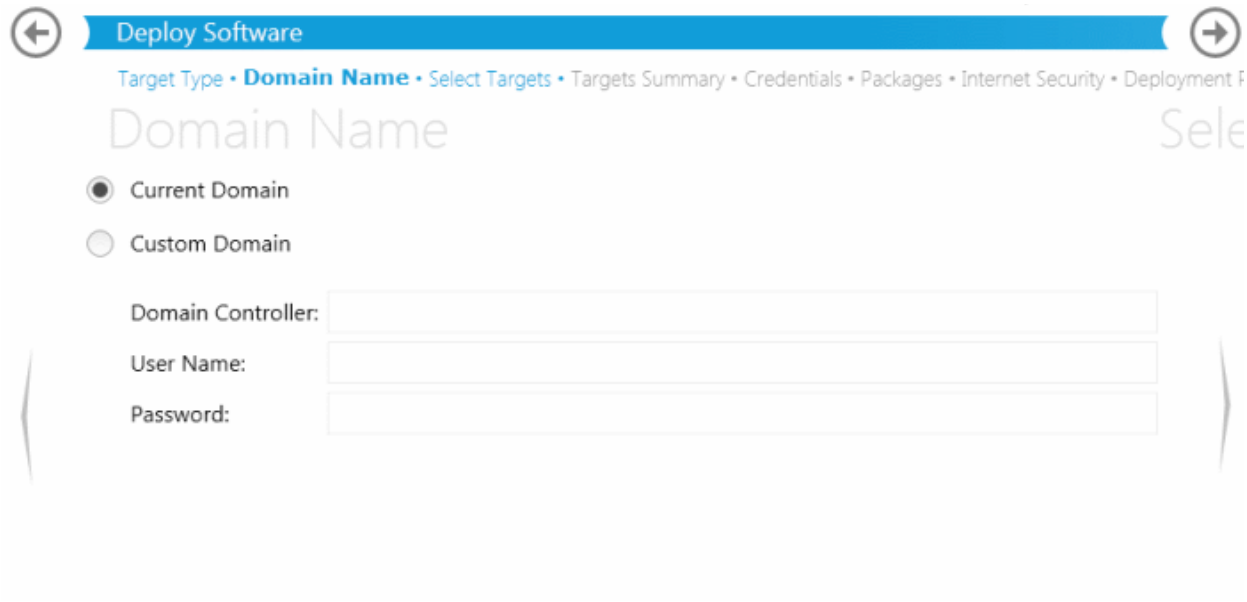


Importing from Active Directory

Choose 'Active Directory' and move to the next step by clicking the right arrow.

Step 2 - Domain Name

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

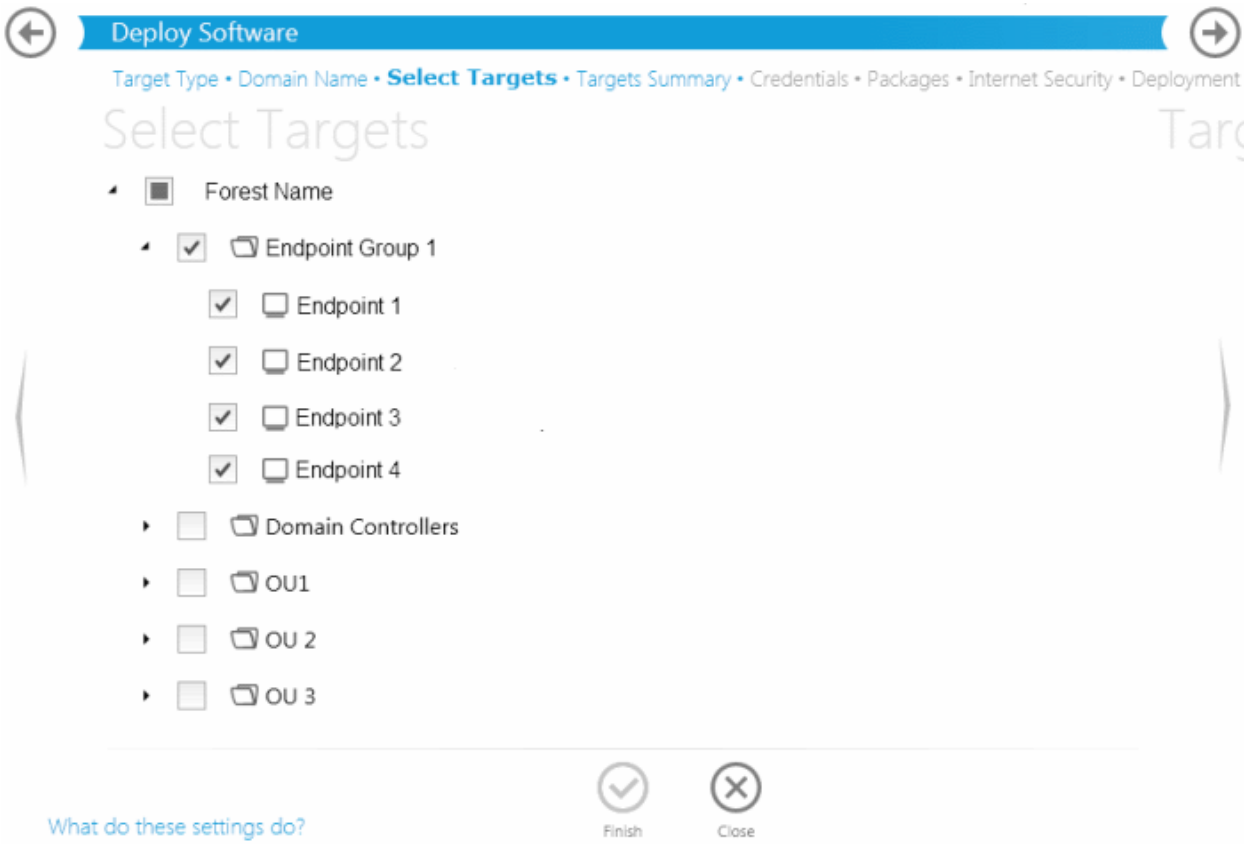


Domain Import Settings - Table of Parameters	
Current Domain (Selected by default)	Selecting this option will import any computers from the Active Directory domain that the CESM server is a member of.
Custom Domain controller	Selecting this option allows the administrator to specify an alternative Active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

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

Select Targets

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



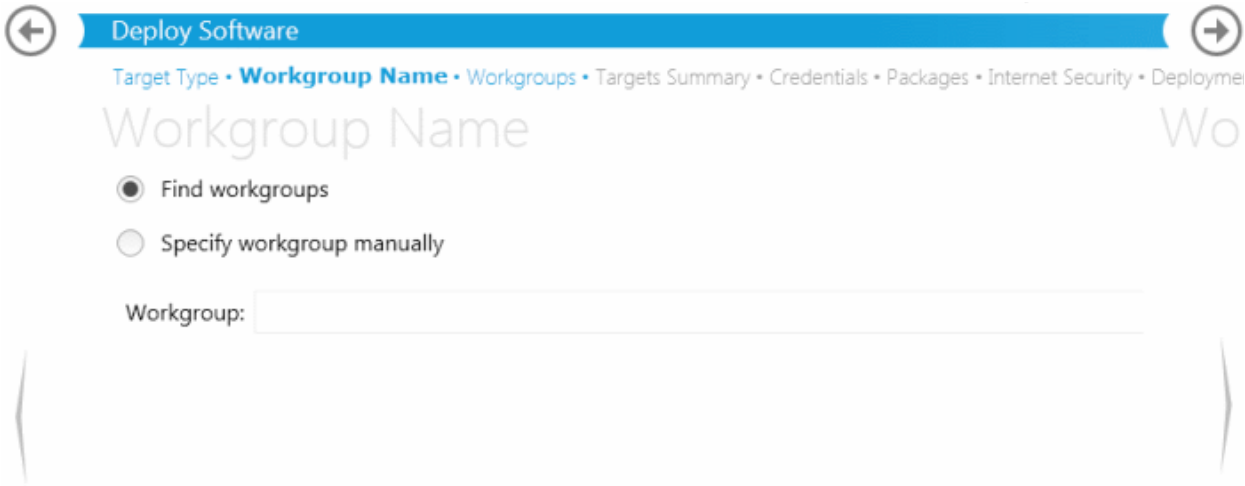
- Click the ▸ icon to expand or collapse the tree structure
- Select the target endpoints onto which you wish to install the agent and import into CESM
- Click the right arrow or swipe left to move to step 3 to select the endpoints

Importing Computers from Workgroup

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

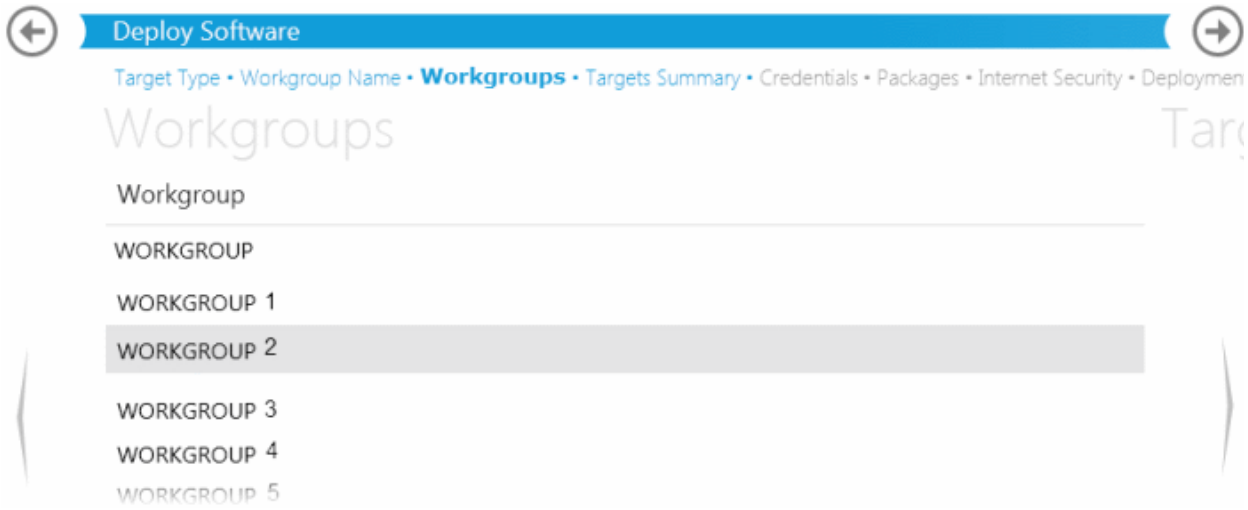
Step 2 - Workgroup Name

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



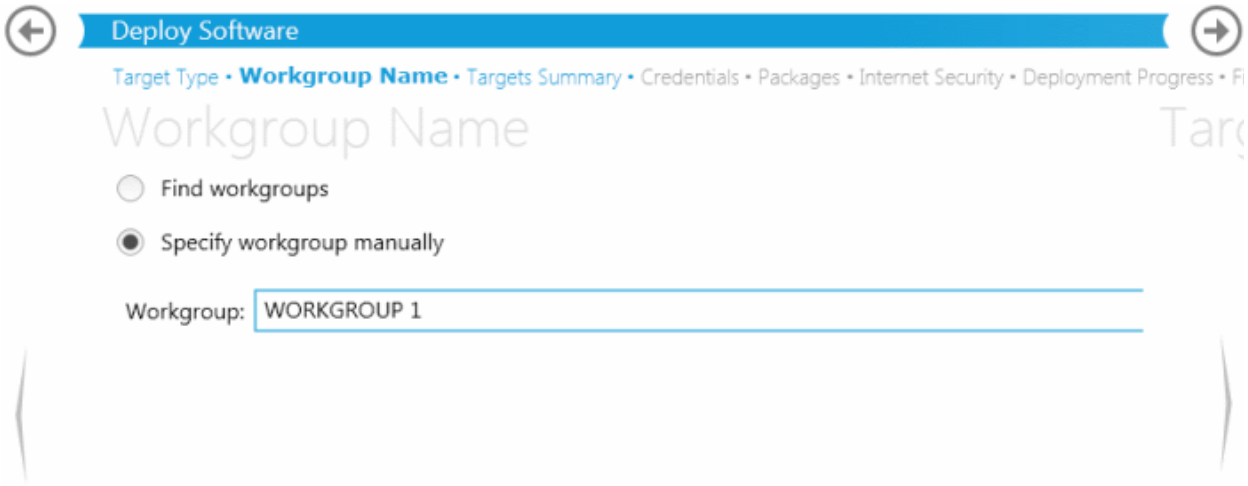
CESM enables the administrator to specify the workgroup name in two ways:

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



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

Note: The Workgroup is discovered from the local area network attached to the CESM service computer.



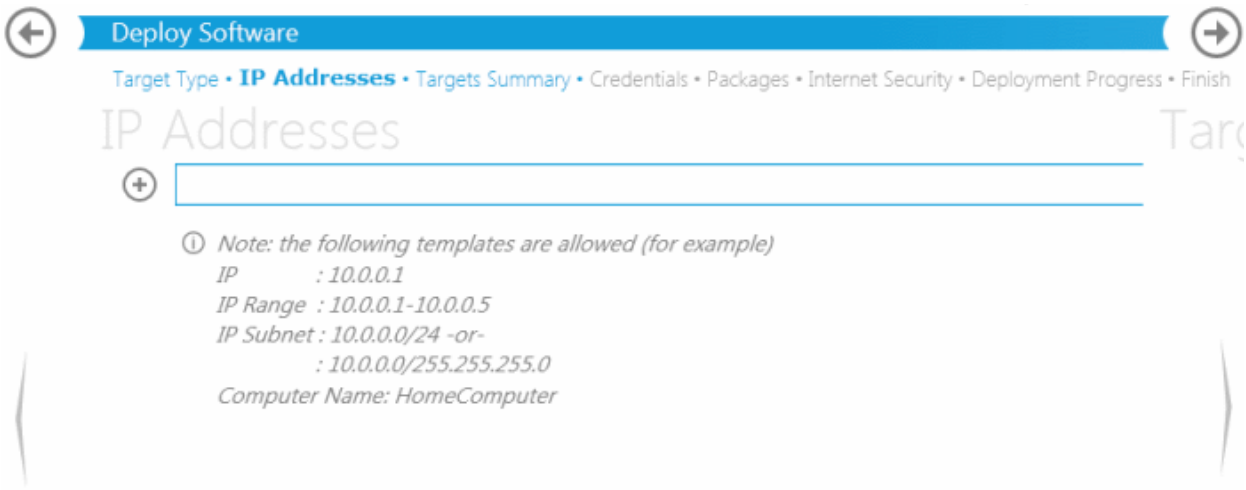
  - Enter the name of a network Workgroup and click the right arrow to move to **step 3** to select the endpoints.

Importing Computers by IP Addresses

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

Step 2 - Adding IP Addresses

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



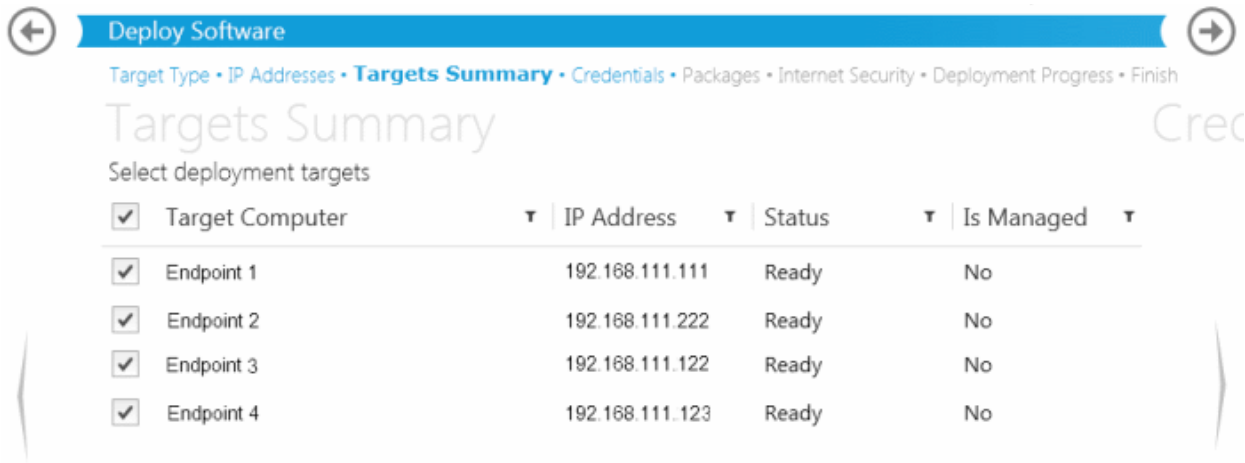
Computers can be added in four ways:

- **Import individual computers by specifying their IP addresses one-by-one** - Enter the IP address of the computer and click the ⊕ icon. 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 ⊕ icon. 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 ⊕ icon. 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 ⊕ icon. 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, click the icon ⊖ that appears on moving the mouse cursor over the added entry.
  - Click the right arrow to move to the next step.

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

Step 3 – Targets Summary

In this step, all the endpoints included in the previous Step 2 will be displayed.

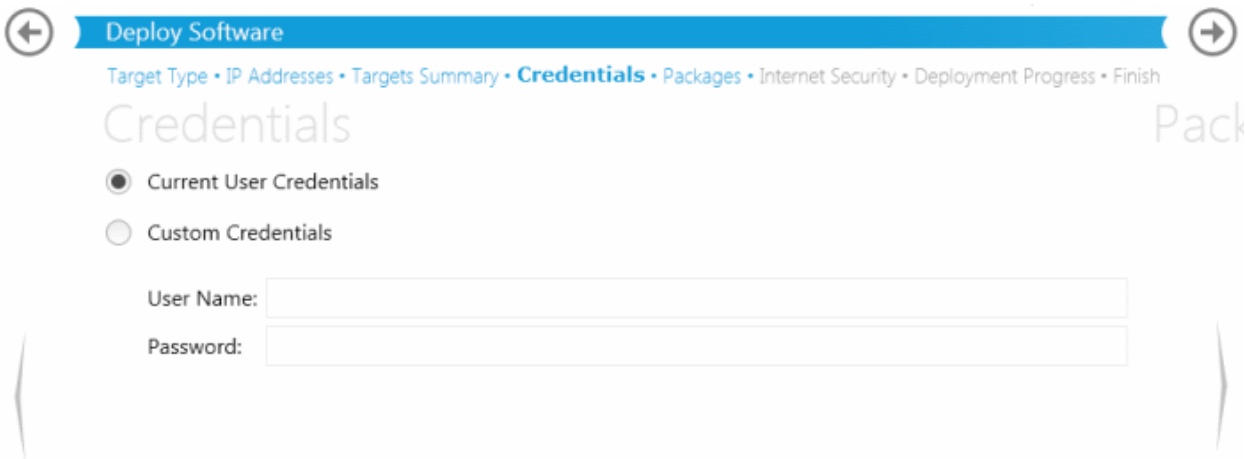


Select the endpoint(s) that you want to deploy the agent and CIS to. You can use the filter option to select the endpoints from the list displayed.

- 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 'Status' column header to search for endpoints that are 'Ready' or 'Unavailable' 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 'Is Managed' column header to search for endpoints that are 'Managed' or 'Not Managed' 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).

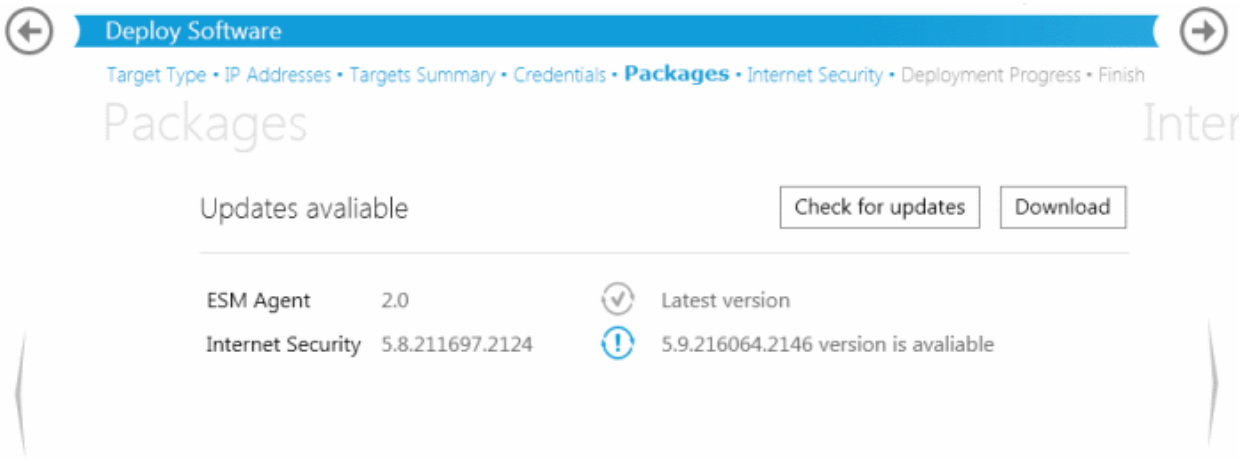


Credentials - Table of Parameters	
Current User Credentials (Selected by default)	Selecting this option will install the agent using the credentials of the currently logged -in CESM administrator account in each endpoint.
Custom Credentials	Selecting this option allows the administrator to specify an 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

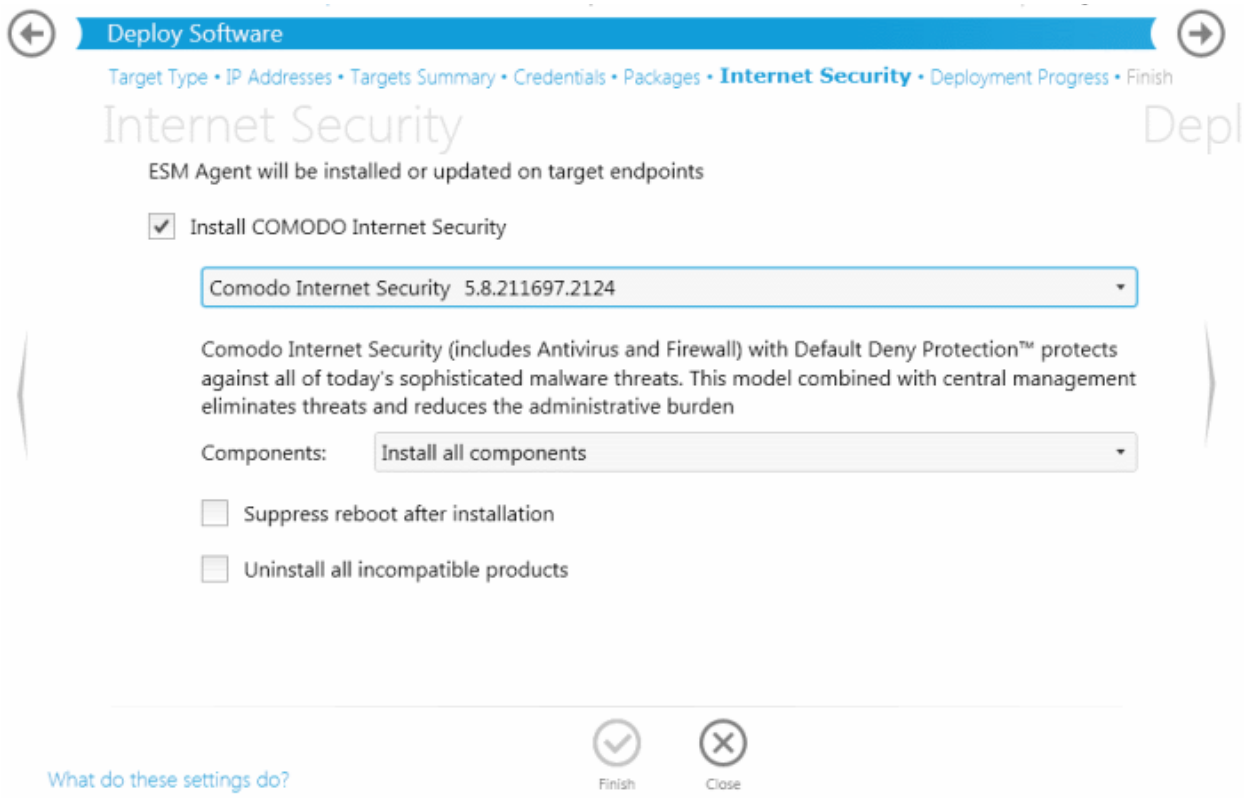
The next stage 'Packages' displays the version details of ESM Agent and CIS. You can also check for updates of these applications and download it in your server for deployment on to the end-points.



- Click 'Check for Updates' to find out if any newer version of ESM Agent and CIS 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 - Internet Security

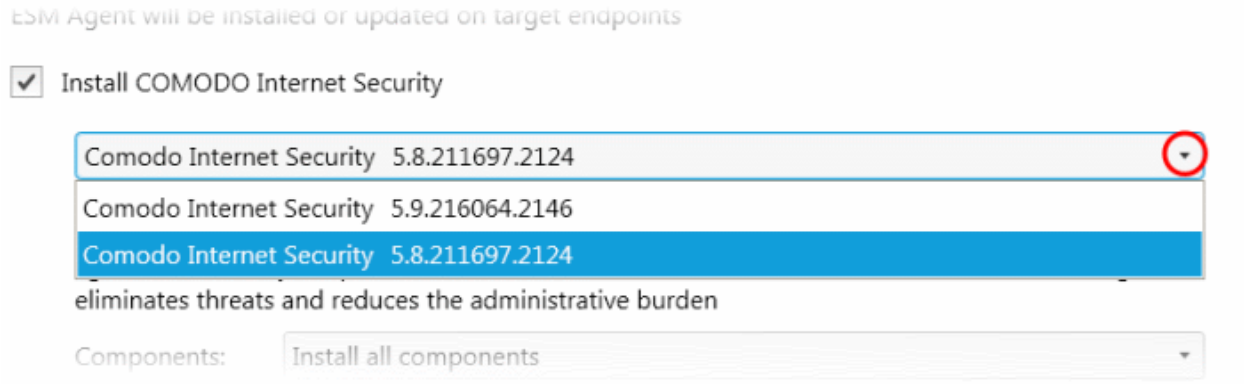
The next step is to choose installation options for Comodo Internet Security (CIS):



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

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

- Select the version of CIS 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.



- 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 - CIS 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. CIS 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 CIS. Performing this step will remove potentially incompatible products and thus enable CIS 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.

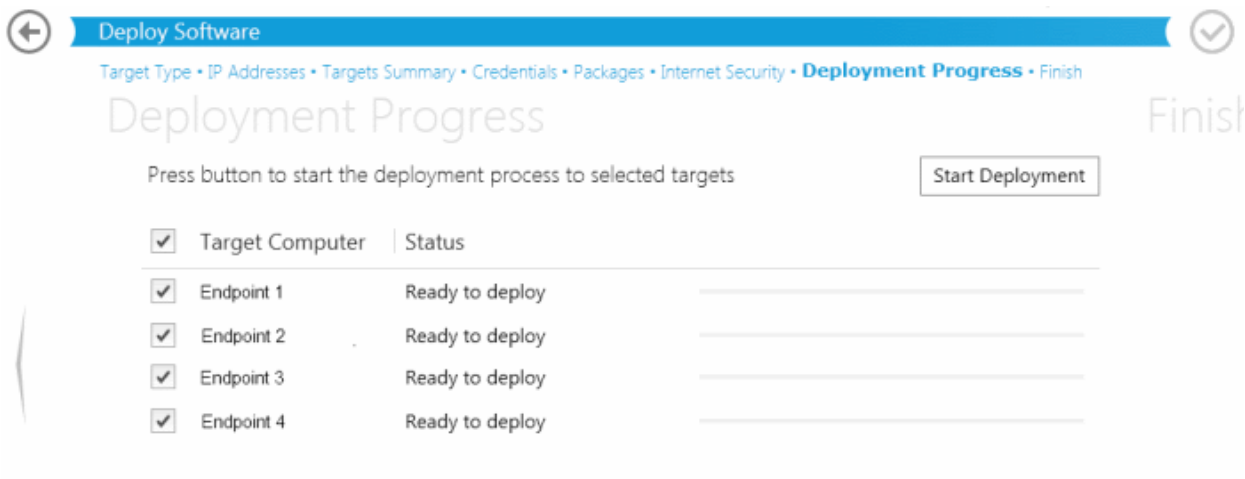
Tip:

You can also:

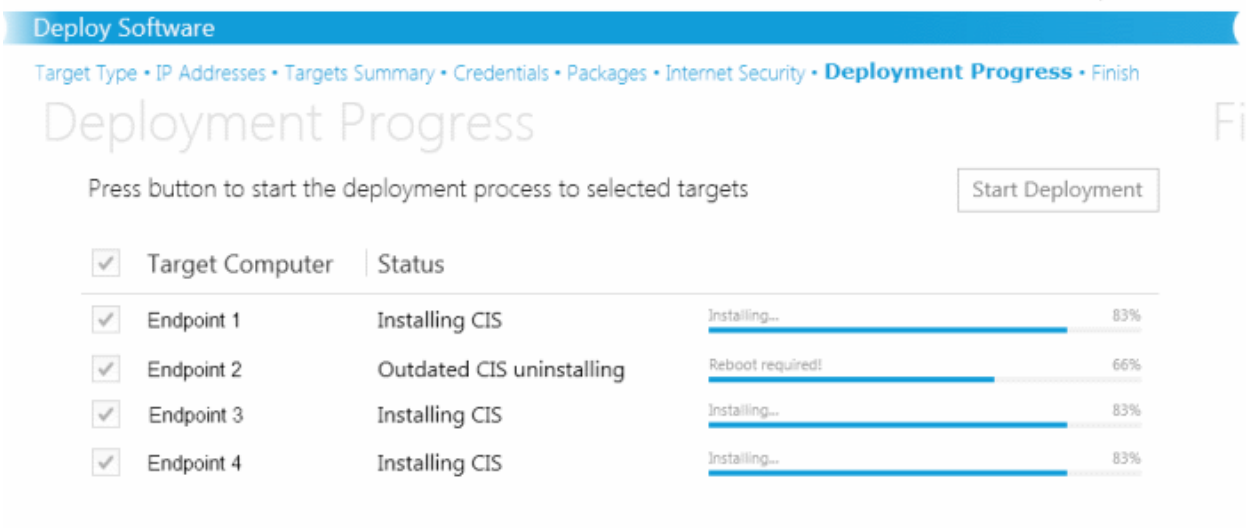
- Install CIS manually onto endpoint computers. Refer to **How to Install CIS**; and
- Import stand-alone CIS application pre-installed at the endpoints under the management of CESM. Refer to **How to connect CIS to CESM at local endpoint**.

Step 7 - Deployment Progress

Click 'Start Deployment'.



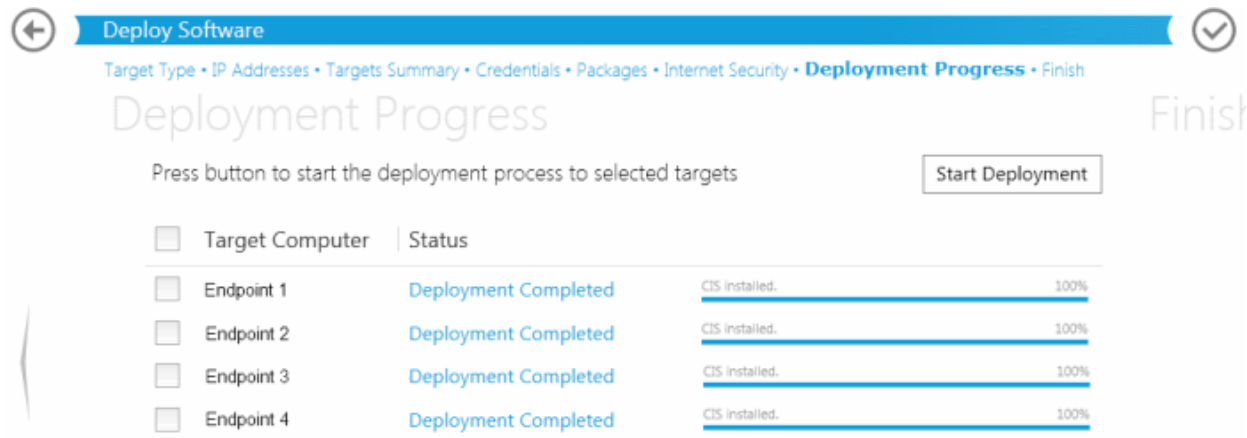
CESM will start installing the agent/CIS on to the selected endpoints and the progress per endpoint will be displayed.



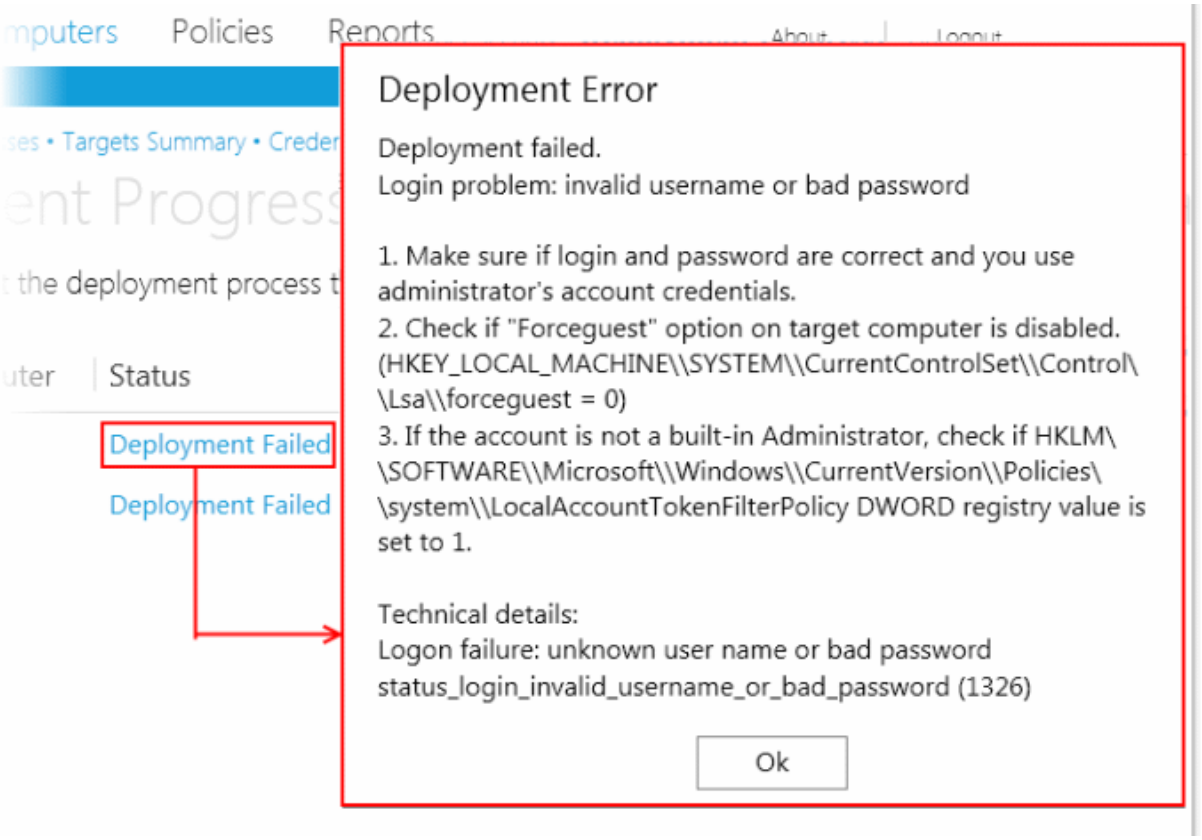
If any of the selected endpoints have older versions of CIS than the one selected in the previous Step 6, they will be automatically uninstalled and the selected version will be installed.

Step 8 - Deployment Complete

On completion of installation, the **results** screen will appear.



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



- Click the Finish icon 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 'Viewing Endpoints' 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 CIS, running AV scans, deploying agents, updating AV databases and more). Refer to Creating Endpoint Groups for more details.

2.3.1.2. Adding Computers by Manual Installation of Agent and CIS

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 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 of the agent it 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 deployment wizard.

The endpoint security software, Comodo Internet Security (CIS) is typically also manually installed in the endpoint can be remotely managed by CESM once installation of the Agent is completed. If the Agent is installed first (with the endpoint having no CIS), the deployment wizard can be used to install CIS via the installed Agent.

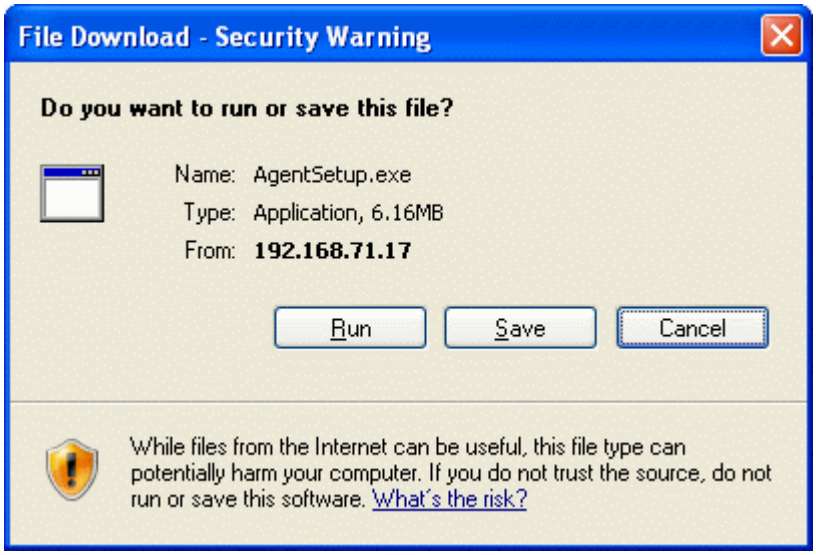
Alternatively, Comodo Internet Security (CIS) can be installed in endpoint computers separately and from the CIS interface the endpoints can be connected to CESM. For more details refer the sections, How to Install CIS and How to Connect CIS to CESM at the Local Endpoint.

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

1. Navigate to the Computers area of the admin console and click 'Download' tile.

2. 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. Refer to Appendix 2 - Configuring Server for download through Web Browser for more details.

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:

- 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.

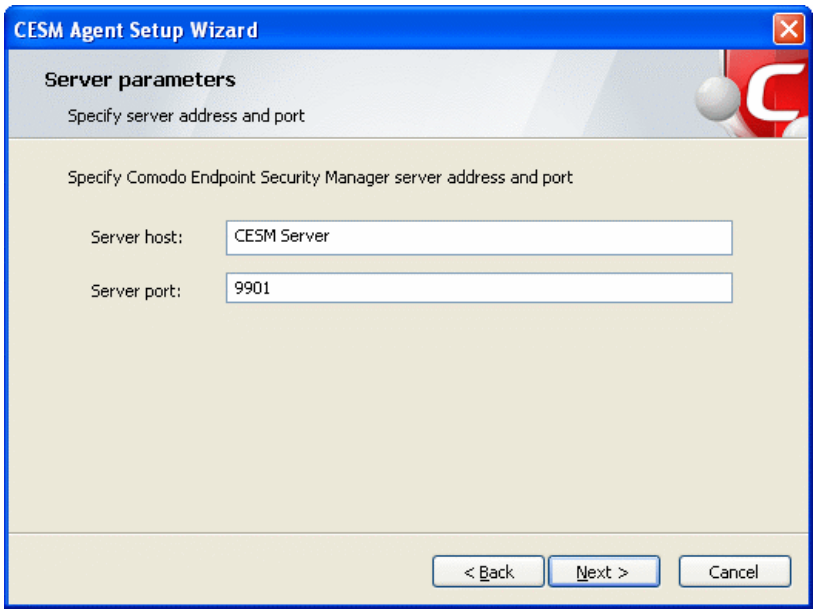
Step 1 - Welcome Screen

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

Click 'Next' to continue.

Step 2 – Specifying Server Address and Port

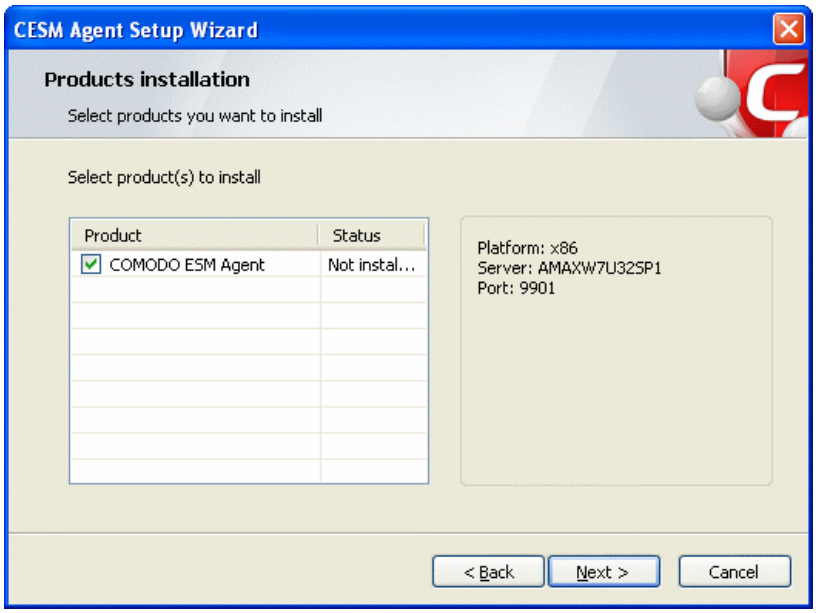
In the next step you must enter the host or IP address of the server in which CESM is installed and the port number the endpoint should be connected. By default, these fields will be populated with the details of the server from which the agent is downloaded.



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

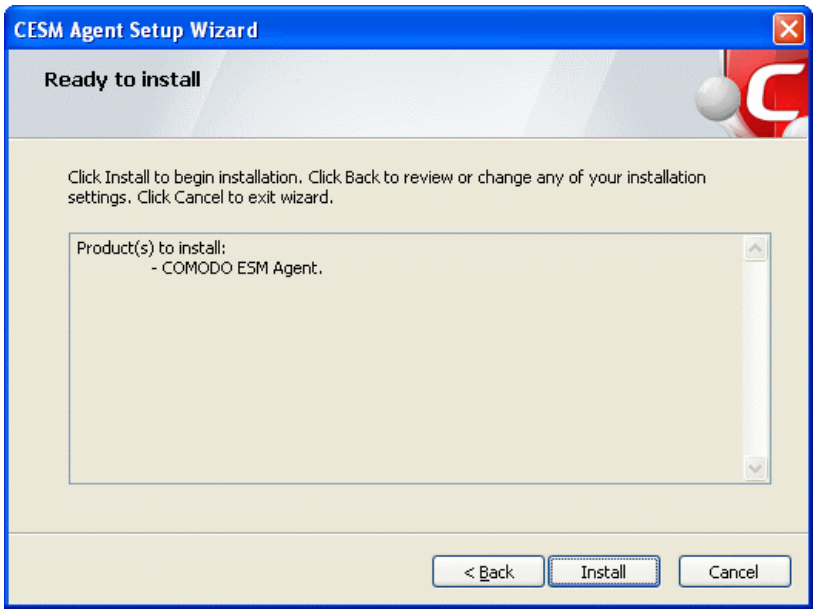
The next stage is to select the products to be installed. The installer will first check whether any of these items are already installed. You must first uninstall any older versions of CIS or the Agent that are detected.



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

Step 4 - Ready to Install

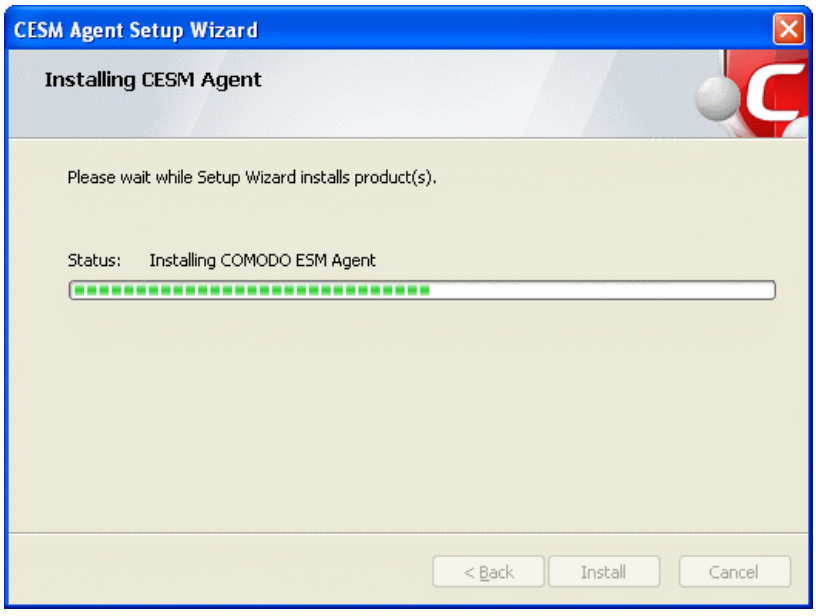
The next step allows you to confirm the choices made in the previous step. Click 'Back' if you want to review and change the choices made.



To commence the installation, click 'Install'.

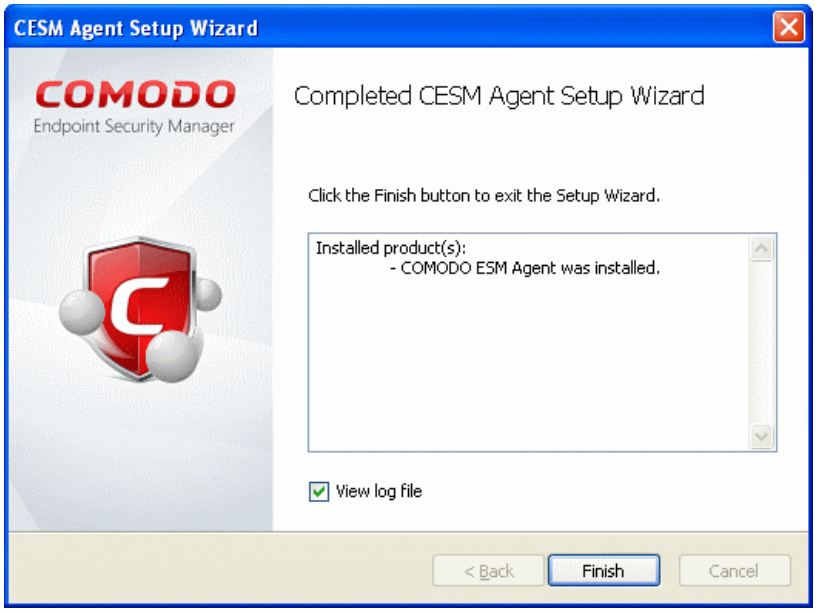
Step 5 - Installation Progress

The installation progress will be displayed.



Step 6 - Installation Complete

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



- Click 'Finish' to exit the wizard.

The agent will now automatically establish the connection to your CESM Service Server.

2.3.1.3. Updating Comodo Software on Managed Computers

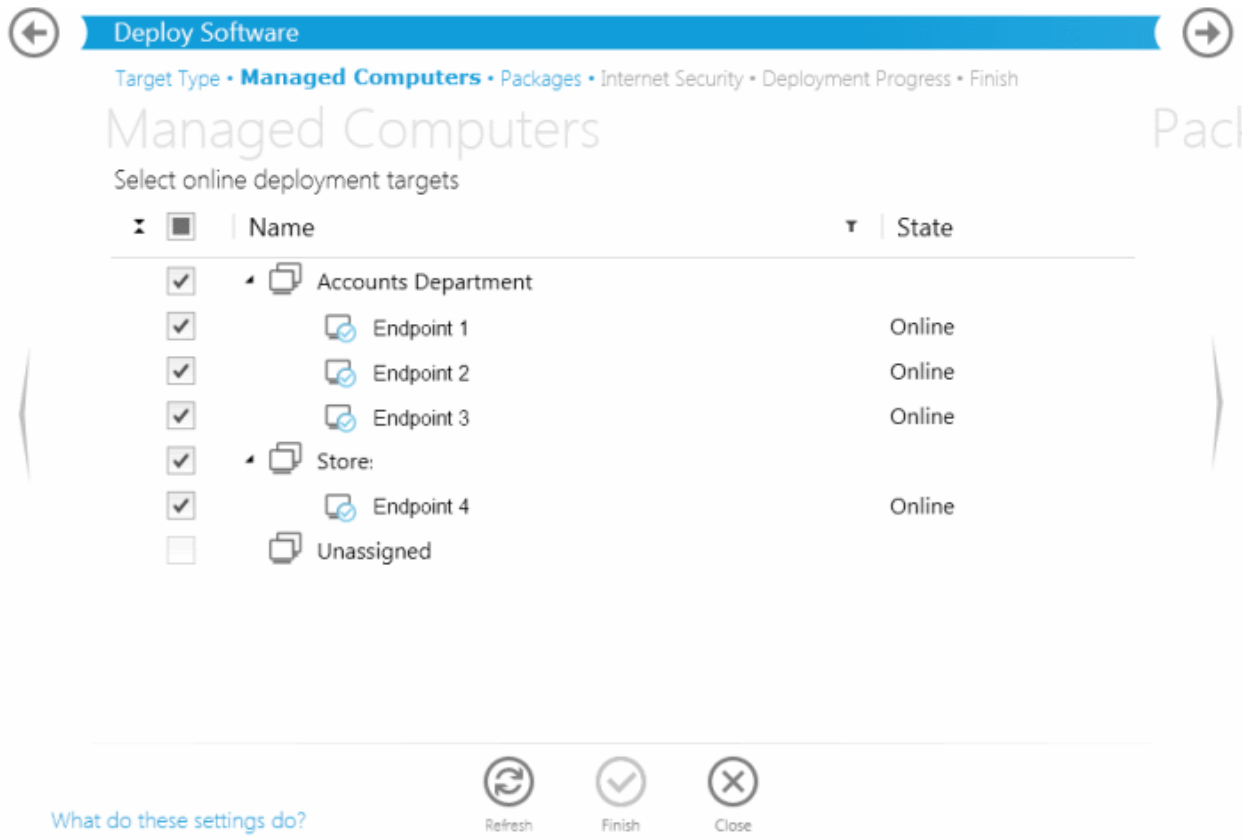
Once an endpoint is managed, CESM allows you to update the CESM agent as well as CIS using the Deploy wizard.

To update software on managed computers

- Click the 'Deploy' tile from the 'Computers' area to start the wizard:

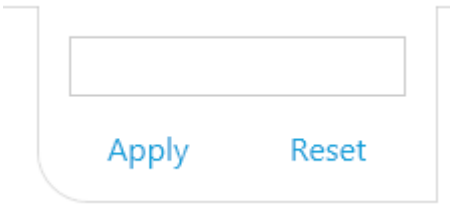
- Select 'Managed Computers' and click the right arrow or swipe left to proceed to the next step.

All the managed computers will be displayed.



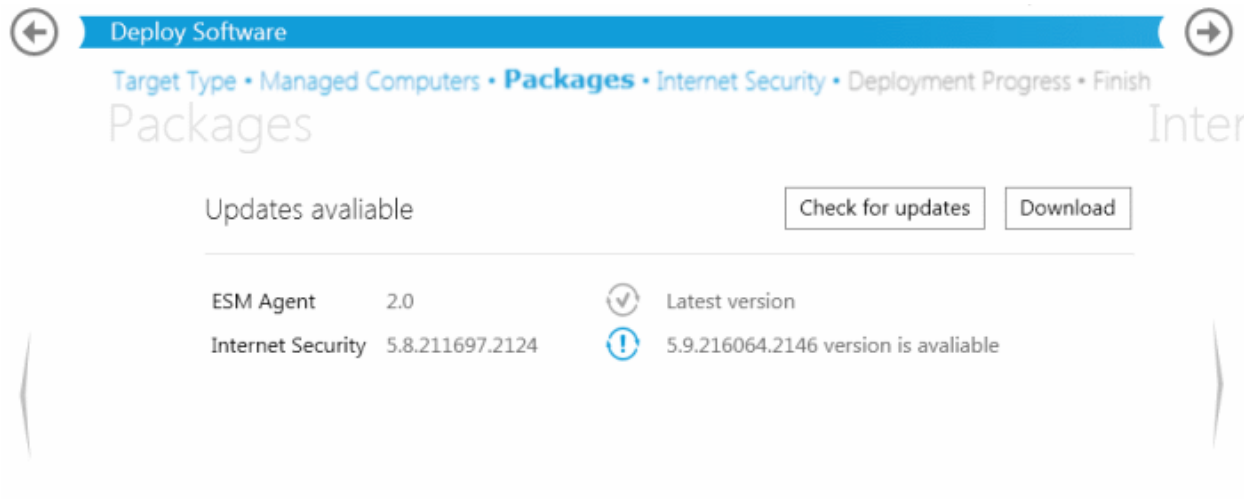
- Select the endpoints that you want to check and update CESM Agent and CIS application from the list.

- Click the icon to display only the groups. Click it once again to display all the endpoints in the groups.
- Click the icon beside any of the group name to expand or collapse the endpoints within the respective groups.
- Click the filter icon in the 'Name' column header to search for a particular endpoint, enter the endpoint name and click 'Apply'.
- Click 'Reset' to expand all the endpoints in the list.



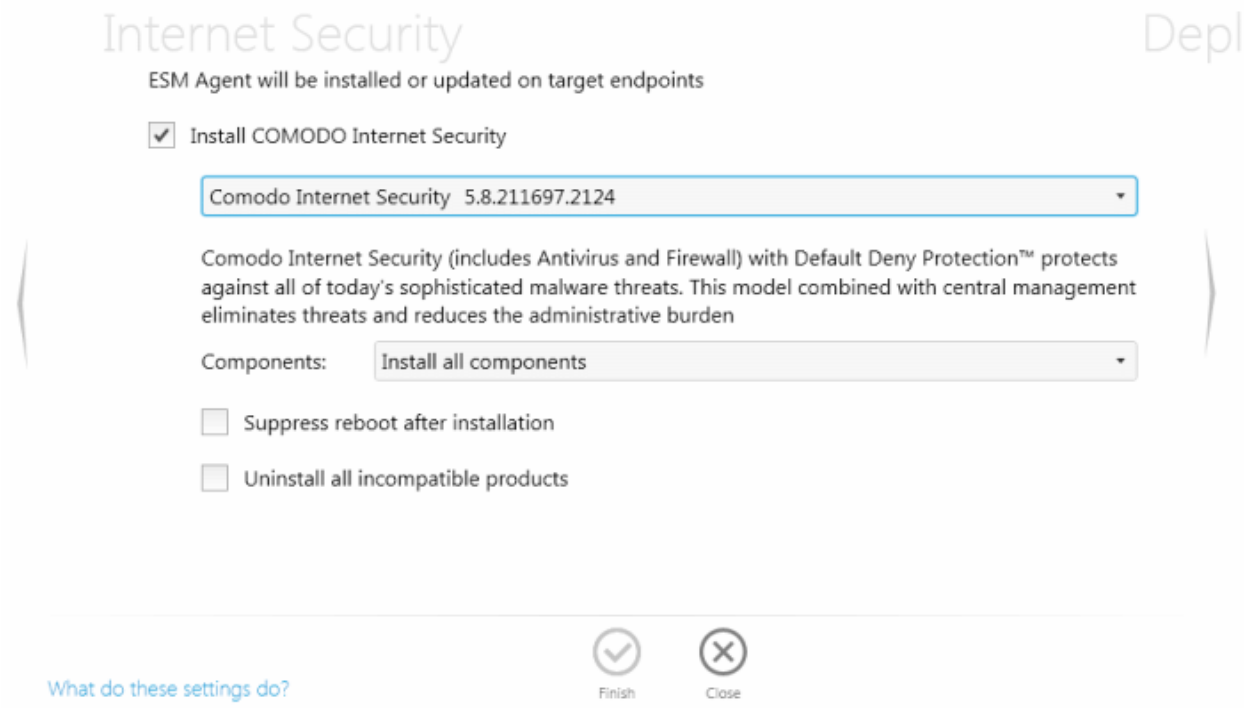
- After selecting the endpoints, click the right arrow or swipe left to proceed to the next step.

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

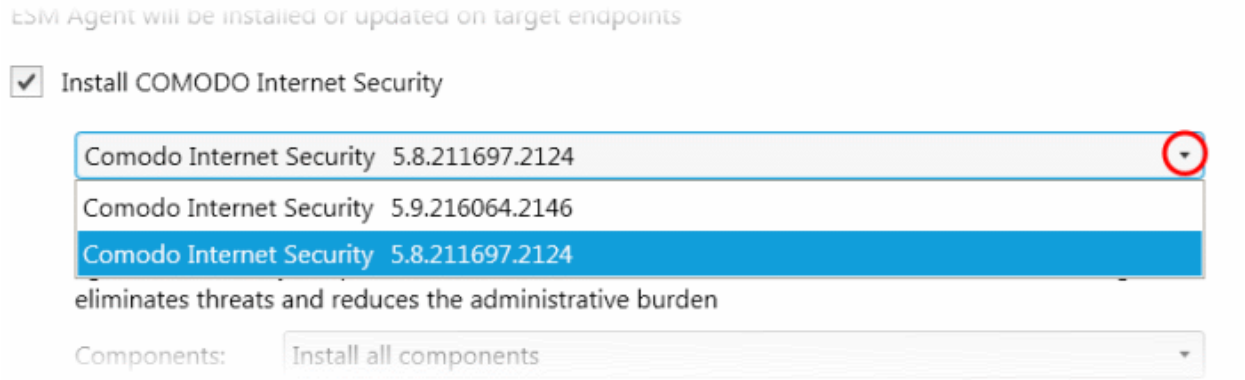


- Click 'Check for Updates' to find out if any newer version of ESM Agent and CIS are available
- If any newer versions are available, you can choose to download them to the CESM server by clicking 'Download'
- Click the right arrow or swipe left to move to the next step

The next step is to choose installation options for Comodo Internet Security (CIS):



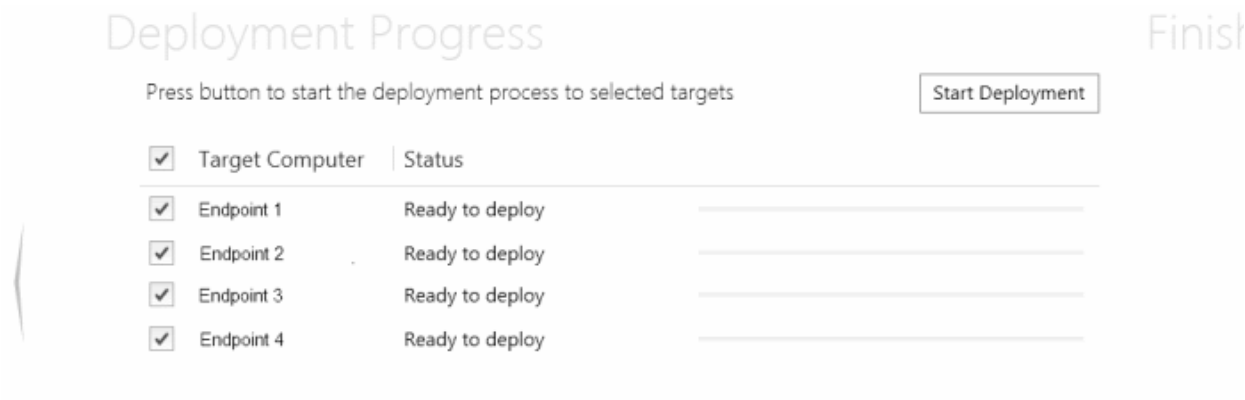
- Select 'Install Comodo Internet Security' check box if you wish CIS to be installed along with the agent.
- Select the version of CIS you wish to install on the selected endpoints from the drop-down.



- 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 - CIS 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. CIS 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 CIS. Performing this step will remove potentially incompatible products and thus enable CIS 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.

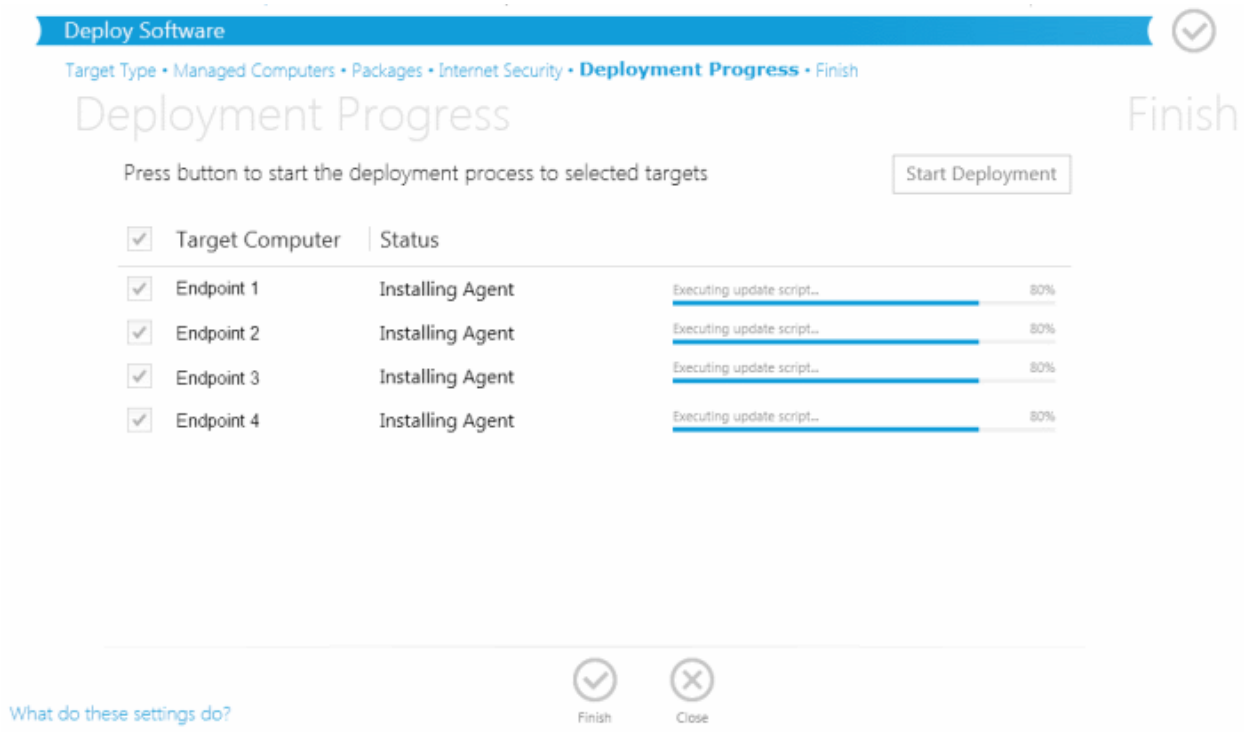
  Click Here to see the full list of incompatible products.
- Click the right arrow to move to the next step.

The next stage moves to deployment progress.

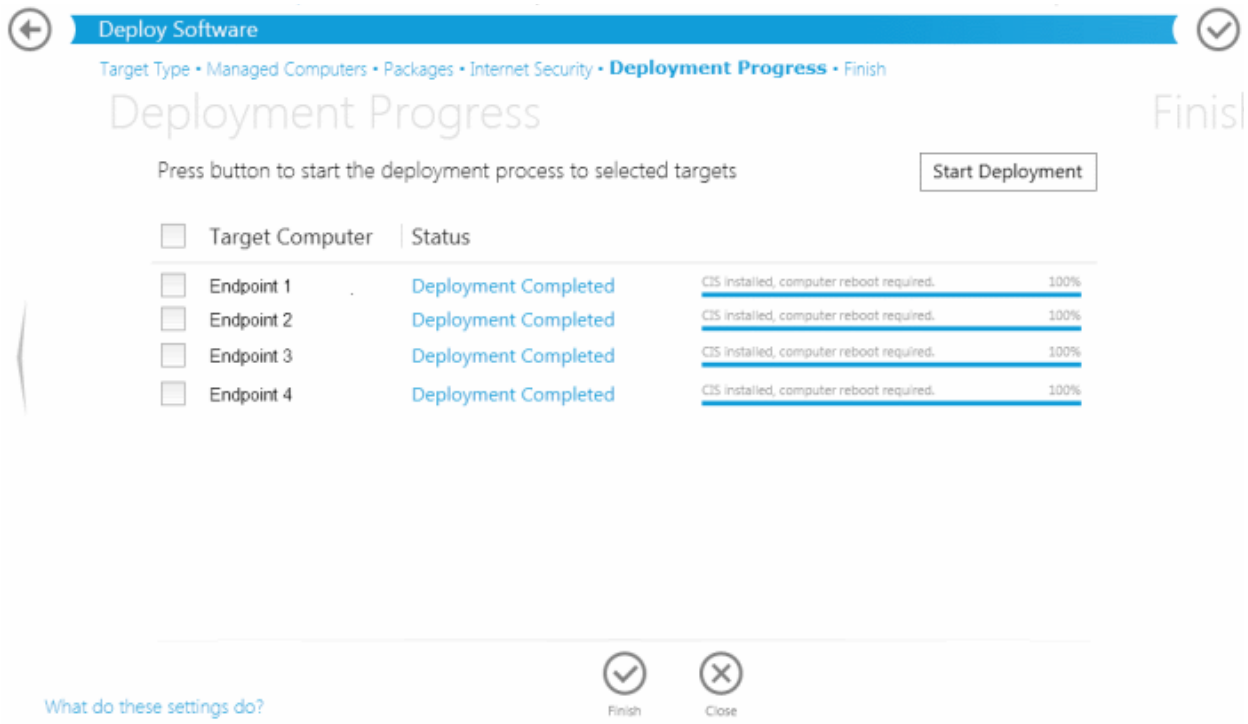


- Click 'Start Deployment'

The deployment progress will be displayed.



On completion of installation, the results screen will appear.



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

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.

2.3.2. Creating Endpoint Groups

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:

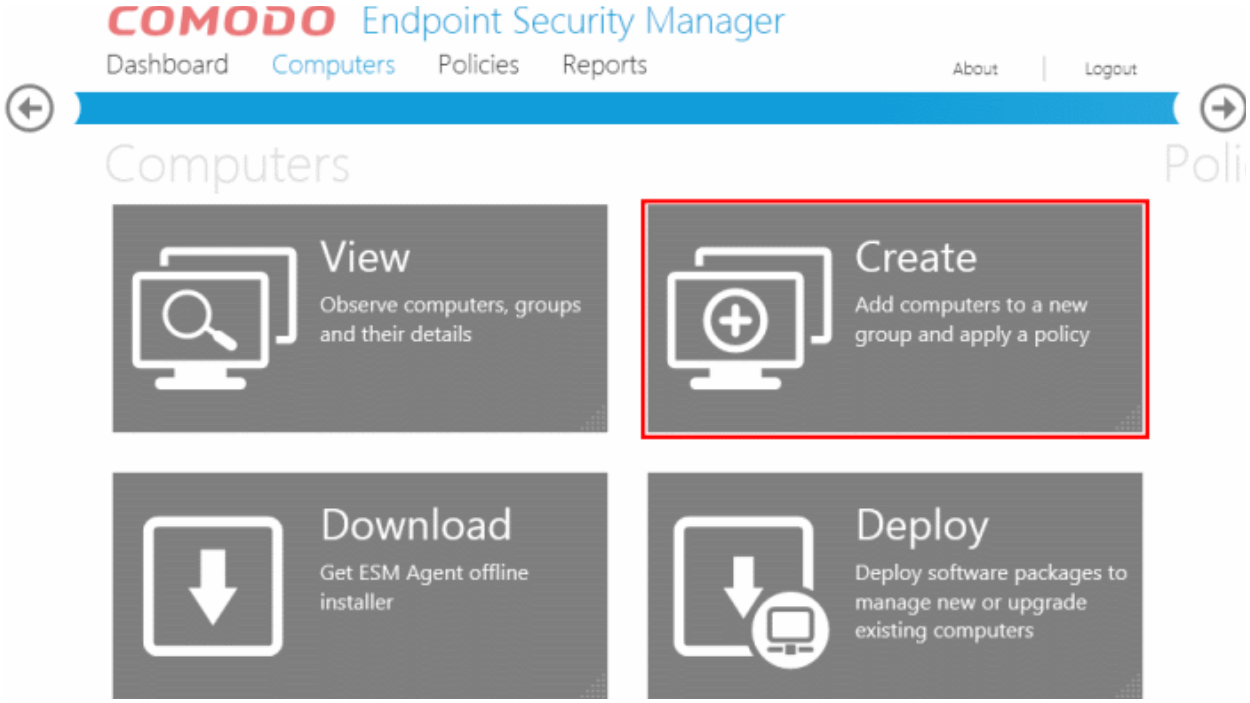
- The CIS security policies can be applied to the endpoints belonging to various groups as per their requirements
- Antivirus (AV) scans can be run on endpoints in a group together
- The AV signature database in the endpoints can be updated together
- Various reports can be generated for the endpoints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

The 'Create' tile in the 'Computers' area enables the administrator to define groups and to add previously imported endpoint computers into them as desired.

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 create a new group

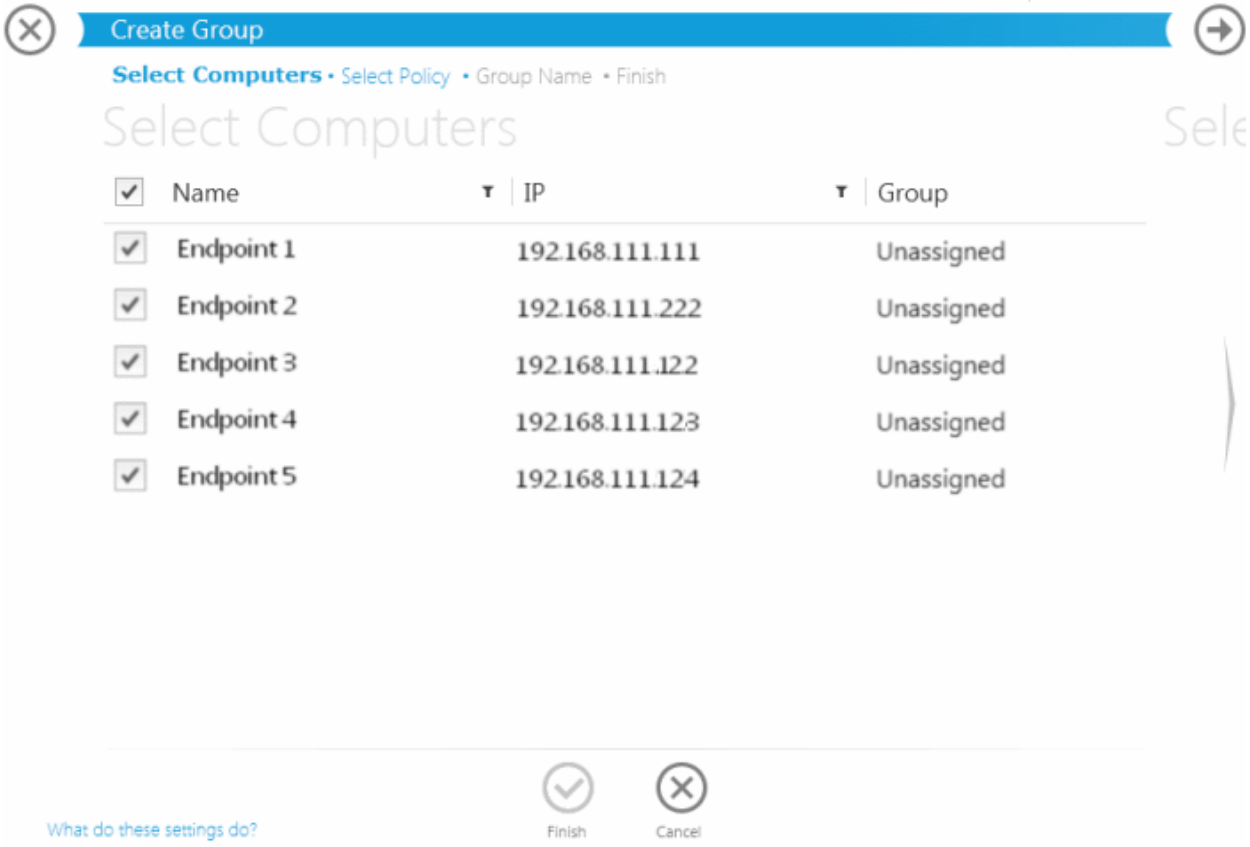
Navigate to Computers area and click the 'Create' tile.



The Create Group wizard will start with Step 1 - Select Computers. The remaining steps are displayed below the blue title bar with the current step highlighted in blue. To move backwards or forwards between steps, use the arrows on either side of the title bar (or left click and drag to swipe the screens left or right).

Step 1 - Selecting Computers

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

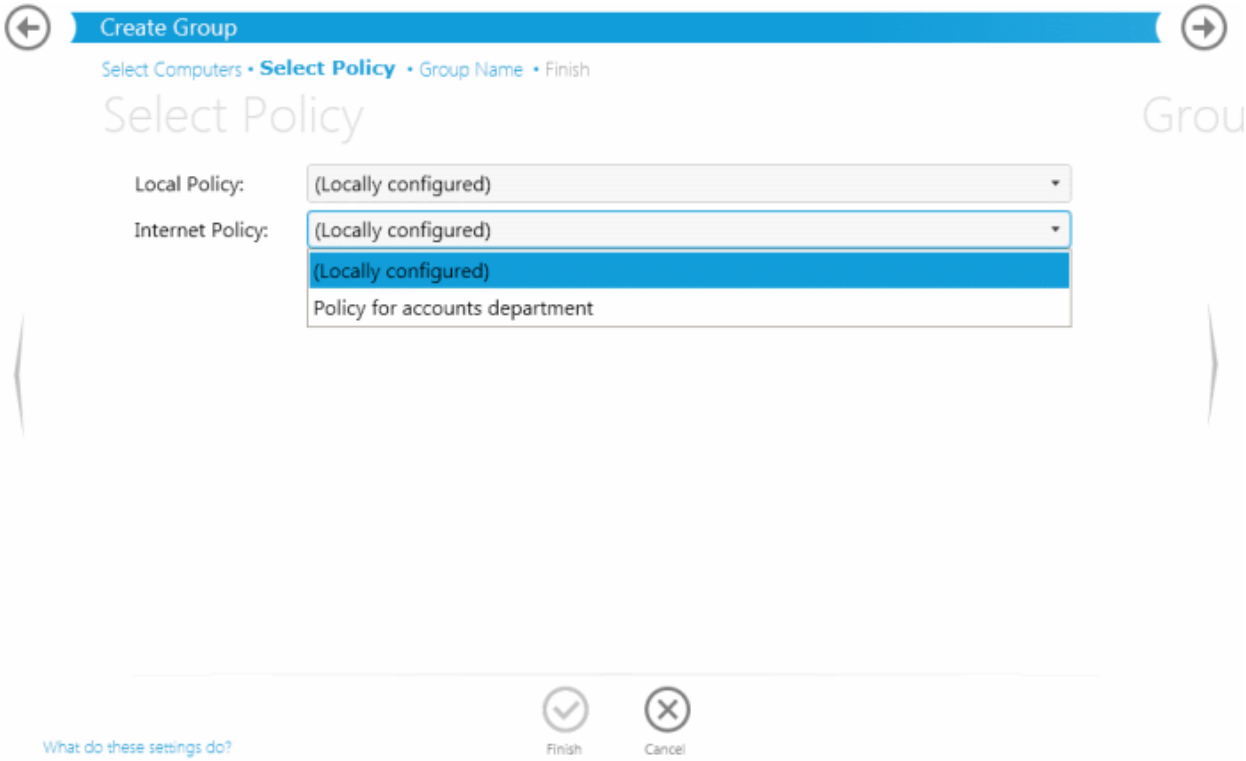


- Click the filter icon in the 'Name' column header to search for a particular endpoint and click 'Apply'
- Click the filter icon in the 'IP' column header to search for endpoints with particular IP(s) and click 'Apply'
- Select the endpoint computers to be added to the new group and click the right 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 CIS installations in the endpoints of the newly created group.

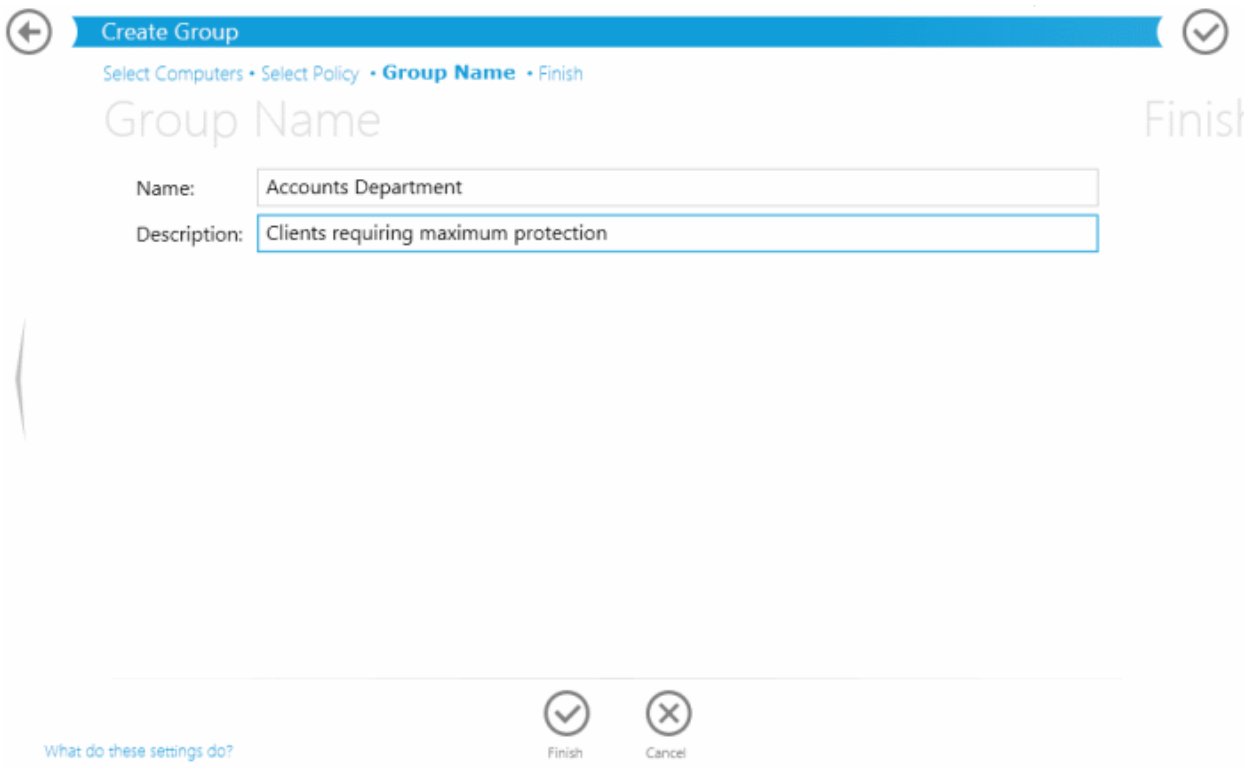
The specifics of each policy are set in the Comodo Internet Security software in one endpoint and can be imported and applied to other endpoints. The Select Policy step allows the administrator to assign a local security policy and Internet security policy for the CIS installations in the endpoints of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



- Select the Local Security Policy and Internet Security Policy for the CIS 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**'.

Step 3 - Naming the Group

The next step is to name the created group.



- Enter a name as the group has to identified by CESM in the 'Name' text field.
- Enter a short description for the created group in the 'Description' text field. This description will appear in the 'View All Computers' Interface.
- Click the right arrow to move to the next step.

Step 4 - Finish

- Upon completion, click the 'Finish' icon (or swipe the screen left) to exit the wizard

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

Note: The policy can be changed for individual endpoints as desired from the '**View All Computers**' interface in the section that follows.

2.3.3. Viewing Endpoints

The 'View All Computers' interface plays a key role by providing system administrators with the ability to view and manage networked computers and their groups that have the agent installed.. The interface displays all defined groups and the managed endpoints within each group. See **Adding Endpoint Computers to CESM** for help deploying the Agent.

From this interface the administrator can:

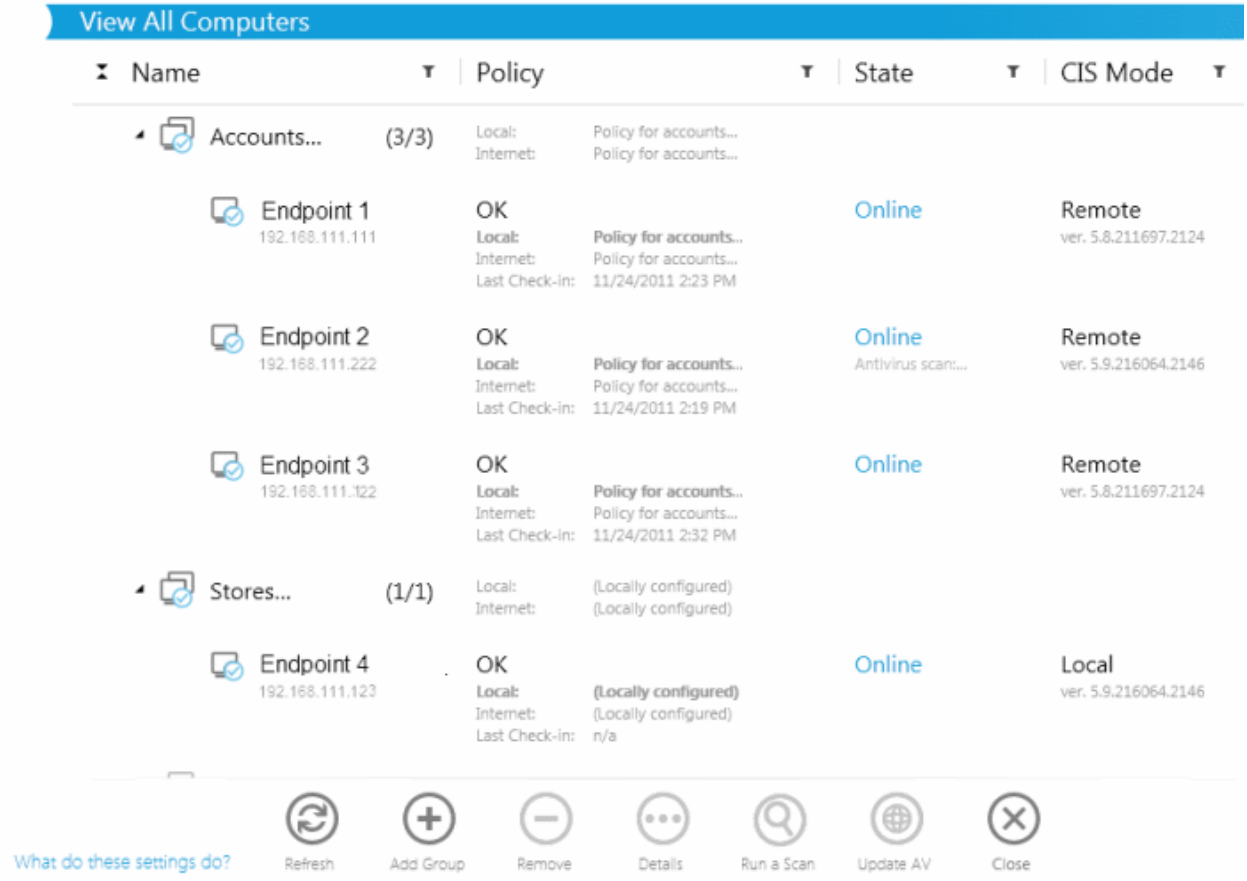
- View a summary on details such as security policy applied, online/offline status and CIS management mode of each group/endpoint from the View All Computers interface
- View granular details of each group and endpoint
- Edit a Group to add or remove member endpoints and to change default security policies assigned to the endpoints
- Edit the security policies assigned to endpoints individually
- Create a new group and add endpoints to it
- Launch and observe progress of tasks like running an antivirus (AV) scan and updating AV database on selected

endpoint(s) or group of endpoints

- Remove groups or endpoints from CESM

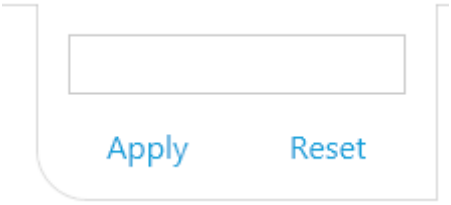
To access the 'View All Computers' interface, click the 'View ' tile from the 'Computers' area.

The View All Computers interface will open.

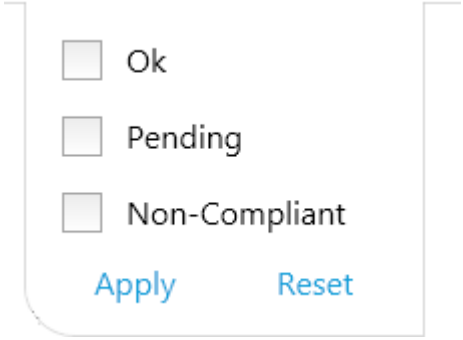


.

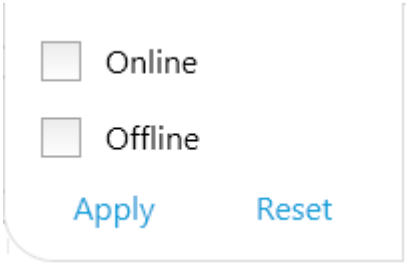
- Click the icon to display only the groups. Click it once again to display all the endpoints in the groups.
- Click the icon beside any of the group name to expand or collapse the endpoints within the respective groups.
- Click the filter icon in the 'Name' column header to search for a particular endpoint, enter the endpoint name and click 'Apply'.



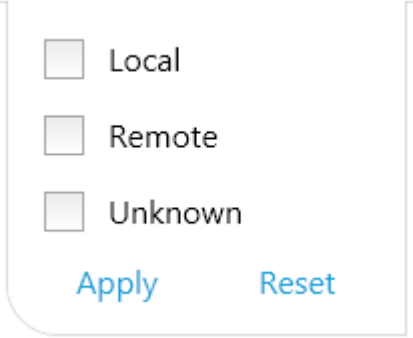
- Click the filter icon in the 'Policy' column header to search for a particular endpoint, select the required checkbox and click 'Apply'.



- Click the filter icon in the 'State' column header to search for a particular endpoint, select the required checkbox and click 'Apply'.



- Click the filter icon in the 'CIS Mode' column header to search for a particular endpoint, select the required checkbox and click 'Apply'.



- Click 'Reset' to expand all the endpoints in the list.

View All Computers Interface - Table of Column Descriptions

Column Heading	Description
Name	Displays the name of the Group or the Endpoint computer. For the Groups - The description provided for the group by the administrator will be displayed beneath the Group name. For Endpoints - The IP address of the endpoint will be displayed beneath the computer name. Also, the endpoint icon indicates whether the endpoint is online or offline. The status of all endpoints in a group will display or "bubble up" to their group icon. - Indicates that the endpoint is online and connected to CESM - Indicates that the endpoint is offline and not connected to CESM - Indicates that the endpoint is added but the license has expired
Policy	Displays the security policy applied and the compliance status of the endpoints to the applied policy. For Groups - Displays the local connection and Internet connection security policies applied for the group. Any new computer added to the group will be assigned this policy unless it is changed individually. For Endpoints - Displays the compliance status of the CIS 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, along with the time of the last setting change or policy application change. Bold indicates which connection policy was last applied.
	The compliance status can be one of the following:
	• **OK** - The CIS installation at the endpoint is compliant to the applied security policy.
	• **Non-Compliant** - The CIS installation at the endpoint is not compliant to the applied security policy.
	  • For endpoints with CIS in Remote Management Mode - CESM will apply the security policy to the endpoint during the next polling time to make it compliant.
	  • For endpoints with CIS in Local Administration Mode - CIS has to be switched to Remote mode at the endpoint or by using '...Details' to make it compliant. Alternatively, a new policy can be applied to make it compliant.
	• **Pending** - The compliance status of the CIS installation at the endpoint is yet to be assessed.
	For further reading on 'Policies', please see '**The Policies Area**'.

State	Indicates whether the endpoints are online or offline. The current action and/or the last action executed of the endpoint like AV scan or AV update is displayed beneath the state. 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
CIS Mode	Indicates whether the CIS installation in the endpoint is remotely managed by CESM or locally managed. The version number of CIS installed at the endpoint is displayed beneath the mode. The CIS mode can be: • **Local** - The CIS installation at the endpoint is being managed locally. • **Remote** - The CIS installation at the endpoint is being managed remotely. • **Unknown** - The management mode of CIS at the endpoint cannot be established. This may be because CIS is not installed; is not active or because of network problems. The CIS Mode can be changed from the 'Computer Properties' interface > 'Advanced View' of the respective endpoint or by using 'Details....'. Refer to **Viewing Details of an Endpoint Computer and Applying Policies** Individually for more details.

The 'View All Computers' screen also allows the administrator to:

- **Create a new group and add computers into it**
- **View and Edit a group**
- **View details of an endpoint computer**
- **Remove group(s) or endpoint computer(s)**
- **Run AV Scans on selected group(s) or selected Endpoint(s)**
- **Run AV database updates on selected group(s) or selected Endpoint(s)**

Creating a New Group

- Click the Add Group icon  from the bottom of the interface. The Create Group Wizard will be started. Refer to the section **Creating Endpoint Groups** for a detailed description on the wizard.

Viewing and Editing a Group

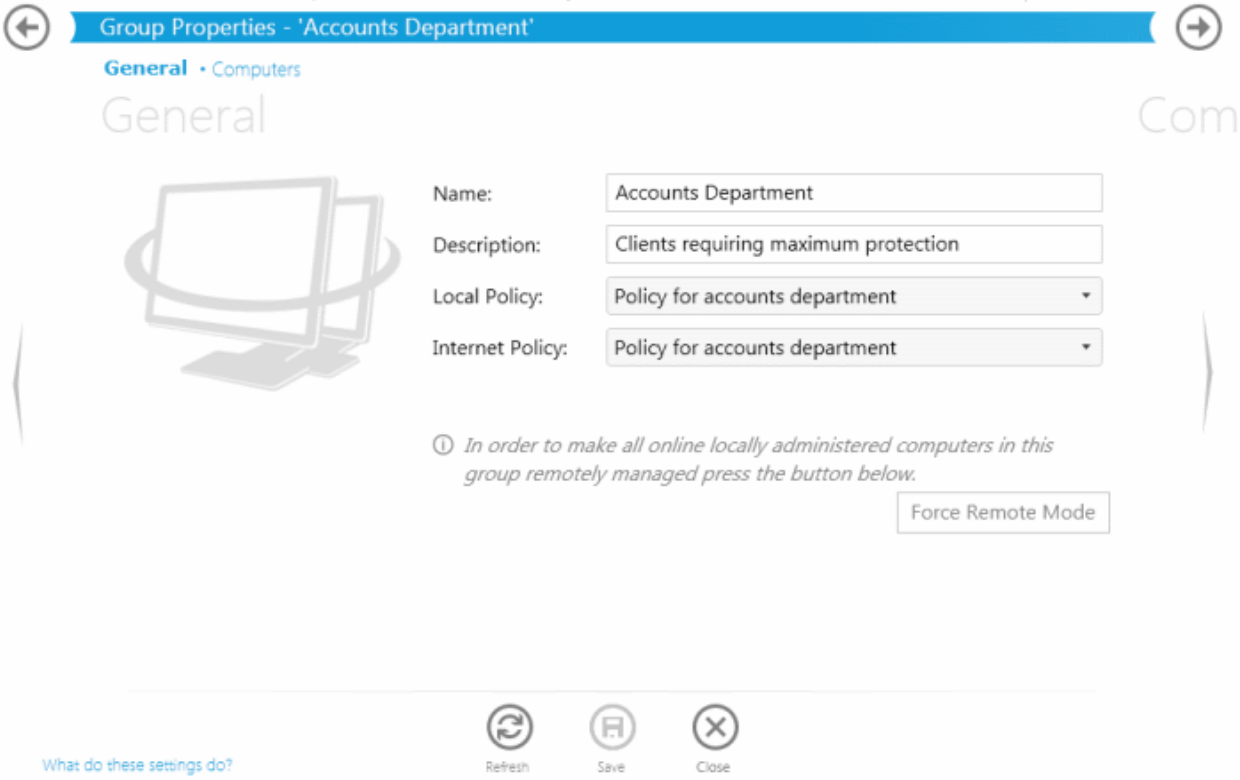
Selecting a group and double-clicking in white space or clicking the Details icon  opens the 'Group Properties' interface. The interface contains two areas:

- **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.

The administrator can switch between these two areas by swiping through the interface or by using the left and right arrows on both sides of the blue title bar.

General Screen

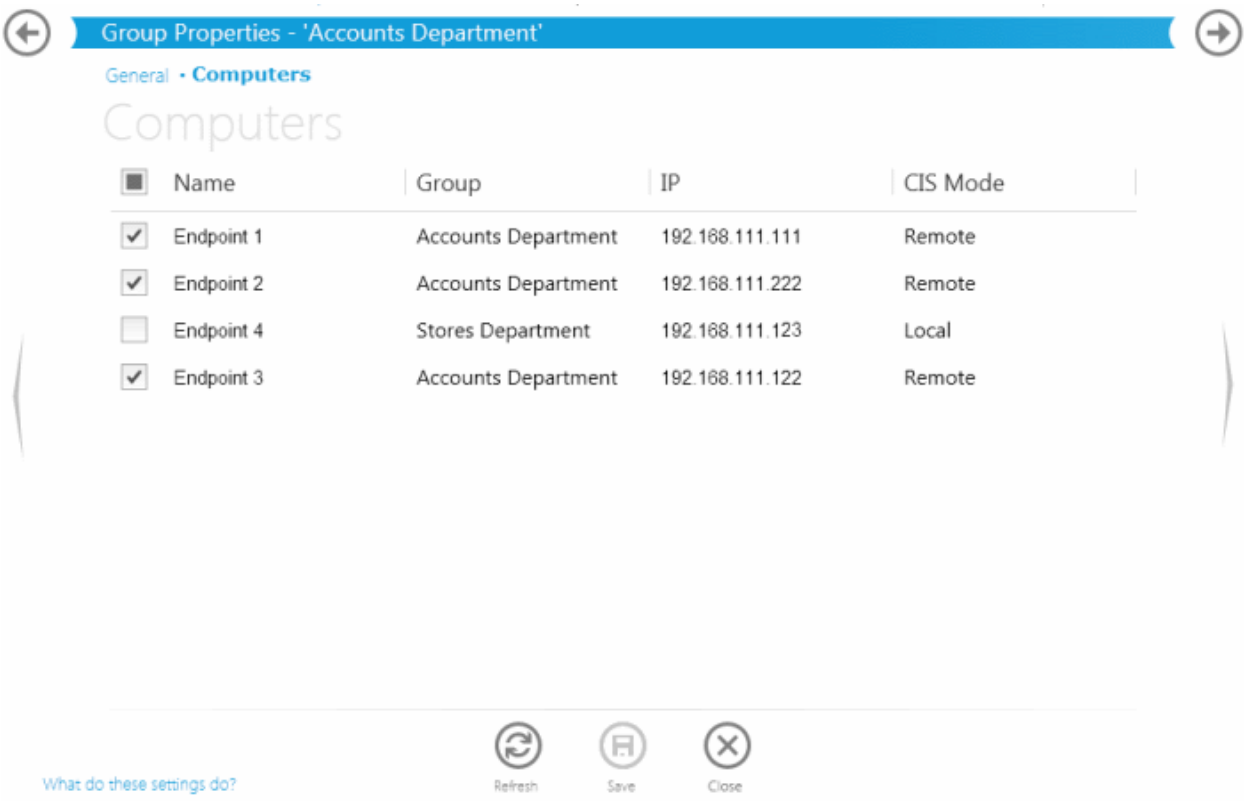
The interface displays the name, description, assigned local and Internet connection security policies of the group.



- To change the name and description, directly edit the respective text fields
- To change the Local and Internet connection security policies applied to the member endpoints of the group, select the policies from the respective drop-downs
- To forcibly change the management mode of CIS installations in the endpoints to Remote mode, enabling management by CESM, click the Force Remote Mode button
- Click 'Save' icon for the changes to take effect

Computers Screen

The Computers interface displays a list of all the computers added to CESM along with details of the group they belong to, IP address and their current CIS management mode. Endpoints that are member of the group are preselected.



- To add more computers to the group, simply select the check-boxes beside the desired computer names
- To remove the existing member endpoints, simply uncheck the items
- Click 'Save' icon for the changes to take effect

Viewing Details of an Endpoint Computer and Applying Policies Individually

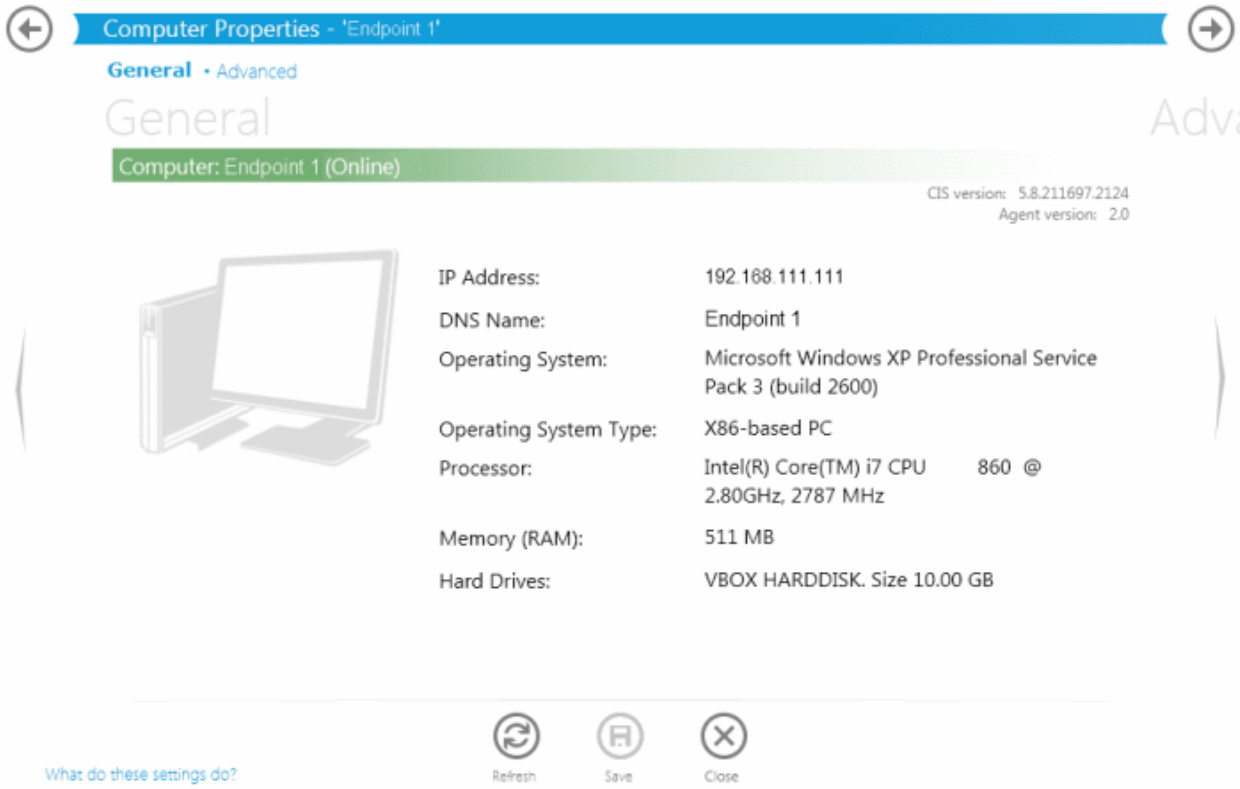
Selecting a group and double-clicking in white space or clicking the 'Details' icon opens the 'Computer Properties' screen. This screen contains two areas:

- General Screen - Displays the general system details like IP address, Computer Name, Hardware Configuration and Operating System details of the endpoint.
- Advanced Screen - Displays CESM connection details like Group to which it belongs, current connection mode, and current security policies applied. The administrator can view the details of the policies and change Local network and Internet connection security policies of the endpoint individually.

The administrator can switch between these two areas by swiping through the interface or by using the left and right arrows on both sides of the blue title bar.

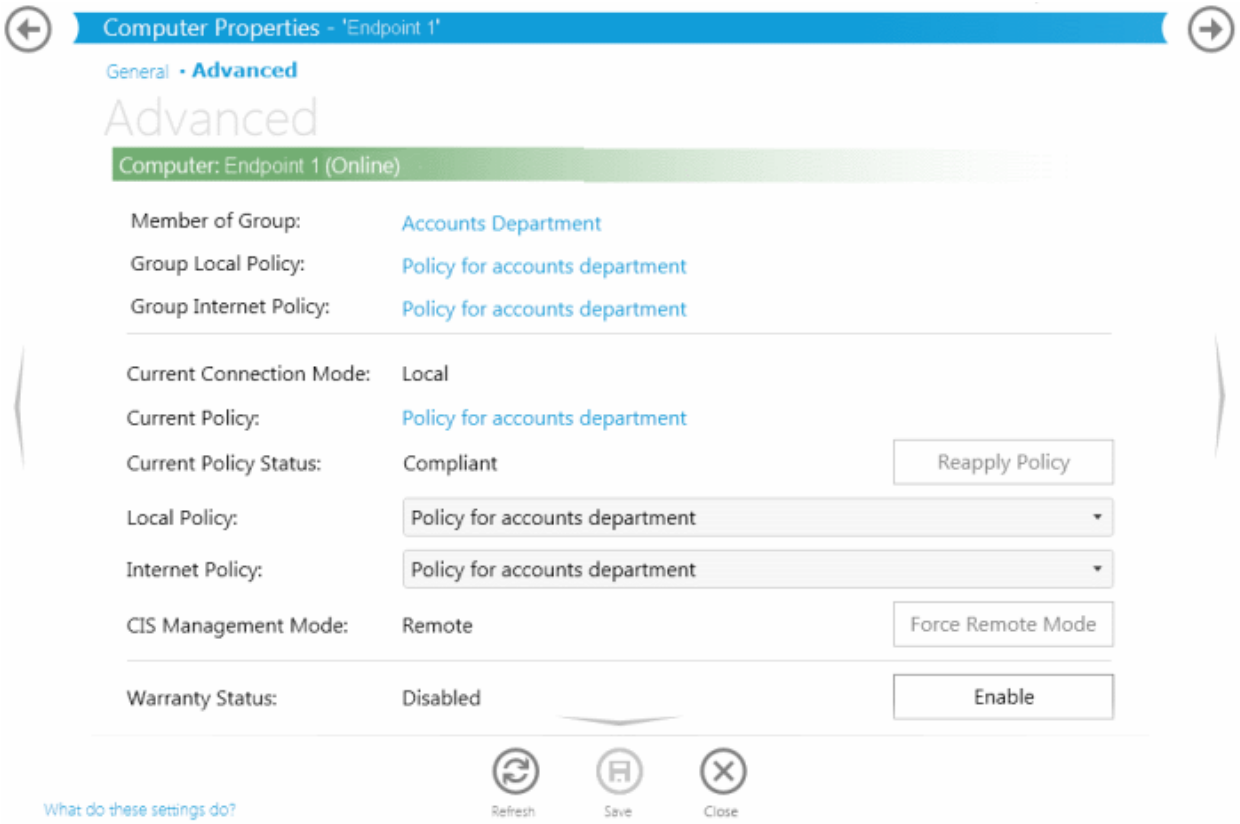
General Screen

The General view area provides the computer related details like the IP Address, Computer name, Operating System and Hardware configuration of the endpoint. The interface also displays the versions of the antivirus (AV) signature database and the CESM agent currently installed at the endpoint at the top right.



'Advanced' Screen

The Advanced area of the Computer Properties interface displays the CESM related details of the endpoint computer.



The upper pane in the Advanced view displays the details of the Group to which the endpoint belongs:

- **Group** - Name of the group. Clicking the Name of the group will open the 'Group Properties' interface of the group.

Refer to Viewing and Editing a Group for more details on this interface.

- Local Group Policy - Displays the Local network connection security policy assigned for the group. Clicking the policy name will open the 'Policy Properties' interface of the policy. Refer to Viewing Details, Editing and Applying a Policy to Endpoints for more details on this interface.
- Internet Group Policy - Displays the Internet connection security policy assigned for the group. Clicking the policy name will open the 'Policy Properties' interface of the policy. Refer to Viewing Details, Editing and Applying a Policy to Endpoints for more details on this interface.

The middle pane displays the details of the endpoint. It also allows the administrator to change the security policy applied to the endpoint individually.

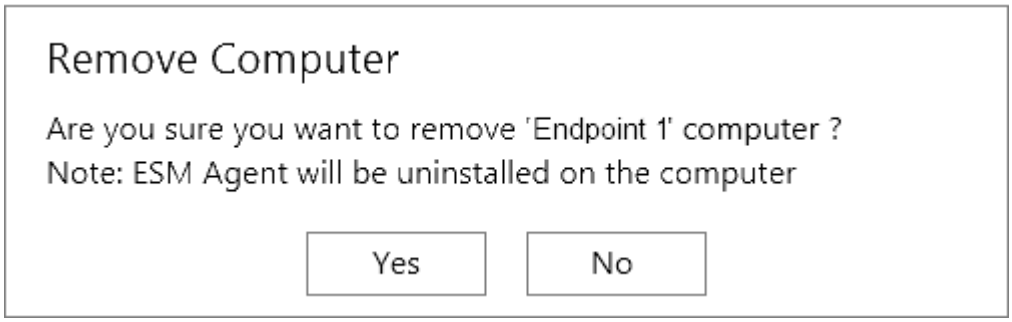
- Current Connection Mode - Indicates whether the endpoint is connected to CESM through local network or Internet, which determines whether the computer will be using the Local Policy or Internet Policy.
- Current Policy - Displays the current security policy applied to the endpoint as per the current connection mode. Clicking the policy name will open the 'Policy Properties' interface of the policy. Refer to Viewing Details, Editing and Applying a Policy to Endpoints for more details on this interface.
- Current Policy Status - Displays whether the endpoint is in complaint or non-compliant policy mode of the group it belongs. If it is non-complaint, click the 'Reapply Policy' button to apply the group's policy to the endpoint.
- 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.
- CIS Management Mode - Displays the current management mode of the CIS installation in the endpoint (either locally managed or remotely managed by CESM). The administrator can forcibly change it to Remote Management mode by clicking the 'Force Remote Mode' button.
- Force Remote Mode - To forcibly change the management mode of CIS installations in the endpoints to Remote mode, enabling management by CESM, click the Force Remote Mode button.

The lower panel displays the warranty status of the endpoint. If it is disabled, click the 'Enable' button.

Removing Groups or Endpoints

Administrators can remove groups or individual endpoints by simply selecting them and clicking the 'Remove' icon .

A confirmation dialog will be displayed:



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

Tip: Press and hold Shift or Ctrl key on the keyboard to select multiple items.

Running Antivirus Scans

The 'View All Computers' interface allows the administrator to run Antivirus (AV) scans on Group(s) or Endpoint(s) directly just by selecting them then clicking the 'Run a Scan' icon . The scan will start immediately and the progress will be displayed under the status column of the target computer(s).

- If malware is discovered during the scan that is not handled successfully (deleted, disinfected or quarantined) then the

'Malware Found' and/or 'Infections' tiles on the dashboard will turn red and display the number of samples and/or affected endpoints. Malware that is successfully dealt with will not show on the 'Malware Found' tile.

- Admins can also receive email notifications upon malware discovery. To set up notifications, click 'Dashboard' > Click 'System Status' at the bottom of the 'Malware Found' tile > Click the 'Edit' icon to open 'System Status Tile Properties > Select 'Send Email Notifications' checkbox (make sure 'Malware Found' is displayed in the drop down box).
- The results of the scan can be viewed as an Infection report from the Reports area - click 'Reports' then the 'Computer Infections' tile. 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.

Running AV Updates

The View All Computers interface allows the administrator to update Antivirus (AV) signature database on Group(s) or Endpoint(s) directly just by selecting them and clicking the 'Update AV' icon . The update process will start immediately and the progress will be displayed under the state column of the target computers.

2.4. The Policies Area

A policy is the security configuration of Comodo Internet Security (CIS) deployed on an endpoint or a group of endpoints. Each policy determines the antivirus settings, Internet access rights, firewall traffic filtering rules, sandbox configuration and Defense+ application control settings for an endpoint.

The 'Policies' area allows administrators to import and manage security polices for endpoint machines and consists of two tiles:

- **View All Policies** - Allows administrators to view, add, reconfigure and export CESM polices
- **Create Policy** - A step-by-step wizard that takes admins through the policy import, specification and deployment process

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 CIS configured and tested on a local machines via the standard CIS interface.
- Policies can be imported from an endpoint into the CESM 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 CIS 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 CIS components that may be installed on an endpoint:- Antivirus, Firewall, and Defense + settings. A policy which excludes settings for one of the CIS components installed on the endpoint receiving policy is considered as locally configured (see below) for the settings of that component.
- The CESM agent installed at each endpoint is responsible for connecting the target machine to the respective CESM server and the remote management of the CIS installation. Only the agent applies the security policy settings to different components of the CIS 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 CIS 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 CESM from an IP address outside the local network.
- Policy and CIS Mode are independent of each other. 'CIS Mode' can be either 'Local' or 'Remote' and this determines whether or not CESM will enforce policy compliance on an endpoint:
    - Remote Mode - The policy of an endpoint in remote management mode will be determined by the CESM console. If the endpoint falls out of compliance (because CIS settings have been altered) then the console will automatically re-apply the assigned policy to the endpoint. This is the ideal situation for ongoing management.

      Exception - if the policy is 'Locally Configured' then remote mode have no effect (see below).
    - Local Mode - An endpoint that is locally managed effectively takes the machine 'offline' so CESM will not automatically re-apply assigned policy if an endpoint falls out of compliance. This allows administrators to change a policy at the local machine without having CESM constantly re-apply the 'old' policy in the background. Once policy specification is complete, the admin can return to the console, import the new policy and deploy it to target machines. The source machine can then, optionally, be returned to remote mode.
    - Policy, as mentioned earlier, refers to the actual security configuration of CIS. An endpoint can have any chosen policy and can be in either 'Remote' or 'Local' mode.
- 'Locally Configured' policy. 'Locally Configured' policy means that CIS settings can be managed by the local user and policy compliance will not be enforced by CESM. Machines or groups with this policy will always report compliance status of 'OK'. Changes made to the CIS 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 CIS configuration settings will be restored to it.

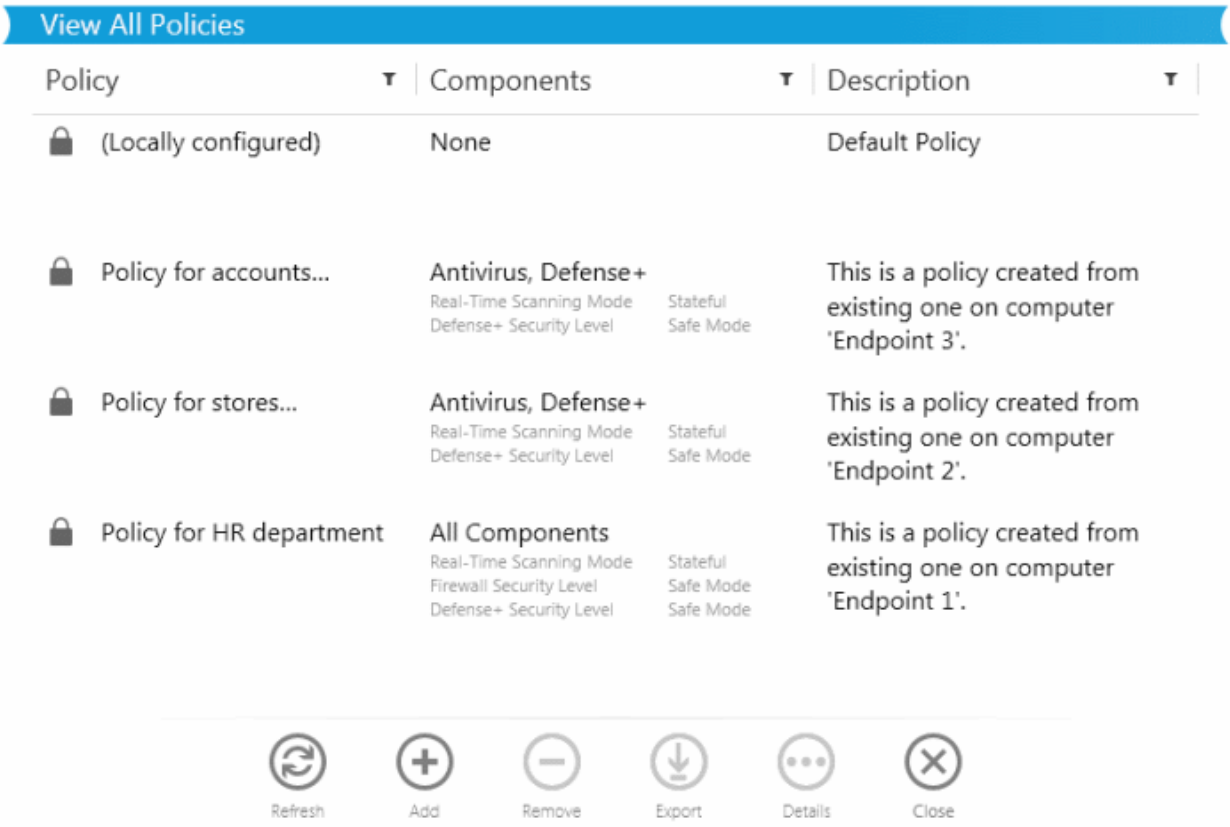
2.4.1. Viewing Policies

The 'View All Policies' interface enables the administrator to:

- View a list of all policies along with their descriptions and the CIS component covered by the policy
- View and modify the details of any policy - including name, description, CIS components, target computers and whether the policy should allow local configuration
- Add or remove policies as per requirements
- Export any policy to .xml file

To open the interface, click the 'View' tile from the Policies interface:

The 'View All Policies' interface will open with the default view being a list of all policies:



- Click the filter icon in any of the respective column header to search for a particular policy, component or policy description, enter or select and click 'Apply'
- Click 'Reset' to display all the items

View All Policies Interface - Table of Column Descriptions

Column Heading	Description
Policy	Displays the name of the Policy.

Description	Displays the description of the policy as entered during its creation or last modification.
Components	Indicates the components of CIS for which the policy applies the configuration settings.

The 'View All Policies' interface also allows the administrator to:

- Create a new policy
- Export a policy into an xml file for importing to CESM at a later time
- View details, edit and apply policies to groups or selected endpoints individually
- Remove policies

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 CESM can be saved as a .xml file to the computer running the administration console. The .xml file can be imported into CESM 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 'View All Policies' interface to highlight it. Click the Export icon. The Windows 'Save As' dialog will appear.
- Select the destination in the computer from which you are accessing CESM, provide a file name and click 'Save'.

The policy will be saved as an xml file. The file can be imported into CESM at any time.

Viewing Details, Editing and Applying a Policy to Endpoints

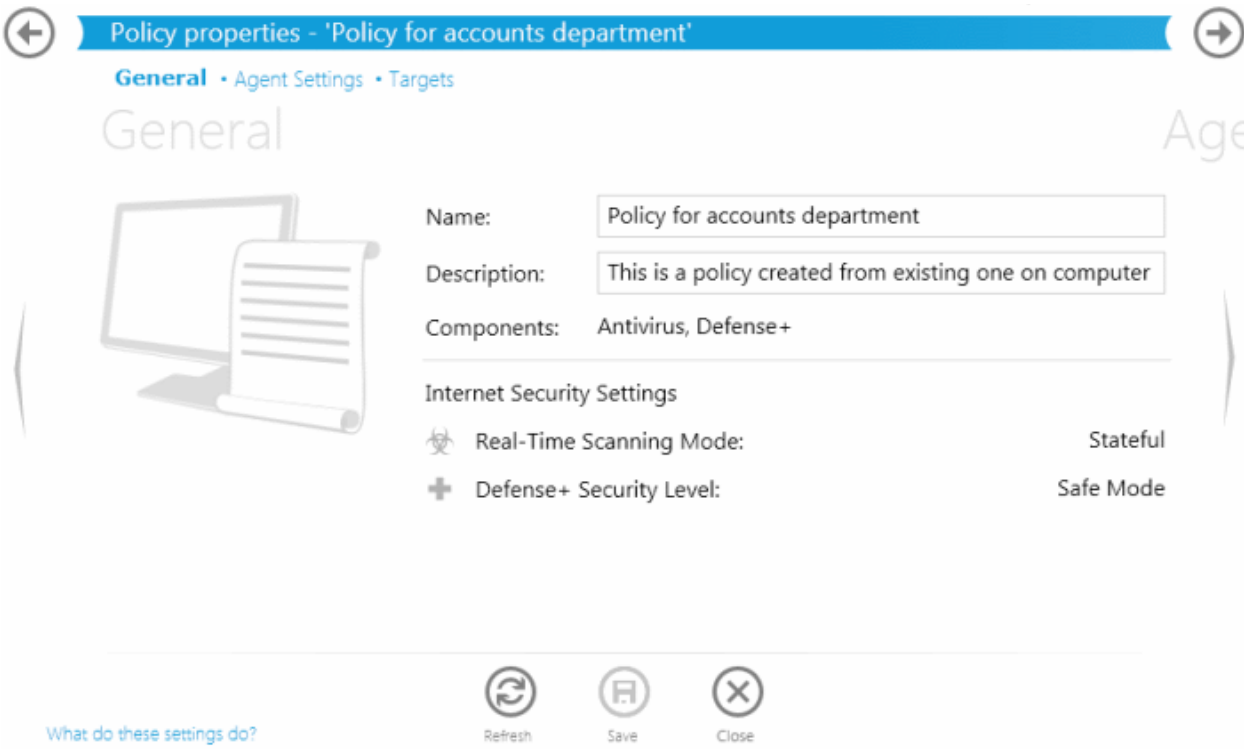
Selecting a policy and clicking the Details icon opens the 'Policy Properties' interface. The interface contains three areas:

- General View - Displays the general system details like name and description of the policy. The administrator can can edit these details directly.
- Agent Settings - Enables the administrator to configure the CESM agent deployed onto the endpoints as per the policy.
- Targets - Enables the administrator to select target endpoint group(s) on which the selected policy has to be applied.

The administrator can switch between these areas by swiping through the interface or by using the left and right arrows on both sides of the blue title bar.

'General' Screen

The General screen shows the name and description of the Policy.



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.

Agent Settings

The agent settings interface allows the administrator to configure how these agents should behave on application of the policy. See **Step 4 – Agent Settings** in the section **Creating a New Policy** for a detailed description of this interface.

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

'Targets' Screen

The '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

See **Step 5 – Selecting Targets** in the section **Creating a New Policy** for a detailed description of this interface.

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

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 Remove icon.

A confirmation dialog will be displayed.

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

Note: Policies which are currently applied and used by groups or endpoints cannot be deleted. Before removing an unwanted policy, the administrator has to apply a different policy to the groups/endpoints to which this policy is currently applied.

Tip: Hold Shift or CTRL to select multiple items.

2.4.2. Creating a New 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 CESM, so that CESM will not overwrite the policy on new discovered computers once the agent is installed in it.

To start the 'Create Policy' wizard

Click the 'Create' tile from the 'Policies' area.

The wizard will start with Step 1- Source Type. The remaining steps are displayed below the blue title bar with the current step highlighted in blue. To move backwards or forwards between steps, use the arrows on either side of the title bar (or left click and drag to swipe the screens left or right) or click a step with a clickable active link (light blue) below the blue title bar.

Step 1 - Select Source Type

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

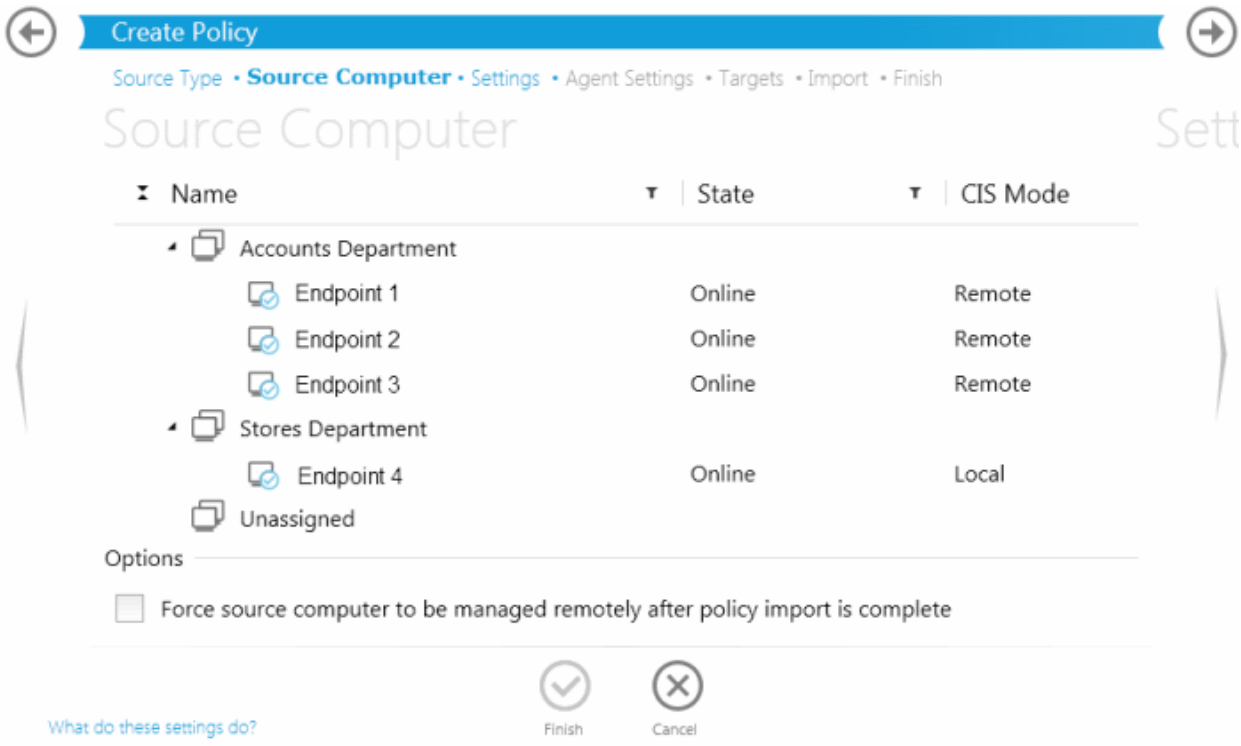
Tip: You might create a policy from another policy if you want to exclude a CIS component from policy but use the settings in other components, or change the agent-specific settings of the policy(such as to have a different compliance polling interval, or to disallow local mode access) for a particular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

Importing from Computers

- Choose 'Computers' 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 - Selecting Source Computer

Step 2 - Selecting Source Computer

All endpoint computers added to CESM will be displayed according to group membership.



- Select the computer from which you wish to import the settings. The computer should have CIS installed and be in local mode, configured as per requirements, and should be online to enable CESM to import the settings.
- Clicking the icon displays only the groups. Click it once again to display all the endpoints in the groups.
- Click the filter icon in the 'Name' column header to search for a particular endpoint, enter the name and click 'Apply'.

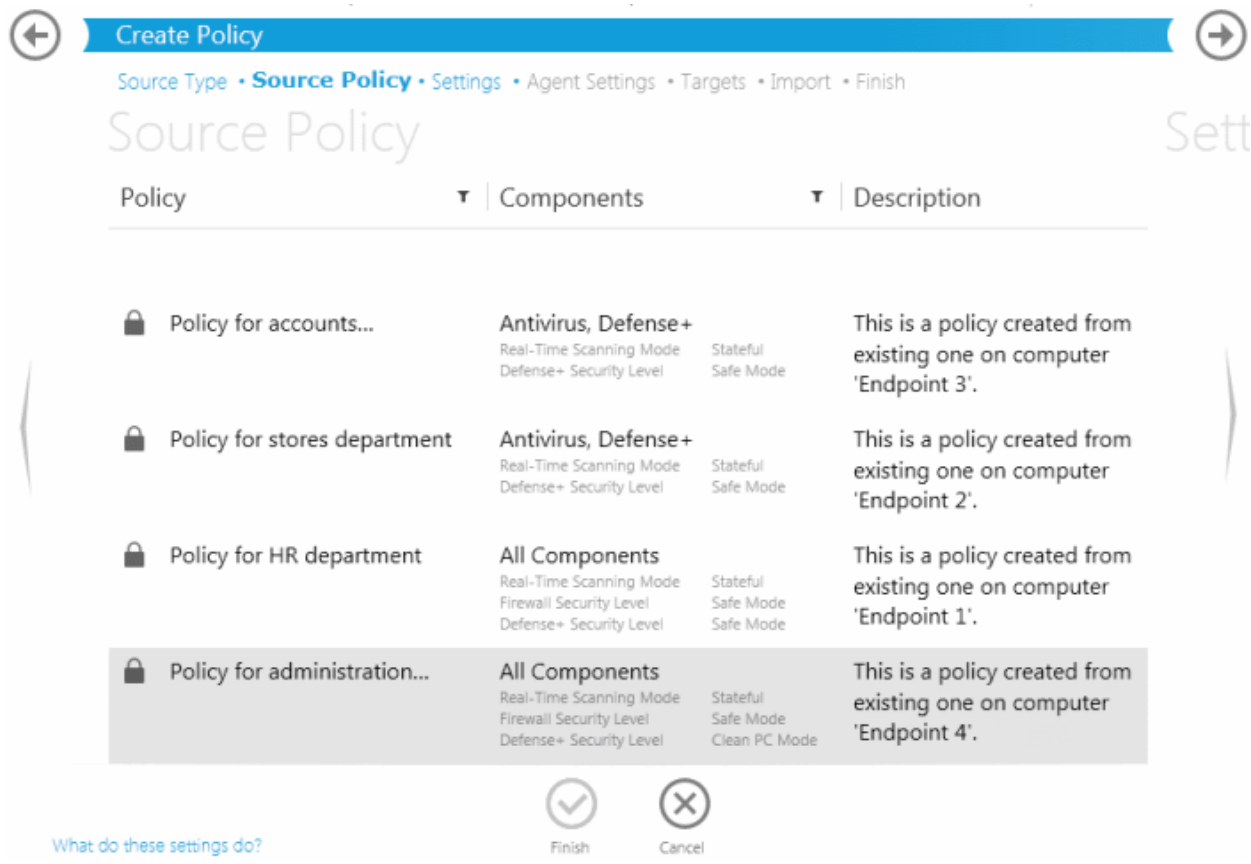
- Click the filter icon in the 'State' column header to search for endpoints that are in online or offline mode and click 'Apply'.
- Click 'Reset' to display all the items.
- **Options:**
  - **Force source computer to be remotely managed after policy import is complete** - To configure the settings 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 '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 CIS components configured by them is displayed.

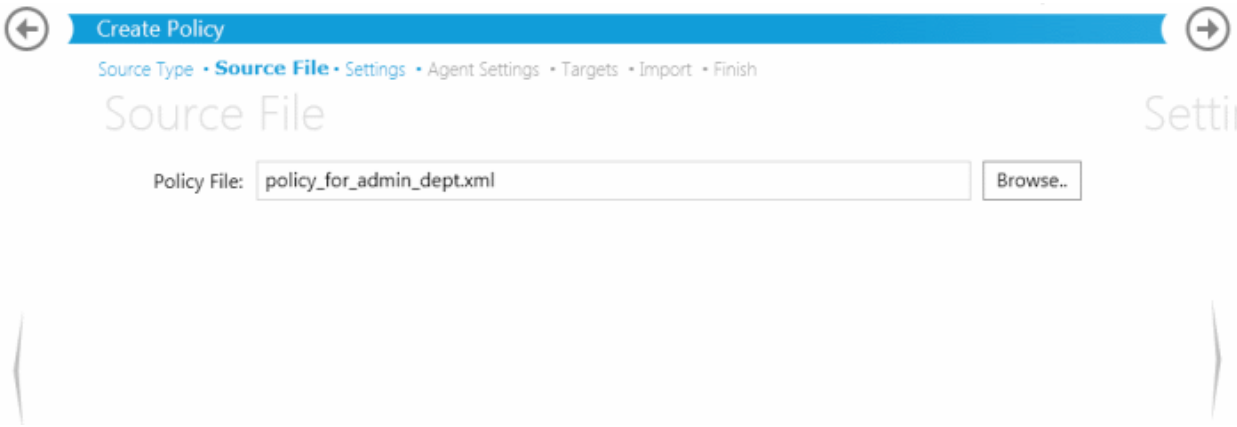


- Click the filter icon in any of the respective column header to search for a particular policy or component, enter or select and click 'Apply'
- Click 'Reset' to display all the items
- Select the source policy from which you wish to create a new policy and click the right arrow to move to **Step 3 – Settings**

Importing from a saved XML File

- Choose 'A saved Policy 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.

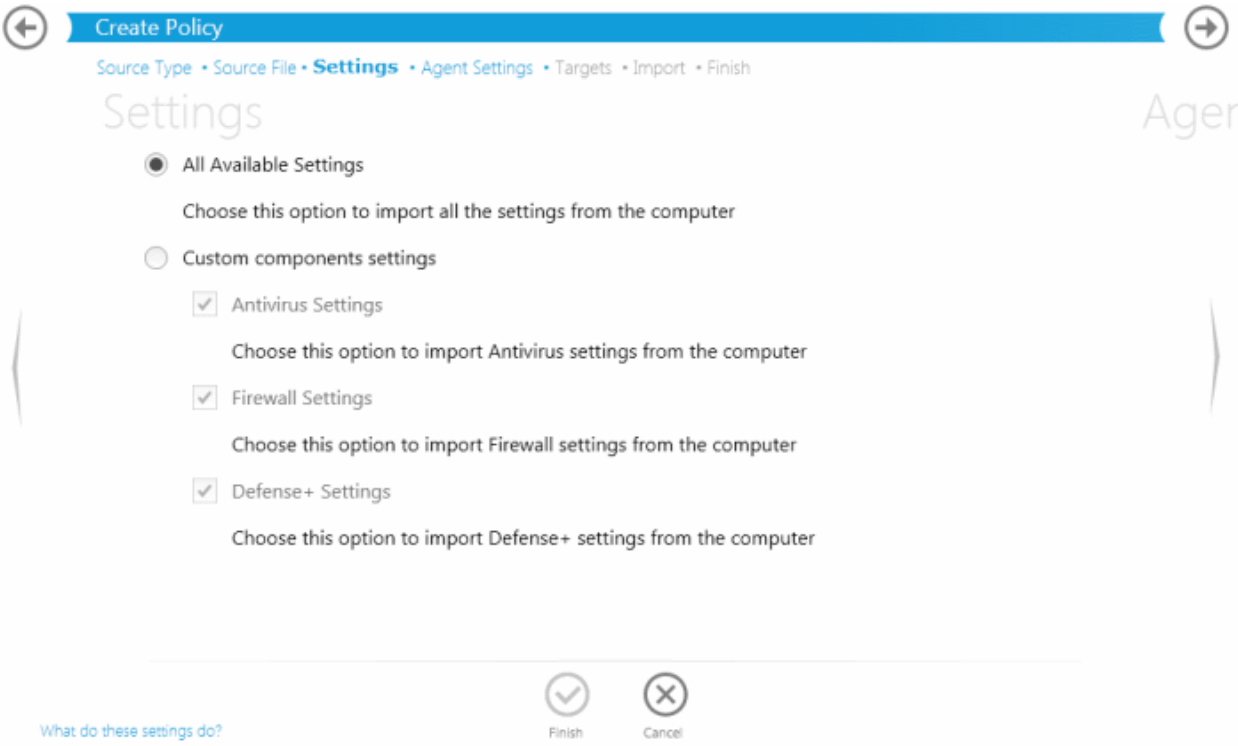
Step 2 - Selecting Source File



- Type the path of the location where the policy xml file is saved or click 'Browse' and navigate to the required policy XML file
- Click the right arrow to move to **Step 3 - Settings**

Step 3 - Settings

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



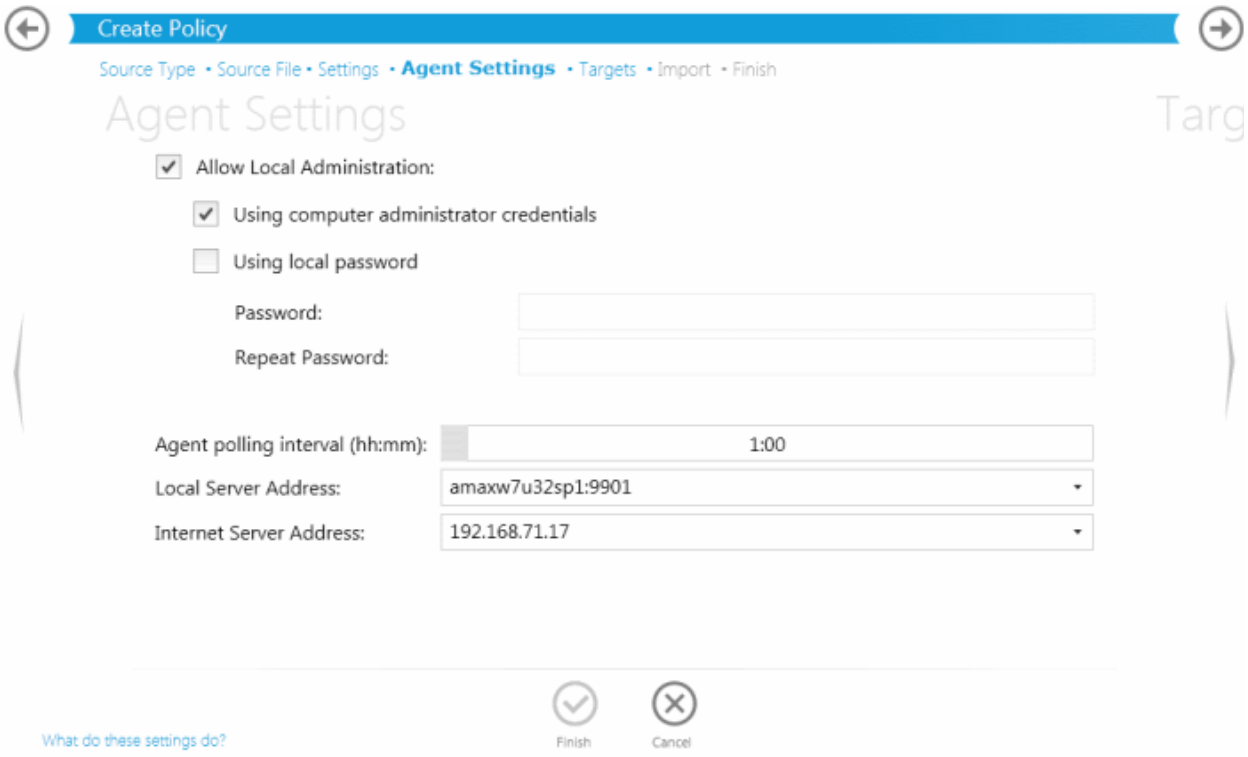
- **All Available Settings** - Imports all the settings from the source selected in the chosen step 2, above
- **Custom components settings** - Enables the administrator to select the components of CIS so that only those settings corresponding to the selected components are imported into the policy from the source selected in step 2

- **Antivirus Settings** - Imports the settings relevant to the Antivirus component
- **Firewall Settings** - Imports the settings relevant to the Firewall component
- **Defense+ Settings** - Imports the settings relevant to the Defense+ component

- Make your selections and click the right arrow to move to step 4 - Agent Settings

Step 4 - Agent Settings

The next step allows the administrator to configure the CESM agent installed at the target computers, for which the policy has to be applied.



- **Allow Local Administration** - Configures the agent to allow the CIS 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:
  - **Using computer administrator credentials** - Selecting this option will require the computer user to either have administrative credentials or enter credentials while switching CIS at the target machine to local administration mode.
  - **Using local password** - Allows the administrator to specify a password in the text box below this option. This password should be entered for switching the CIS 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 CIS 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: CESM can also be configured to alert the administrator by sending automated emails on the occurrence of a target computer going non-compliant. See System Status Tiles for more details.

- **Local Server Address** - The administrator can specify the address of the server machine in the local network, on which

the CESM central service is installed.

- **Internet Server Address** - The administrator can specify the address of the external server on which the CESM central service is installed if the endpoint should connect to the CESM 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:

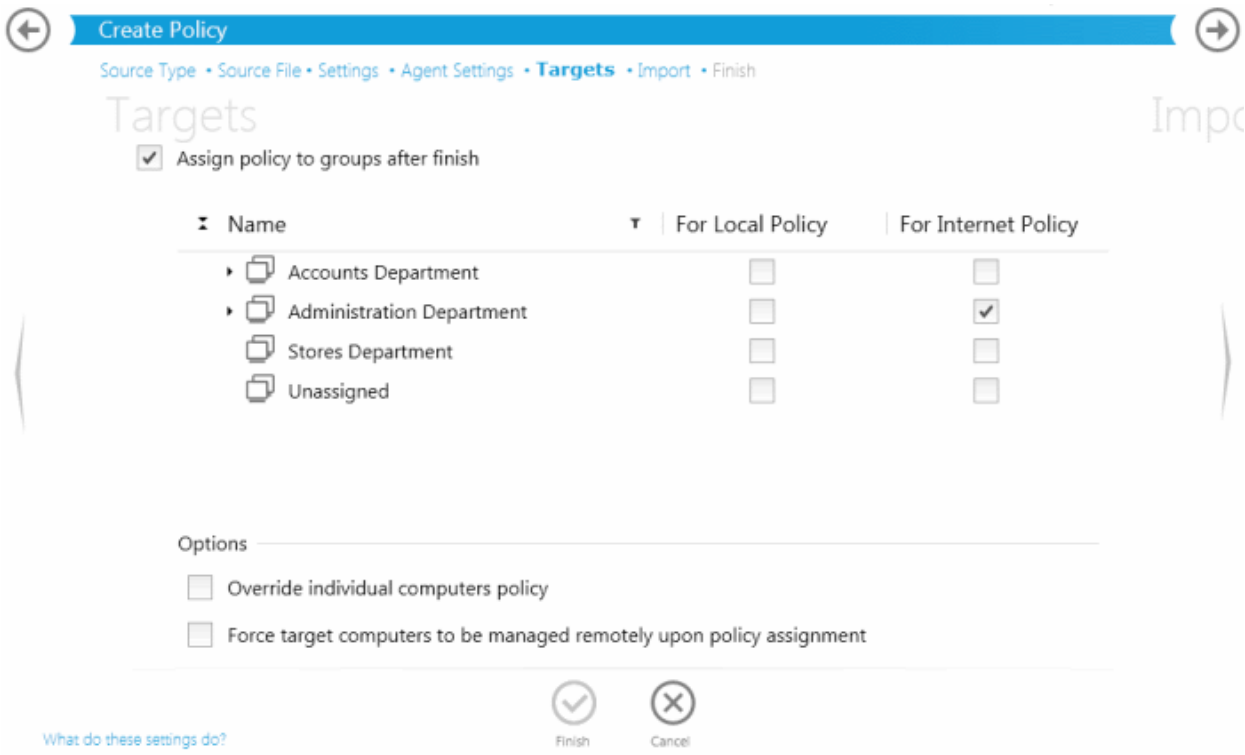
1. The Local Server Address value, mandatory in policy settings, specifies that if this connection is established Local Policy should be applied.
2. Internet Server Address value is optional in policy settings. If specified it is tried to be reached ONLY if the specified local address connection fails. 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 the right arrow to move to the step 5 - Selecting Targets.

Step 5 - Selecting Targets

The administrator can select the target computer group(s) onto which the created policy has to be applied.



- Click the check box for 'Assign policy to groups after finish' if you 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 Viewing Policies 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' checkbox.
- For the group(s) of computers connected through the Internet you wish to apply the new policy, select 'For Internet Policy' checkbox.
- **Options**:
  - **Override individual computers policy** - Selecting this option will apply the new policy onto target computers in

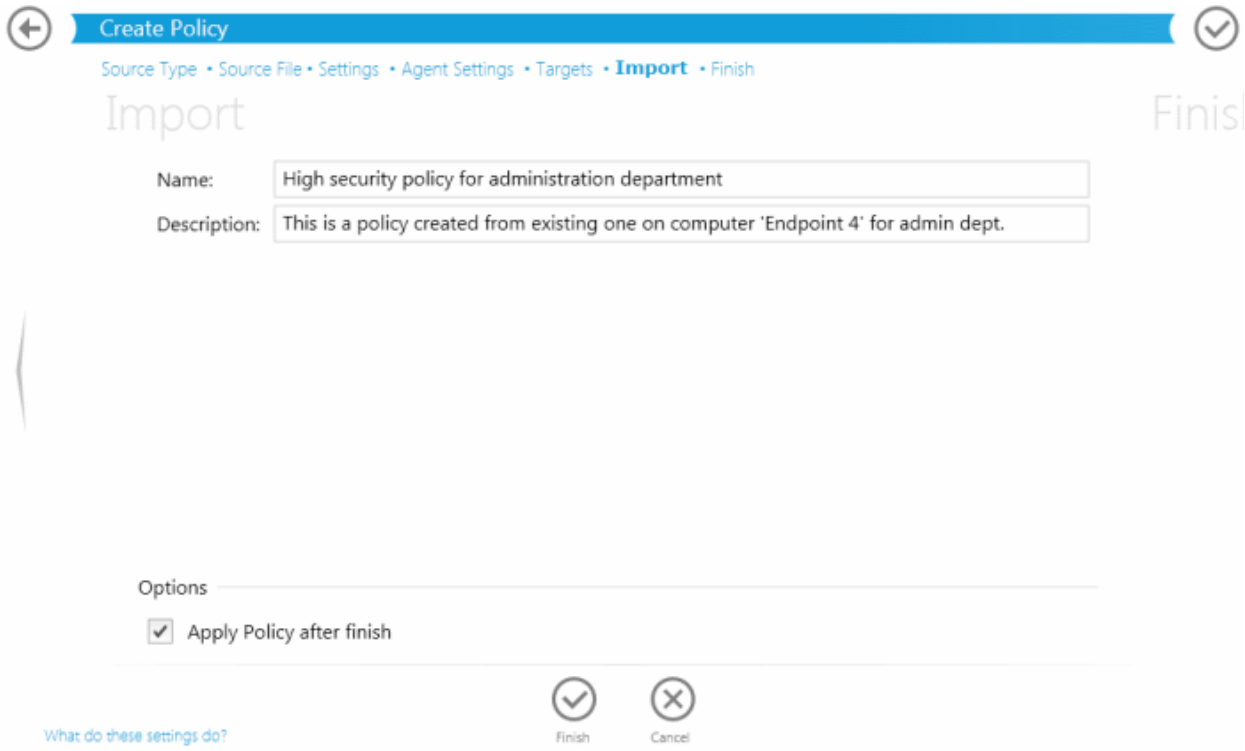
the selected groups that currently have individual policies that differ from the group policy, thereby reverting their policies to come from their group membership.

- **Force target computers to be remotely managed upon policy assignment** - Selecting this option will forcibly switch the CIS installations in the selected target endpoints to remote management mode on assigning the new policy, irrespective of their current management mode.

- Make your selections and click the right arrow to move to step 6 - Importing the Settings and Creating the Policy.

Step 6 - Importing the Settings and Creating the Policy

The next step requires the administrator to specify a name and provide a description for the policy created.



- **Name** - Enter a name according to criteria deemed suitable to the security settings.
- **Description** - Enter short text that best describes the policy.
- **Options:**
  - **Apply Policy after Finish** - The newly created policy will be only be applied to the target endpoints immediately if this checkbox is selected. If not selected, **the endpoints will pick up the new policy when they check in at the next policy poll.**

Note: This option will be available only if you had selected 'Assign policy to groups after finish' checkbox in the previous step 5.

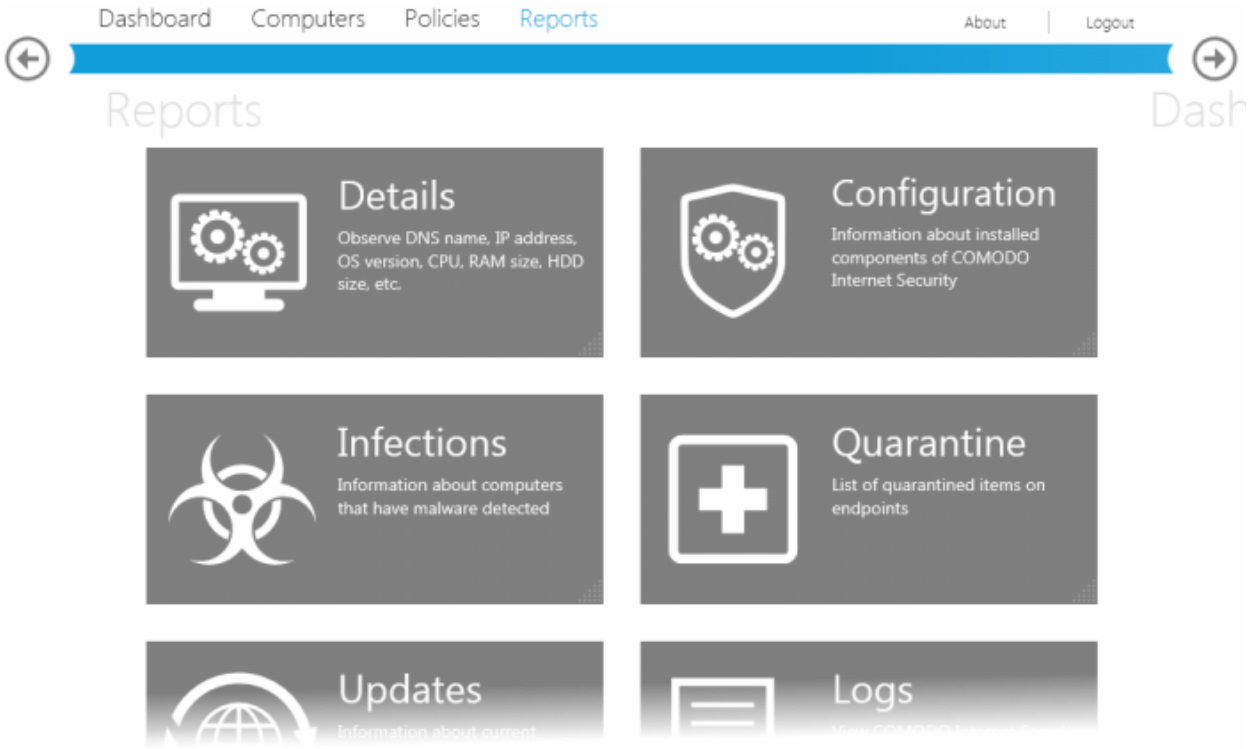
- Make your selection and click the Finish icon or swipe the screen to left to complete the policy creation process. On completion:
  - The 'View All Policies' interface will open with the new policy added.
  - The new policy will be applied to the target computers selected in step 5 as per the options selected in the same.

2.5. The Reports Area

CESM Active 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' so problems can be immediately addressed and can be

ordered for anything from a single machine right up to the entire managed environment. Administrators can filter reports by results returned and use the links in each report to drill-down to underlying data.

Reports can be exported to .pdf or spreadsheet format for printing and archiving purposes.

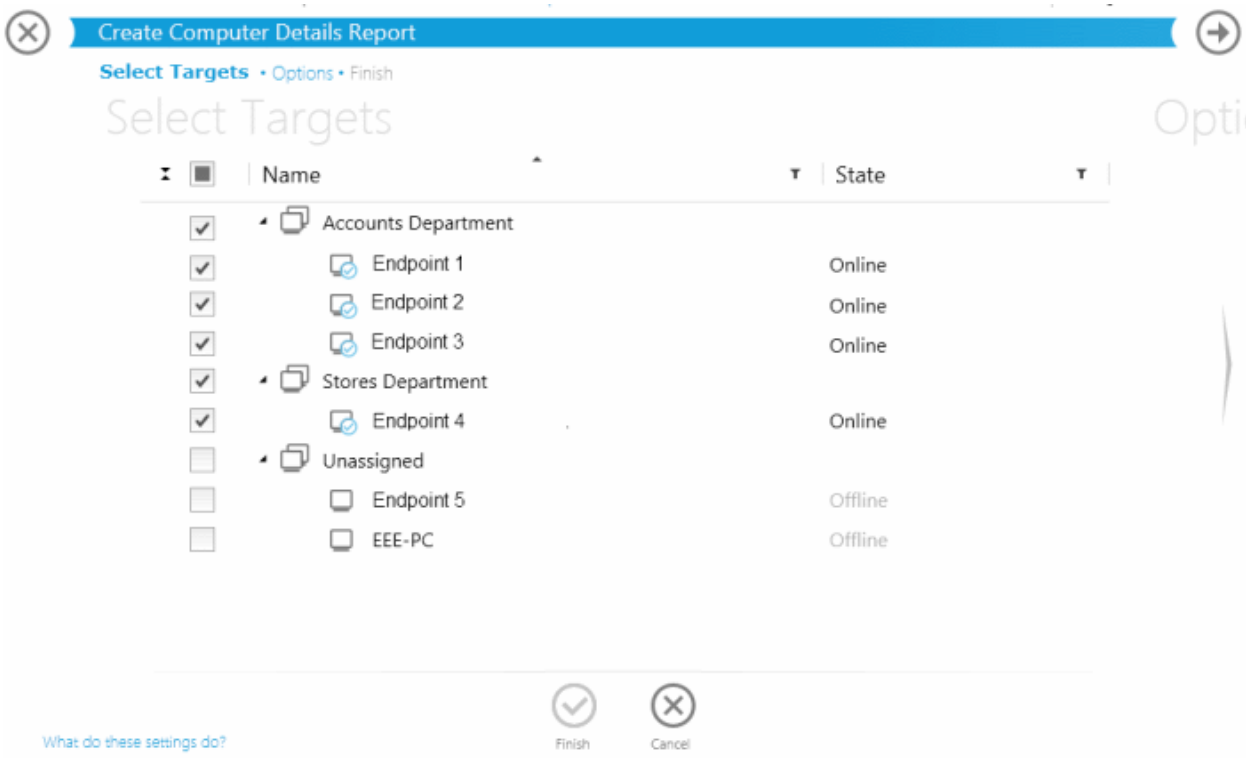


Available report types are:

- **Computer Details** - General information about target endpoint(s) such as operating environment and hardware details.
- **CIS Configuration** - Information on components of CIS installed at the endpoints and their configuration status.
- **Computer Infections** - Information on malware discovered during the antivirus (AV) scans and not handled successfully (deleted, disinfected or quarantined) locally by CIS and the endpoints affected by them.
- **Quarantined Items** - Information on virus and other malware identified by AV scans and quarantined locally by CIS.
- **Antivirus Updates** - Information on versions of AV signature databases at the endpoints.
- **CIS Log** - Logs of events related to CIS at the endpoints.
- **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.
- **Malware Statistics** - Statistical information on the malware detected at various AV scans run on the target endpoint(s), with the actions taken against them.
- **Top 10 Malwares** - A list of top-ten malware discovered during the antivirus (AV) scans from the target endpoints during the specified time period.

Sorting the Entries

Clicking on the arrow in the middle of the 'Name' column header sorts the endpoints in their respective groups in ascending/descending order.



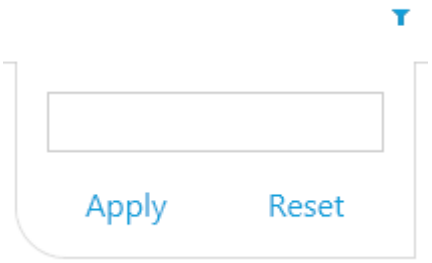
Filtering the Entries

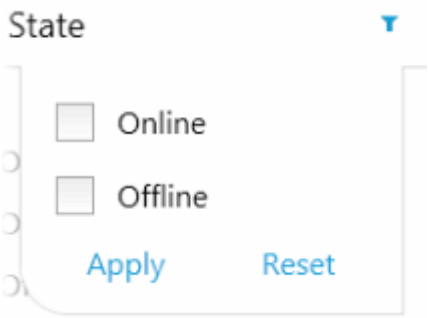
The report enables the administrator to filter the entries based on any criteria like computer name, malware name and location. This is helpful to the identify specific item(s) that the administrator wishes to remove permanently from the target computers or to restore them from quarantine to their original location in the target endpoint.

To filter the results:

- Clicking the icon displays only the groups. Click it once again to display all the endpoints in the groups.
- Click the icon beside any of the group name to expand or collapse the endpoints within the respective groups.
- Click the filter icon in any of the respective column header to search for a particular item.

The filter drop-down will appear.





- Type or enter the filter criteria fully or partly or select the required checkbox and click 'Apply'.

Only the entries that match the criteria will be displayed in the report.

- Click 'Reset' to display all the items.

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 icon at the bottom of the report page. You can choose the printable file to be generated in portable document (.pdf) or spreadsheet (.xls) format.

Viewing the Report

The Active Reports™ elements within a report are clickable links that lets you drill down to such information as you may need to further troubleshoot or view details about, for example, a listed computer. Clicking the computer name from the list opens the 'Computer Properties' interface – clicking Close icon will take you back to the report.

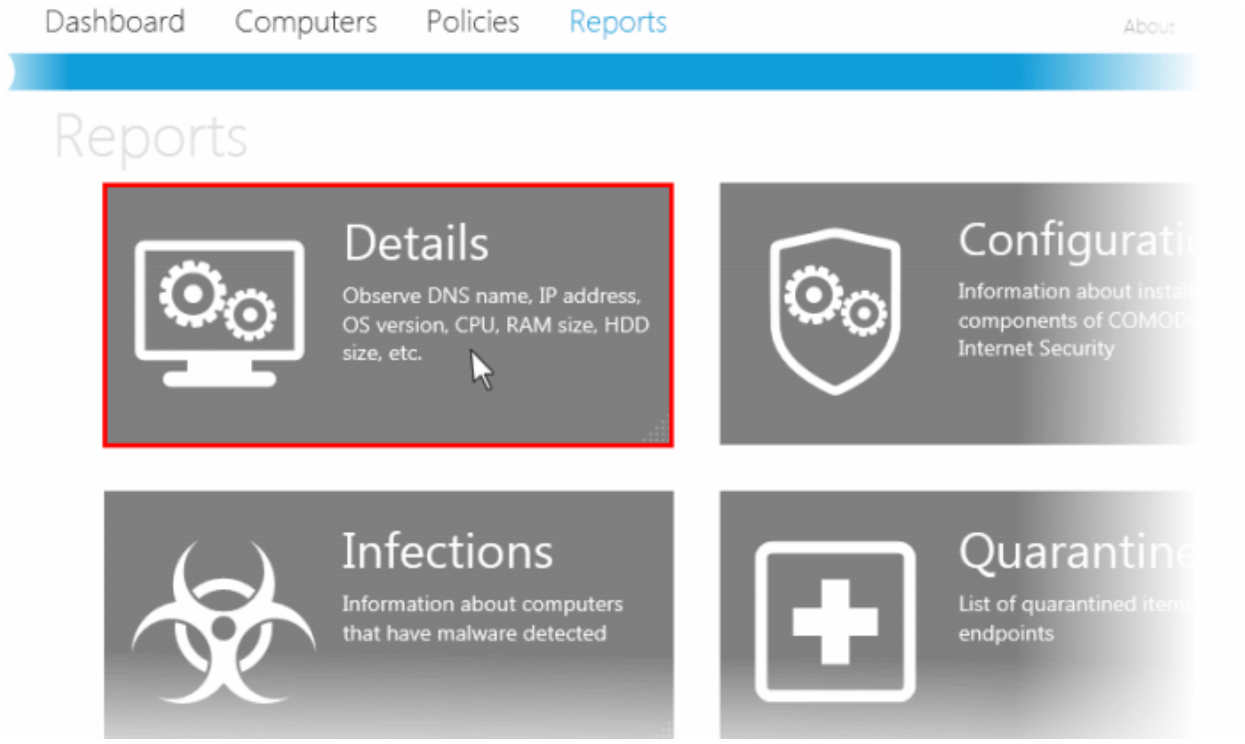
In addition, certain additional buttons may appear in a report – these allow single-click remediation of issues shown in the report, such as to run a scan on infected computers or reapply policy to computers that are non-compliant.

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

2.5.1. 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.

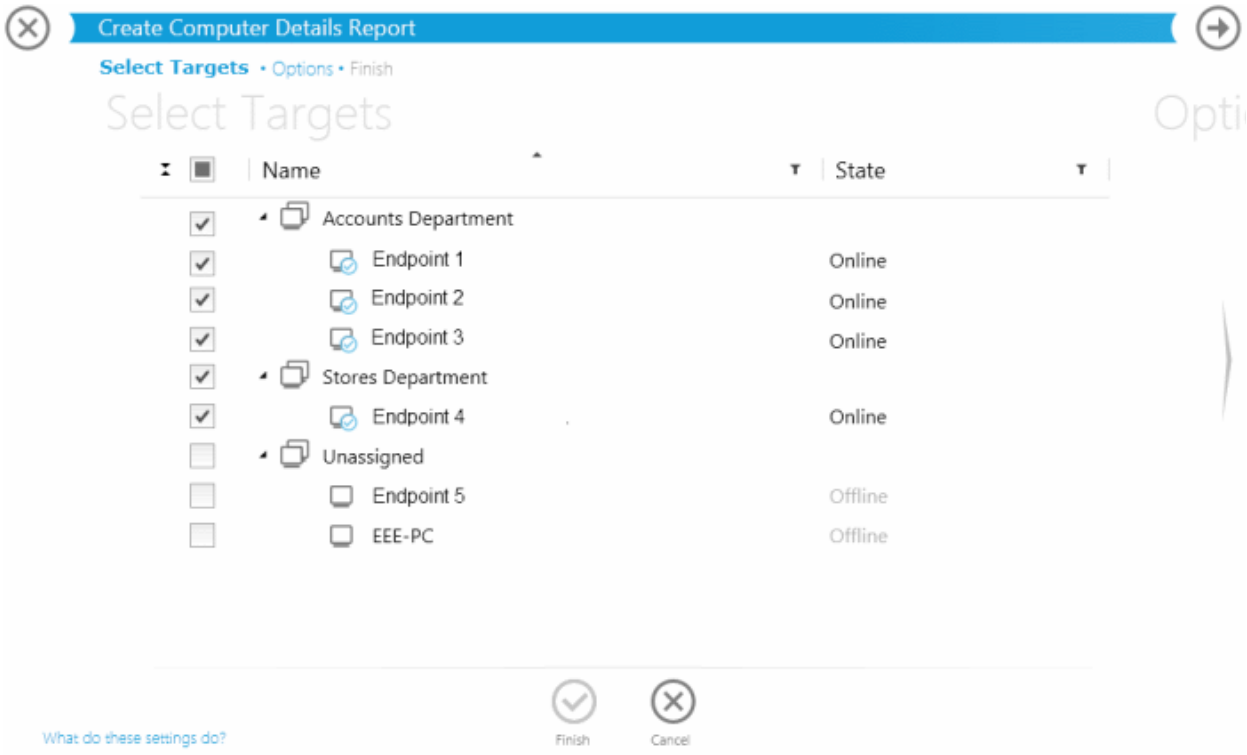
To generate a Computer Details report, click the 'Details' tile from the 'Reports' area.



The 'Create Computer Details Report' wizard will start.

Step 1 - Selecting Targets

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



- Select the endpoint(s) for which you wish to generate the computer details report

Step 2 - Options

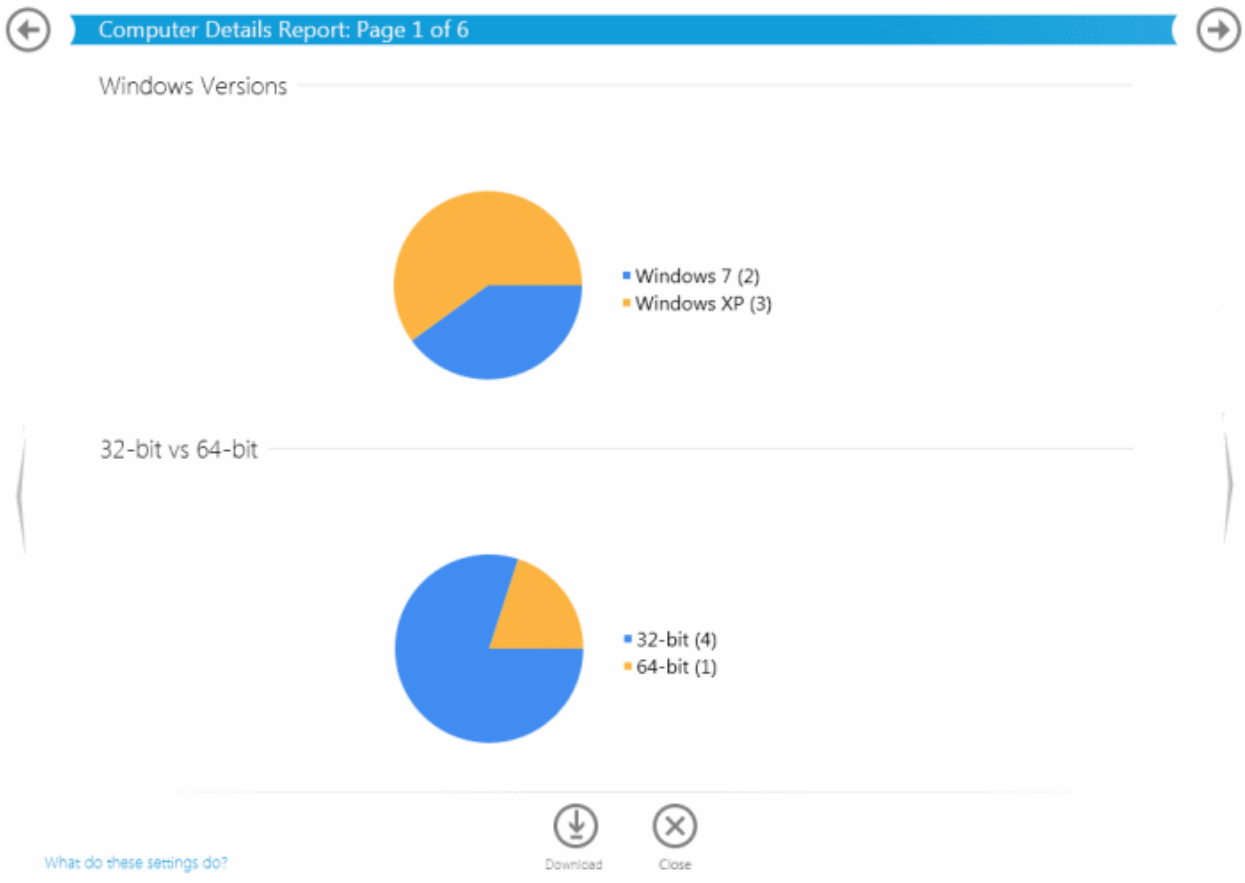
- **Include software details into report** - Select this option if you want the details on the software installed on the target computer(s) included in the report.
- **Generate downloadable report file** - Select this option if you need to print or archive the report. You can choose the printable file to be generated in portable document (.pdf) or spreadsheet (.xls) format. On completion, the report generated can be downloaded to the administrator's computer.

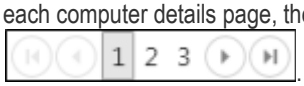
Step 3 - Generate Report

- Click the Finish icon or swipe the screen to left to start generating the report. On completion, the report will be displayed.

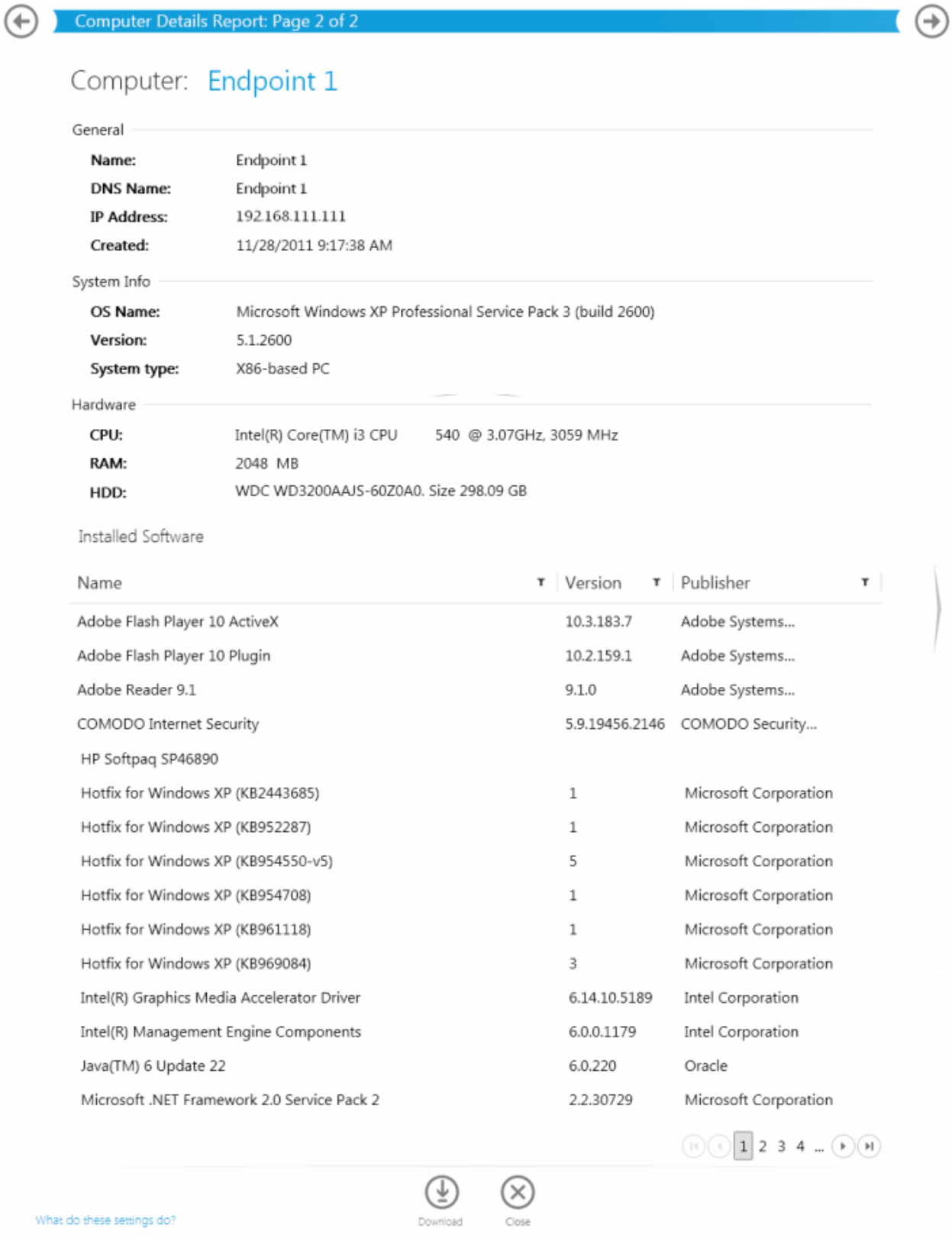
View the Report

- The report contains several pages depending on the number of endpoints chosen in step 1. The administrator can move through the pages by clicking the left and right arrows on both sides of the blue title bar or by swiping through the window. If the administrator had opted for generating a printable report file in step 1, the report can be downloaded by clicking the Download icon at the bottom of the report page.
- 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 network addresses, hardware details, software details etc, with each page dedicated for an endpoint. At the bottom of each computer details page, there may be additional details that can be displayed by clicking the pagination control 

.



Available Report Filters

The report screen allows the administrator to optimize the search by using the filter option. The available filters for the Computer Details report are:

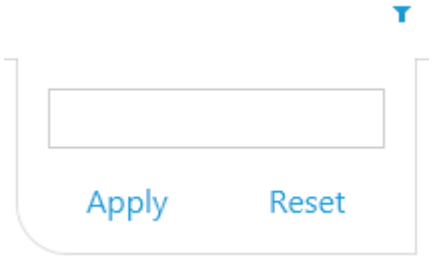
- Installed software
- Version of the software

- Publisher of the software

To filter the results:

- Click the filter icon in any of the respective column header to search for a particular item

The filter drop-down will appear.



- Type or enter the filter criteria fully or partly and click 'Apply

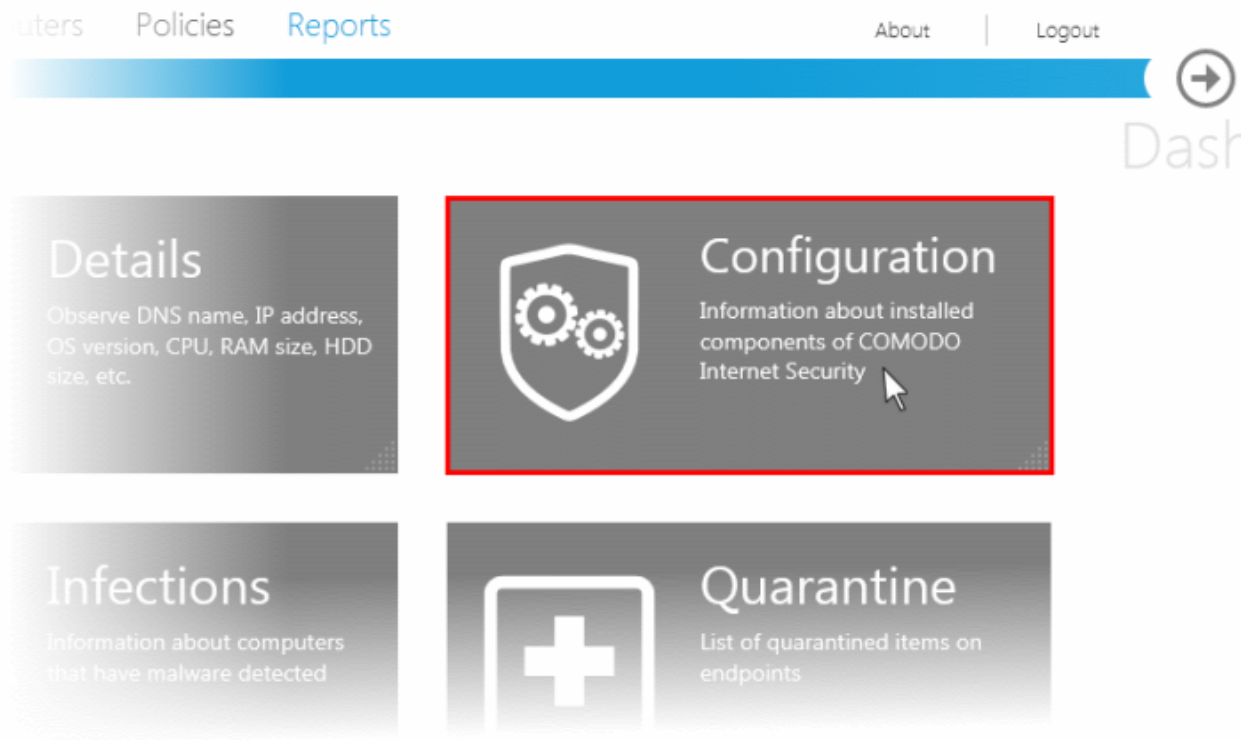
Only the entries that match the criteria will be displayed in the report.

- Click 'Reset' to display all the items

2.5.2. CIS Configuration Report

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

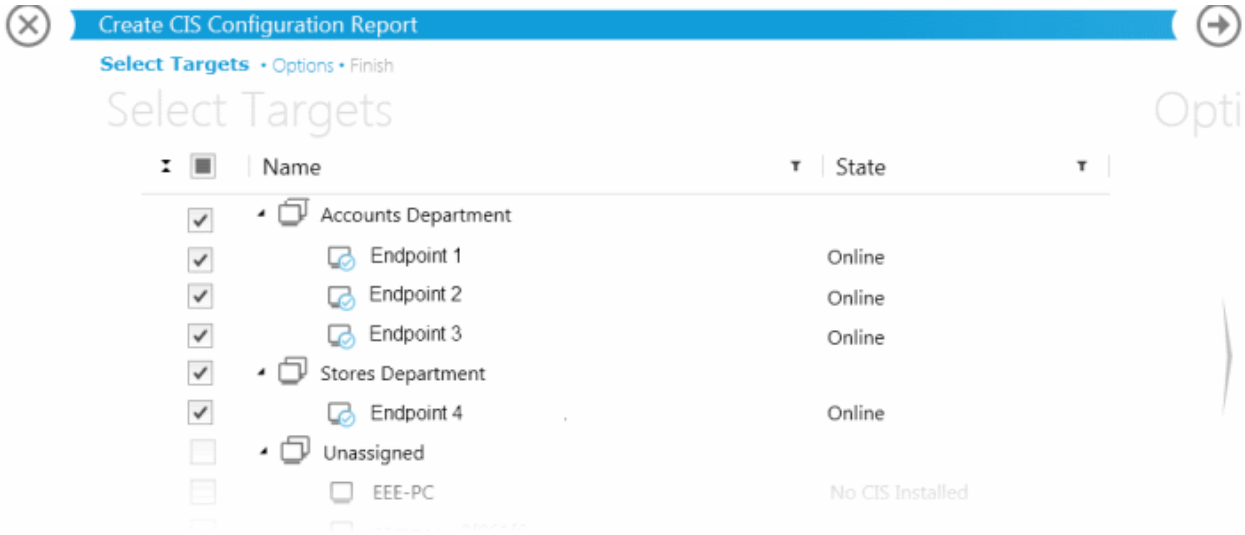
To generate a CIS Configuration report, click the 'Configuration' tile from the 'Reports' area.



The 'Create CIS Configuration report' wizard will start.

Step 1 - Selecting Targets

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



- Select the endpoint(s) for which you wish to generate the CIS Configuration report

Step 2 - Options

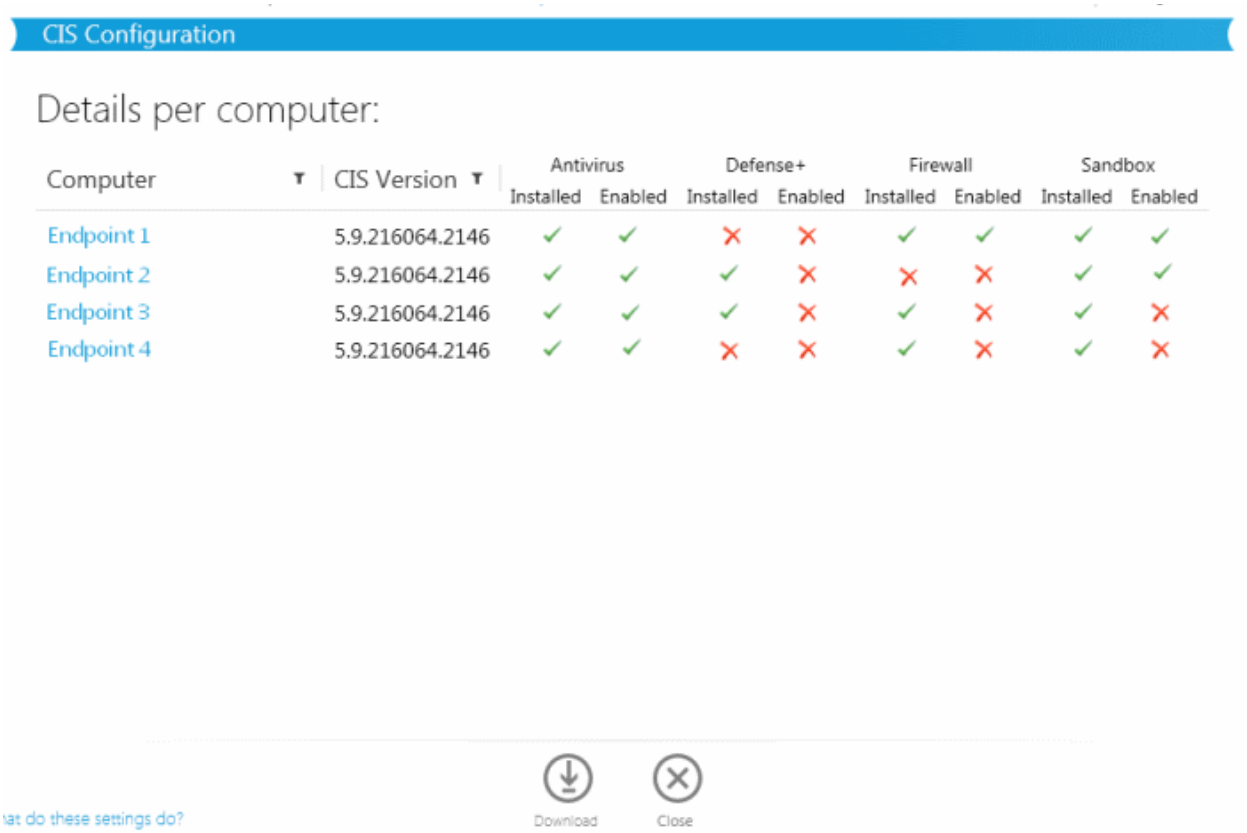
- **Generate downloadable report file** - Select this option if you need to print or archive the report. You can choose the printable file to be generated in portable document (.pdf) or spreadsheet (.xls) format. On completion, the report generated can be downloaded to the administrator's computer.

Step 3 - Generate Report

- Click the Finish icon or swipe the screen to left to start generating the report. On completion, the report will be displayed.

View the Report

- The report contains a table showing the CIS versions and the components installed and enabled in the target endpoints selected in step 1.



- If the administrator had opted for generating a downloadable report file in Step 2 - Options, the report can be downloaded by clicking the Download icon at the bottom of the report page.

Available Report Filters

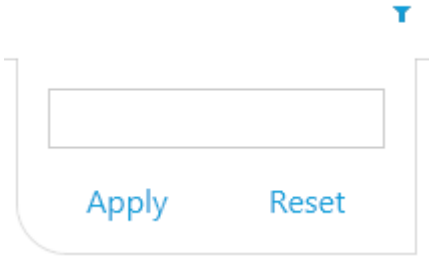
The report screen allows the administrator to optimize the search by using the filter option. The available filters for the CIS Configuration report are:

- Computer
- CIS Version

To filter the results:

- Click the filter icon in any of the respective column header to search for a particular item.

The filter drop-down will appear.



- Type or enter the filter criteria fully or partly and click 'Apply'.

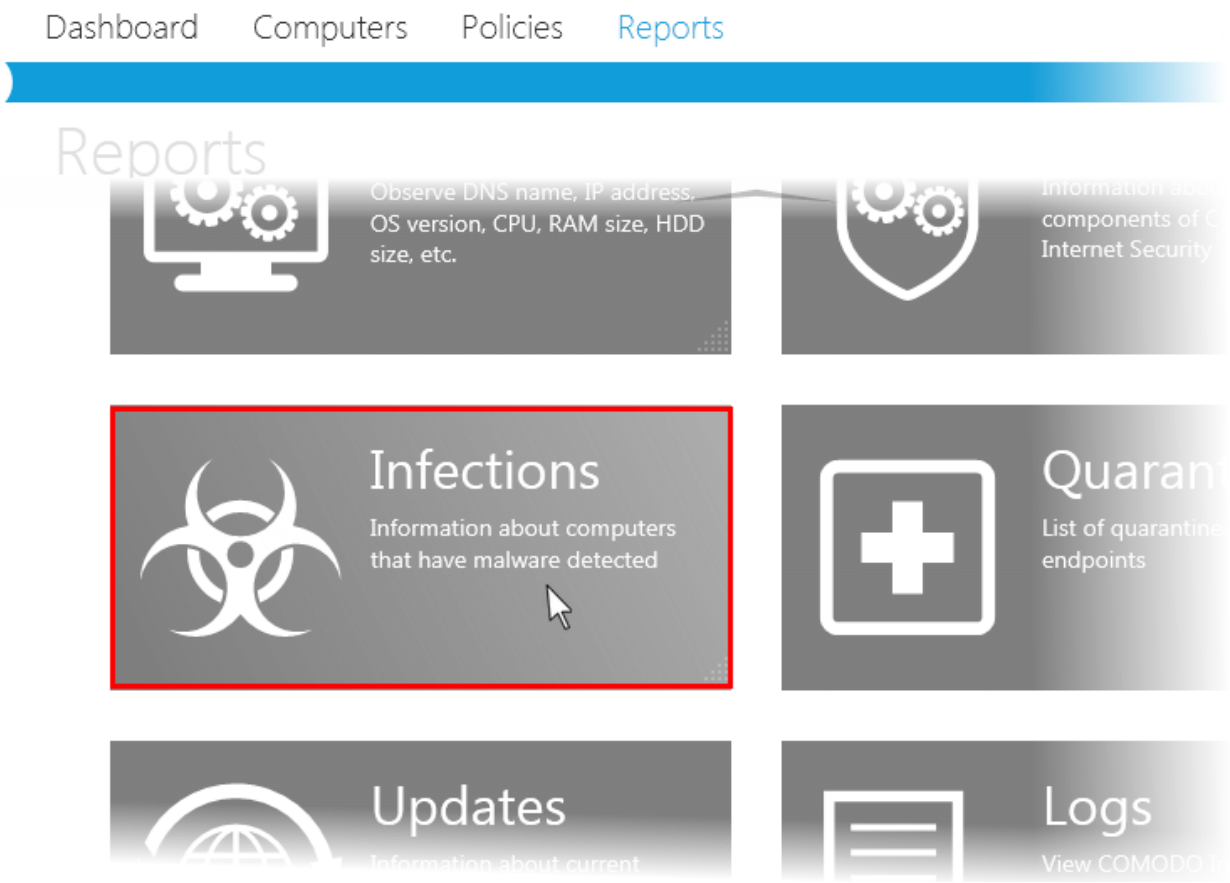
Only the entries that match the criteria will be displayed in the report.

- Click 'Reset' to display all the items.

2.5.3. 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 CIS.

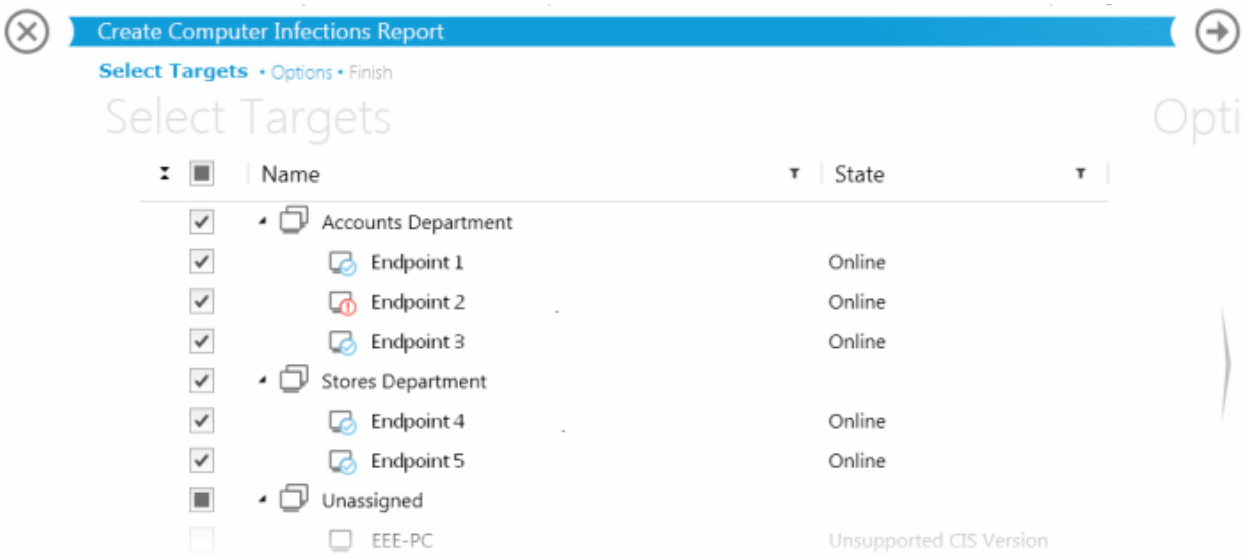
To generate a 'Computer Infections' report, click the 'Infections' tile from the 'Reports' area.



The 'Create Computer Infections Report' wizard will start.

Step 1 - Selecting Targets

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



The icon  besides an endpoint indicates that it is infected.

- Select the endpoint(s) for which you wish to generate the computer infections report and swipe left

Step 2 – Options

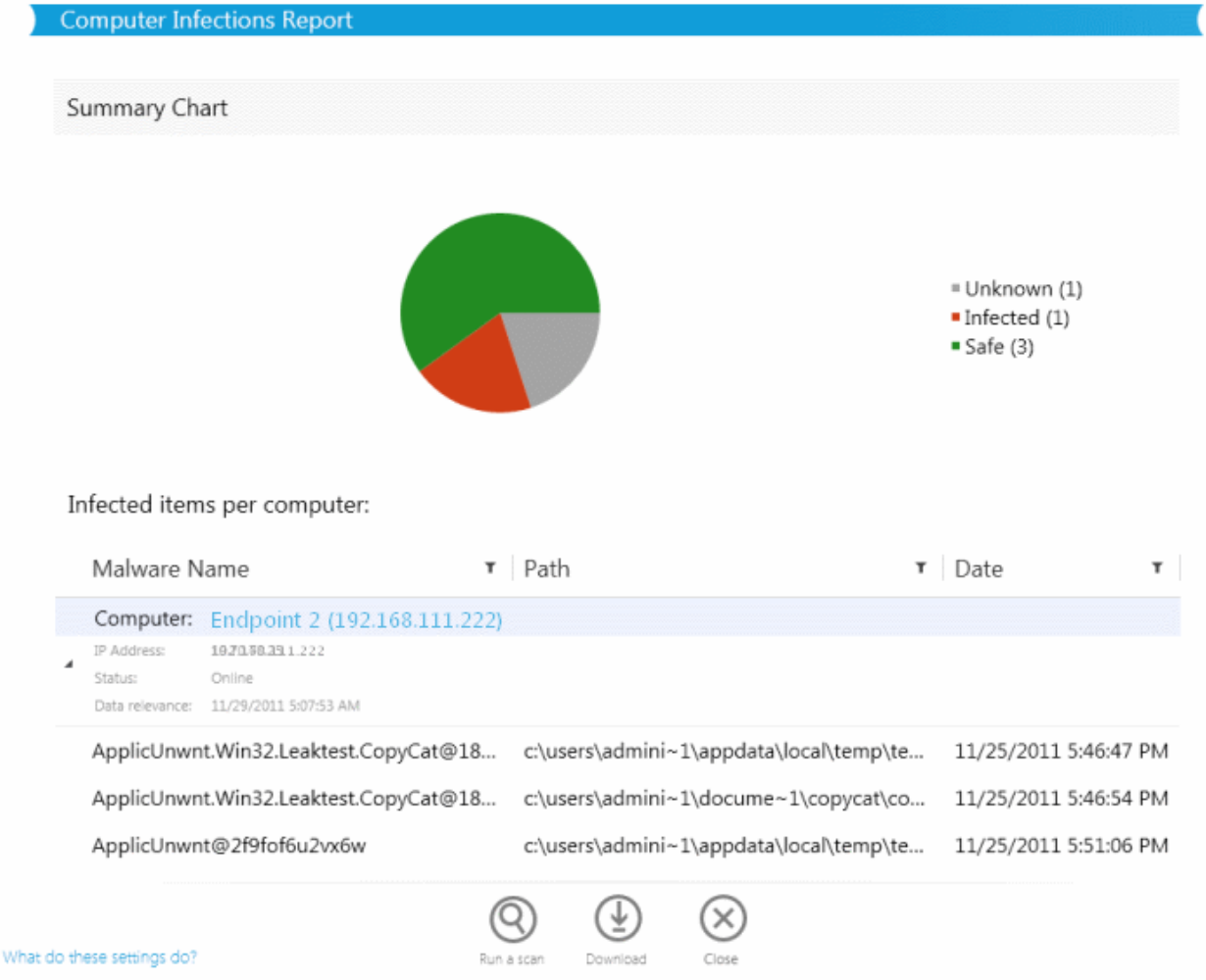
- **Include cached data for offline computers** - The report will include infection data for endpoints that are offline.
- **Generate downloadable report file** - Select this option if you need to print or archive the report. You can choose the printable file to be generated in portable document (.pdf) or spreadsheet (.xls) format. On completion, the report generated can downloaded to the administrator's computer.

Step 3 - Generate Report

- Click the Finish icon or swipe the screen to left to start generating the report. On completion, the report will be displayed.

View the Report

- 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.



- Clicking the computer name from the list opens the 'Computer Properties' interface of it. The interface allows the administrator to apply a different security policy to the computer in order to attend to the malware identified. Refer to **Viewing Details of an Endpoint Computer and Applying Policy Individually** for more details.
- Clicking the Run a Scan button at the bottom of the interface commences the full My Computer antivirus (AV)scan on the infected computers. The wizard will then move to the 'View All Computers' screen which will display scan progress notifications beneath the name of the target computers. This screen can be accessed at any time by clicking 'Computers' then the 'View' tile.
- If the administrator had opted for generating a printable report file in step 1, the report can be downloaded by clicking the Download icon at the bottom of the report page.

Available Report Filters

The report screen allows the administrator to optimize the search by using the filter option. The available filters for the Computer Infections report are:

- **Malware** - Filters the report based on malware name
- **Path** - Searches the report based on the path where the malware is located in the endpoint.
- **Date** - Searches the report based on the start date and end date

To filter the results:

- Click the filter icon in any of the respective column header to search for a particular item.
- Type or enter the filter criteria fully or partly or select and click 'Apply'.

Only the entries that match the criteria will be displayed in the report.

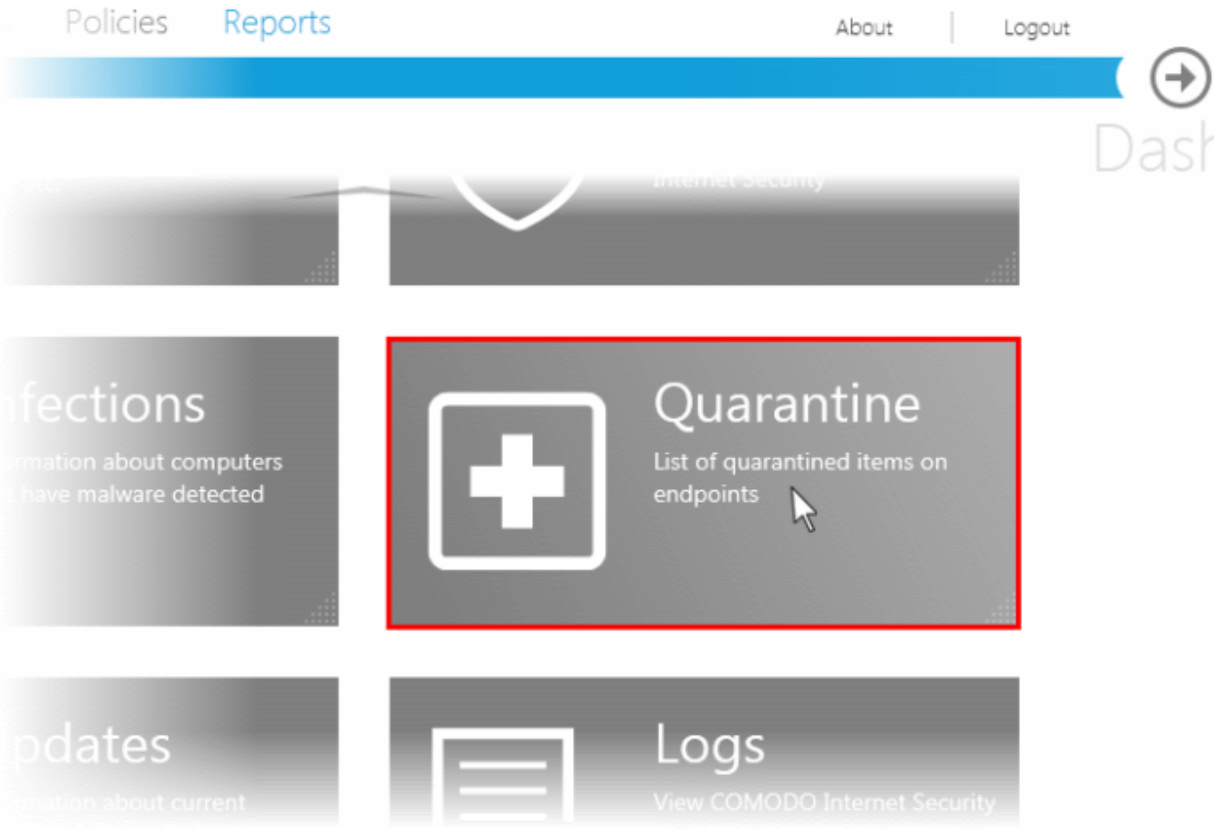
- Click 'Reset' to display all the items.

2.5.4. 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 CIS 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 CIS has been configured to automatically quarantine the threats identified from various scans. For more details on configuring CIS refer to the online help guide at http://help.comodo.com/.

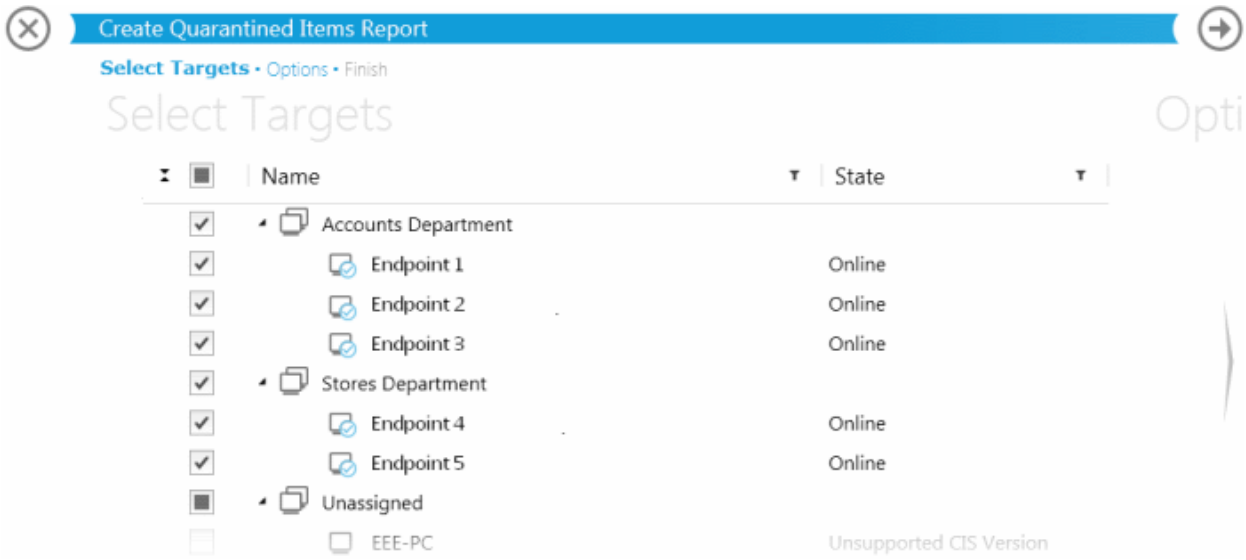
To generate a 'Quarantined Items' report, click the 'Quarantine' tile from the 'Reports' area.



The 'Create Quarantined Items Report' wizard will start.

Step 1 - Selecting Targets

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



- Select the endpoint(s) for which you wish to generate the 'Quarantined Items' report and swipe left

Step 2 - Options

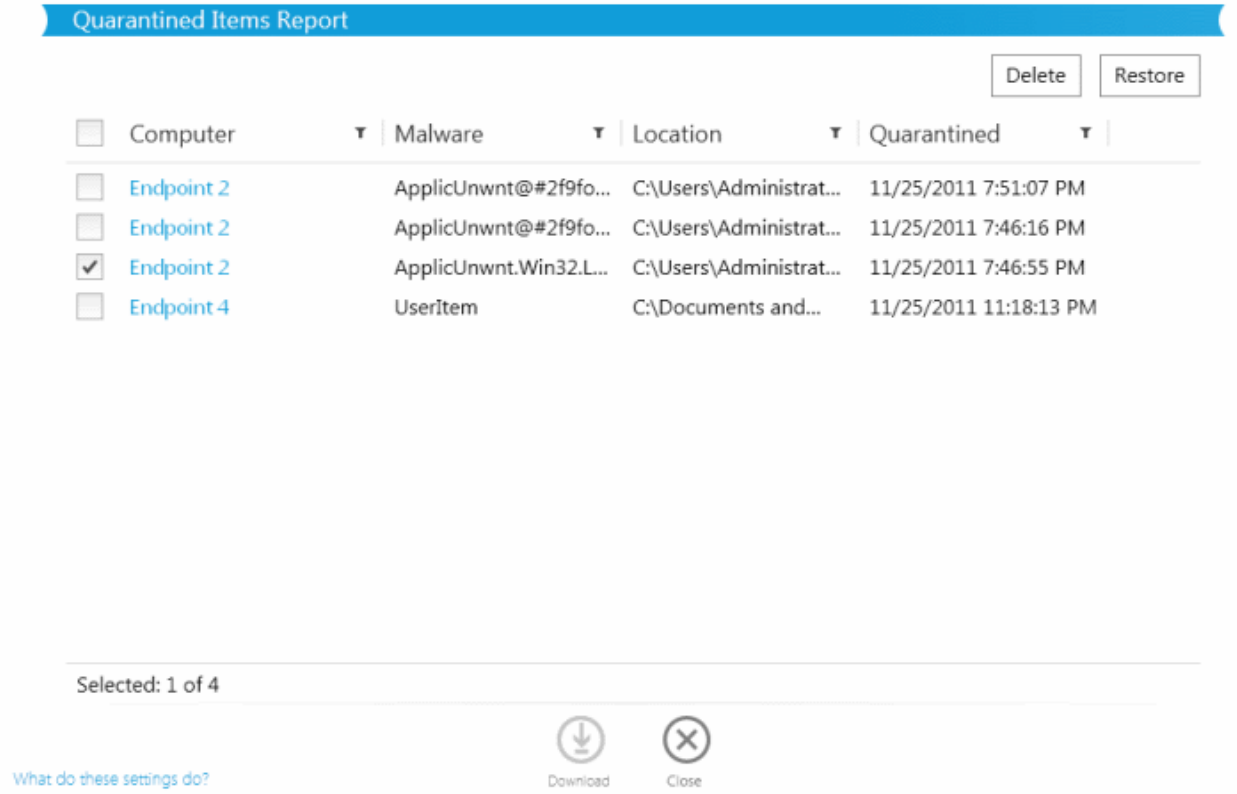
- **Generate downloadable report file** - Select this option if you need to print or archive the report. You can choose the printable file to be generated in portable document (.pdf) or spreadsheet (.xls) format. On completion, the report generated can downloaded to the administrator's computer.

Step 3 - Generate Report

- Click the Finish icon or swipe the screen to left to start generating the report. On completion, the report will be displayed.

View the Report

The report will contain a table showing the malware quarantined at each endpoint selected in step 1.



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 icon at the bottom of the report page.

Removing or Restoring Quarantined Items

After the analysis of the report:

- If the administrator finds an entry to be a safe application or file, the administrator can restore it to the original location in the target endpoint from quarantine
- On the other hand, if the administrator finds an entry to be a harmful application or a file, the administrator can permanently remove it from the target endpoint

Note: When you restore a quarantined item to a computer, the file will be scanned again by Comodo Internet Security and, unless a new policy or update was applied otherwise, it may again be found to be malware, at which point it will just be placed back into quarantine.

To restore or remove a file or application

1. Select the checkbox in the left end of the row(s) of the entry(ies) to be removed or restored.
2. Click 'Delete' or 'Restore' from the top right of the interface as required.

Available Report Filters

The report screen allows the administrator to optimize the search by using the filter option. The available filters for the Quarantined Items report are:

- **Computer** - Searches the report based on the computers' name
- **Malware** - Searches the report based on the malware's name
- **Location** - Searches the report based on the path where the malware is located in the endpoint

- **Quarantined** - Searches the report based on the start date and end date

To filter the results:

- Click the filter icon in any of the respective column header to search for a particular item
- Type or enter the filter criteria fully or partly or select and click 'Apply'

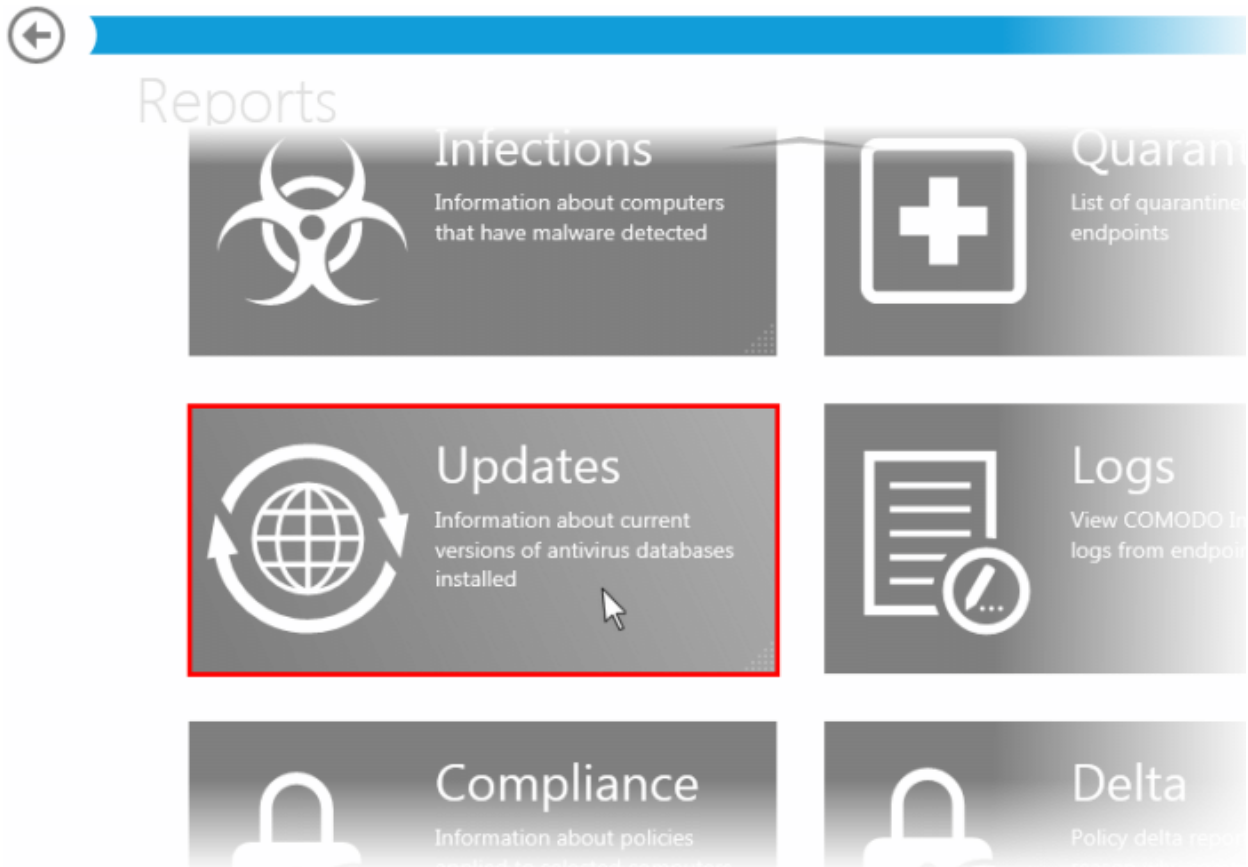
Only the entries that match the criteria will be displayed in the report.

- Click 'Reset' to display all the items

2.5.5. Antivirus Updates Report

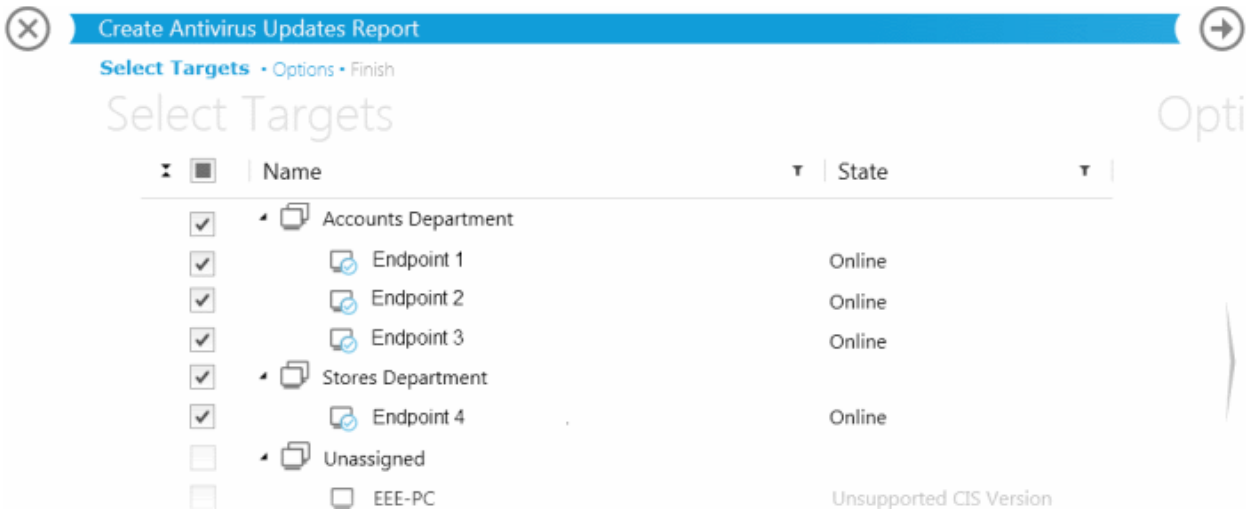
The Antivirus Updates report provides details on the antivirus (AV) signature database versions in the target computers and whether they are up-to-date. The report assists the administrators to decide on the target computers whose AV databases are to be updated and to run an Update AV base task on the 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, click the **'Updates' tile from** the 'Reports' area.



The 'Create Antivirus Updates Report' wizard will start.

Step 1 - Selecting Targets
A list of all the endpoint computers connected to CESM is displayed.



- Select the endpoint(s) for which you wish to generate the AV Updates report

Step 2 - Options

- **Include cached data for offline computers** - The report will include the AV signature database update details for the endpoints that are offline.
- **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.

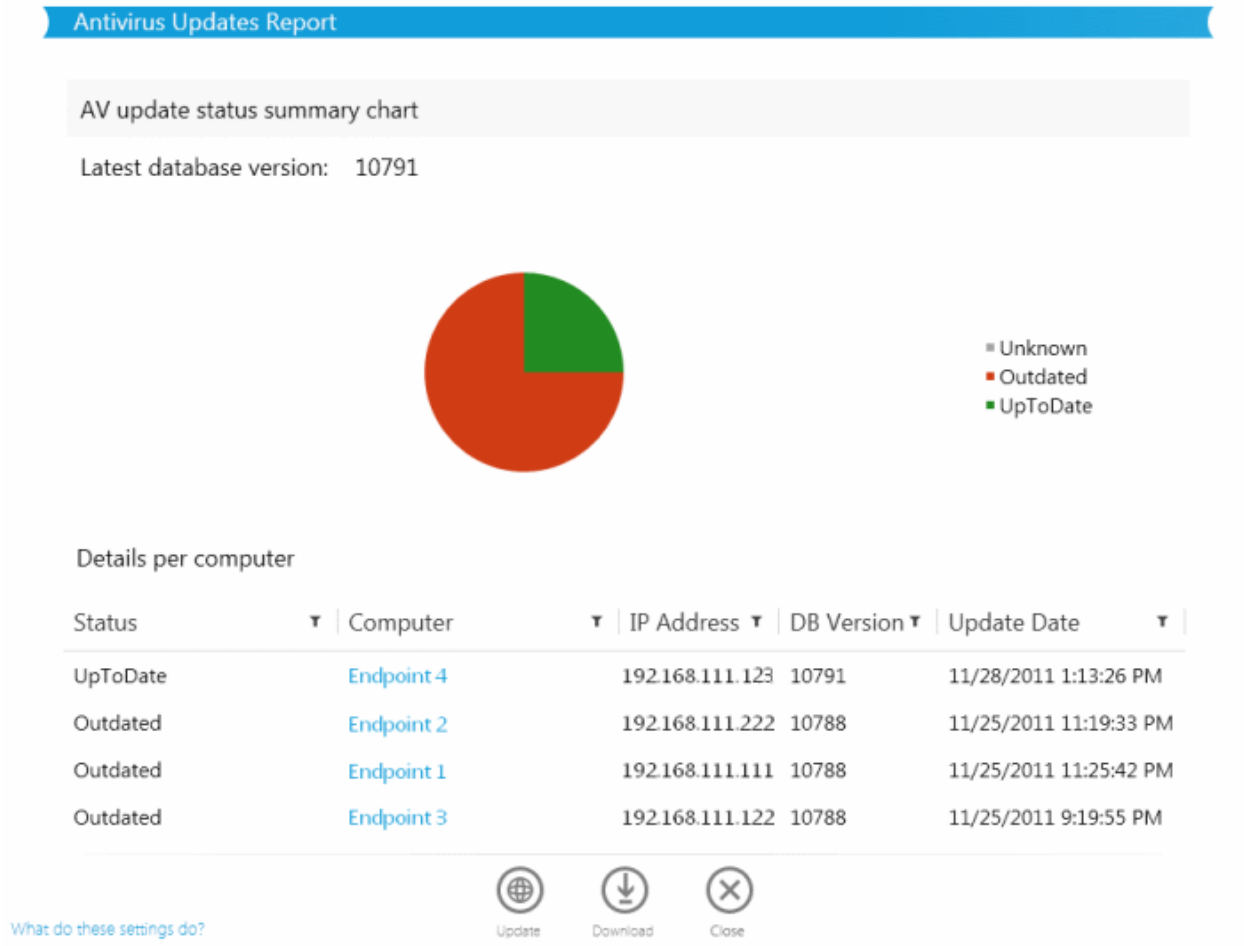
Step 3 - Generate Report

- Click the Finish icon or swipe the screen to left to start generating the report. On completion, the report will be displayed.

View the Report

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

- The report will contain a summary pie chart and 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.
- Clicking the computer name from the list opens the 'Computer Properties' interface of it. Refer to **Viewing Details of an Endpoint Computer and Applying Policy Individually** for more details.

Downloading the Report

If the administrator had opted for generating a printable report file in step 2, the report can be downloaded by clicking the Download icon at the bottom of the report page.

Update Computers with Outdated databases

Clicking the 'Update' icon from the bottom of the interface commences the antivirus (AV) database update task on the outdated computers. The 'View All Computers' screen will display update progress beneath the name of the outdated target computers. This screen can be accessed at any time by clicking 'Computers' then the 'View ' tile.

Available Report Filters

The report screen allows the administrator to optimize the search by using the filter option. The available filters for the Antivirus Updates report are:

- **Status** - Filters the report based on either Up-To-Date, Outdated or Unknown criteria of the endpoints
- **Computer** - Searches the report based on the computers' name
- **IP Address** - Filters the report based on the IP Address of the endpoints
- **DB Version** - Filters the report based on the virus database version
- **Update Date** - Searches the report based on the start date and end date

To filter the results:

- Click the filter icon in any of the respective column header to search for a particular item
- Type or enter the filter criteria fully or partly or select and click 'Apply'

Only the entries that match the criteria will be displayed in the report.

- Click 'Reset' to display all the items

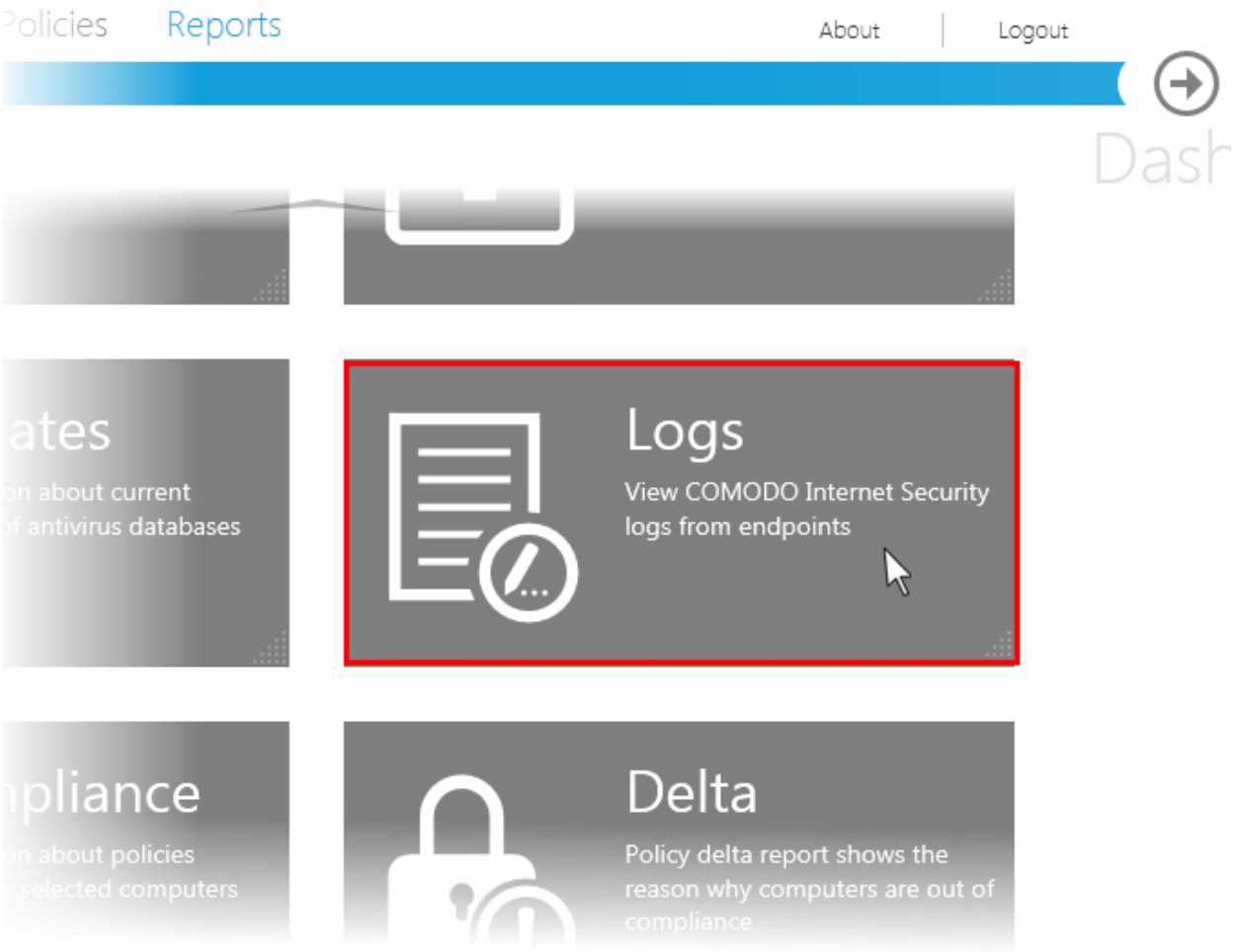
2.5.6. CIS Log Report

The CIS 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 Policy, 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 Policy.

The CIS 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.

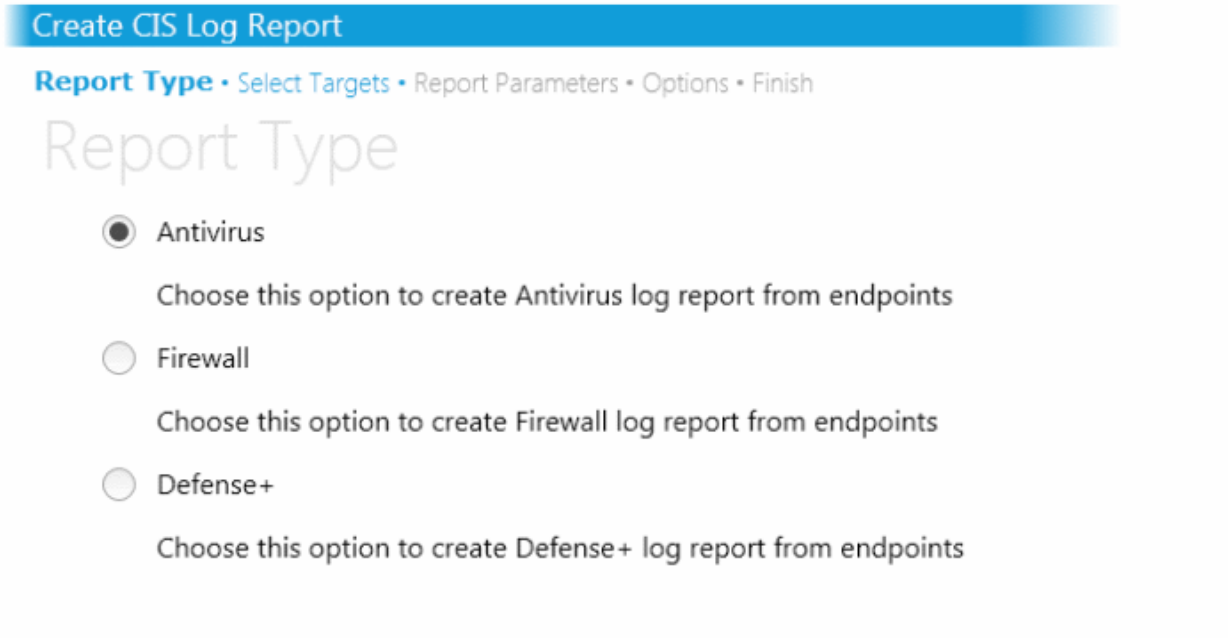
To generate a 'CIS Log' report, click the 'Logs' tile from the 'Reports' area.



The 'Create CIS Log Report' wizard will start.

Step 1 - Select Report Type

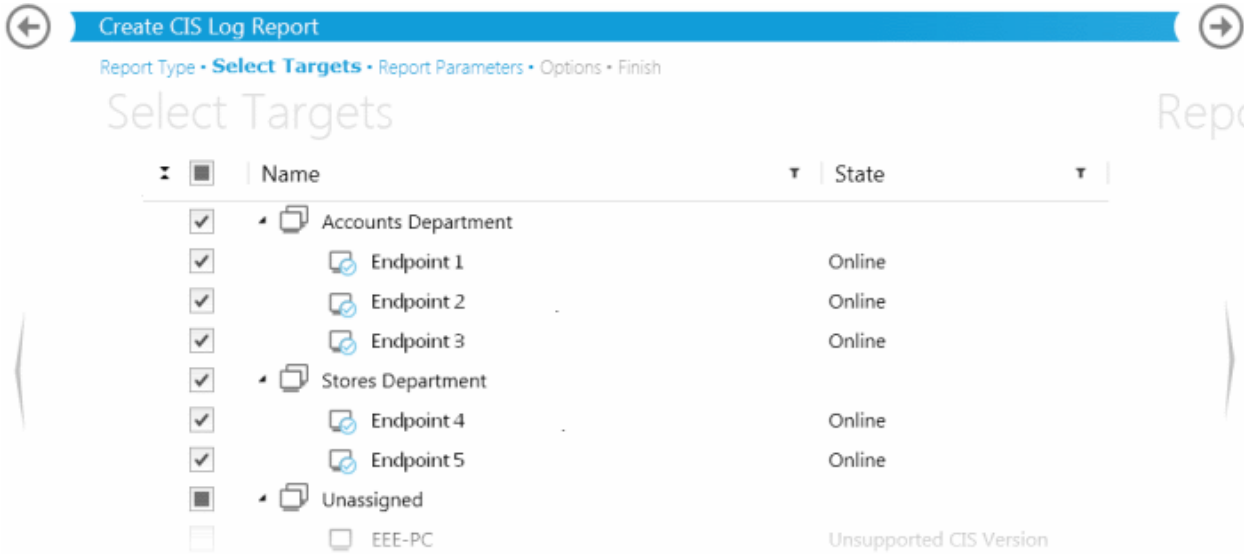
The first step is to choose the CIS component for which you want to generate a log report.



- Choose the component from Antivirus, Firewall and Defense+ and swipe the screen or click the right arrow to move to step 2 - Selecting targets

Step 2 - Selecting Targets

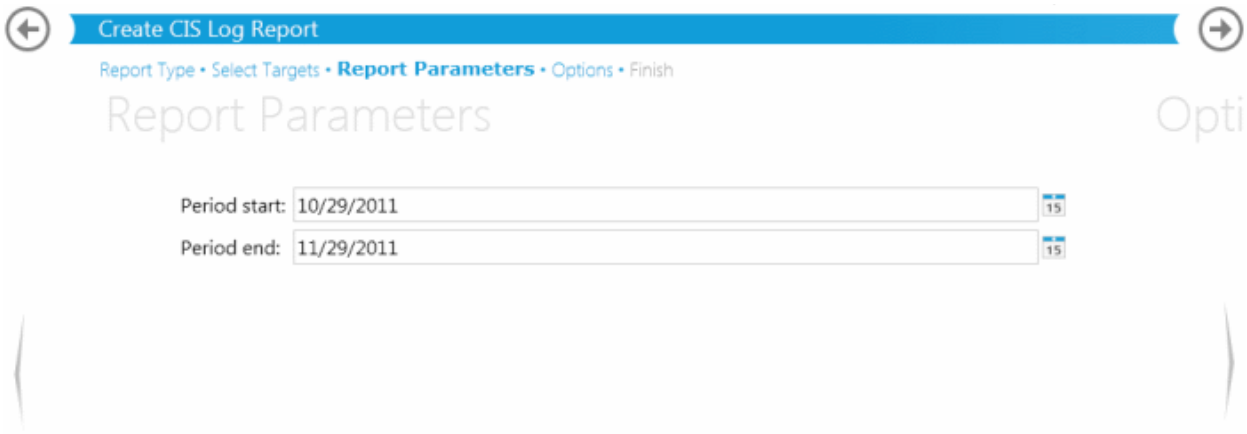
A list of all the endpoint computers connected to CESM is displayed.



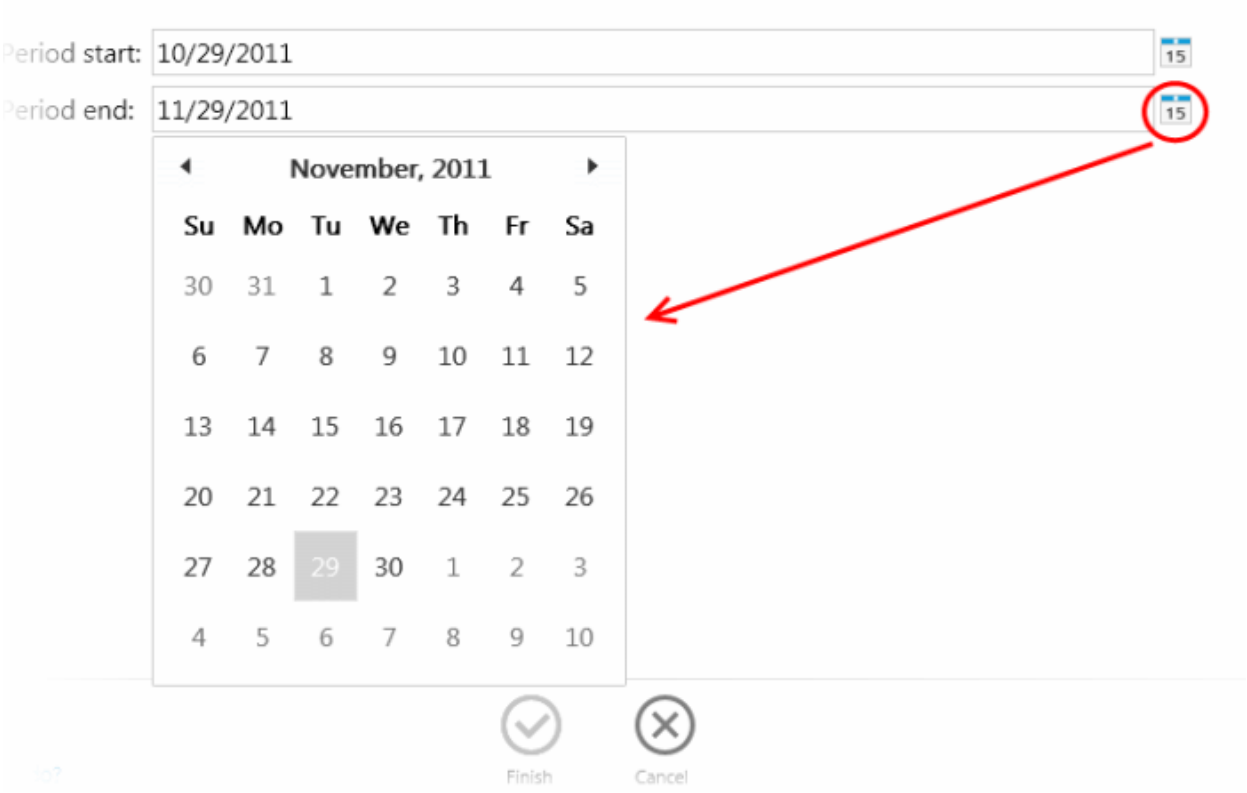
- Select the endpoint(s) for which you wish to generate the CIS Log report

Step 3 - Selecting the Report Period

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



- Specify the period start and end dates in the respective text fields in MM/DD/YYYY format. Alternatively, clicking the calendar icon at the right end of the text box displays a calendar to select the dates.



Step 4 - Options

- **Generate downloadable report file** - Select this option if you need to print or archive the report. You can choose the printable file to be generated in portable document (.pdf) or spreadsheet (.xls) format. On completion, the report generated can be downloaded to the administrator's computer.

Step 5 - Generate Report

- Click the Finish icon or swipe the screen to left to start generating the report. On completion, the report will be displayed.

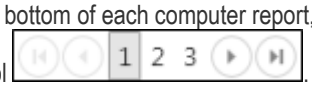
Viewing the Report

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. The administrator can move through the successive pages by clicking the right arrow or the required page number at the bottom of the report.

Examples of:

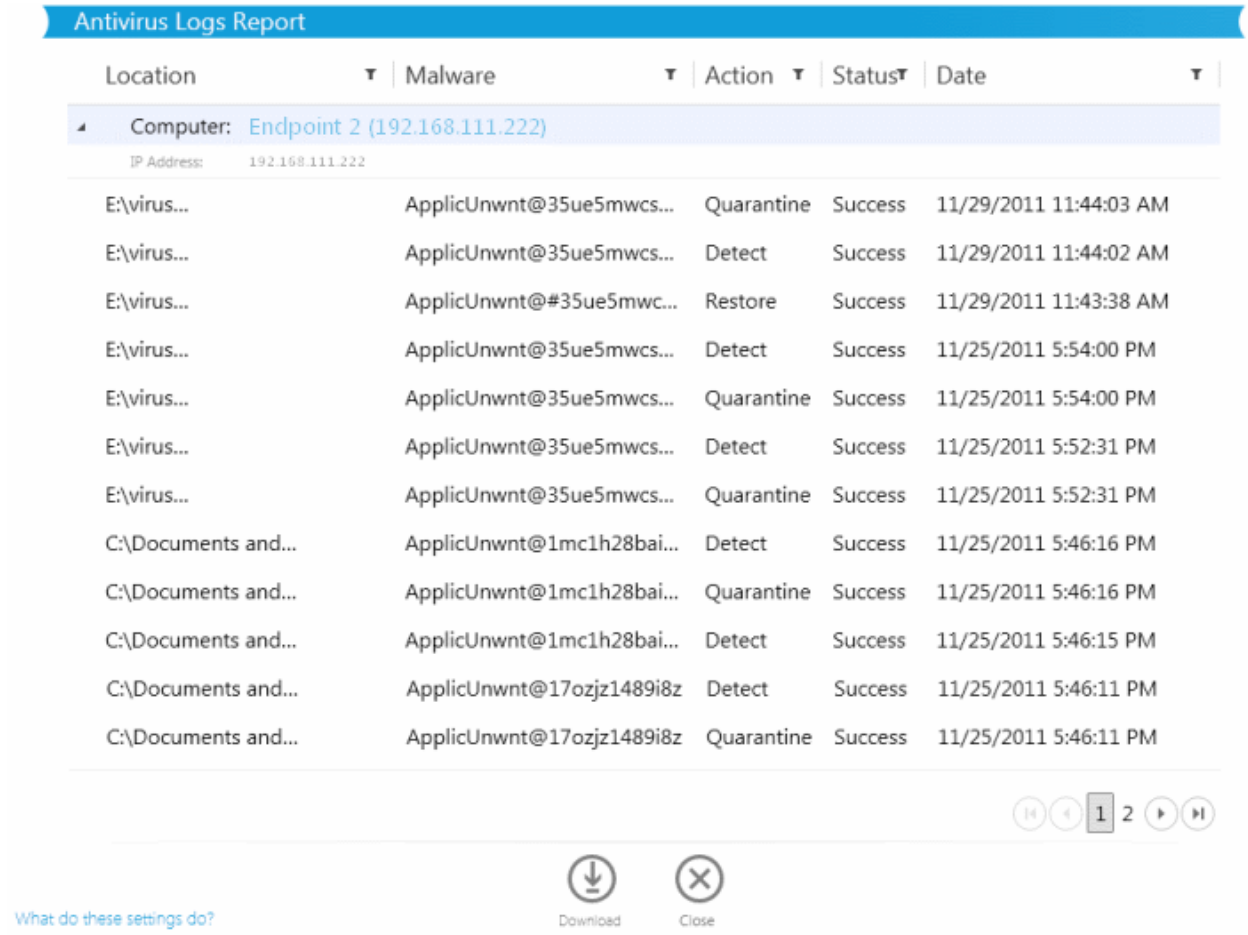
- Antivirus Log Report
- Firewall Log Report and
- Defense+ Log Report

... are shown below.

At the bottom of each computer report, there may be additional log entries that can be displayed by clicking the pagination control 

.

Viewing Antivirus Log Report



Column Descriptions

- Location - Indicates the location where the application detected with a threat is stored.
- Malware - Name of the malware event that has been detected.
- Action - Indicates action taken against the malware through Antivirus.
- Status - Gives the status of the action taken. It can be either 'Success' or 'Fail'.
- Date - Indicates the date and time of the event.

Available Filters for Antivirus Log Report

The report screen allows the administrator to optimize the search by using the filter option. The available filters for the Antivirus Log report are:

- **Location** - Searches the report based on the path where the malware is located in the endpoint

- **Malware** - Filters the report based on malware name
- **Action** - Filters the report based on the action taken whether detected or quarantined
- **Status** - Filters the report based on the result of the action taken
- **Date** - Searches the report based on the start date and end date

To filter the results:

- Click the filter icon in any of the respective column header to search for a particular item
- Type or enter the filter criteria fully or partly or select and click 'Apply'

Only the entries that match the criteria will be displayed in the report.

- Click 'Reset' to display all the items

Viewing Firewall Log Report

Column Descriptions

- Application - Indicates which application or process propagated the event.
- Action - Indicates how the firewall has reacted to the connection attempt.
- Protocol - Represents the Protocol application attempted to use to create the connection. This is usually TCP/IP or UDP - which are the most heavily used networking protocols.
- Source IP - States the IP address of the host that made the connection attempt. This is usually the IP address of your computer for outbound connections.
- Source Port - States the port number on the host at the source IP which was used to make this connection attempt.
- Destination IP - States the IP address of the host to which the connection attempt was made. This is usually the IP address of your computer for inbound connections.
- Destination Port - States the port number on the host at the destination IP to which the connection attempt was made.
- Date - Contains precise details of the date and time of the connection attempt.

Available Filters for Firewall Log Report

The report screen allows the administrator to optimize the search by using the filter option. The available filters for the Firewall Log report are:

- **Application** - Searches the report based on the application name
- **Action** - Filters the report based on action taken whether 'Blocked' or 'Asked'
- **Protocol** - Filters the report based on the Protocol
- **Source IP** - Searches the report based on source IP entered
- **Source Port** – Filters the report based on the source port entered
- **Destination IP** - Searches the report based on the destination IP
- **Destination Port** - Filters the report based on the destination port entered
- **Date** - Searches the report based on the start date and end date

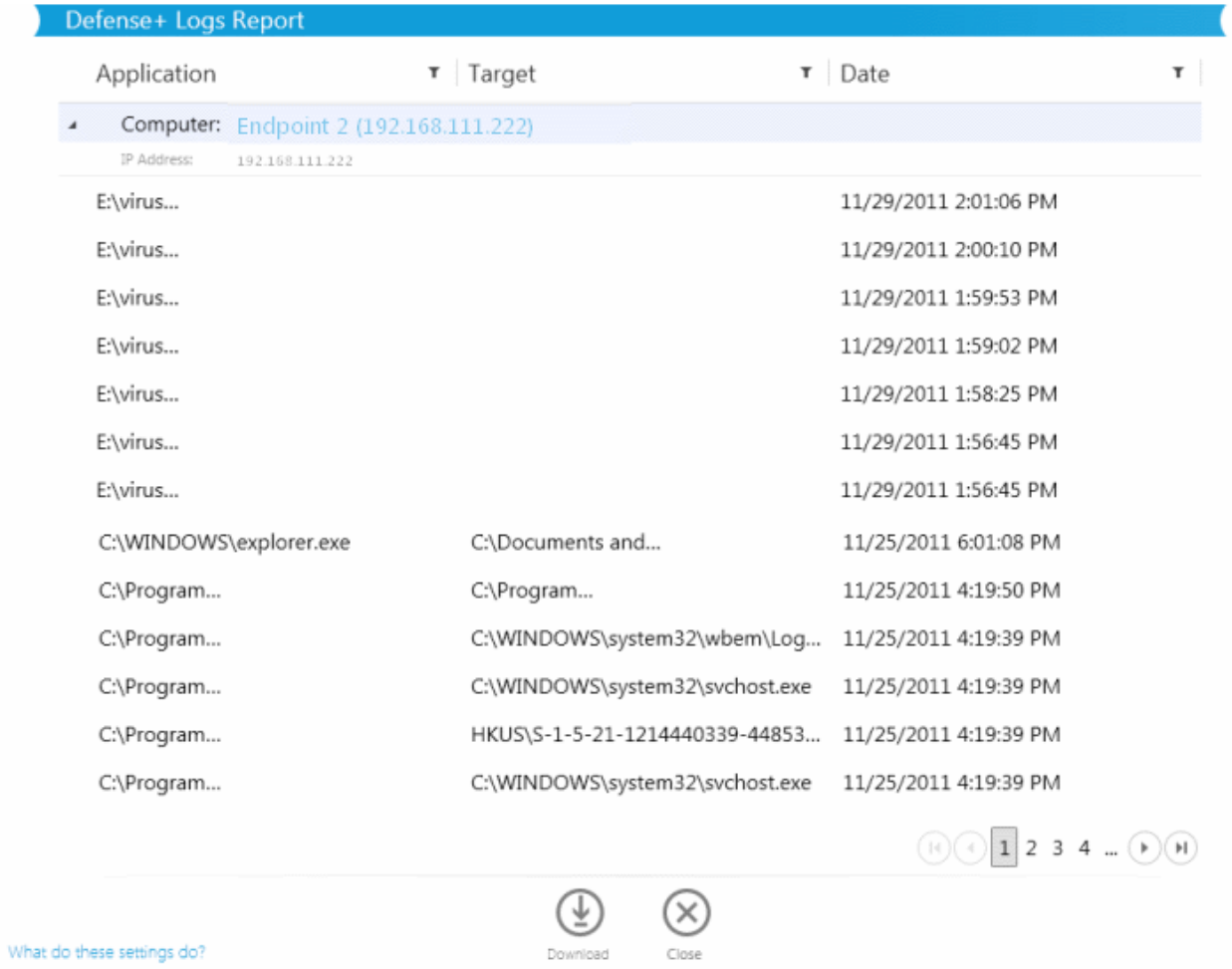
To filter the results:

- Click the filter icon in any of the respective column header to search for a particular item
- Type or enter the filter criteria fully or partly or select and click 'Apply'

Only the entries that match the criteria will be displayed in the report.

- Click 'Reset' to display all the items

Viewing Defense+ Log Report



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

Available Filters for Defense+ Log Report

The report screen allows the administrator to optimize the search by using the filter option. The available filters for the Defense+ Log report are:

- **Application** - Searches the report based on the path where the application is located in the endpoint
- **Target** - Filters the report based on the target location
- **Date** - Searches the report based on the start date and end date

To filter the results:

- Click the filter icon in any of the respective column header to search for a particular item
- Type or enter the filter criteria fully or partly or select and click 'Apply'

Only the entries that match the criteria will be displayed in the report.

- Click 'Reset' to display all the items

Downloading the Report

If the administrator had opted for generating a printable report file in **step 4**, the report can be downloaded by clicking the Download icon at the bottom of the report page.

2.5.7. 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 CIS installed at the target computer. The CIS installation at the target endpoint will automatically be configured as per the applied policy when CIS is in remote management mode.

If the end-user or the network administrator changes any of the security settings in their local installation of CIS 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 computer will be retained in Non-Compliant status under the following conditions:

- CIS on the target computer is maintained in local administration mode and settings were modified
- CIS on the target computer was switched to Remote Management mode but the policy has not yet been applied because CESM has not yet polled the computer

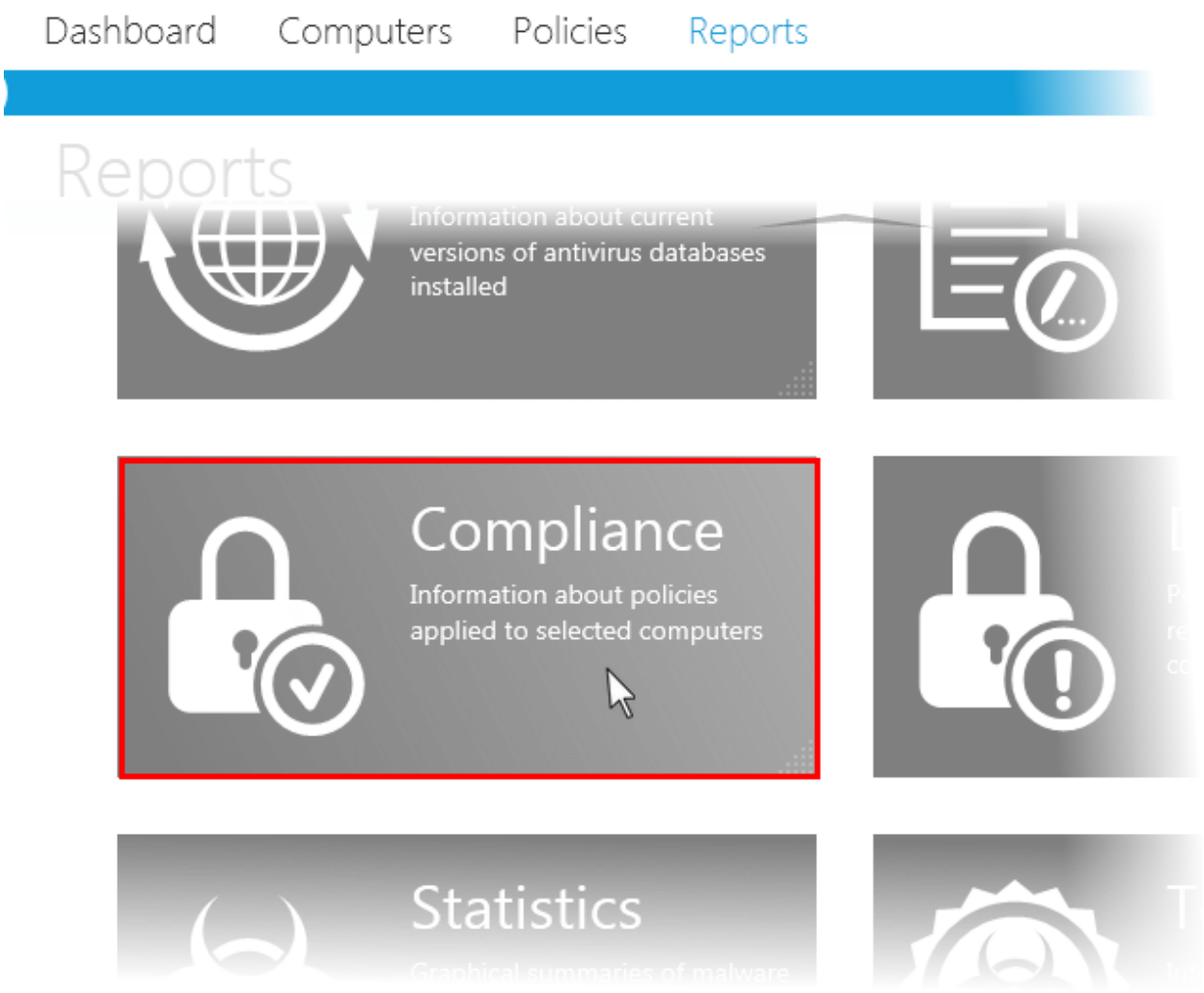
The target computers applied with the 'Locally Configured' policy will always be retained in 'Compliant' status as CESM does not enforce any policy compliance on to them. Also, 'Locally Configured' policy allows the user to change the CIS configuration settings locally and stores the changes dynamically.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

Tip: To ensure a new configuration is applied permanently, leave the endpoint in local administration mode, import the configuration as a new policy into CESM and apply it to the required target computer(s) (including the one from which the settings are imported). See 'Creating a New Policy' for more details.

Administrators are advised to regularly check whether imported computers are compliant with their assigned policy. Non-compliance can indicate changes in management mode and/or unauthorized changes to CIS 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 CIS security configuration and thus returning them to 'Compliant' status.

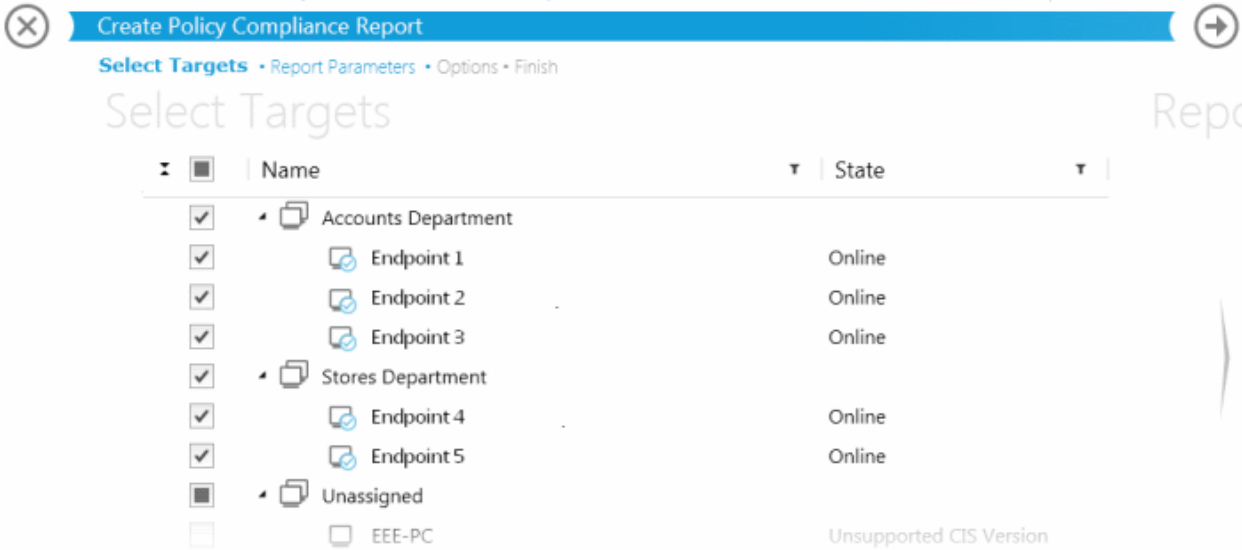
To generate a Policy Compliance report, click the 'Compliance' tile from the reports interface.



The Create 'Policy Compliance Report' wizard will be started.

Step 1 - Selecting Targets

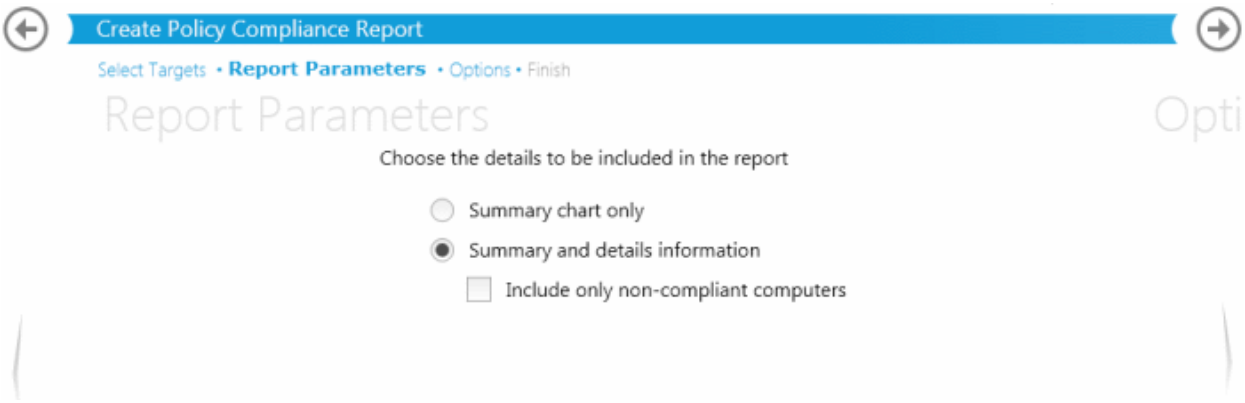
A list of all the endpoint computers connected to CESM will be displayed.



- Select the endpoint(s) for which you wish to generate the 'Policy Compliance' report
- Swipe the screen or click the right arrow to move to step 2 - Selecting report Parameters

Step 2 - Selecting Report Parameters

The next step allows the administrator to choose between a summary report and a detailed report.



- **Summary Chart only** - The report will only contain a pie chart that gives an at-a-glance comparison of number of target computers that are compliant and non-compliant
- **Summary and details information** - The report will will first contain the pie chart that gives an at-a-glance comparison of number of target computers that are compliant and non-compliant and details on policy applied and compliancy status of each computer
    - **Include only non-compliant computers** - The report will contains details of only the computers that are non-compliant
- Choose the type of report you wish to have

Step 3 - Options

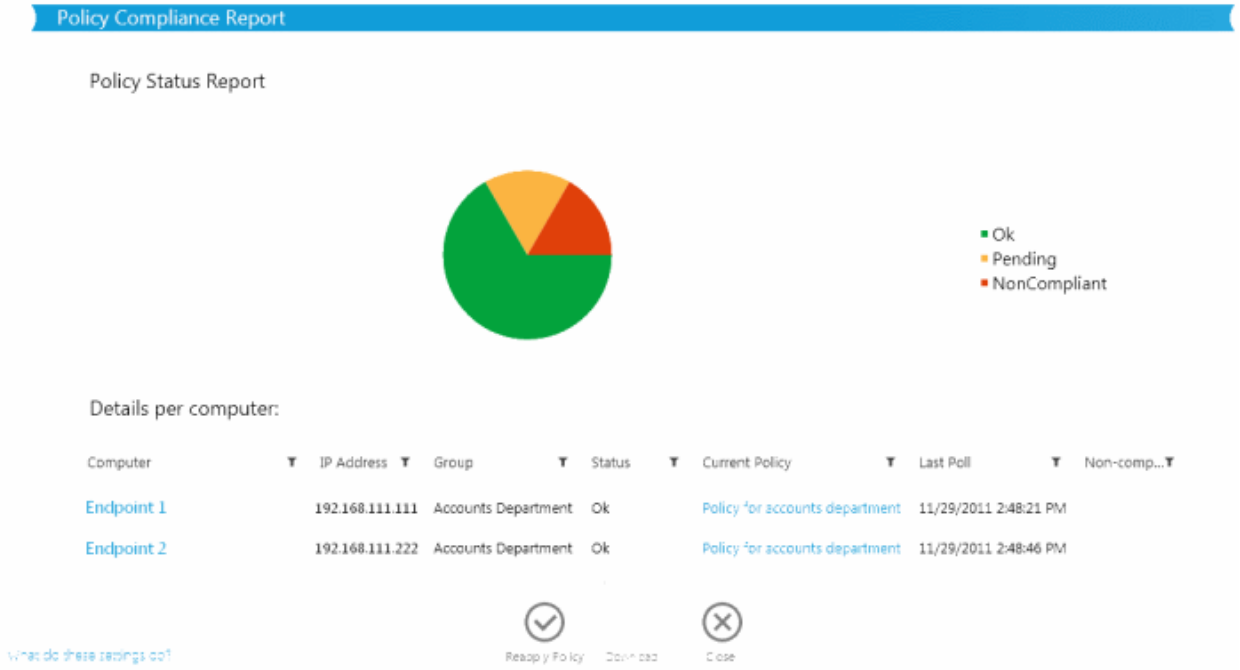
- **Generate downloadable report file** - Select this option if you need to print or archive the report. You can choose the printable file to be generated in portable document (.pdf) or spreadsheet (.xls) format. On completion, the report generated can downloaded to the administrator's computer.
- Swipe the screen or click the right arrow to move to next step.

Step 4 - Generating the Report

- Click the Finish icon or swipe the screen to left to start generating the report. On completion, the report will be displayed.

Viewing the Report

- 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.



- Clicking the computer name from the list opens the 'Computer Properties' interface of it. The interface allows the administrator to apply a different security policy to the computer in order to it become compliant. Refer to **Viewing Details of an Endpoint Computer and Applying Policy Individually** for more details.

Available Report Filters

The report screen allows the administrator to optimize the search by using the filter option. The available filters for the Policy Compliance report are:

- **Computer** - Searches the report based on the computers' name
- **IP Address** - Filters the report based on the IP Address of the endpoints
- **Group** - Searches the report based on the group's name
- **Status** - Filters the report based on the status of policy whether it is pending, non-complaint or OK
- **Current Policy** - Searches the report based on the policy name
- **Last Poll** - Searches the report based on poll period start and poll period end
- **Non-compliance** - Filters and displays endpoints that were non-complaint during the period entered or selected in these fields

To filter the results:

- Click the filter icon in any of the respective column header to search for a particular item
- Type or enter the filter criteria fully or partly or select and click 'Apply'

Only the entries that match the criteria will be displayed in the report.

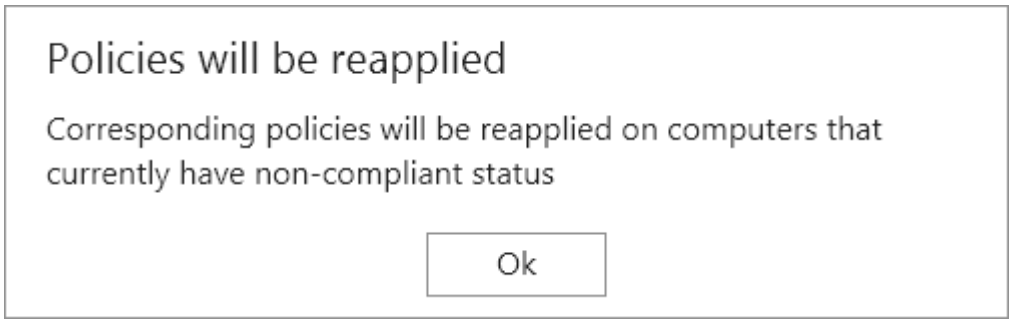
- Click 'Reset' to display all the items

Downloading the Report

If the administrator had opted for generating a printable report file in step 3, the report can be downloaded by clicking the Download icon at the bottom of the report page.

Reapplying Policy to Non-Compliant Computers

Clicking the Reapply Policy button from the bottom starts applying the corresponding policies to the non-compliant endpoints, overriding the current configuration of the local CIS installations in the target computers, on clicking 'OK' to the confirmation dialog.

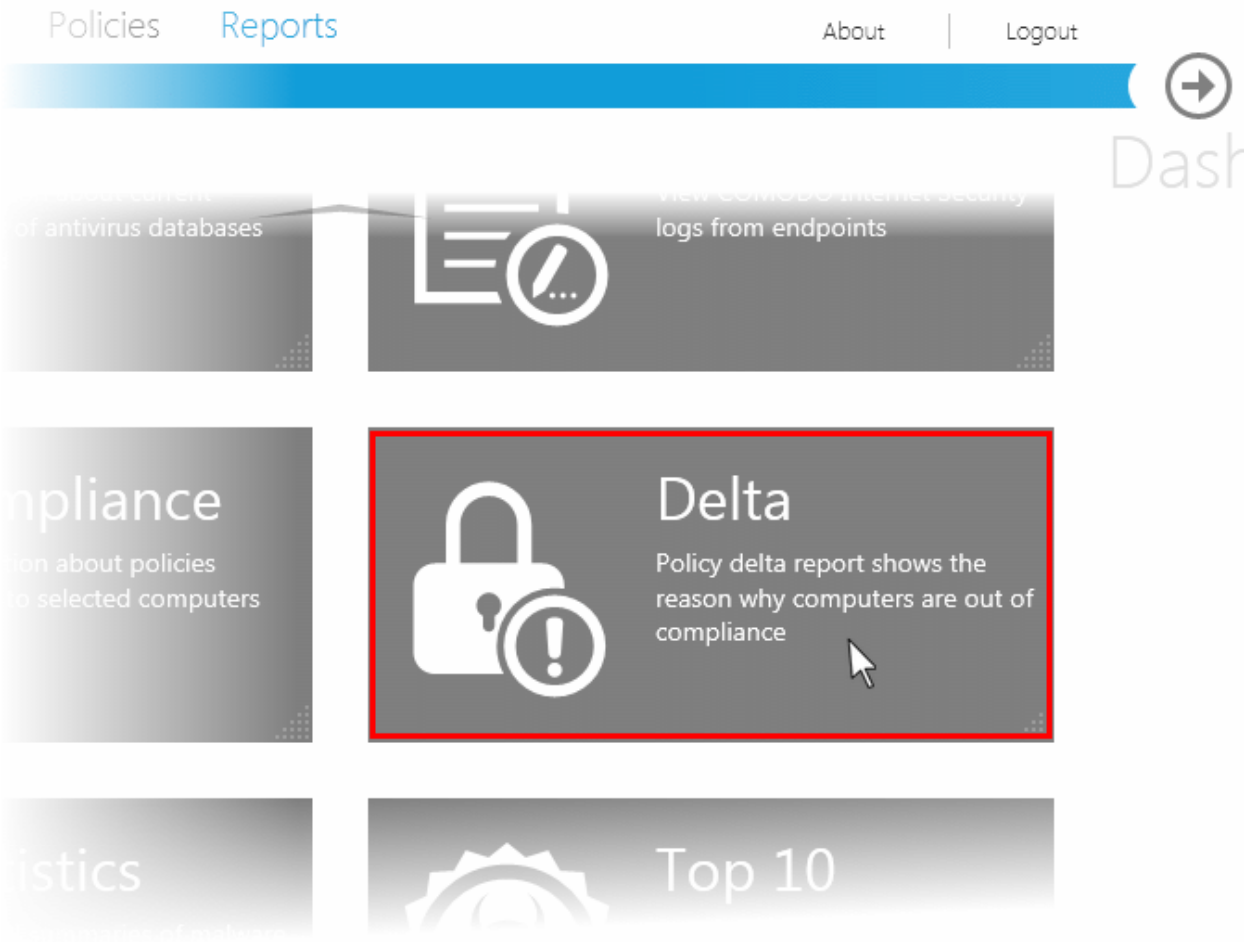


After re-application of the policies, all the target computers can be observed to have a policy status of Pending before being returned to 'compliant' status.

2.5.8. Policy Delta Report

The Policy Delta report provides a summary of the changes in the configuration of components of CIS 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 CIS settings in the target computer and the reason(s) the computer received its non-compliant status.

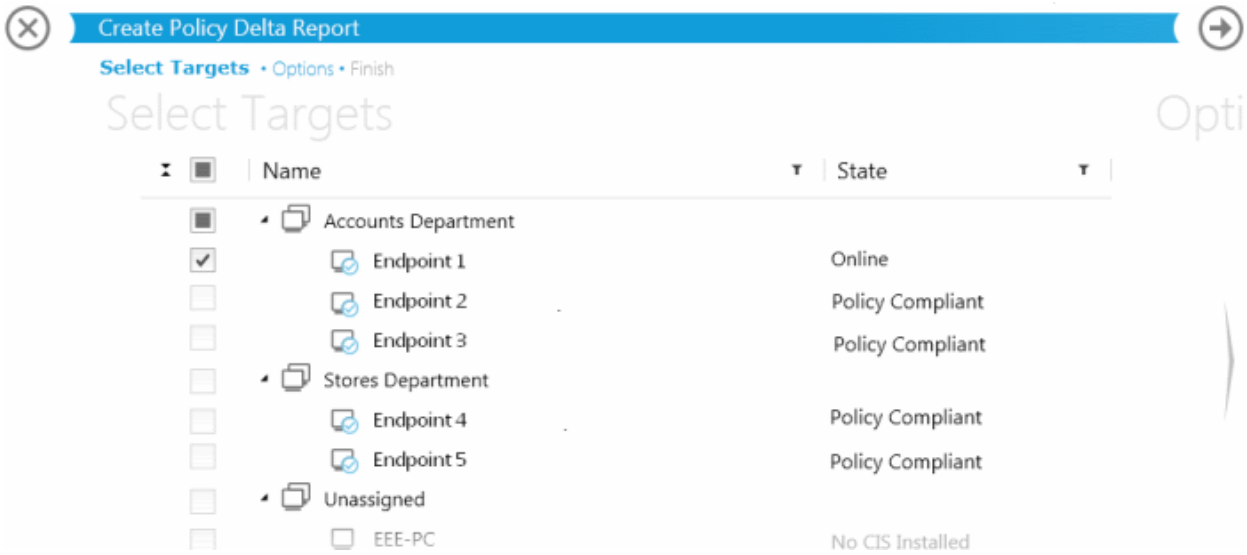
To generate a 'Policy Delta' report click the 'Delta' tile from the 'Reports' interface.



The 'Create Policy Delta Report' wizard will start.

Step 1 - Selecting Targets

All the endpoints connected to CESM will be displayed with the endpoints that are not complaint with their respective group's policy preselected.



- De-select the endpoint(s) for which you do not want to generate the Policy Delta report

Step 2 - Options

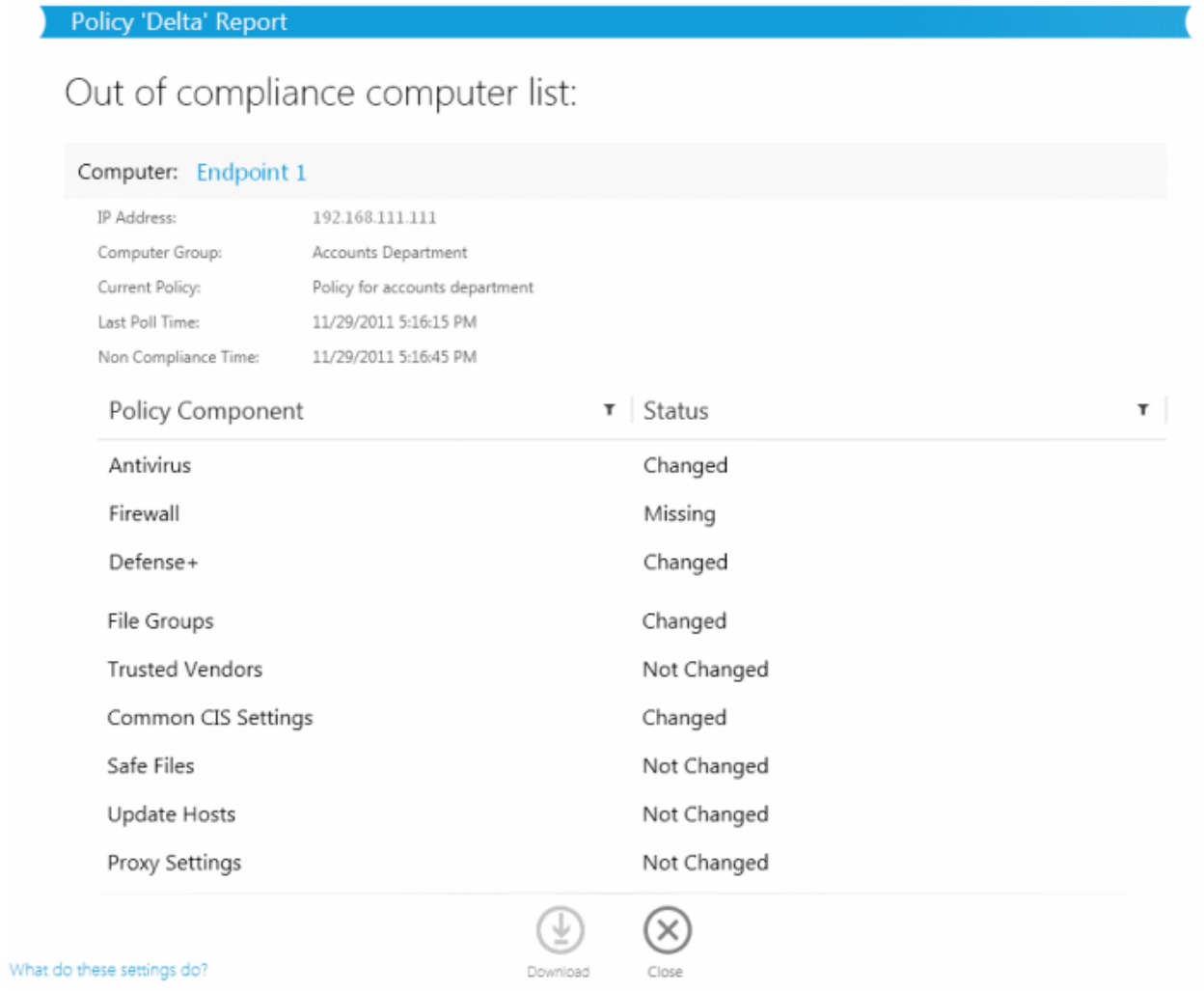
- **Generate downloadable report file** - Select this option if you need to print or archive the report. You can choose the printable file to be generated in portable document (.pdf) or spreadsheet (.xls) format. On completion, the report generated can downloaded to the administrator's computer.

Step 3 - Generate Report

- Click the Finish icon or swipe the screen to left to start generating the report. On completion, the report will be displayed.

Viewing the Report

The report will contain a list of 'Non-Compliant' computers with the status of each component of CIS in the computer.



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 in target policy** - 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.

Sorting the Entries

Clicking any column heading switches the sorting of the entries based on the ascending/descending order of the entries as per the information displayed in the respective column.

Available Report Filters

The report screen allows the administrator to optimize the search by using the filter option. The available filters for the Policy Delta report are:

- **Policy Component** - Searches the report based on the policy component's name
- **Status** - Filters the report based on the status of the policy component

To filter the results:

- Click the filter icon in any of the respective column header to search for a particular item
- Type or enter the filter criteria fully or partly or select and click 'Apply'

Only the entries that match the criteria will be displayed in the report.

- Click 'Reset' to display all the items

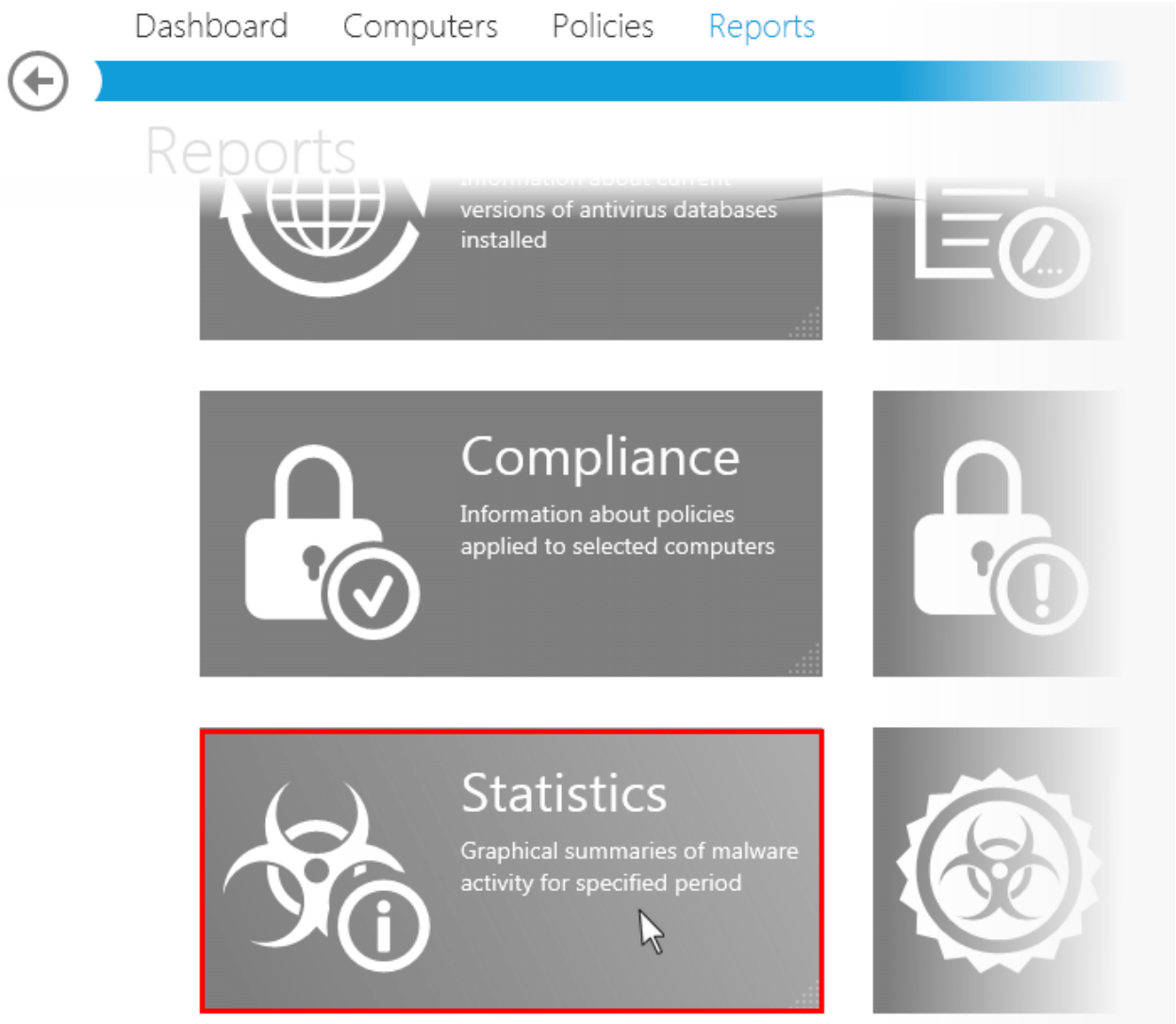
Downloading the Report

If the administrator had opted for generating a printable report file in step 2, the report can be downloaded by clicking the Download icon at the bottom of the report page.

2.5.9. Malware Statistics Report

The Malware Statistics report provides a graphical representation of the total malware identified at the target endpoints and the actions taken against them by CIS 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.

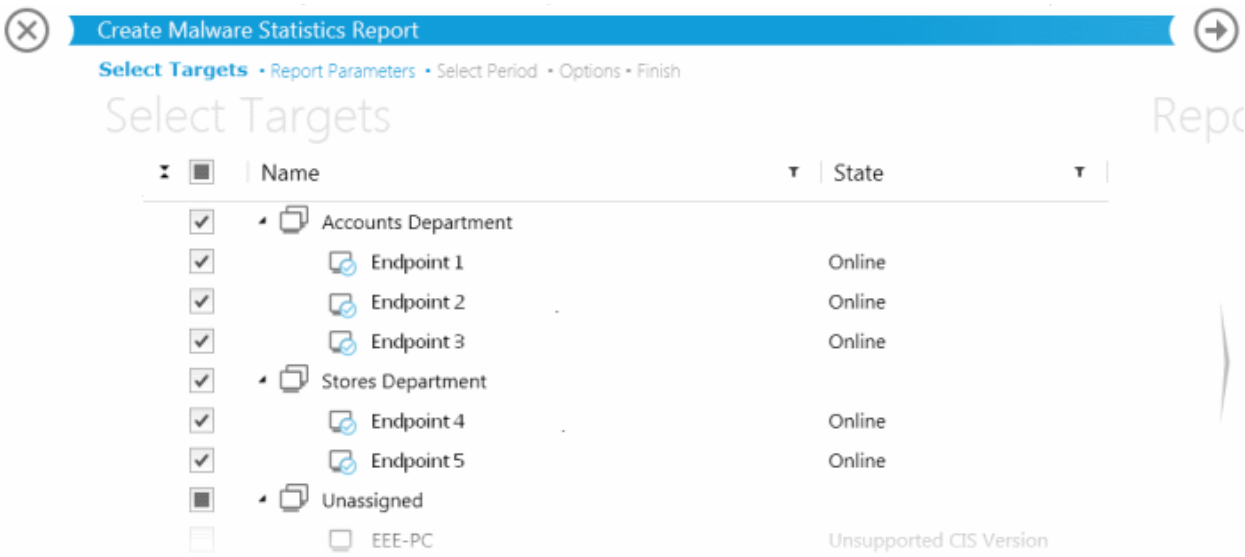
To generate a 'Malware Statistics' report click the 'Statistics' tile from the 'Reports' interface.



The 'Create Malware Statistics Report' wizard will start.

Step 1 - Select Targets

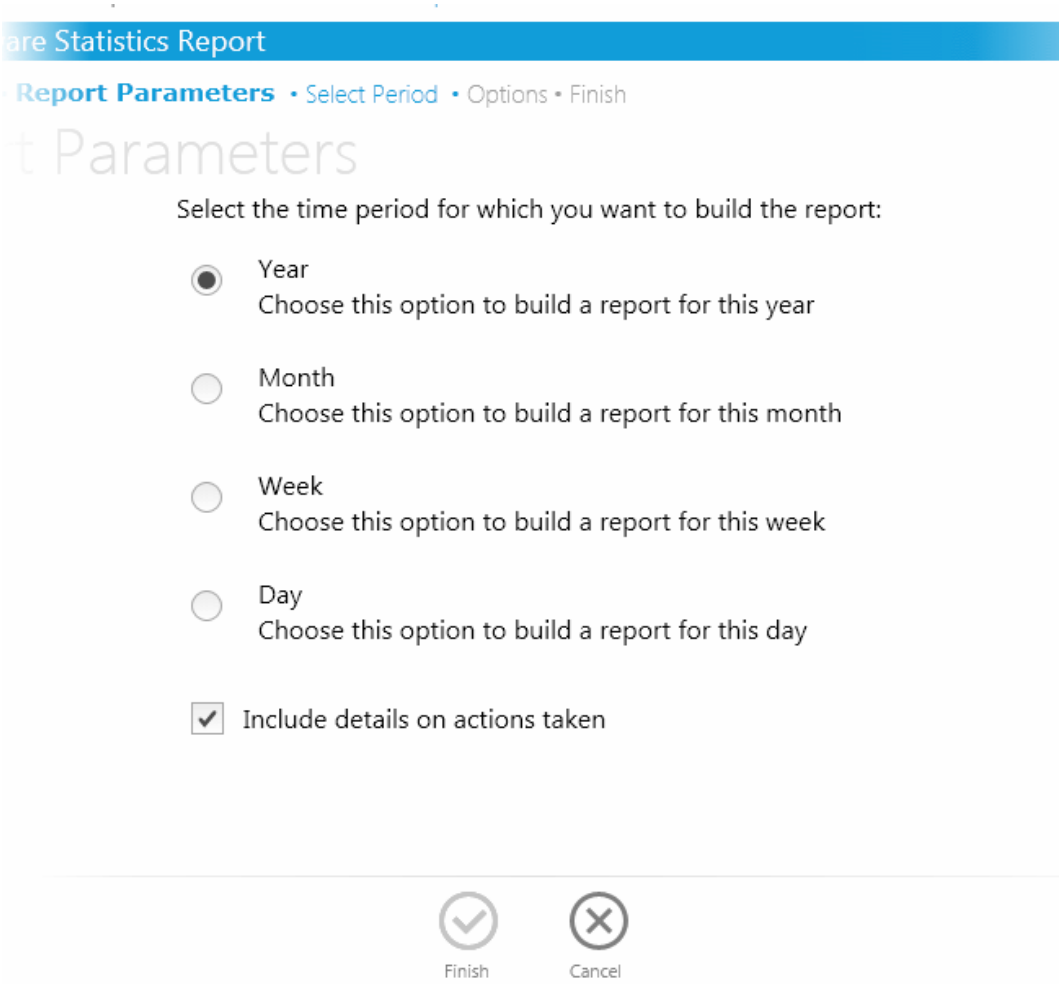
All the target computers connected to CESM are displayed.



- Select the endpoint(s) for which you wish to generate the 'Malware Statistics' report and swipe the screen or click the right arrow to move to step 2 - Selecting Report Parameters

Step 2 - Selecting Report Parameters

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



- The time period options available are:

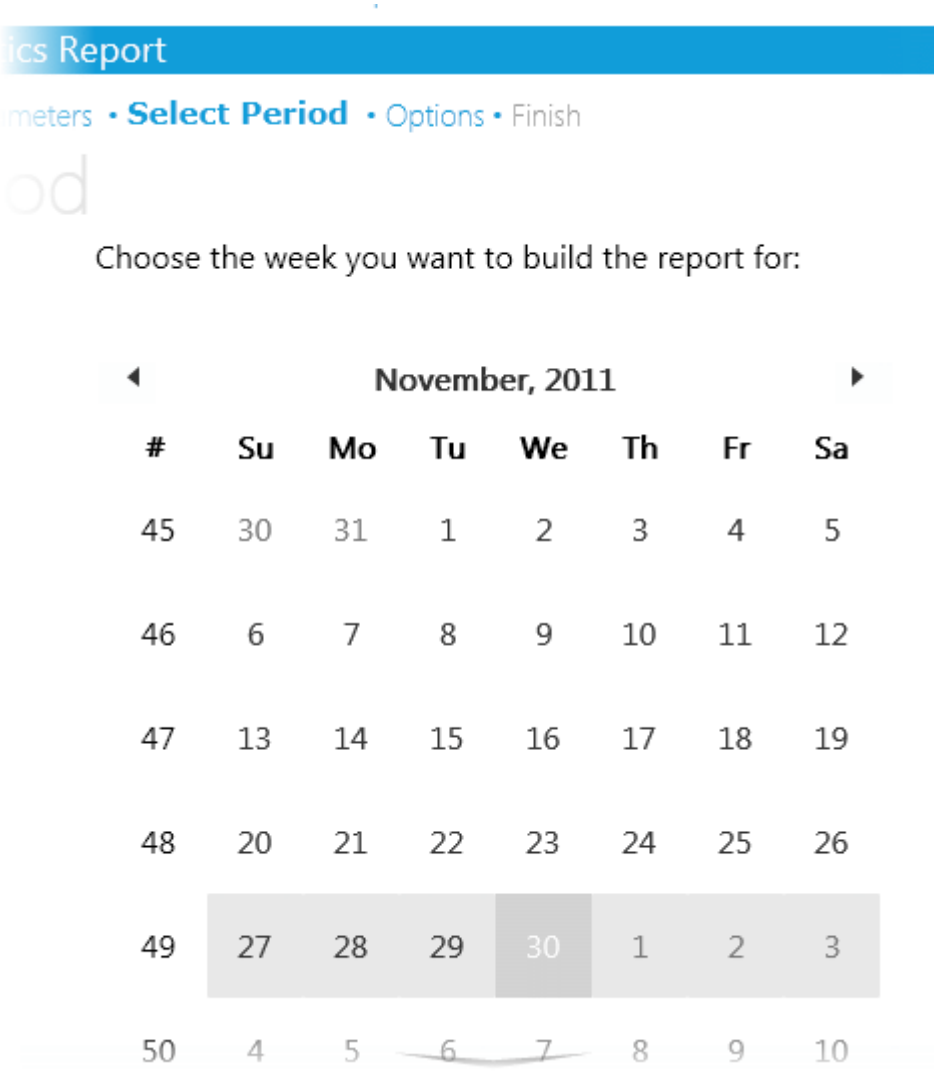
- Year - Generates statistics from any year (from 1st January YYYY).
- Month - Generates statistics from the beginning of the current month (from 1st MM YYYY).
- Week - Generates statistics for any of the weeks between Sunday and Saturday. The week can be selected from a calendar in the next step 'Select Period'.
- Daily - 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 CIS at the endpoint(s). The report will contain only graphical representations of the statistics of malware detected from various target computers if this option is not selected.
  - Swipe the screen or click the right arrow to move to step 3 - Select Period.

Step 3 - Select Period

The next screen allows you to choose the specific time period as per the selection made in step 2.



- Swipe the screen or click the right arrow to move to step 4 - Options

Step 4 - Options

- **Generate downloadable report file** - Select this option if you need to print or archive the report. You can choose the printable file to be generated in portable document (.pdf) or spreadsheet (.xls) format. On completion, the report generated can be downloaded to the administrator's computer.

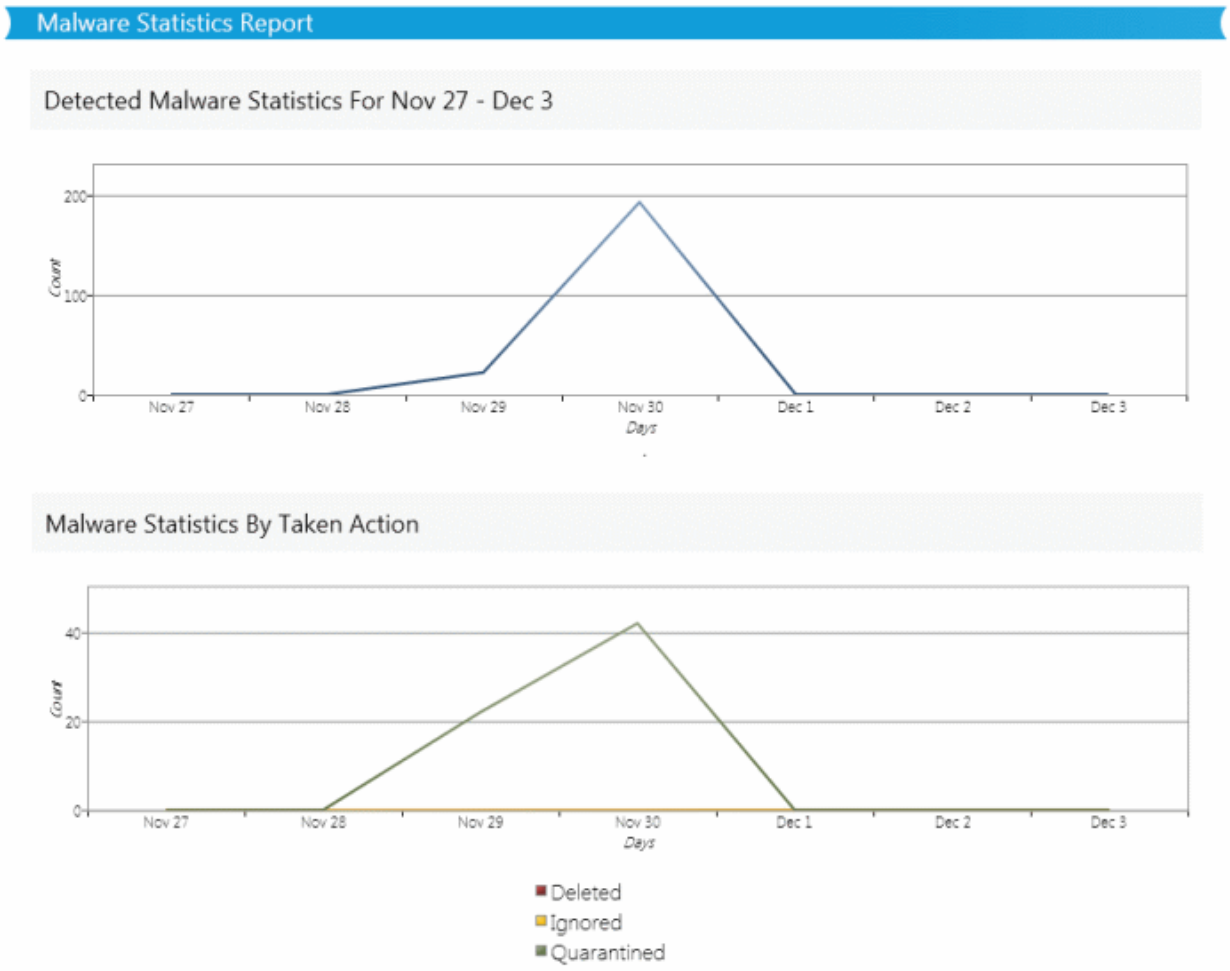
Step 5 - Generate Report

- Click the Finish icon or swipe the screen to left to start generating the report. On completion, the report will be displayed.

Viewing the Report

The report will contain a graphical representation malware statistics of the selected target computers for the selected time period. If the option 'Include details on actions taken' is chosen in step 2, the report will also contain 'Details per Computer' with granular details on the malware found at each endpoint and the action taken against them.

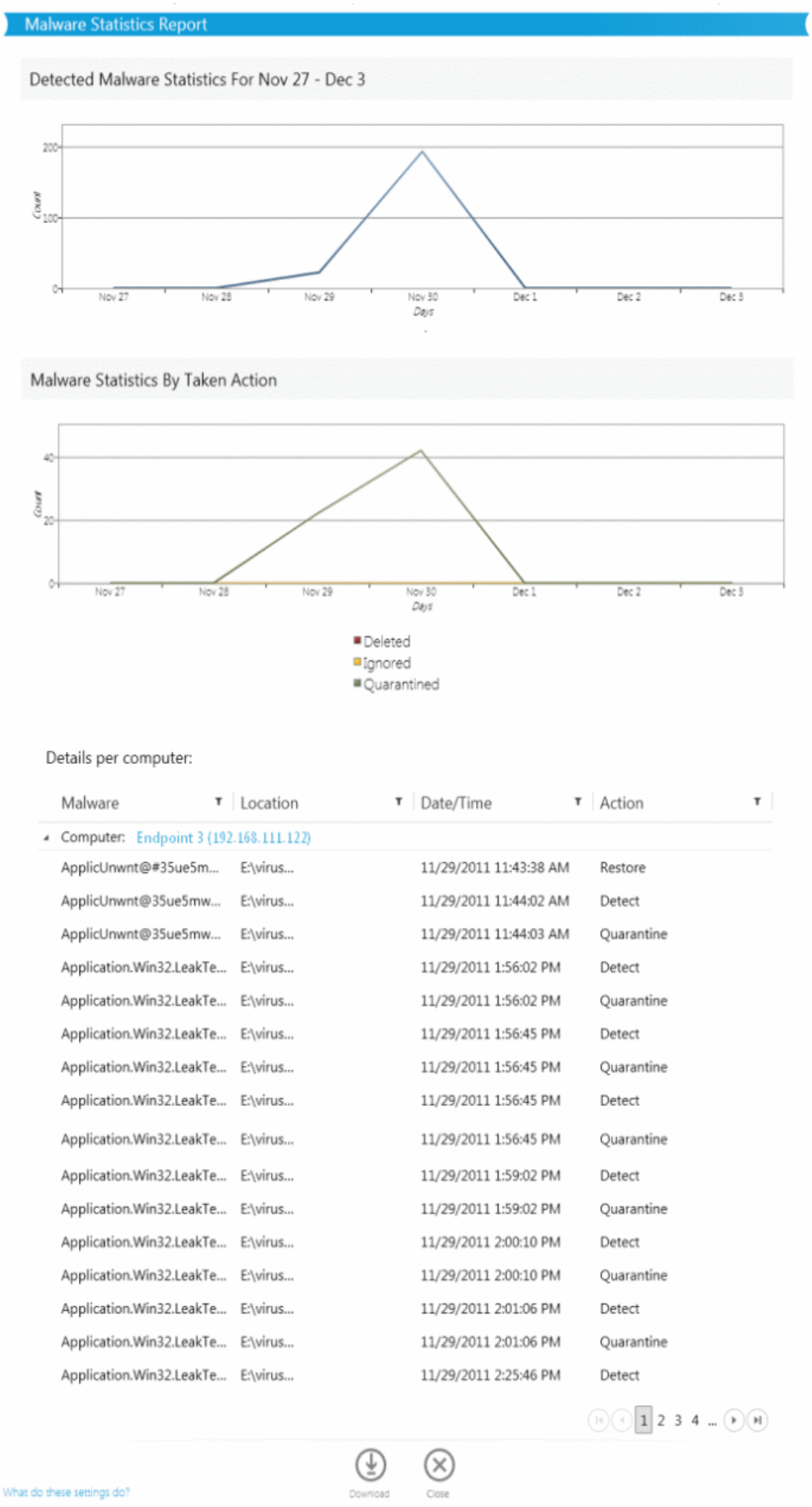
Example 1 - Malware Statistics only:



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

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.



Available Report Filters

The report screen allows the administrator to optimize the search by using the filter option. The available filters for the Malware

Statistics report are:

- **Malware** - Searches the report based on the malware's name
- **Location** - Searches the report based on the path where the malware is located in the endpoint
- **Date/Time** - Searches the report based on the action taken date and time
- **Action** - Filters the report based on the action taken

To filter the results:

- Click the filter icon in any of the respective column header to search for a particular item
- Type or enter the filter criteria fully or partly or select and click 'Apply'

Only the entries that match the criteria will be displayed in the report.

- Click 'Reset' to display all the items

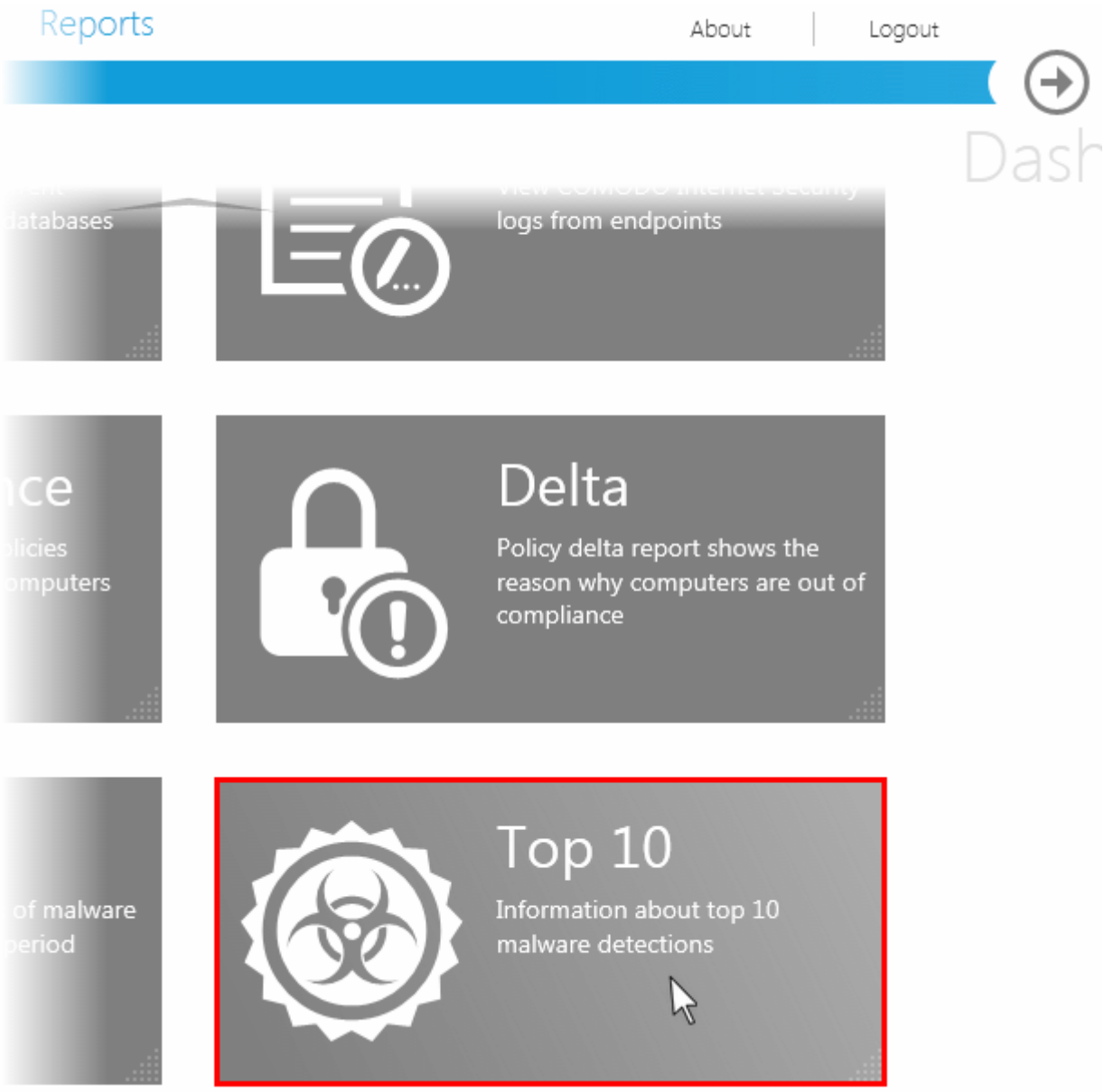
Downloading the Report

If the administrator had opted for generating a printable report file in step 4, the report can be downloaded by clicking the Download icon at the bottom of the report page.

2.5.10. Top Ten Malware Report

The 'Top Ten Malware' 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 Ten Malware' 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.

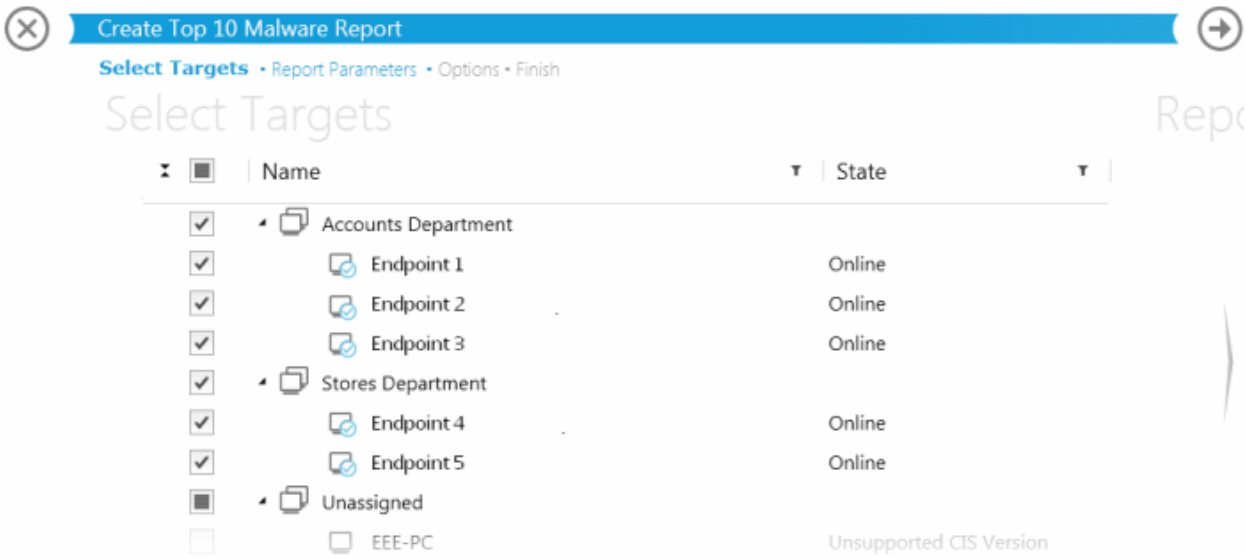
To generate a 'Top Ten Malware' report click the 'Top 10' tile from the 'Reports' interface.



The 'Create Top 10 Malware Report' wizard will start.

Step 1 - Selecting Targets

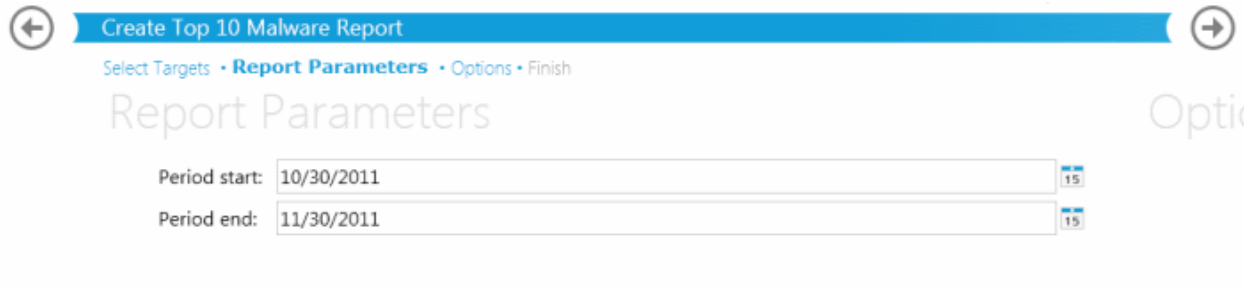
A list of all connected endpoint computers is displayed.



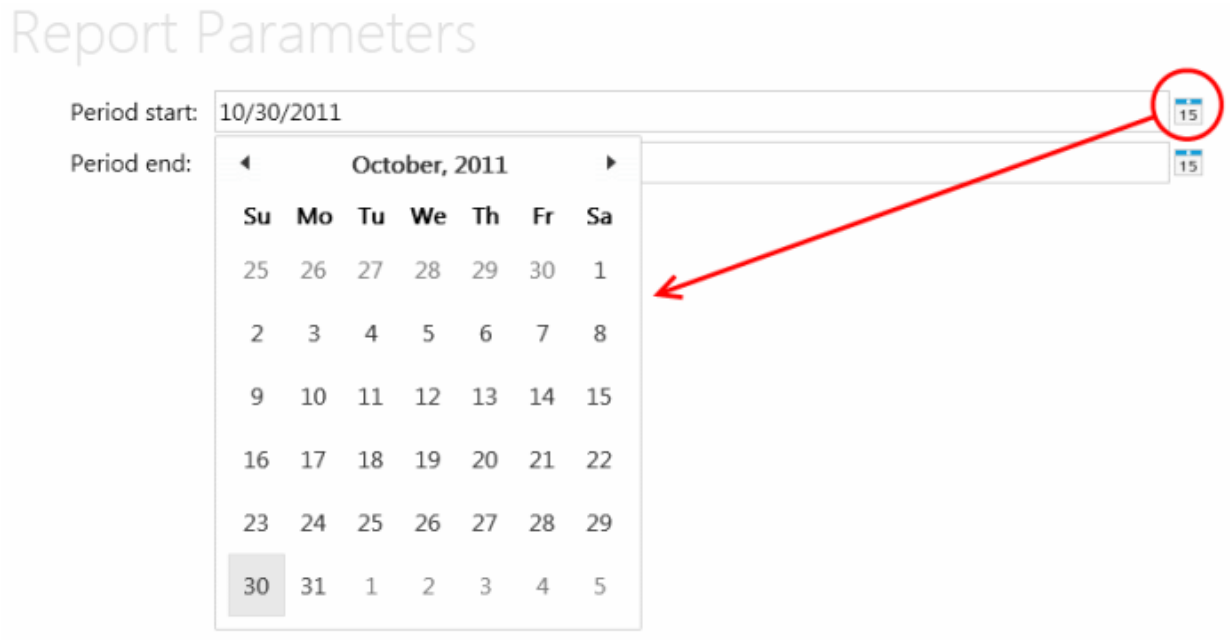
- Select the endpoint(s) for which you wish to generate the 'Top 10 Malware' report and swipe to the left or click the right arrow

Step 2 - Selecting the Report Period

The next step is to choose the time period that the report should include the top 10 malware identified.



- Specify the period start and end dates in the respective text fields in MM/DD/YYYY format. Alternatively, clicking the calendar icon at the right end of the text box displays a calendar to select the dates.



Step 2 - Options

- **Generate downloadable report file -** Select this option if you need to print or archive the report. You can choose the printable file to be generated in portable document (.pdf) or spreadsheet (.xls) format. On completion, the report generated can be downloaded to the administrator's computer.

Step 3 - Generate Report

- Click the Finish icon or swipe the screen to left to start generating the report. On completion, the report will be displayed.

Viewing the Report

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 malware with details on number of appearances and the target computer(s) at which the malware is detected.

Available Report Filters

The report screen allows the administrator to optimize the search by using the filter option. The available filters for the Top 10 Malware report are:

- **Malware** - Searches the report based on the malware's name.
- **Number of appearances** - Filters the report based on the number of times the malware has affected the endpoints..

To filter the results:

- Click the filter icon in any of the respective column header to search for a particular item.
- Type or enter the filter criteria fully or partly or select and click 'Apply'.

Only the entries that match the criteria will be displayed in the report.

- Click 'Reset' to display all the items.

Downloading the Report

If the administrator had opted for generating a printable report file in step 2, the report can be downloaded by clicking the Download icon at the bottom of the report page.

2.6. About

The 'About' screen displays the copyright information and the current CESM version number. The screen also has a download link if any newer version of the application is available. It also provides the server information and license information. You can also upgrade the license in the license information screen.

To view the current CESM version, server and license information

- Click the 'About' link at the top right of the interface.

About

The current CESM version will be displayed.

- If any newer version of the application is available, you can download it by clicking the 'Download version...' link.
- End-user license agreement - Click this link to read the full end user license agreement.
- Online help - Opens the online help guide of CESM BE. The CESM help guide contains detailed explanations of the functionality and usage of the application.

- Support forums - Click this link to get further assistance on CESM by posting your question on Comodo Forums, a message board exclusively created for our users to discuss anything related to our products.

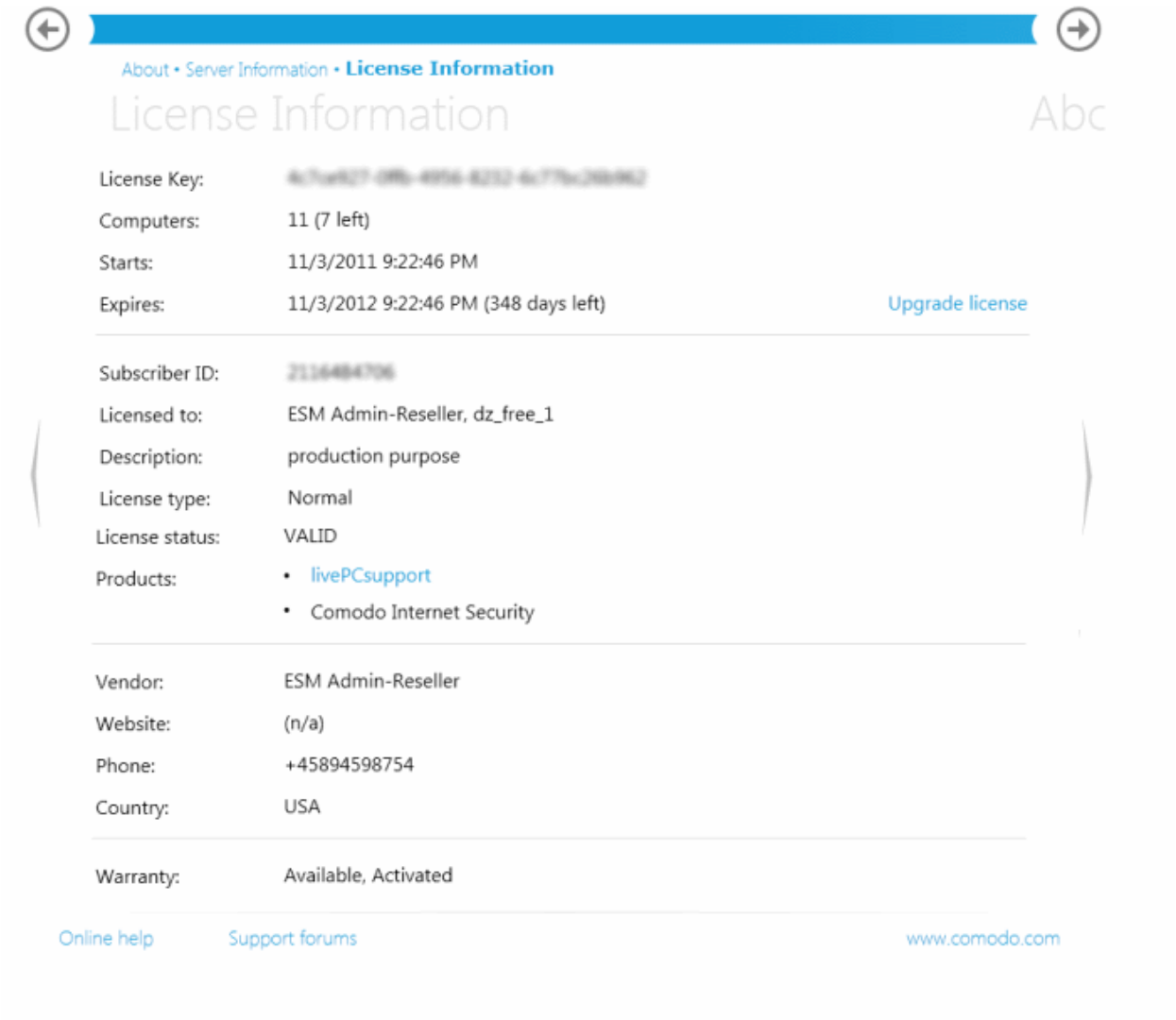
Server Information

Click the right arrow or swipe the screen to the left to open the server information screen.

A snapshot of the CESM server configuration information is displayed. Refer **Appendix 1** for more information on the service configuration tool.

License Information

Click the right arrow or swipe the screen to the left to open the license information screen.



The details of the current license information is displayed. If you want to include more endpoints than is allowed for your current license and manage them, the license has to be upgraded. Click the 'Upgrade license' link in the top pane. Refer **License Status Tile** section for more information on upgrading your license.

2.7. Logging out of CESM Console

Administrators can logout of the CESM console by clicking the 'Logout' link at the top right of the interface.

Closing the browser window or tab containing the console or pressing the 'Refresh' button will also logout the administrators.

3.How To... Tutorials

The 'How To...' section of the guide contains guidance on using CESM effectively. Click on the links below to go the respective tutorial page for guidance of the respective feature.

- How to connect CIS to CESM at the local endpoint
- How to configure CIS policies - an introduction
- How to set up external access from the Internet
- How to install CIS

3.1.How to Connect CIS to CESM at the Local Endpoint

This page explains how computers that have standalone Comodo Internet Security (CIS) installed on them can be connected to the CESM service via the CIS interface (directly from the endpoint itself).

In short:

- Open CIS on the endpoint.
- Click 'More' at the top right corner of the interface; then '**Manage This Endpoint**'.
- Specify the hostname / IP address and port of the CESM server (default to be entered = 57193 unless changed in the Configuration Tool).
- The CESM agent will be installed on the local machine and a connection will be established with the CESM server.
- Connection details will be displayed at the bottom left of the main interface in the 'Managed Client' area. The machine will initially be placed in the 'Unassigned' group in CESM and will inherit that group's security Policy.

  The *default* parameter for the 'Unassigned' group is security policy = 'Locally configured'. Because the policy is 'Locally Configured', this means that CESM will not enforce policy on the endpoint and the endpoint will use the CIS settings that are currently in place.

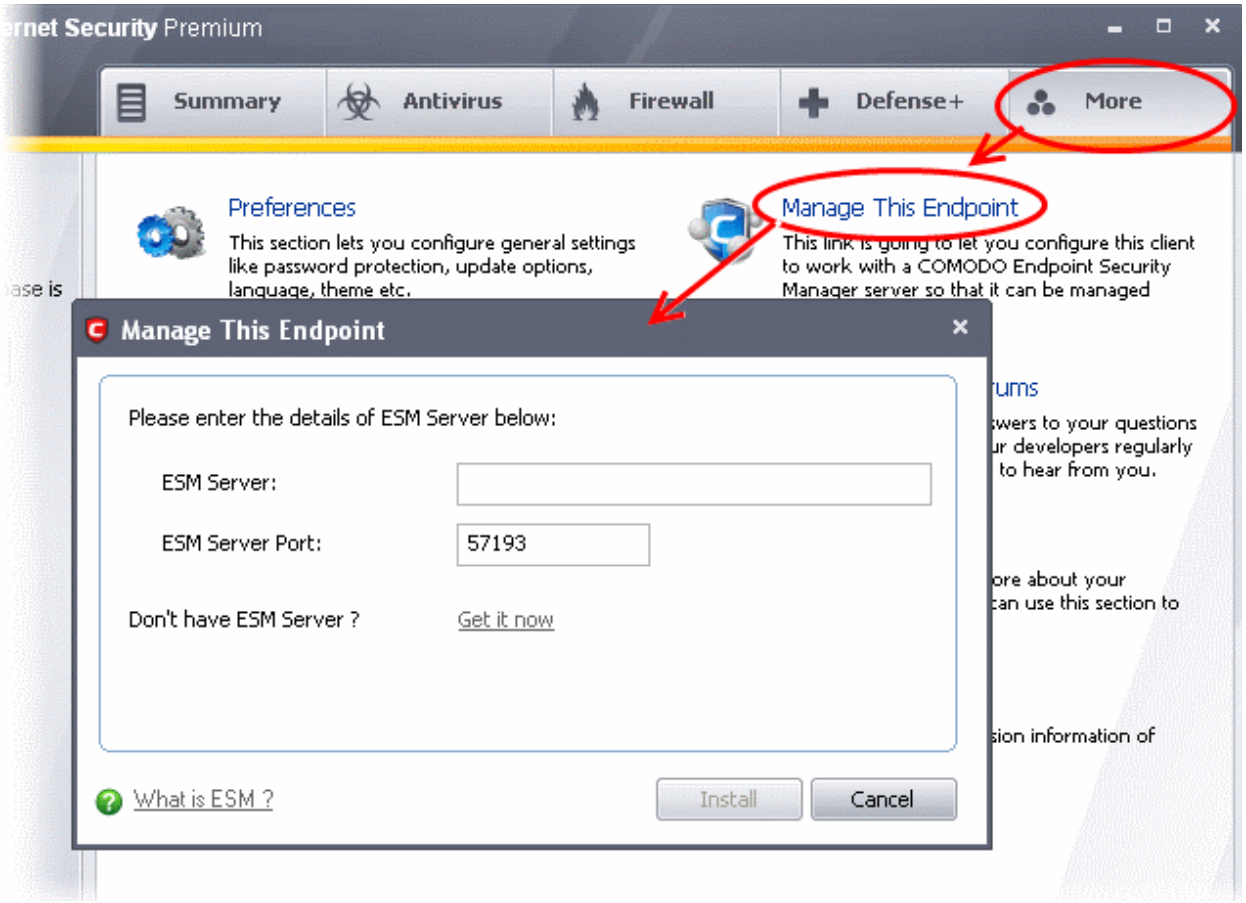
  - Endpoints can be moved into groups in the 'Computers' area. See '**Creating Endpoint Groups**' for more details.
  - Policies can be specified and assigned to groups/individual computers in the 'Policies' area. See '**Creating a New Policy**' and '**The Policies Area - Key Concepts**' for more details.
  - Switch between local and remote administration modes at the local endpoint by using the 'Manage Remotely/Manage Locally' link underneath 'Managed Client'.

Expanded version of the process

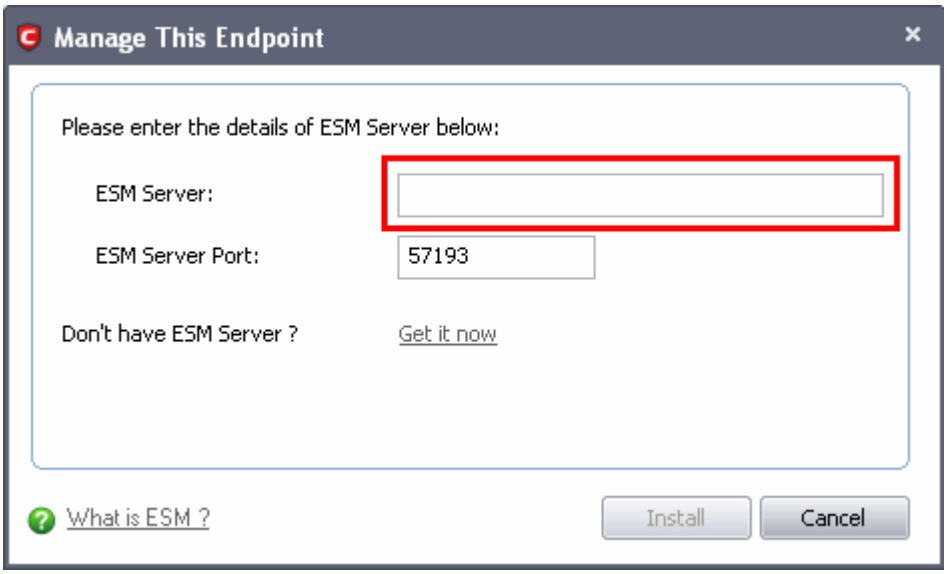
1. On the endpoint to be managed, open the CIS interface using one of the following methods:
   - Windows Start Menu - Start > All Programs > COMODO > COMODO Internet Security > Comodo Internet Security
   - Double-click the desktop shortcut or tray icon

The CIS Summary screen will display details of the connection on the bottom left pane of the interface only after the installation of the ESM agent.

2. Click the 'More' button at the top of the navigation. Click 'Manage This Endpoint'.

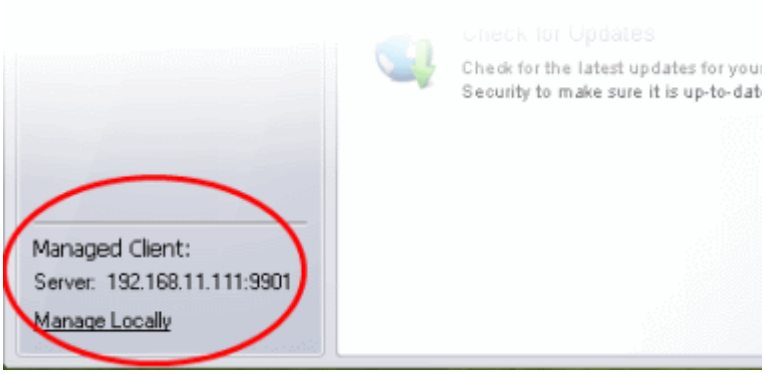


3. Enter the hostname / IP address of the server in which the CESM service is installed in the ESM Server field. These details, if required, can be found by opening the configuration CESM tool on the server (Start > All Programs > COMODO > Endpoint Security Manager > CESM configuration tool). See **Configuration Tool** for more details.
4. Do not change the port number from 57193 in the ESM Server Port field unless the administrator changed the port using the **Configuration Tool**.



5. Click 'Install' to begin installation of the agent. Once complete, you will be presented with a confirmation message in the 'Status' area. Click 'Close' to exit the wizard.

The endpoint should now be successfully connected to CESM service. Connection details can be viewed at the bottom left of the interface:



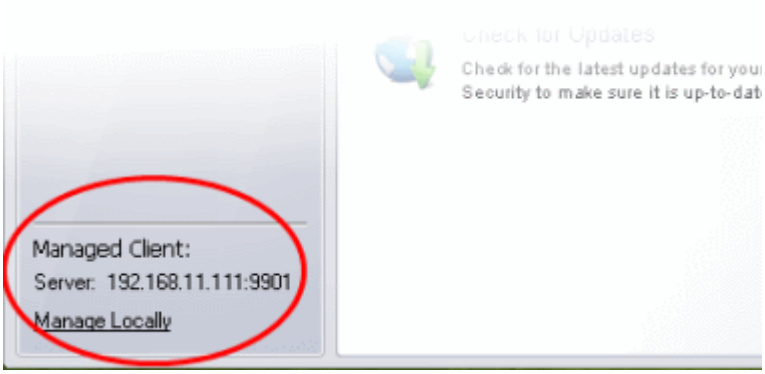
The administrator can switch to 'Local Mode' from 'Remote Mode' by clicking the 'Manage Locally' link (and vice versa if the machine is currently under 'Local Mode').

3.2. How to configure CIS Policies - An Introduction

A CESM policy is the security configuration of Comodo Internet Security (CIS) deployed on an endpoint or a group of endpoints. Each policy determines the antivirus settings, Internet access rights, firewall traffic filtering rules, sandbox configuration and Defense+ application control settings for an endpoint.

In order to configure Antivirus, Firewall and Defense+ settings in CIS 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 CIS interface to enable local administration mode:



Once the machine is in 'Local Mode', the link will be 'Manage Remotely':

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). Note - remember to keep the machine in 'Local Mode' until import and deployment is complete. After policy has been deployed, it can be switched back to 'Remote Mode'. See '**Creating a New Policy**' for more details.

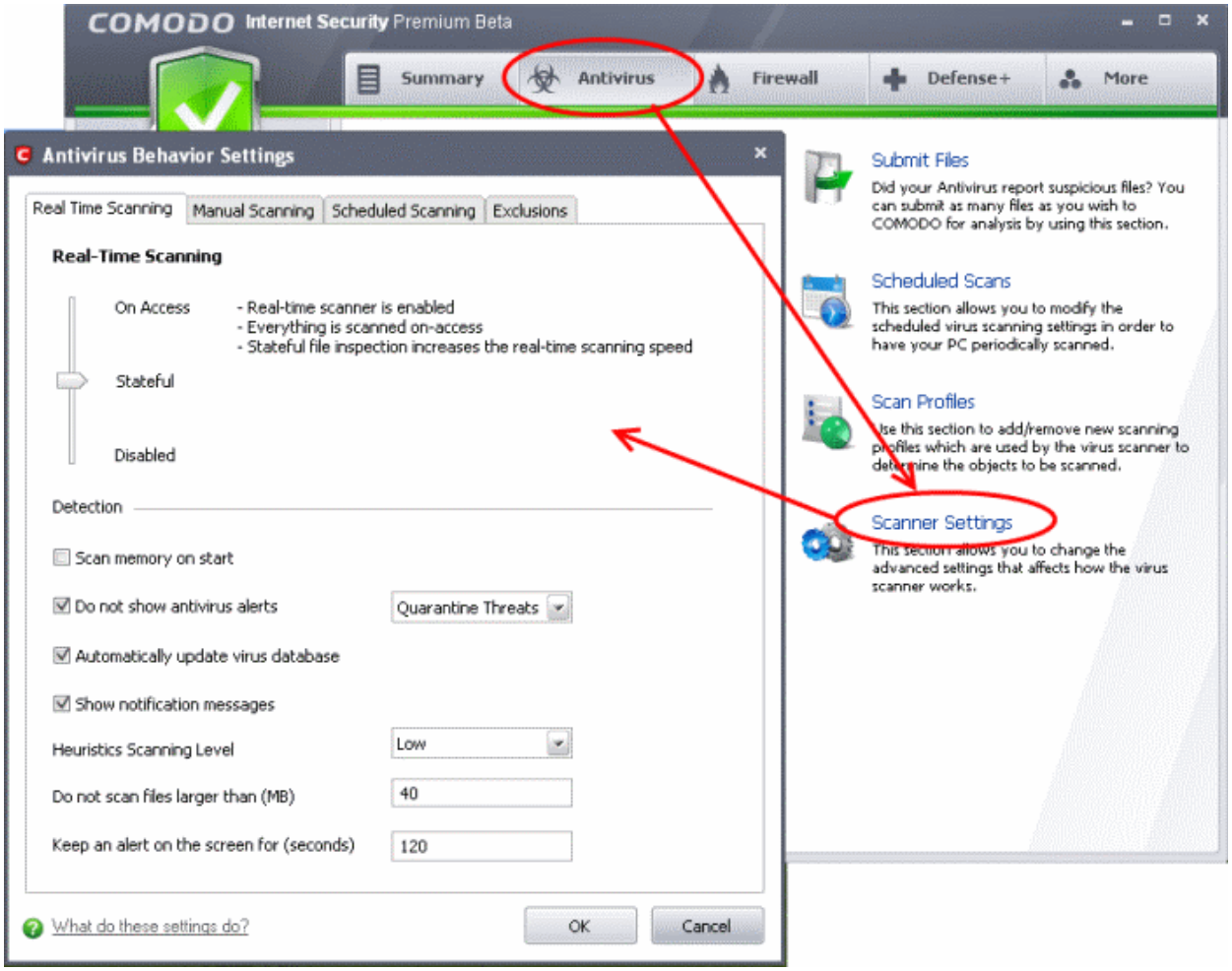
The remainder of this page is a quick primer to key areas within CIS for modifying Antivirus, Firewall and Defense+ settings along with links to the appropriate section in the dedicated CIS user-guide should further help be required.

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 'Antivirus' from the top navigation of the CIS interface and click 'Scanner Settings' from the Antivirus tasks interface. The Antivirus Behavior Settings interface will open.

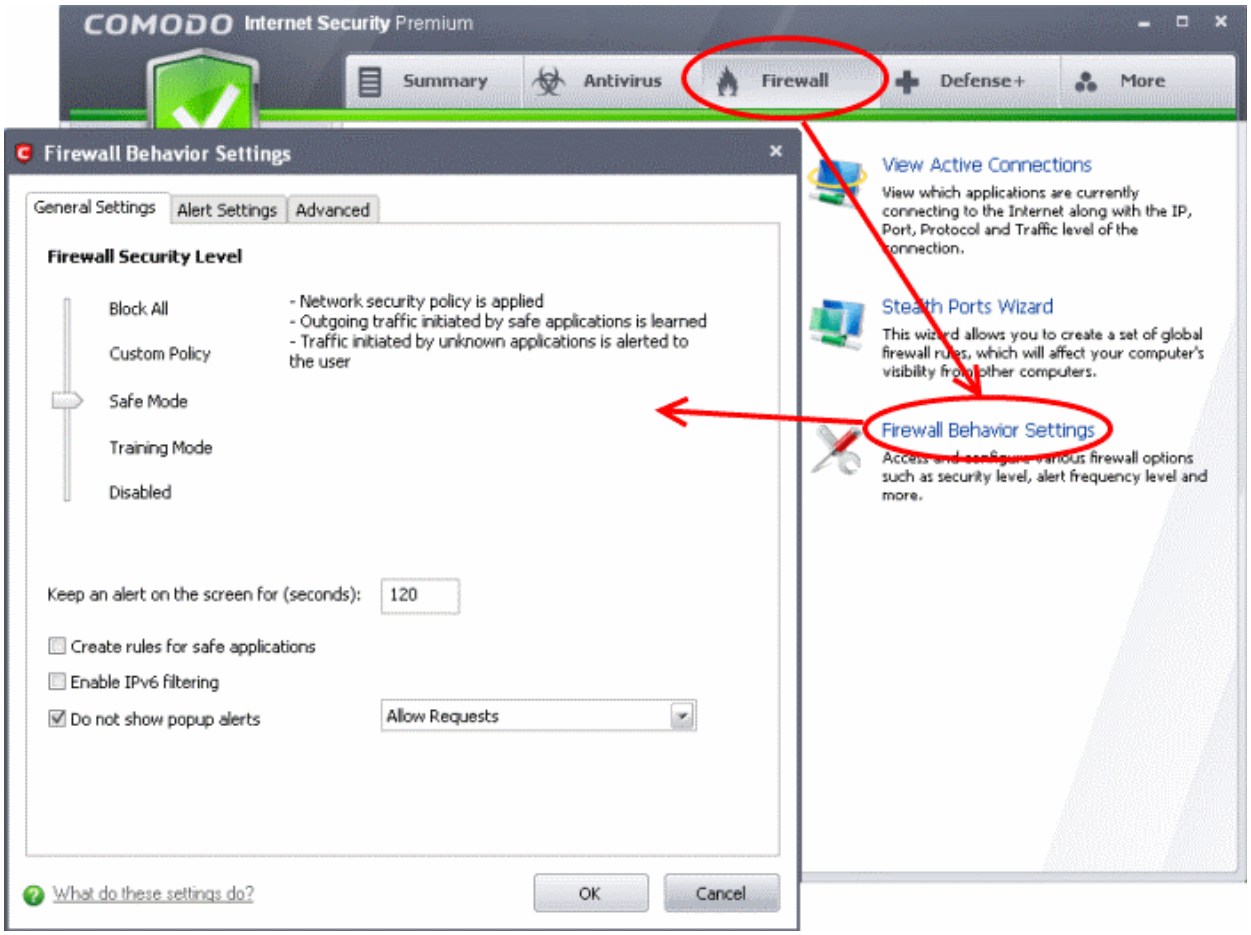


Firewall Settings

The firewall component of Comodo Internet 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 'Firewall' from the top navigation of the CIS interface and click 'Firewall Behavior Settings' from the Firewall tasks interface. The Firewall Behavior Settings interface will open.

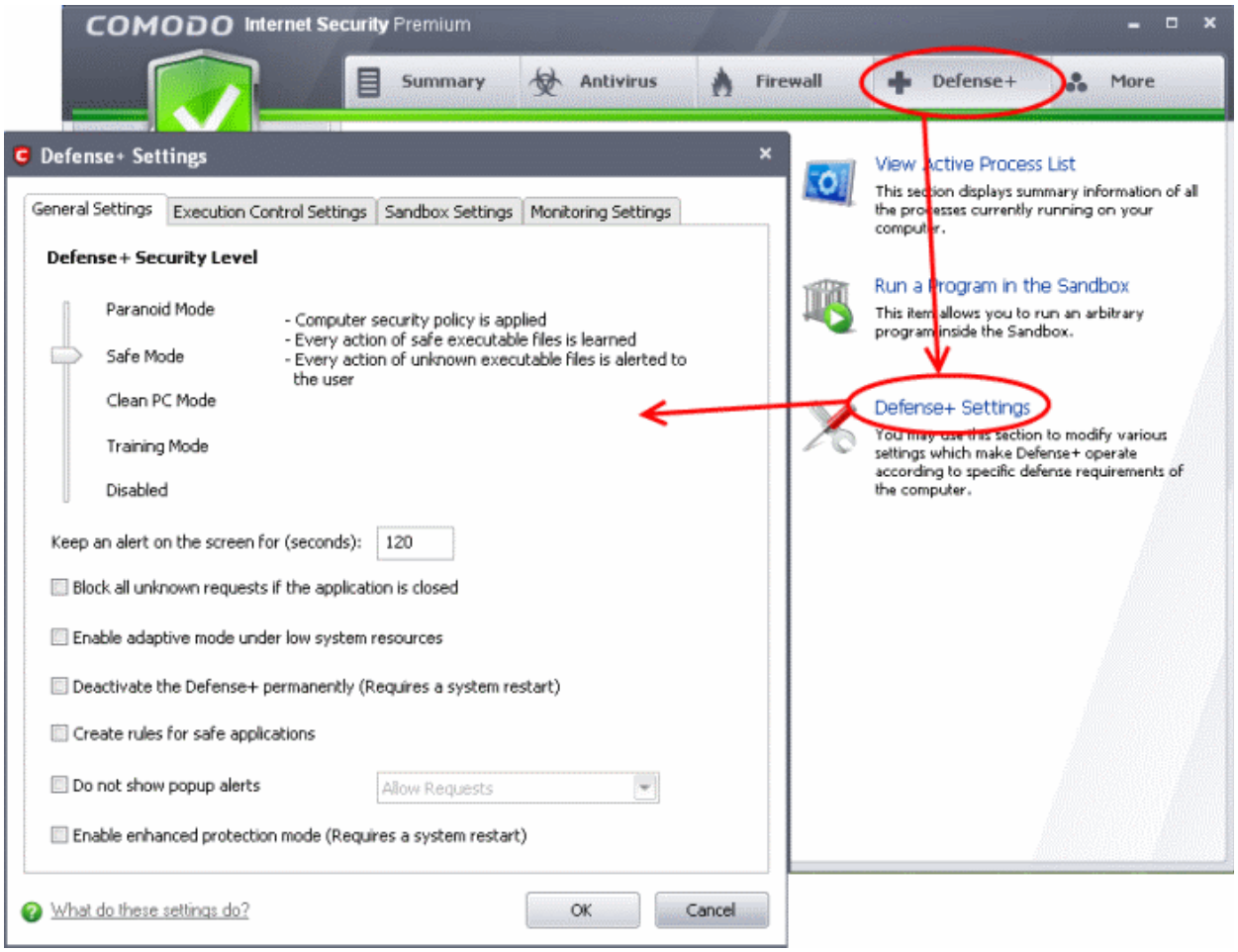


Defense+ Settings

The Defense+ component of Comodo Internet Security is a host intrusion prevention system that constantly monitors the activities of all executable files on endpoint PCs. With Defense+ activated, the only executables that are allowed to run are the ones you give permission to. The Defense+ area also allows admins to configure sandbox settings.

To configure Defense+ Settings

- Click 'Defense+' from the top navigation of the CIS interface and click 'Defense+ Settings' from Defense+ Tasks interface. The Defense+ Settings interface will open.



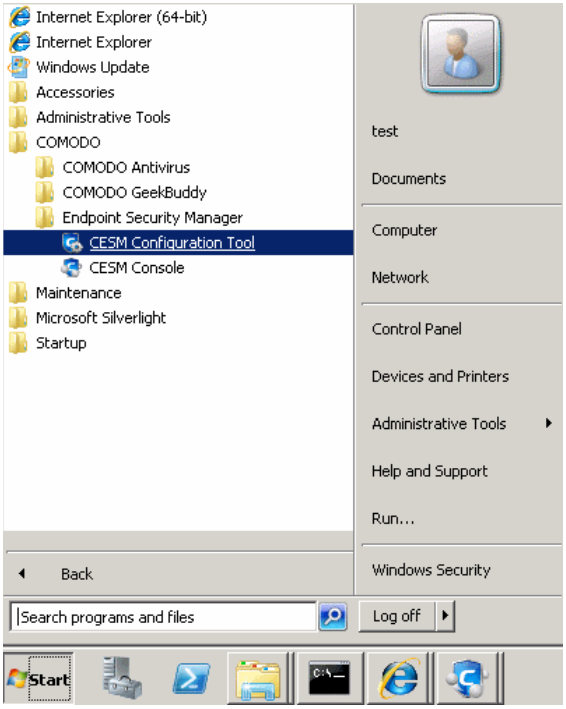
- If more details are required for these settings, see http://help.comodo.com/ for Comodo Internet Security.

For more details on installing CIS in an endpoint computer and connecting it to CESM from the CIS interface, refer the sections How to Install CIS and How to Connect CIS to CESM at the Local Endpoint.

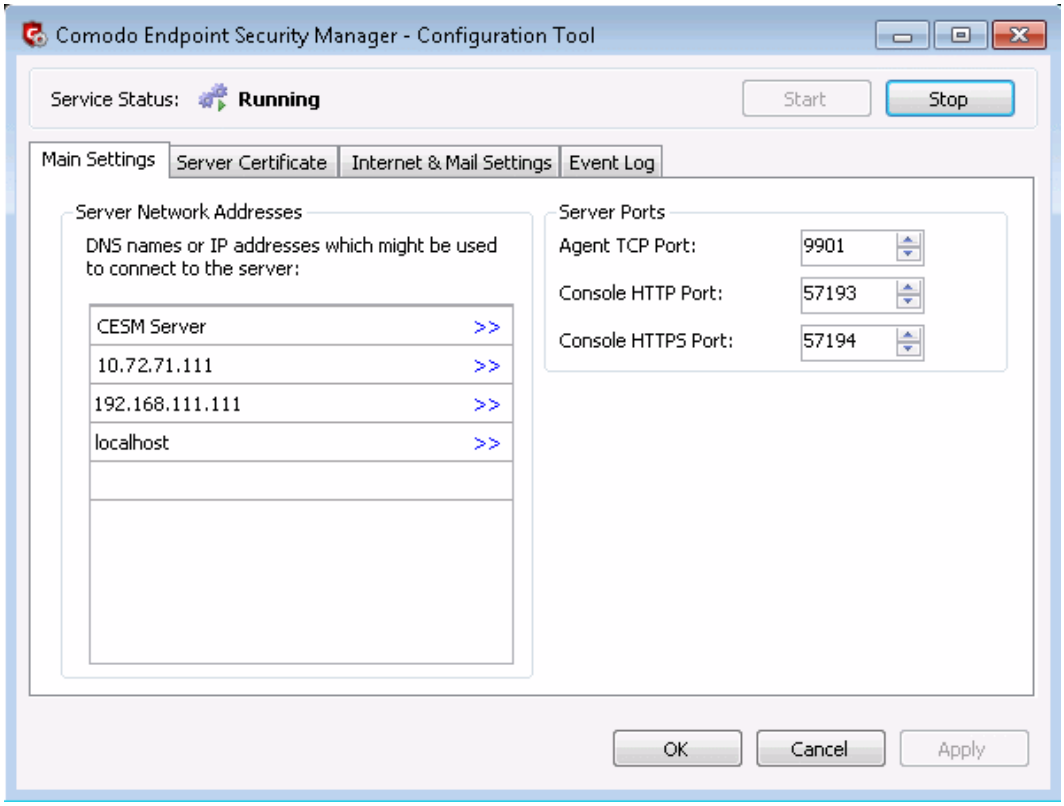
3.3. How to Setup External Access from Internet

The following guide explains how to configure CESM so that it can remotely manage endpoints that are connected via the Internet:

- Make sure that the CESM server has an externally accessible IP address
- Open the CESM configuration tool - click 'Start > All Programs > COMODO > Endpoint Security Manager > CESM Configuration Tool'



- Add the Internet reachable server IP address (alternatively hostname or FQDN) to the 'Server network addresses' list (just begin typing in the first blank row)



- Restart CESM service

See the 'Service Status' at the top of this interface, and after you click Apply, accept the prompt to restart the service:

- **If your network is equipped with a router or other similar device, it should be configured with CESM ports forwarding** (list of ports to be forwarded are listed in the 'Server Ports' on the right. Default ports are 57193, 57194 (console) and 9901 (agent).

To install agents on endpoints that are not on the local network

- At the 'Computers' area of the administrative interface, click the 'Download Agent' tile.
- 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 laptops that will be used outside the network.
- Double clicking on the setup file  will start the installation wizard. For more details, please see **Adding Computers by Manual Installation of Agent and CIS**.

  OR
- Install CIS on the local machine then click the '**Manage This Endpoint**' link. This will start a connection wizard. On specifying the Internet reachable IP address or hostname of the CESM server the wizard starts installation of the agent and establishes the connection between the endpoint and the CESM server. This process can be carried out by the administrator or by end-users if the endpoint is already in a remote location outside of the network. See '**How to connect CIS to CESM at the local endpoint**' for more details on this process.

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 Endpoint Groups** for more details on creating endpoint groups
- See section **Creating a New 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

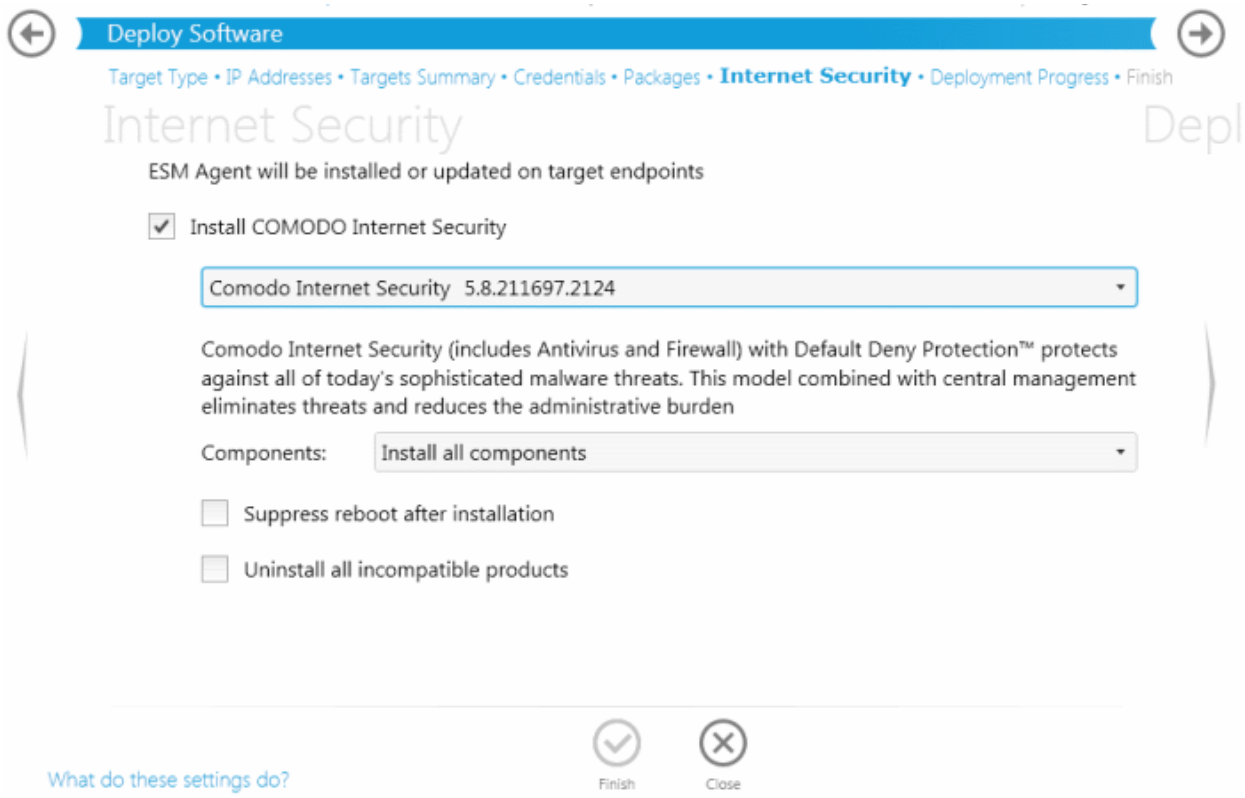
3.4. How to Install CIS

An Administrator can install CIS in endpoint computers either by using the CESM interface during agent deployment or manually by downloading the latest CIS setup file.

- **Installing CIS via CESM**
- **Manually installing CIS in endpoint computers.**

To install CIS using the CESM interface:

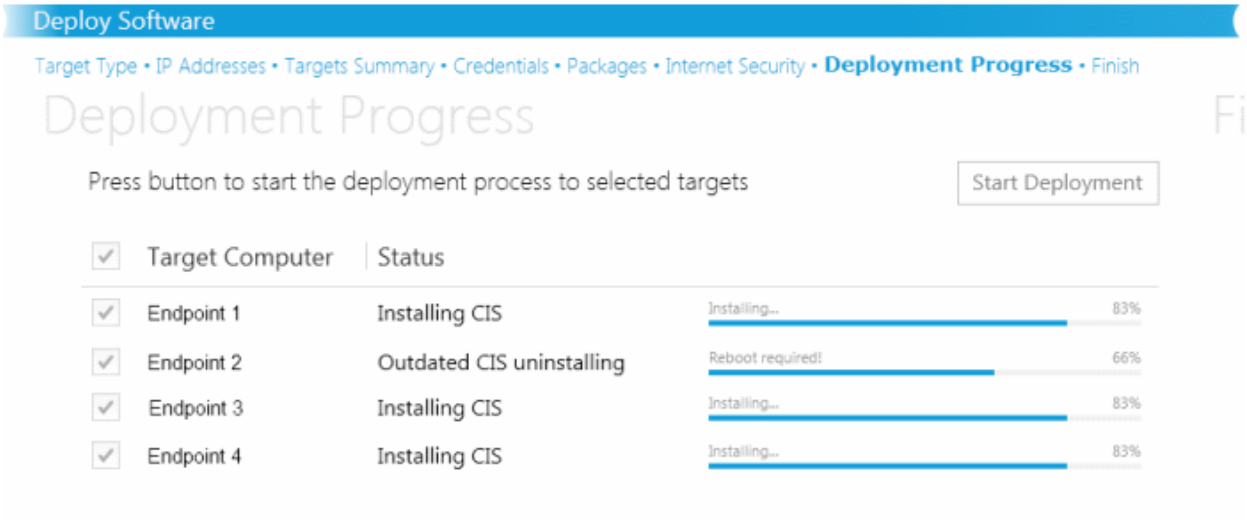
1. Click the 'Agent' tile from the 'Computers' area to start the wizard.
2. Select the Target Type from Active Directory, Workgroup or IP Addresses and click the right arrow.
3. Specify the parameters for the chosen target type, then in the next step, a summary of endpoints will be displayed.
4. Select the endpoints onto which you wish to install the agent and CIS and click the right arrow.
5. The next step is to select whether the agent and CIS has to be installed under the currently logged in user account or the network administrator account.
6. The next step allows you to check for newer versions of ESM agent and CIS. Click 'Check for updates' and download if the screen displays updates are available.
7. The next step is opting for installation of Comodo Internet Security (CIS) on to the selected endpoints.



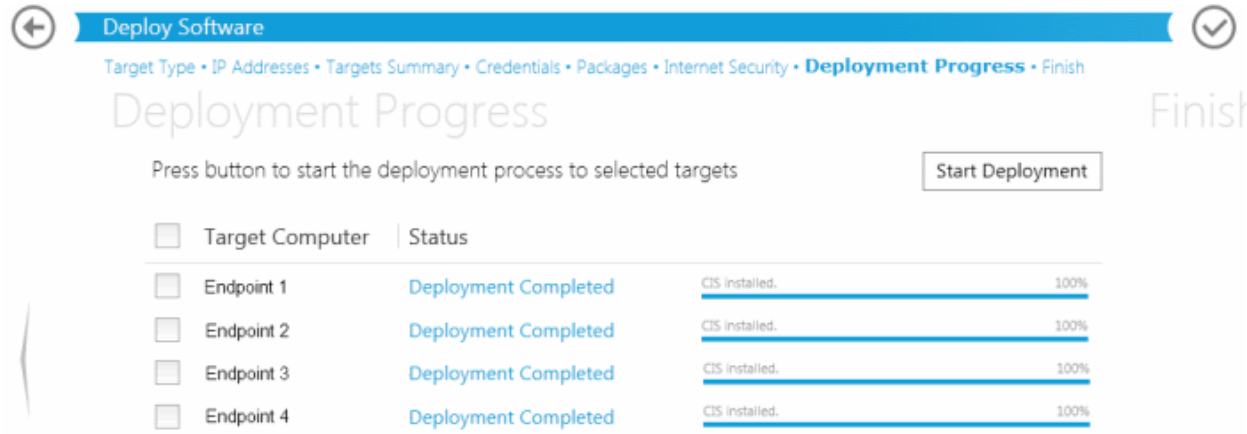
8. Select 'Install Comodo Internet Security' check box.
9. Select the version of CIS you wish to install on the selected endpoints from the drop-down.
10. Select whether you want to include all the components (Firewall and Antivirus), Antivirus only or Firewall only from the Components drop-down.
11. Suppress reboot after installation - CIS 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. CIS installation will complete but will take effect only on the next restart of the endpoint.
12. Uninstall all incompatible products - Selecting this option will uninstall select third party antivirus, firewall and other desktop security software from the endpoints, prior to the installation of CIS. Performing this step will remove potentially incompatible products and thus enable CIS 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.
13. Click the right arrow to move to the next step.
14. Click 'Start Deployment' to begin the installation process.

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



On completion of installation, the result screen will appear.



15. Click Finish icon to exit the wizard.

The agent and CIS are installed in the selected endpoints successfully.

See section '**Importing Computers by Automatic Installation of Agent**' for more details on installation of agent and CIS automatically.

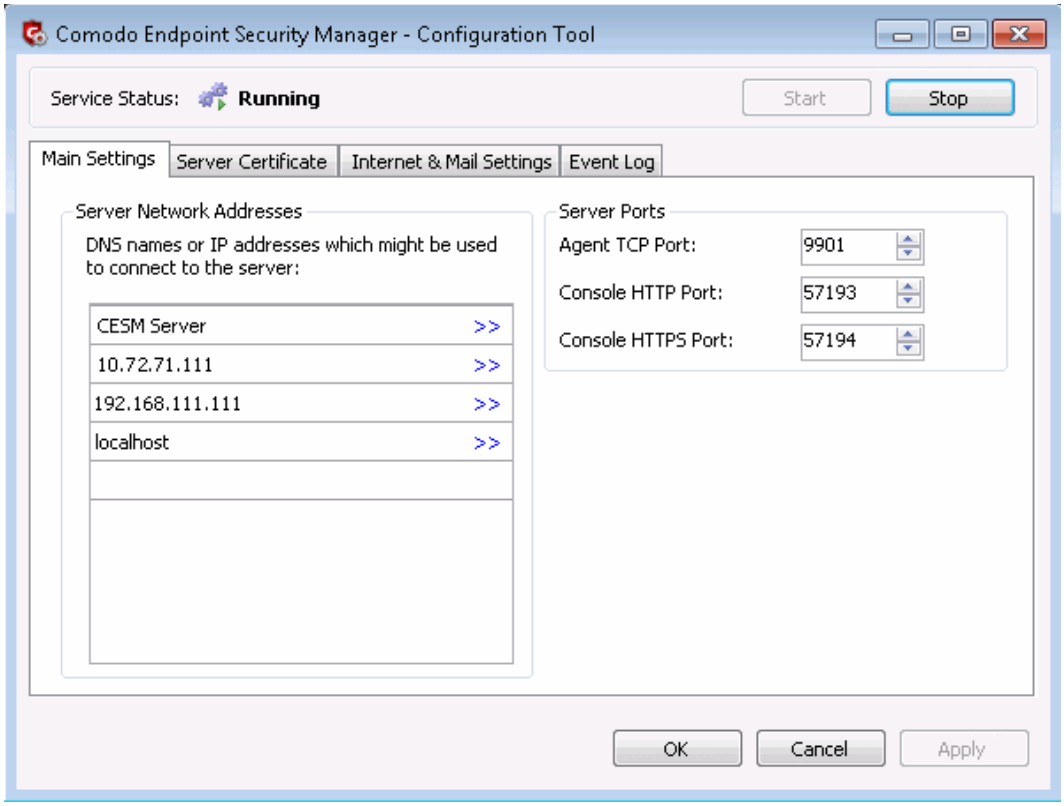
To install CIS in endpoint computers manually

1. Download the latest version of CIS and copy the setup file in the endpoint computer that you want to install the CIS.
2. Double-click 'cispremium_installer.exe' to begin the setup process.
3. For more details on the installation procedure, see **http://help.comodo.com/** for Comodo Internet Security.
4. If you wish to connect the endpoint computer to CESM directly from the CIS interface, please see How to Connect CIS to CESM at the Local Endpoint.

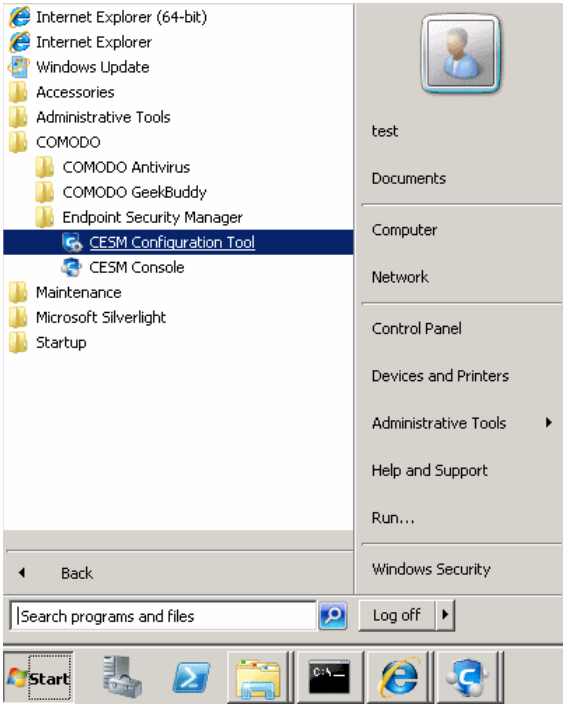
Appendix 1 The Service Configuration Tool

The Service Configuration Tool enables the administrator to start and stop the CESM 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 and can be accessed from the Windows Start Menu.



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

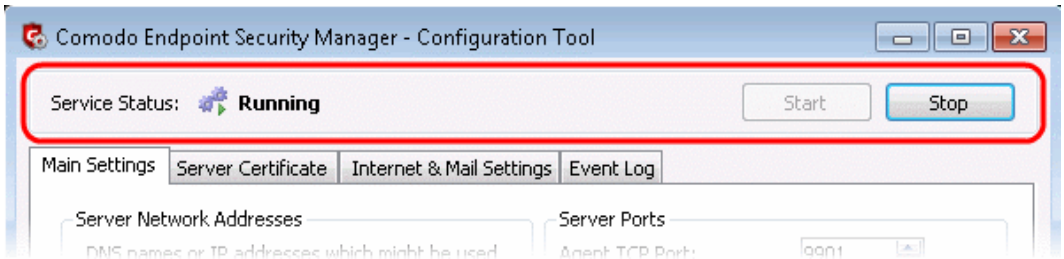


The main interface of the tool will be opened. It contains four areas:

- Service Status Area - Indicates the current service CESM 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
- Event Log - Enables the administrator to view the log of database events

Start and Stop the CESM Service

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

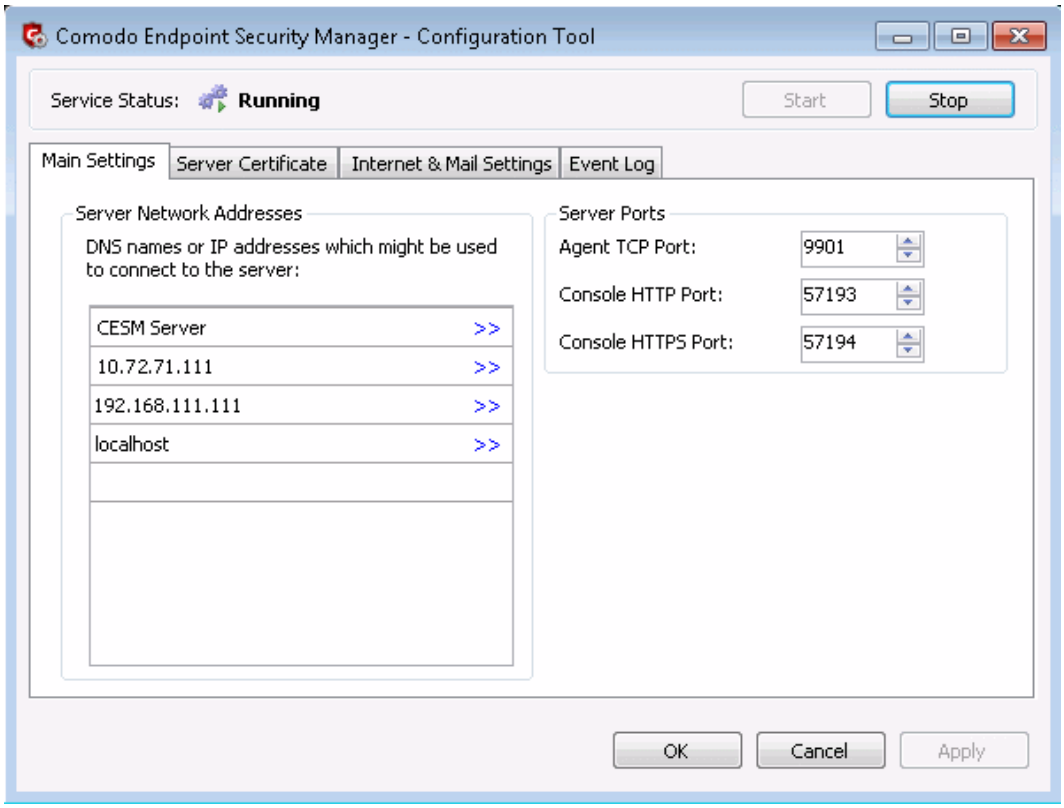


- To stop the running service, simply click the 'Stop' button
- To start the service, simply click the 'Start' button

Main Settings

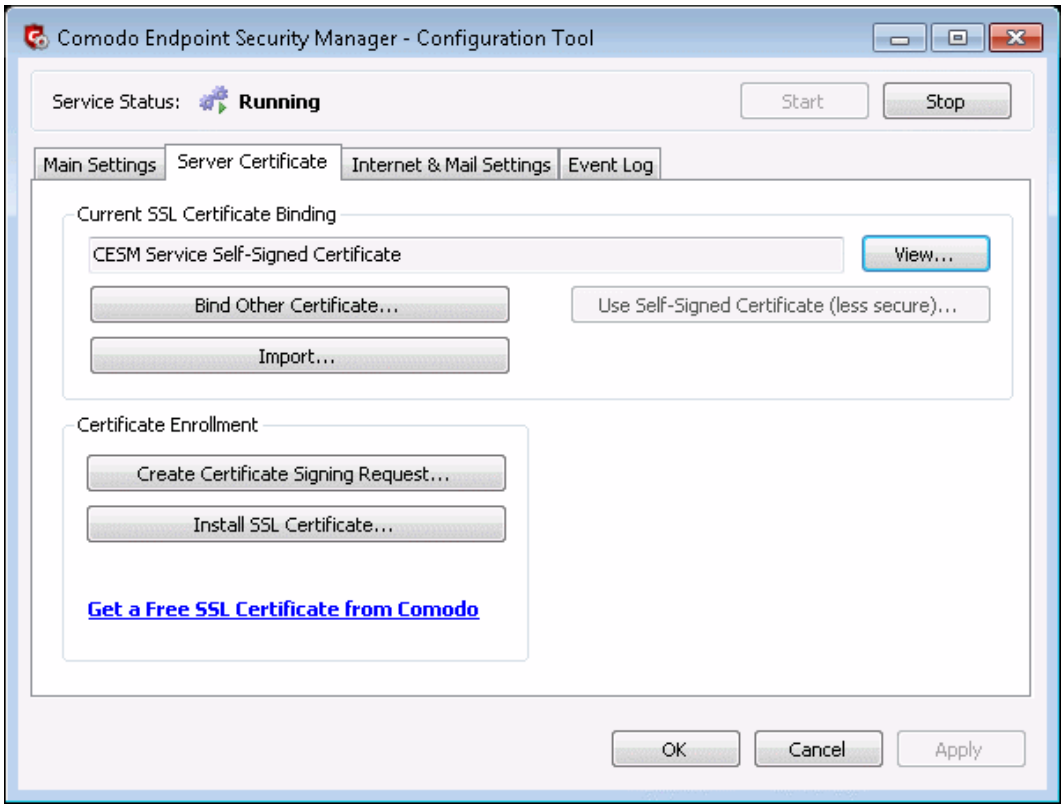
The CESM server IP addresses and/or hostnames are displayed in the 'Server Network Addresses' field of the interface. Console Port, Secure Console Port and Agent Ports are listed to the right.

- 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. Computers that have standalone Comodo Internet Security (CIS) installed on them can be connected to the CESM service via the CIS interface (directly from the endpoint itself) through this port. See section 'How to Connect CIS to CESM at the Local Endpoint' for information on connecting endpoints locally to CESM.
- You will need to enter the hostname/IP and console port in the address bar of your browser to connect to the CESM server. For example, https://192.168.111.111:57194 will open the CESM 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

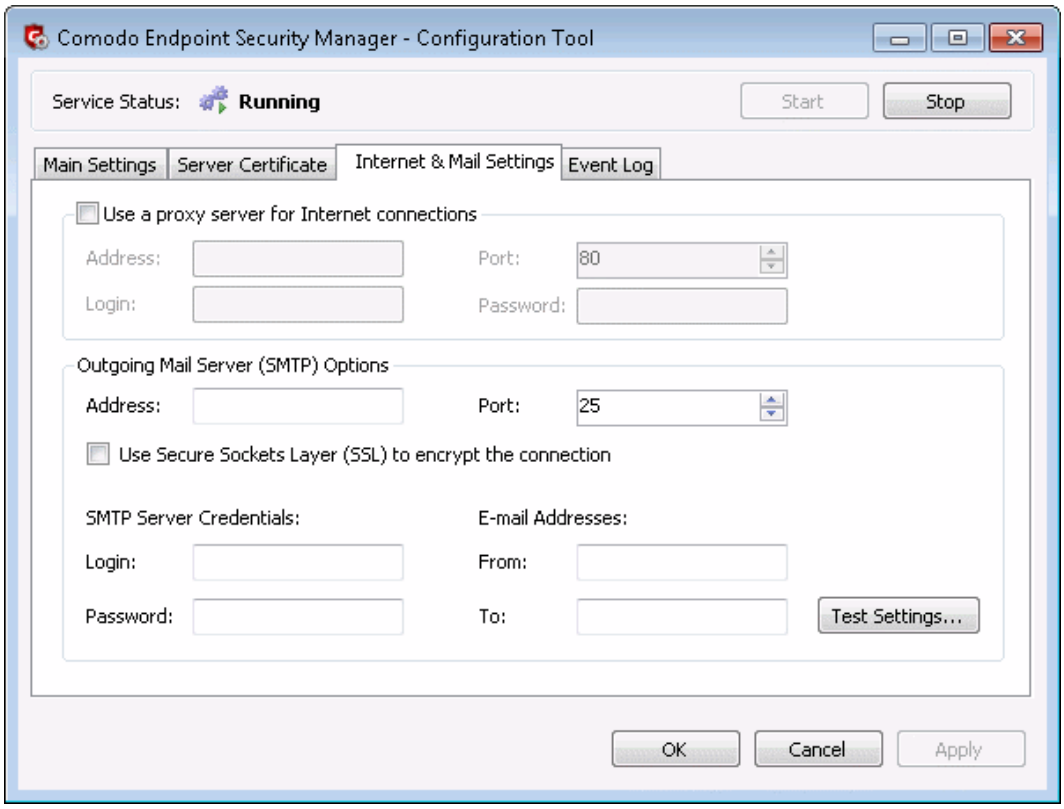
This tab allows administrators to manage server certificate such as view the details of current certificate installed on the server, import new certificate, create certificate signing request and install new SSL certificate.



- To view the details of the currently installed server certificate, click the 'View' button.
- If multiple SSL certificates are used in the server, a certificate name error may occur when a HTTPS connection is established. To avoid this, bind the required certificate using the 'Bind Other Certificate' option.
- To import certificates from other locations, click the 'Import' button.
- To create a certificate signing request for your server, click the 'Create Certificate Signing Request' button and fill in the required details in the 'Request Certificate' dialog.
- 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 download a free SSL certificate from Comodo.

Internet and Mail Settings

This tab allows administrators to specify mail settings for receiving alerts from CESM and any to specify any Internet proxy connection settings.



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...

Viewing Database Event Log

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

- The type of alerts that are displayed can be filtered by clicking the 'Errors', 'Warnings' and 'Information' buttons
- Alternatively, type a specific search term into the text field then click the 'Apply Filter' button
- Each cell can be individually selected by clicking it
- Multiple cells can be selected whilst holding down the 'Shift' or 'CTRL' keys and left-clicking on target cells
- Cells can be copied to the clipboard by clicking the 'Copy' button

Column	Types/Format	Definition / Description
Type (of event)		**Error** - 'Errors' are those events whereby the CESM Central Service failed to execute a command.
		**Warning -** High severity errors that may (or already have) prevented the CESM service from connecting to the data source. For example, a critical application crash.
		**Information -** 'Information' events typically inform the administrator of the successful completion of task by the CESM 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. 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
	*Filter by event*	Click this button to add or remove events of type 'Error' from the displayed list.
	*Filter by event*	Click this button to add or remove events of type 'Warning' from the displayed list.
	*Filter by event*	Click this button to add or remove events of type 'Information' from the displayed list.
	*Remove filters and refresh list*	Clears any active filters so all event types are displayed. Also loads the latest event entries.
	*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 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.

525 Washington Blvd. Jersey City,

NJ 07310

United States

Tel: +1.888.256.2608

Tel: +1.703.637.9361

Email: EnterpriseSolutions@Comodo.com

Comodo CA Limited

3rd Floor, 26 Office Village, Exchange Quay, Trafford Road, Salford, Greater Manchester M5 3EQ,

United Kingdom.

Tel : +44 (0) 161 874 7070

Fax : +44 (0) 161 877 1767

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