COMODO
Creating Trust Online®

Comodo
Endpoint Security Manager
Professional Edition

Software Version 3.5

Quick Start Guide

Guide Version 3.5.053016

Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

Comodo Endpoint Security Manager - PE Quick Start Guide

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

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

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

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

1. Download and run the CESM PE setup file. A link to this file is provided in your license confirmation email. This file will install the central service on the machine you intend to use as the CESM server.

   Supported operating systems are Windows Vista (SP2), Windows 7, Windows 8, Windows 8.1, Windows 10, Windows Server 2008 (SP2 or higher), Windows Server 2008 R2, Windows Server 2008 Small Business Server, Windows 2011 Small Business Server, Windows Server 2012 and Windows 2012 Server R2.

   You also need a Silverlight 5.1 capable browser to use the management console (Internet Explorer 10+, Firefox 21+ and Chrome versions 27 to 42).

   See the online help page **Software Components and System Requirements** for further information on this.

   There is a choice of two setup files. The '..._FULL.exe' file contains all additional required software:

   - Microsoft® .NET Framework 4.5.2
   - Microsoft System CLR Types for SQL Server 2012
   - Microsoft Report Viewer 2012 Runtime

   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, Microsoft report viewer and Microsoft System CLR Types for SQL Server).

3. Choose the installation type:

   - Select 'Typical' as the installation type for fastest setup experience. After installation you will need to provide a valid license key in the 'License Information' screen of the console interface to start using the service. The License Information screen can be accessed by selecting 'Help' from the drop-down at the top left and clicking 'License Information' from the options.
   - Select 'Custom' if you wish to change install location or select which components are installed. You will be able to enter a valid license key during setup.
   - Select 'Complete' if you want to install full set of CESM components.

4. At the setup finalization dialog, make sure 'Launch CESM Configuration Tool' is selected before clicking 'Finish'.
5. In the configuration tool, take note of the hostname/IP address of the server and the port settings. You will need these if you wish to access the console from remote machines and if you want to setup protection for laptops and other computers that are outside the local network (you will also need to open these ports to the Internet on your enterprise firewall).
6. This tool also allows you to modify Internet connection settings and specify mail server settings (required for email notifications).
7. Since the ESM console can be accessed via the Internet, you may desire to obtain an SSL certificate and apply it using the Configuration Tool or you can distribute the self-signed certificate already installed to computers that you will use to administer ESM.

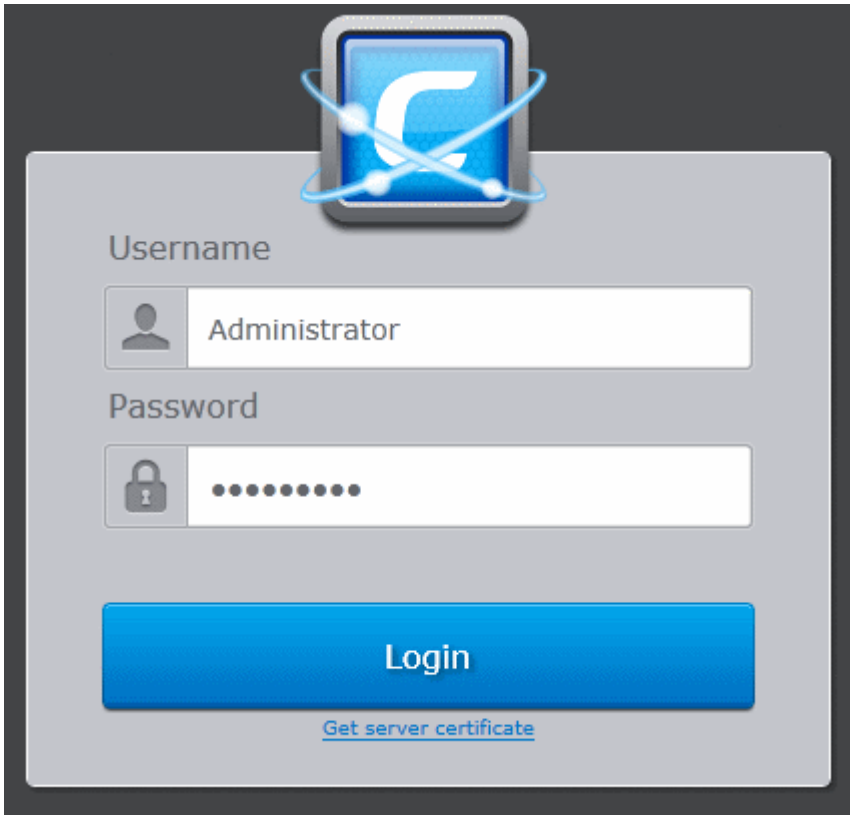
Step 2 - Login to the Admin Console

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



3. To log out of the console, close the browser window or tab containing the console, or press the 'Refresh' button or choose 'Logout' from the drop-down at the top left of the interface.

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

Prerequisite - Before importing the endpoints, you need to download the latest versions of the CESM Agent,CES/CAVS/CAVM packages for remote or manual installation on to the endpoints to be managed. Refer to the online help page **http://help.comodo.com/topic-84-1-496-5289-Downloading-ESM-Package.html** for more details

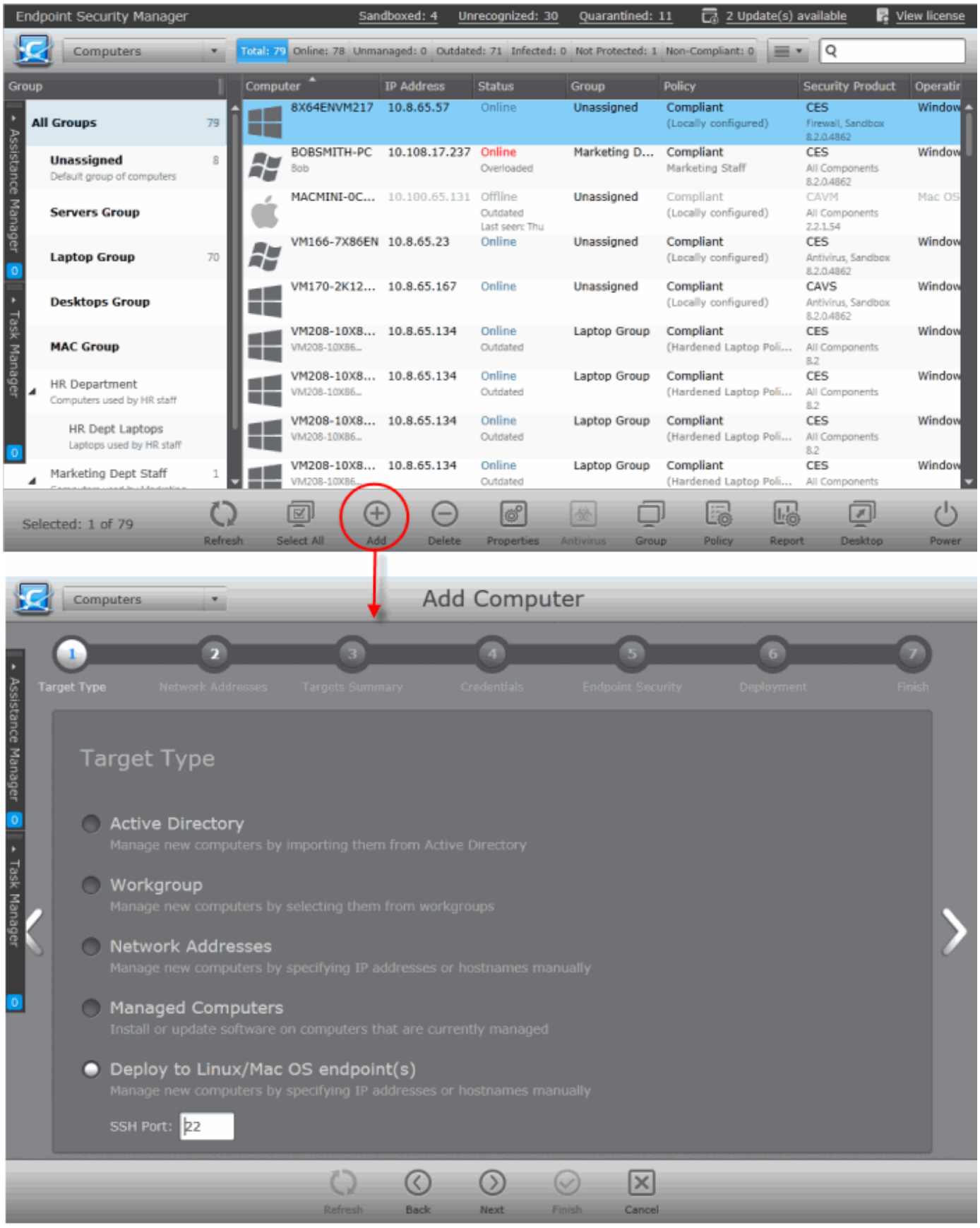
Next, we need to import endpoints by installing the agent and the security software (CES, CAVS or CAV for Mac) on them. The agent facilitates communication between the endpoint and the CESM server.

There are two ways to accomplish this:

- **Remotely -** using a console wizard to automatically push the agent and (optionally) the security software onto target machines. This wizard is started by clicking 'Add' from the Computers interface of the console.
- **Locally** - 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. Further explanations on this method can be found in the online help page **Adding Computers by Manual Installation of Agent**..

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

1. Open the 'Computers' interface by selecting 'Computers' from the drop down at the top left
2. Click inside the right pane to switch to the 'Computers' area.
3. Click the 'Add' from the 'Computers' area to start the wizard:



4. The first stage is to choose how you want to import (Target Type). Computers can be imported using one of three methods: Active Directory, Workgroup or by IP Address. Linux and Mac Os computers can be imported by specifying their IP addresses. Administrators should, of course, repeat this wizard until they have imported all computers in their network.

5. Select the appropriate import method then swipe the screen to move to the next stage. 'Swiping' is done by clicking the arrows in the middle on the left and right side of the interface.
    - 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 'Network Addresses', you next have to specify the IP, IP range, host name or subnet of the target machines. Click the 'Add' button to confirm your choice. Repeat until you have added all IP addresses or ranges that you wish to scan.
    - If you chose 'Deploy to Linux/Mac OS X endpoint(s)', you next have to specify the secure shell (SSH) port, the IP, IP range, host name or subnet of the Linux and/or Mac OS target machines (CESM will install the appropriate agent facilitating device management). Click the 'Add' button to confirm your choice. Repeat until you have added all IP addresses or ranges that you wish to scan.

    Click the right arrow button to continue.
6. The next stage, 'Select Targets', allows you to choose those imported computers onto which you want to install the Agent and the security product (CES/CAVS/CAVM). Select the check-boxes next to your intended targets and click the right arrow button.
7. The next step, 'Target Summary', provides an overview of the IP addresses and connection/management status of your selected endpoint(s). Select the check boxes beside those endpoints upon which you want to install. If you want to select all the computers, select the check box beside the 'Target Computer' text. Click the right arrow button to move onto the next step.
8. Credentials. Next up is to choose whether the agent has to be installed under the currently logged in user account or the network administrator account. If you choose 'Custom Credentials', enter the user name and password of an account with administrative privileges on the machine - such as Administrator, hostname\administrator, domain\administrator as the login ID. Click the right arrow button to move onto the next step.
9. The final step prior to deployment is to decide whether you want to install Comodo Endpoint Security (CES), Comodo Antivirus for Servers (CAVS) or Comodo Antivirus for Mac (CAVM) *also* at this time.

- Select the language in which the agent is to be installed from the 'Agent Language' drop-down.
- Choose the endpoint group to which the imported endpoints are to be assigned.

CESM ships with a set of pre-defined groups, each assigned with appropriate security policies and allows user to create custom groups too. The 'Default Group' drop-down displays both the pre-defined and custom groups to choose from. On completion of the import process, all the imported endpoints will be added to the group chosen. The administrator can then move the endpoints to different groups if required.

By default, the imported computers will be added to the predefined group 'Unassigned'. Putting endpoints in the 'unassigned' group will not implement a CESM policy, rather the endpoint will retain its local CES configuration (aka 'Local Policy'). You may want to choose this option if you'd rather define policies later.

- To specify the group to which the imported computers are to be added, select the 'Default Group' checkbox and choose the group from the drop-down.
- If you want the imported endpoints to be added to the 'Unassigned' group, leave the 'Default Group' checkbox unselected.

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

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

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

  - Full Suite, which contains all the components (Sandbox, Antivirus and Firewall)
  - Sandbox and Antivirus
  - Sandbox and Firewall (Not applicable for CAVS/CAVM)
  - Sandbox only

  (3) Select the language in which the CES/CAVS is to be installed from the Language drop-down.

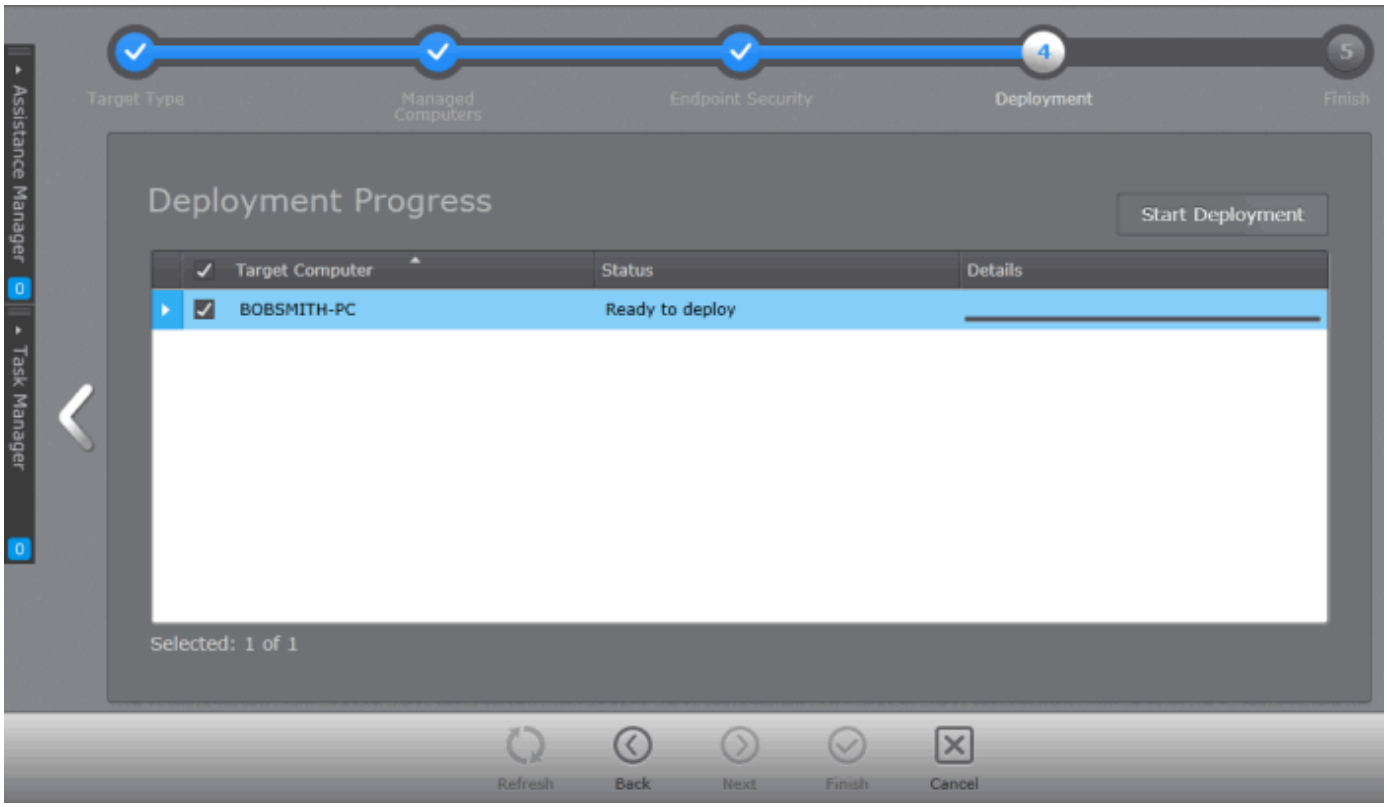
(4) Check 'Suppress Reboot' if you do not want the target endpoint to automatically restart after installation.

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

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

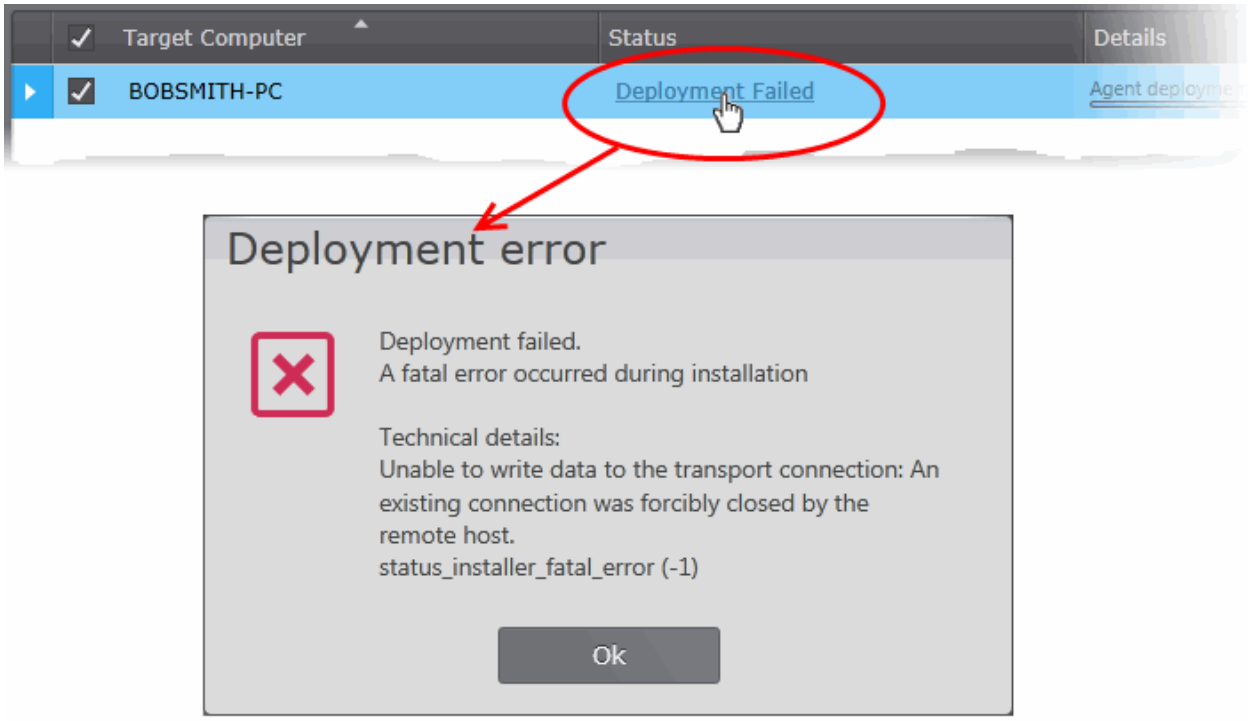
Click here to see the full list of incompatible products.

- Click the right arrow button to move onto the next step to move to deployment step.



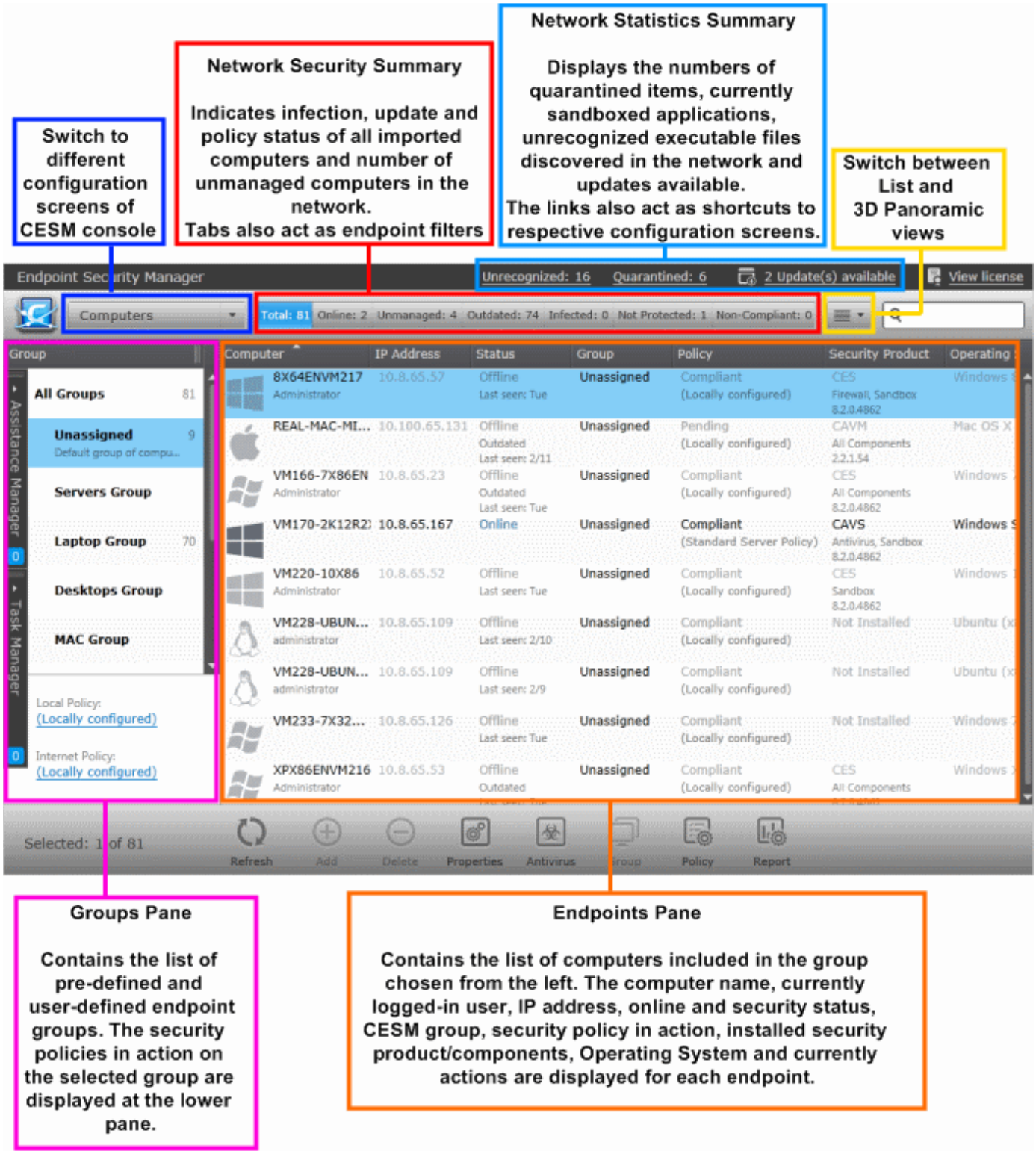
10. Deployment.

- Click 'Start Deployment'. You will see installation progress per-endpoint. Once deployment is successful, click the 'Finish' icon at the base of the interface to exit the wizard. If you have chosen to install both the agent & the security software then those endpoints should now be reporting to CESM.
- If deployment fails, click on the words 'Deployment Failed' to discover the reason. The info box also contains advice that may remediate the issue.



Step 4 - Check that target endpoints are reporting correctly

1. Select 'Computers' from the drop-down at the top left to open the 'Computers' interface
2. Choose 'All Groups' from the left to view the list of all the imported computers. The number at the right of All Groups indicates the total number of managed computers. To view the list of computers imported to a specific group, choose the group from the left.



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

- After checking that all computers are reporting correctly, it is a good idea to make sure the latest virus database is installed. Select all the computers and click the 'Update AV' at the base of the interface.
- After updating, we advise running a virus scan on all computers. Select all computers and click Antivirus ->Scan -> Full Scan at the base of the interface to do this. **Note** - real-time AV protection is

already running on all endpoints. If any malware is discovered, it will be brought to your attention via the status indicators.

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

Step 5 - Create Groups of computers

In CESM, security policies are applied to 'groups' of computers rather than individual endpoints. Once a group has been created, admins can run tasks on entire groups of computers (such as applying policy, running AV scans, updating AV databases and more). 'Policies' are the security configuration of CES/CAVS and can be 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 their default group(s) chosen during their import process and inherit the security policy applied to the respective group(s). All security settings for CES/CAVS/CAVM will be configured as per the applied policy at the endpoints.
- Endpoints for which a default group was not chosen, will be placed in the 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, administrators can assign a policy to the '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,
  - Select 'Computers' from the drop-down at the top left to open the 'Computers' interface,
  - Click inside the left pane to switch to the 'Groups' area,
  - Click 'Add' from the bottom to start the 'Create New Group' Wizard',
  - Leave policy as 'Locally Configured',
  - Type a name for the group then finish.
- If you wish to create multiple groups, repeat the previous step until all computers have been assigned.
- See '**Creating New Endpoint Groups**' if you need help with this wizard. See '**Endpoint Groups**' for an overview of functionality.

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

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

The next tasks are to import a policy from a tested and configured endpoint and apply the policy to a group.

- To set the parameters of a particular security policy, you need to apply 'Locally Configured' policy to the endpoint and configure the security settings.
- Once you have set and tested the policy at the endpoint, you should return to the CESM console and prepare to import this policy. Note - leave the endpoint in locally managed mode while doing this.
- At the console,
  - Open the 'Policies' interface by selecting 'Policies' from the drop-down at the top left.
  - Click 'Add' from the 'Policies' interface to start the 'Create Policy' wizard.
  - Select 'Create New' and choose the specific computer from which you want to import. Modify 'Settings' and 'Agent Settings' if required.
- For 'Targets', choose which groups you want to apply the policy to and how you want it applied. 'For local policy' and 'For Internet policy' are the policies to be used depending on whether the machine connects from

inside or outside of the VPN. Select 'Override individual computer's policy' to make sure this policy is applied correctly. Select 'Apply Policy after finish' to immediately apply the policy to all the selected endpoints upon completion of policy creation. If you want to apply the policy later, do not select 'Apply Policy after finish'.

- Finally, give the policy a name and description and click 'Finish'.

  Please see **Policies - Key Concepts** for more details about policies - including how to create, import and manage it.

Step 7 - View Reports

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

- Antivirus Scans
- Antivirus Updates
- Assistance Logs
- Computer Details
- Computer Infections
- Hardware Inventory
- Installed Software Inventory
- Malware Statistics
- Policy Compliance
- Policy Delta Report
- Quarantined Items
- Security Product Configuration
- Security Product Logs
  - Antivirus Logs
  - Firewall Logs
  - Sandbox Logs
  - HIPS Logs
- Top 10 Malwares
- Warranty Report

Click here to read more about reports.

About Comodo Security Solutions

Comodo Security Solutions is a global innovator of cybersecurity solutions, protecting critical information across the digital landscape. Comodo provides complete, end-to-end security solutions across the boundary, internal network and endpoint with innovative technologies solving the most advanced malware threats. With over 80 million installations of its threat prevention products, Comodo provides an extensive suite of endpoint, website and network security products for MSPs, enterprises and consumers.

Continual innovation and a commitment to reversing the growth of zero-day malware, ransomware, data-breaches and internet-crime distinguish Comodo Security Solutions as a vital player in today's enterprise and home security markets.

About Comodo Cybersecurity

In a world where preventing all cyberattacks is impossible, Comodo Cybersecurity delivers an innovative cybersecurity platform that renders threats useless, across the LAN, web and cloud. The Comodo Cybersecurity platform enables customers to protect their systems and data against even military-grade threats, including zero-day attacks. Based in Clifton, New Jersey, Comodo Cybersecurity has a 20-year history of protecting the most sensitive data for both businesses and consumers globally. For more information, visit comodo.com or our **blog**. You can also follow us on **Twitter** (@ComodoDesktop) or **LinkedIn**.

1255 Broad Street

Clifton, NJ 07013

United States

Tel : +1.877.712.1309

Tel : +1.888.551.1531

https://www.comodo.com

Email: **EnterpriseSolutions@Comodo.com**