

C·O·M·O·D·O

Creating Trust Online™

Comodo Endpoint Security Manager

Administrator Guide

1 Introduction to Comodo Endpoint Security Manager.....	6
1.1 Enterprise Benefits.....	6
1.2 Overview of Modules.....	6
1.2.1 Administrative Console.....	6
1.2.2 Central Service.....	6
1.2.3 Remote Agents.....	7
2 Installing Comodo End Point Security Manager.....	7
2.1 System Installation Requirements.....	7
2.1.1 Central Service Computer.....	7
2.1.2 Administrative Console.....	8
2.1.3 CESM Agent Computer(s).....	9
2.2 Installation.....	10
2.2.1 Installing CESM Central Service and CESM Administrative Console.....	10
i. Downloading and running the installer.....	11
ii. Preliminaries and License Agreement.....	11
iii. Choosing Installation Preferences.....	12
iv. Specify Database and CESM Administrator parameters for Central Service.	14
v. Specify CESM Administrator Console Connection Parameters.	15
vi: Finalizing the installation.....	15
3 The Administrative Console	17
3.1 Logging in to the Administrative Console	17
3.2 Administrative Console Overview.....	19
3.2.1 Persistent Navigational Elements -The File Menu and Shortcut Menus.....	20
3.3 The 'Computers' and 'Group Manager' Windows.....	22
3.3.1 Overview.....	22
3.3.2 The 'Computers' Window – Functionality and Purpose.....	23
3.3.3 The 'Group Manager' Window– Functionality and Purpose.....	26

3.4 The Package Management window	29
3.4.1 Overview.....	29
3.4.2 Opening the Package Manager window.....	29
3.4.3 Adding a Package to Comodo Endpoint Security Manager.....	30
3.5 The Discovery Profiles window.....	33
3.5.1 Overview.....	33
3.5.2 Opening the Discovery Profiles window.....	34
3.5.2.1 'OS Version' Profile.....	35
3.5.2.2 'Windows Services' Profile.....	36
3.5.2.3 'Installed Products' Profile.....	37
3.5.2.4 'CFP Config' Profile.....	38
3.5.2.5 Example: Using 'CFP Config' Discovery Profile to roll out an existing CFP configuration onto other machines.....	40
3.6 The Sequence Manager window	41
3.6.1 Overview.....	41
3.6.2 Opening the Sequence Manager window.....	41
3.6.3 Creating a Sequence and Adding Actions to that Sequence.....	42
3.6.3.1 Table of Actions – Definitions and Usage	43
3.7 The 'Task Manager' window.....	46
3.7.1 Overview.....	46
3.7.2 Opening the Task Manager Window.....	46
3.7.3 Creating and Executing a Task.....	47
3.8 The Task Result Manager window.....	51
3.8.1 Overview.....	51
3.8.2 Opening the Task Result window.....	51
3.8.3 Task Result Manager – Table of Columns, Controls and Icons:.....	52
3.9 The Notification Monitor window.....	55

3.9.1 Overview.....	55
3.9.2 Opening the Notification Monitor.....	55
3.9.3 The Notification History Window	57
3.10 The Request Monitor	57
3.10.1 Overview.....	57
3.10.2 Opening the Request Monitor window.....	57
3.10.3 The Request History Window	59
4 Importing Network Structure.....	60
4.1 Section Overview.....	60
4.1.1 Initiating the import.....	61
4.1.2 Importing from Active Directory.....	62
4.1.3 Importing from a Workgroup.....	64
4.1.4 Additional Information.....	65
5 Workstation/Workgroup Management.....	66
5.1.1 Managing Computer tree items	66
5.1.2 Context management menu - Table of parameters.....	66
5.1.3 Managing groups of computers.....	67
5.1.3.1 Creating groups.....	67
5.2 Preparing Imported Computers For Remote Management.....	69
5.2.1 Assigning Managed Status to Imported Computers.....	69
5.2.2 Installing CESM Remote Agent.....	71
5.2.2.1 About Agent Versions.....	73
5.2.2.2 Uninstalling CESM Remote Agents.....	74
6 Managing computers using the CESM Administrative Console.....	74
6.1 Prerequisites.....	74
6.2 Installation and Management of Comodo Firewall Pro using CESM.....	75
6.2.1 Step 1. Run a full set of Discovery Profiles on the Managed Computers.....	75

6.2.2 Step 2. Upload the Comodo Firewall installation Package to the CESM Console.....	80
6.2.3 Step 3: Create a Sequence of Actions to install the Comodo Firewall Package on Managed computers.....	82
6.2.4 Step 4: Add the Sequence to a Task and execute that Task on Managed Computers.....	83
6.2.5 Step 5: Managing Requests (Alerts) from Comodo Firewall Pro on Managed Computers.....	84
7 About Comodo.....	85

1 Introduction to Comodo Endpoint Security Manager

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

1.1 Enterprise Benefits

Total Protection for networked computers

CESM allows administrators to leverage and maximize the protection offered by Comodo's end point 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), Comodo Disk Encryption, Comodo DiskShield, Comodo Secure Email, Comodo AntiSpam and much more. 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 end-point 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 management processes 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

Huge Cost Savings

Apart from the operational and support cost savings that are inherent in centrally managing a single-vendor suite of client security software, CESM's low cost pricing structure also makes sound economic and managerial sense. Instead of hard-to-manage individual license fees for each security application, Comodo have instituted a flat, per workstation charging system whereby organizations pay for the number of computer's they manage irrespective of the number of Comodo applications that are installed on any one computer. As soon as new CESM controlled applications are launched they will be provided to your administrator as free-of-charge packages ready for seamless deployment across your entire network.

1.2 Overview of Modules

The CESM solution is a complex but easy to use multi-tier application consisting of three inter-dependent modules: The **Administrative Console module**; The **Central Service module** and the **Remote Agent module**.

1.2.1 Administrative Console

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

1.2.2 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. The Central Service requires a local installation of Microsoft SQL Express for building its databases.

1.2.3 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 MSI packages, configuring and re-configuring security products, managing Windows' Local Services and rebooting of managed computers)

2 Installing Comodo End Point Security Manager

2.1 System Installation Requirements

The Central Service computer (or Server PC) requires Microsoft Windows 2003/2008 Server with .NET Framework 2.0 and local Microsoft SQL Server 2005 Express.

The Administrative Console can, if desired, be installed on the same machine as the Central Service running under the same installation of Windows 2003/2008. Alternatively, the console can be installed on a separate computer (Console PC). If installed on a separate machine, the Console PC must have Microsoft Windows XP SP2 or Windows Vista SP1 with .NET Framework 2.0.

The installation of the Administrative console and/or the Central service is done from a single, unified installer. Administrators are given the choice of installing either or both components during the setup process. See section [2.2.Installation](#) for more details.

The Comodo Remote Agent is installed onto Managed PC's directly from the Administrative console. Managed PC's must be running either Windows XP SP2 (and above) or Windows Vista. The exact computing power of Managed PCs (usually network workstations) should, of course, be determined by the general needs of the users within that organization but should also meet the minimum specifications of the Comodo Packages that are installed on them (e.g. Comodo Firewall Pro, Comodo Internet Security etc)

The remainder of this section contains detailed system installation requirements for each of the three components listed above.

2.1.1 Central Service Computer

The following table lists the minimum requirements for the machine upon which CESM Central Service will be installed.

Central Service Computer – System Requirements		
Hardware		
Component	32 bit	64-Bit
Processor	1 GHz Intel Pentium III or equivalent	1 GHz Intel Pentium IV 64 bit processor or equivalent
Memory	1 GB RAM minimum (2-4 GB recommended)	1 GB RAM minimum (2-4 GB recommended)

Central Service Computer – System Requirements		
Hard Disk	4 GB (This incorporates the space required for the SQL server)	4 GB (This incorporates the space required for the SQL server)
Display	Super VGA (1024x768) or higher resolution video adapter and monitor	Super VGA (1024x768) or higher resolution video adapter and monitor
Software		
Operating System	<p>The following operating systems are supported:</p> <p>Windows Server 2008 Standard Edition / Enterprise Edition / Data center Edition / Storage Edition / Web Edition / Small Business Server</p> <p>Windows Server 2003 SP 1 or later Standard Edition / Enterprise Edition / Data center Edition / Storage Edition / Web Edition / Small Business Server</p> <p>Windows XP Professional - SP2 or later</p> <p>Windows Vista – SP1 or later</p>	<p>The following operating systems are supported:</p> <p>Windows Server 2008 x64 Standard Edition / Enterprise x64 Edition / Data center x64 Edition with Service Pack 1 or later</p> <p>Windows Server 2003 SP 1 or later x64 Standard Edition / Enterprise x64 Edition / Data center x64 Edition with Service Pack 1 or later</p> <p>Windows XP x64 Edition</p> <p>Windows Vista x64 Edition</p>
Software Environment	Microsoft .NET Framework 2.0	Microsoft .NET Framework 2.0
Database	Microsoft SQL Server 2005 Express – SP2 or higher	Microsoft SQL Server 2005 Express – SP2 or higher
Other Requirements	<p>CESM program modules (Agent, Service and Console) may require firewall and personal firewall configuration changes in order to operate successfully. Each of the program modules should be added to the list of “trusted” applications.</p> <p>By default, CESM Central Service is assigned:</p> <ul style="list-style-type: none"> • Port number 9001 for connections with CESM Agent Service • Port number 9900 for connections with CESM Administrative Console. <i>(For receipt of callbacks CESM Administrative Console occupies a random, ephemeral port.)</i> 	

2.1.2 Administrative Console

The following table lists the minimum requirements for the machine upon which CESM Administrative Console will be installed.

Administrative Console Computer – System Requirements

Hardware

Component	32 bit	64-Bit
Processor	1 GHz Intel Pentium III or equivalent	1 GHz Intel Pentium IV 64 bit processor or equivalent
Memory	128 MB RAM minimum	128 MB RAM minimum
Hard Disk	10 MB	10 MB
Display	Super VGA (1024x768) or higher resolution video adapter and monitor	Super VGA (1024x768) or higher resolution video adapter and monitor

Software

Operating System	<p>The following operating systems are supported:</p> <p>Windows XP Professional - SP2 or later</p> <p>Windows Vista – SP1 or later</p> <p>(Note – If desired, both the Administrative console and the Central Service can be installed on the same operating system on the same machine)</p>	<p>The following operating systems are supported:</p> <p>Windows XP Professional x64 Edition</p> <p>Windows Vista x64 Edition</p> <p>(Note – If desired, both the Administrative console and the Central Service can be installed on the same operating system on the same machine)</p>
Software Environment	Microsoft .NET Framework 2.0	Microsoft .NET Framework 2.0
Other Requirements	<p>CESM program modules (Service, Console and Agent) may require firewall and personal firewall configuration changes in order to operate successfully. Each of the program modules should be added to the list of “trusted” applications.</p> <p>By default, CESM Central Service is assigned:</p> <ul style="list-style-type: none"> • Port number 9001 for connections with CESM Agent Service • Port number 9900 for connections with CESM Administrative Console. <i>(For receipt of callbacks CESM Administrative Console occupies a random, ephemeral port.)</i> 	

2.1.3 CESM Agent Computer(s)

The following table lists the minimum requirements for the machine upon which CESM Remote Agent will be installed.

Agent / Managed PC Computer – System Requirements

Hardware

Component	32 bit	64-Bit
Processor <i>recommended</i>	1 GHz Intel Pentium III or equivalent	1 GHz Intel Pentium IV 64 bit processor or equivalent
Memory <i>recommended</i>	64 MB RAM	64 MB RAM

Software

Operating System <i>required</i>	The following operating systems are supported: Windows XP Professional - SP2 or later Windows Vista – SP1 or later	The following operating systems are supported: Windows XP Professional x64 Edition Windows Vista x64 Edition
Other Requirements	CESM program modules (Service, Console and Agent) may require firewall and personal firewall configuration changes in order to operate successfully. Each of the program modules should be added to the list of “trusted” applications. By default, CESM Central Service is assigned: <ul style="list-style-type: none"> • Port number 9001 for connections with CESM Agent Service • Port number 9900 for connections with CESM Administrative Console. <i>(For receipt of callbacks CESM Administrative Console occupies a random, ephemeral port.)</i> 	

2.2 Installation

Before installation, please make sure the target machine meets the hardware and software prerequisites for the particular component you are installing. Full details regarding system requirements can be found in the preceding section, [System Installation Requirements](#).

2.2.1 Installing CESM Central Service and CESM Administrative Console



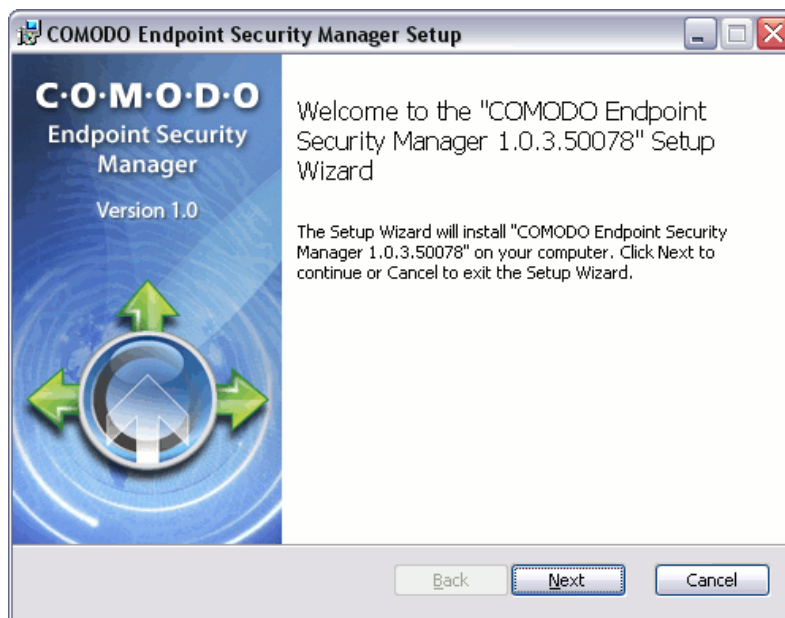
Firstly, decide which computers you will use as Central Service and Administrative Console hosts. If you intend to run the Service and Console applications on the same machine you should opt to install both components at [iii. Choosing Installation Preferences](#) stage of the installation wizard. If you choose to install only the Central Service application on the Server PC then the Administrative Console should be installed on a separate machine (aka the 'Console PC'). Administrators can re-run the installer should they wish to install components on a particular machine that they omitted first time round

i. Downloading and running the installer

Download and save 'CesmSetup.msi' installation file. This unified installer can be used to setup both the Central Service and Administrative Console.

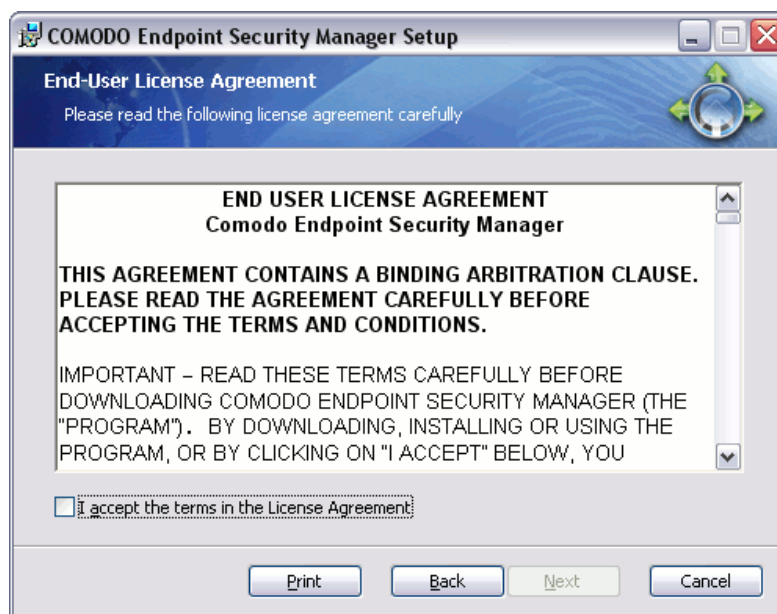
ii. Preliminaries and License Agreement

The set up program starts automatically and the Welcome wizard is displayed. At this time, you may cancel the installation process or continue with the [Comodo Endpoint Security](#) Manager Setup program.

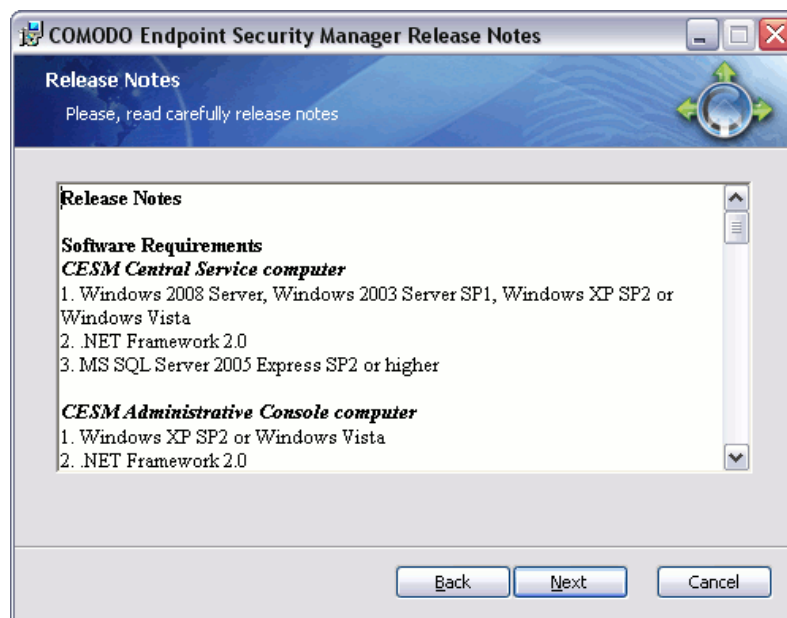


Click 'Next' to continue.

To complete the initialization phase you must read and accept 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.



After assenting to the license agreement, carefully read the release notes. Apart from displaying a reminder of system installation requirements the release notes can also contain the very latest information regarding new product features, developments, known issues and installation advice to help you to avoid possible installation and configuration problems.



iii. Choosing Installation Preferences

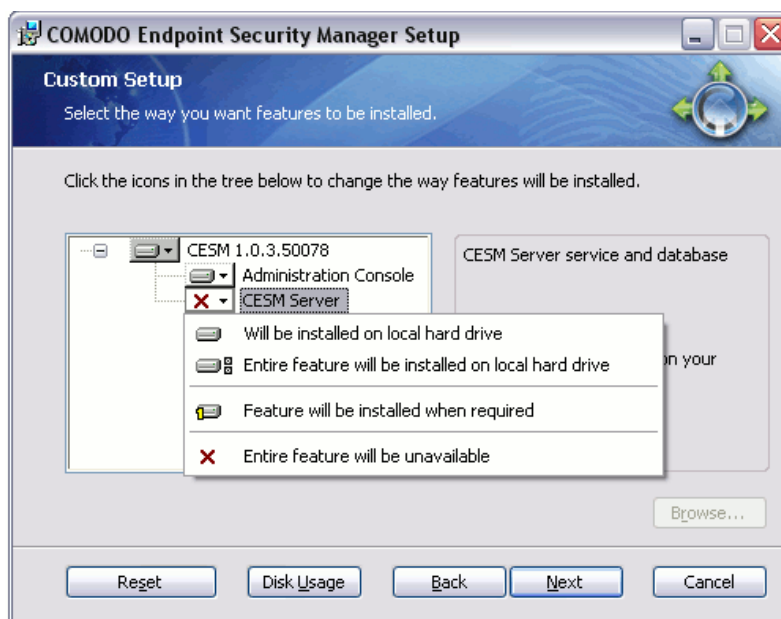
The next stage of the installation process is to specify which components of CESM to install:



By default, the installer will offer installation of only the Administrative Console on the target computer. Administrators should modify the relevant controls according to their installation preferences. ([More details](#))



The default installation location is 'C:\Program Files\COMODO\RemoteManagement' Administrators can specify an alternative installation location by clicking the 'Browse...' button. ([More details](#))



Installation Options – Table of Parameters

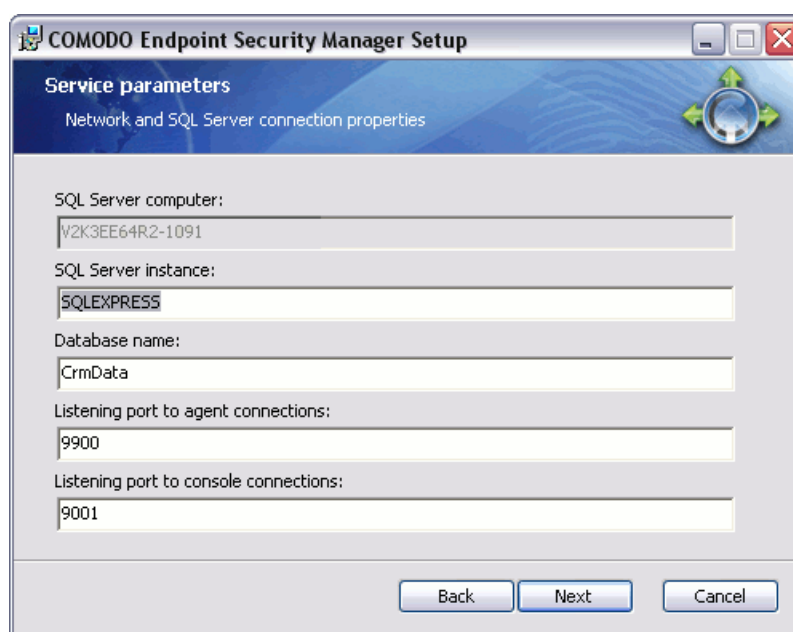
Control	Description
	Icons with the ▼ symbol to the right are the currently selected installation option. Clicking this icon will open a menu allowing the user to select alternative installation options. These alternative installation options are explained in the next four rows of this table.
	Indicates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

Installation Options – Table of Parameters

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.

iv. Specify Database and CESM Administrator parameters for Central Service.

If you elected to install the CESM Central Service when Choosing Installation Preferences then you now need to provide configuration details so that this service can (i) Connect to the SQL Express Database (ii) Connect to the CESM Administrative Console. Both of these tasks are carried out at the 'Service Parameters' dialog box:



'Service Parameters' dialog – Table of Parameters

Field Name	Description
SQL Server computer	Administrators should enter Server computer's name
SQL Server instance	Administrators should specify SQL Server instance
Database name	Administrators should enter database name.
Listening port to agent connections	Administrators should specify port for agent connections. Default: 9900

'Service Parameters' dialog – Table of Parameters

Listening port to console connections	Administrators should specify port for console connections. Default: 9001
---------------------------------------	---

v. Specify CESM Administrator Console Connection Parameters.

If you elected to install the CESM Administrative Console when [Choosing Installation Preferences](#) then you now need to provide configuration settings so the Console can connect to the Central Service. Please specify the host name and port number of the computer upon which CESM Central Service is installed:



- If you are also installing (or have already installed) the Central Service on the same machine that you are now installing the Administrative Console, then you can leave the 'Service Computer' field at the default setting of 'localhost'.
- If you have installed the Central Service on a different machine to one that the Administrative Console is (or is to be) installed on, then you must specify the host name of that machine in the 'Service Computer' field.
- Port 9001 is the default port number that the Central Service will listen to for connections from the Administrative Console. If you wish to change this port number, then remember to also make the corresponding alteration to the Central Service Listening Port Number.

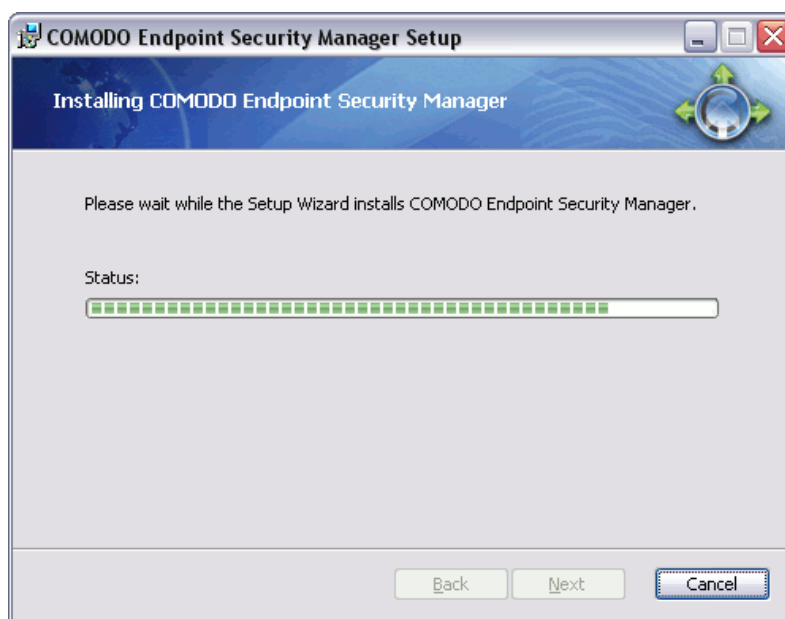
vi: Finalizing the installation

After completing the configuration options to your satisfaction in the preceding steps, a confirmation dialog box will be displayed.



Click the 'Back' button to review and/or modify any of settings you have previously specified. To confirm your choices and begin the installation of the selected CESM components, click 'Install'.

A setup status dialog box is displayed. You will see a progress bar indicating that files are being installed.



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

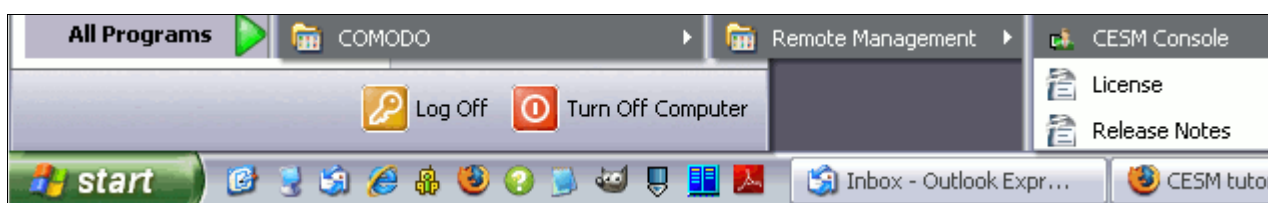


3 The Administrative Console

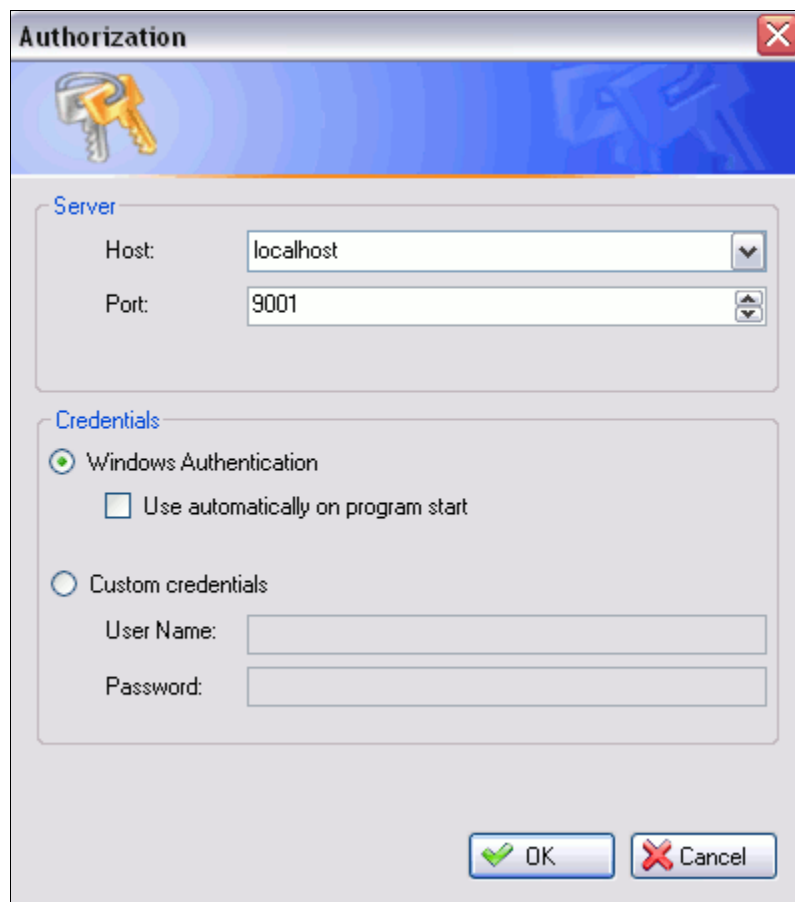
3.1 Logging in to the Administrative Console

After installation of the Administrative Console and Central Services is complete, Administrators can start the Administrative Console interface via the Windows Start Menu. Providing that the default installation paths were chosen during installation, the CESM Administrator Console can be started by selecting:

Start > All Programs > Comodo > Remote Management > CESM Console.



The CESM Administrative Console requires authorization before granting access to the interface:



CESM Administrative Console Authorization Parameters

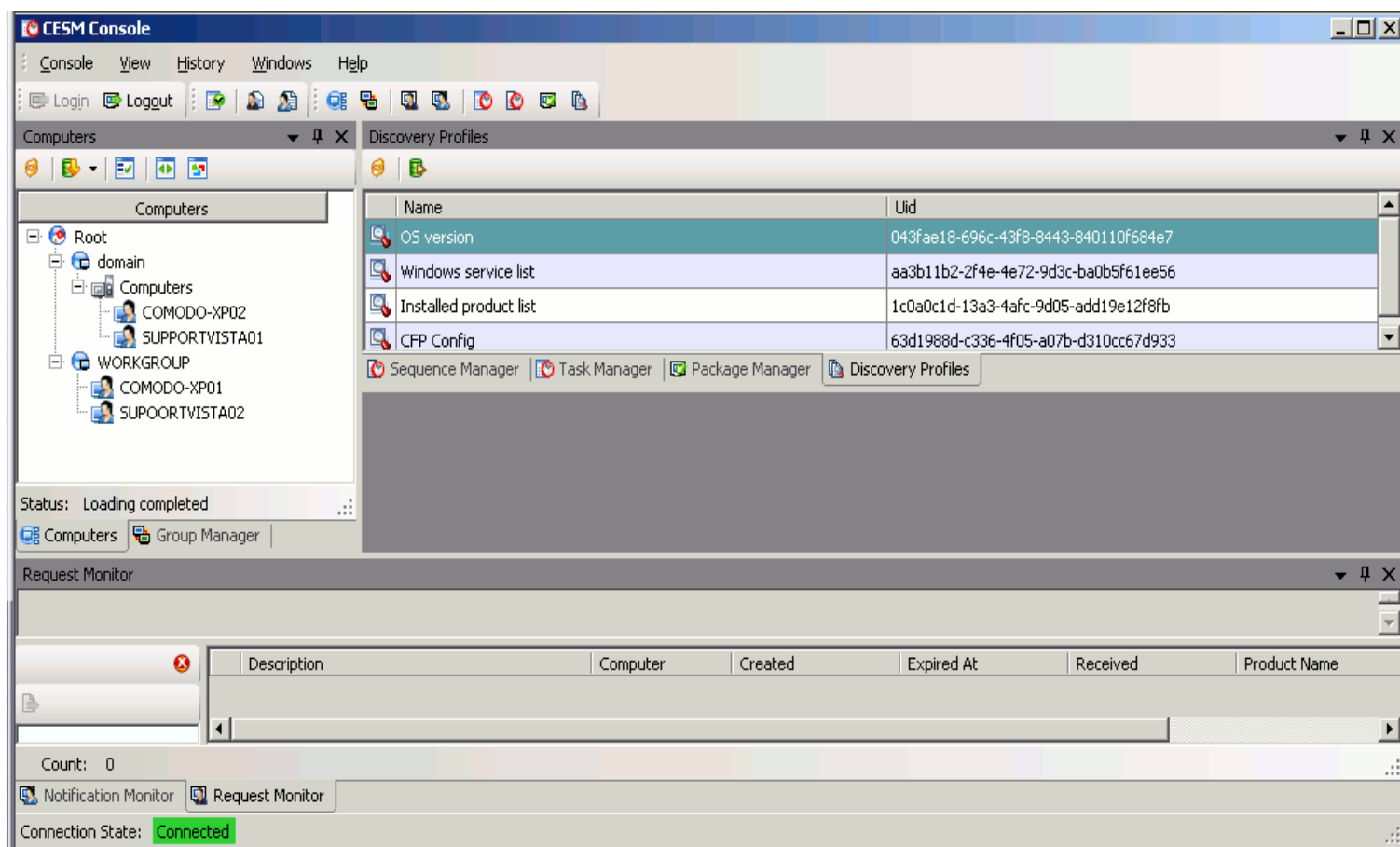
Field Name	Description
Server	<ul style="list-style-type: none"> • If you have installed the Central Service on the same physical machine that you are now attempting to open the Administrative Console from, then leave the 'Host' field at the default setting of 'localhost'. • If you have installed the Central Service on a separate machine to one that you are now attempting to open the Administrative Console from, then you must specify the host name of that machine in the 'Host' field in order to connect. • Port 9001 is the default port number that the Central Service will listen to for connections from the Administrative Console. If you specified an alternate port number during Central Service Installation then you should type that port number here. If you did not specify an alternate port number then you should leave this setting unchanged.
Credentials: Windows Authentication	<p>If you are currently logged into the Windows domain as the administrator that originally installed the CESM application, then your login credentials will automatically be drawn from the Active Directory database. You should choose “Windows Authentication” and do not need to enter a user name and password in order to access the Administrator interface. If not, you will need to authenticate yourself to the CESM Administrator Console by entering</p>

CESM Administrative Console Authorization Parameters	
	User Name and Password details in the 'Custom Credentials' fields.
Credentials: Custom Credentials	If you are not currently logged into the Windows Domain as the administrator that originally installed the CESM application then you will need to enter a valid User Name and Password in the 'Custom Credentials' field. This User Name and Password must belong to a member of the Workgroup 'CrmUsers' group that has access rights to the CESM Central Service. The 'CrmUsers' Workgroup is created automatically during the installation process.

Click 'OK' to login to the interface. After successfully logging in the CESM Administrative console will become available. The Administration Interface is fully explained in the next section - [3.2.Administrative Console Overview](#).

3.2 Administrative Console Overview

The Administrative Console is the nerve center of Comodo End Point Security Manager and is designed to help administrators of corporate networks deploy, manage and monitor Comodo endpoint security software on networked computers. The interface has a modular design that is entirely reconfigurable. Each window or management area can be dragged, dropped and docked to virtually anywhere within the interface, allowing administrators to create the custom workspace that suits their needs and preferences.



CESM Administrative Console

The Administrative Console is sub-divided into the following main functional areas:

The '**Computers and Group Manager**' windows – Enable administrators to import, view and manage network computers

The '**Package Management**' window – Enables administrators to view, manage and upload Comodo .msi packages

The '**Discovery Profiles**' window – Enables administrators to choose information to retrieve from network computers

The '**Sequence Manager**' window – Enables administrators to define a set of actions to be carried out as part of a task

The '**Task Manager**' window – Enables administrators to define tasks based on sequences of actions to run on computers

The Administrator Console also contains the following Monitoring and Reporting areas:

The '**Task Result**' window – Enables administrators to view whether a task executed on a computer was successful or not.

The '**Notification Monitor**' – Enables administrators to view service messages from Comodo packages running on computers

The '**Notification History**' window – Enables administrators to view all service status messages from CESM Central Service

The '**Request Monitor**' – Enables administrators to view and react to alerts from Comodo packages running on computers.

The '**Request History**' window – Enables administrators to view all alerts including those dealt with and removed from the monitor

Note: Most Monitoring and Reporting areas contain shortcuts that initiate activities carried out by the functional areas.














3.2.1 Persistent Navigational Elements -The File Menu and Shortcut Menus


The CESM File and Shortcut Menus provide access to all functional areas of the CESM interface. The File Menu can be accessed at all times and consists of five areas: Console, View, History, Windows and Help. The Shortcut Menu, positioned directly below, provides fast and easy access to many of the functions contained in the 'Console', 'View' and 'History' areas of the the file menu. Both these menus are always visible at the upper left hand side of the screen irrespective of the layout chosen by the user.



The following table contains a brief summary of these areas:

File Menu Element	Equivalent Shortcut Menu Icon	Description
Console		Contains program commands relating to user login and shutdown.

Log in		Allows a new user to log into the CESM Administrator session.
Log out		Logs the current user out of the Administration Interface but does not close the interface down.
Exit	None	Logs the current user out of the Administration Interface then closes down the application.
View		Contains shortcuts that open up the various functional and task management areas of the interface.
Computers		Opens the 'Computers' window.
Group Manager		Opens the 'Computers' window.
Request Monitor		Opens the 'Request Monitor' window
Notification Monitor		Opens the 'Notification Monitor' window.
Task Manager		Opens the 'Task Manager' window.
Sequence Manager		Opens the 'Sequence Manager' window.
Discovery Profiles		Opens the 'Discovery Profiles' window.
Package Manager		Opens the 'Package Manager' window.
History		Contains shortcuts that open 'History' windows relating to Tasks, Requests or Notifications.
Task Result		Opens up the 'Task Results' window.
Request History		Opens up the 'Request History' window.
Notification History		Opens up the 'Notification History' window.
Windows		Contains workspace related options and presets.
<u>Layout</u>	None	
Save Current Layout	None	Saves the currently configured arrangement of windows. This workspace will be loaded by default upon next login.
Reset Layout	None	Resets layout of windows to the arrangement that was loaded upon first login.
Optimal	None	Comodo pre-configured workspace. Provides visibility and fast access to all major functional areas.
Scheduling	None	Comodo pre-configured workspace. Provides greater visibility and access to the Task Manager and Request and Notification History windows. Remaining windows are docked to the left hand side of the interface.
Monitoring	None	Comodo pre-configured workspace. Provides greater visibility and access to the Notification and Request Monitoring Windows. Remaining windows are docked to the left hand side of the interface.
Results and Monitoring	None	Comodo pre-configured workspace. Provides greater visibility and access to overall monitoring of network tasks results and request notifications. Remaining windows,

		apart from 'Discovery Profiles' are docked to the right hand side of the interface.
<u>Custom Layout 1/2/3</u>	None	Allows the user to quickly select then deploy 1 of 3 user-defined workspace layouts.
Set this as Current	None	Loads the workspace layout previously saved as layout 1,2 or 3.
Save current Layout to this	None	Saves the current arrangement of windows as Custom Layout 1,2 or 3.
Close All Windows	None	Closes all open windows but does not close down the main Administration Interface.
Help	None	
Help		Opens the internal help guide.
About	None	Provides the user with license and software version information.

3.3 The 'Computers' and 'Group Manager' Windows

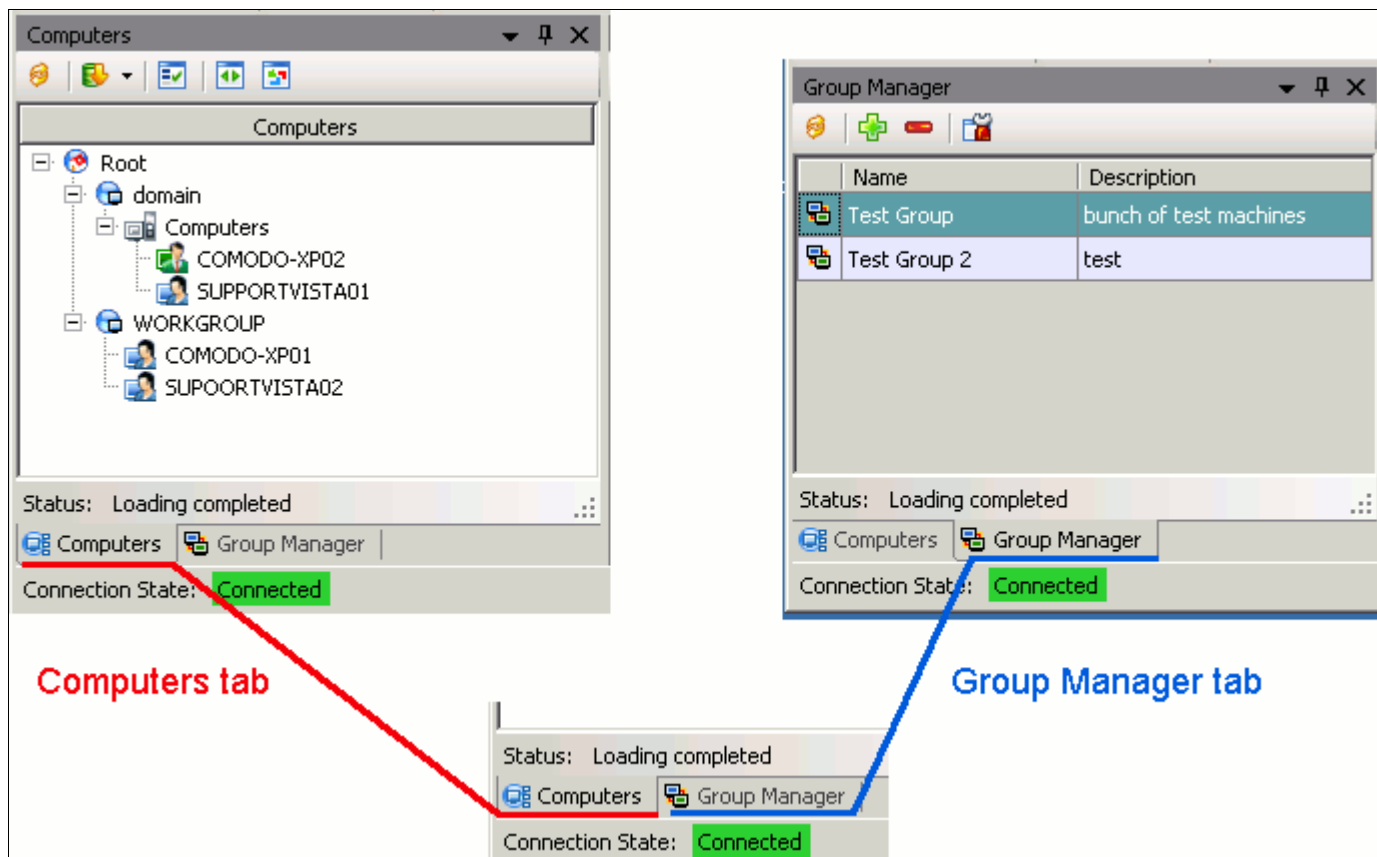
3.3.1 Overview

The 'Computers' and 'Group Manager' windows play a key role in the CESM Administrative interface window by providing system administrators with the ability to import, view and manage networked computers.

The 'Computers' window displays the network structure of imported machines in a familiar hierarchical tree structure and can also be used as the launchpad for running tasks and controls on imported machines. For a more detailed summary of the functionality of the Computers window, see section [3.3.2.The 'Computers' Window – Functionality and Purpose](#) . For a detailed tutorial explaining how to import computer structures then configure those computers for management under CESM, see section [4.Importing Network Structure](#)

The 'Group Manager' window displays a list of user-defined groups of imported computers. 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 create and deploy tasks to run all machines belonging to that group. For a more detailed summary of the functionality of the Group Manager window, see section [3.3.4.The 'Group Manager' Window– Functionality and Purpose](#) . For a tutorial explaining how to set up a group of imported computers, see section [5.1.3.Managing groups of computers](#)

By default, the 'Computers' and 'Group Manager' windows are displayed next to each other in a tab structure as shown below. Administrators can view each as an individual window and re-position them according to their preferences by simply left-clicking + hold on either tab then dragging the window to the desired location.



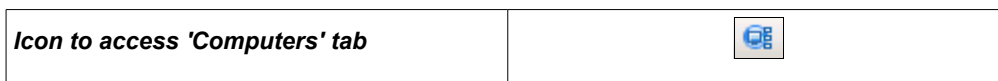
3.3.2 The 'Computers' Window – Functionality and Purpose

The 'Computers' window allows the administrator to:

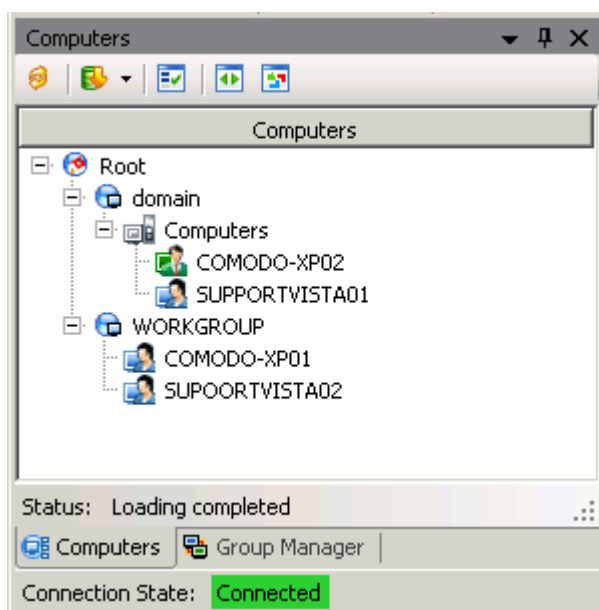
- Import network structures from Active Directory Domains and Windows Workgroups into the CESM Administrative Console. For a detailed tutorial on importing network structures, see [4.Importing Network Structure](#)
- Assign 'Managed' status to individual computers, Domains, Domain controllers or Workgroups for which control of Comodo applications is required. For more details on assigning 'Managed Status', see [5.2.Preparing Imported Computers For Remote Management](#)
- Install or uninstall the CESM Remote Agent onto computers with 'Managed' status so that the CESM Central Service can establish or relinquish control of the machine. See [5.2.2.Installing CESM Remote Agent|outline](#) for more details
- Create a new Task to run on this computer. Selecting 'Create Task' from the right-click menu will open the 'New Task' dialog with the selected computer already preselected as the target. See [3.7.The 'Task Manager' window](#) for more details .
- View 'Discovered Data' about the selected computer. 'Discovered Data' is information that has been collected by a Task that ran a Discovery Profile on the selected computer. See section [3.5.The Discovery Profiles window](#) for more details

Administrators can open the 'Computers' window in the following ways:






- Via the File Menu. Select **View > Computers** to open the 'Computers' window
- Via the shortcut menu button:









- Via keyboard shortcut. Press 'CTRL + ALT + C' to open the 'Computers' window

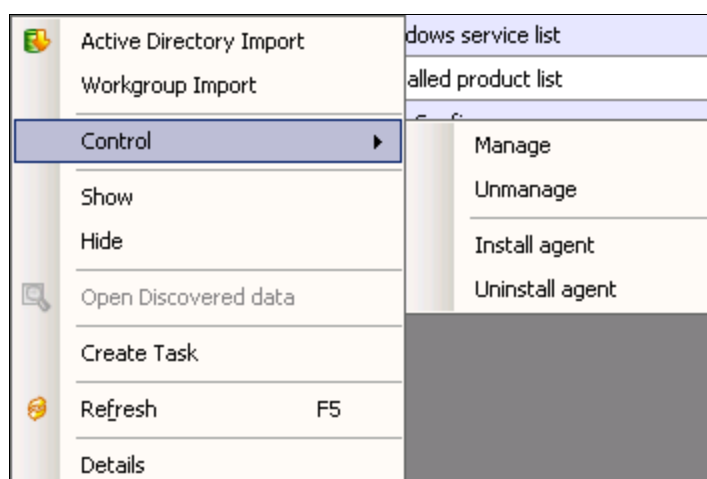


Window Specific Controls - 'Computers'

Menu Element	Description
 Refresh	Refreshes the list of imported computers by re-auditing the network structure.
 Active Directory Import (Default)	Initiates either the Active Directory or Workgroup import wizard. Simply clicking this button will begin the 'Active Directory' import wizard. Clicking the arrow to the right of the icon allows the user to choose between initiating the 'Active Directory' or 'Workgroup' import wizards.
 Show All	Click the 'Show all' button to view all hidden items (workstations)
 Expand All	Click the 'Expand All' command to expand all of the items in the tree.
 Collapse All	Click the 'Collapse All' command to collapse all of the currently items in the view.

'Computers' Window - Tree Icons	
Tree Icon	Description
	Root folder icon
	Domain / Workgroup icon
	Organizational Unit
	Computer Status = Unmanaged. All newly imported computers are unmanaged until the administrator chooses to manage them. CESM cannot interact with a computer unless it has 'Managed' status.
	Computer Status = Managed but not connected to CESM Central Service. The CESM Remote Agent must be installed on a workstation in order for it to connect to central service.
	Computer Status = Managed and connected to CESM Central Service.

Right clicking on any workstation, Domain, Domain controller or workstation listed in the 'Computers' window will open a context sensitive menu that allows further actions to be carried out on the group:



'Computers' Context Sensitive Menu - Table of parameters

Action's name	Description
Active Directory Import	Imports the list of computers you want to manage from Active Directory. More...
Workgroup Import	Imports the Workgroup of computers you want to manage. More...
Control	<p>Manage – Assigns “Managed” Status the selected item</p> <p>Unmanage – Removes “Managed” status from the selected item.</p> <p>Install Agent – Will initiate the CESM Remote Agent installation procedure on the selected item</p> <p>Uninstall Agent – Will initiate the CESM Remote Agent uninstallation procedure on the</p>

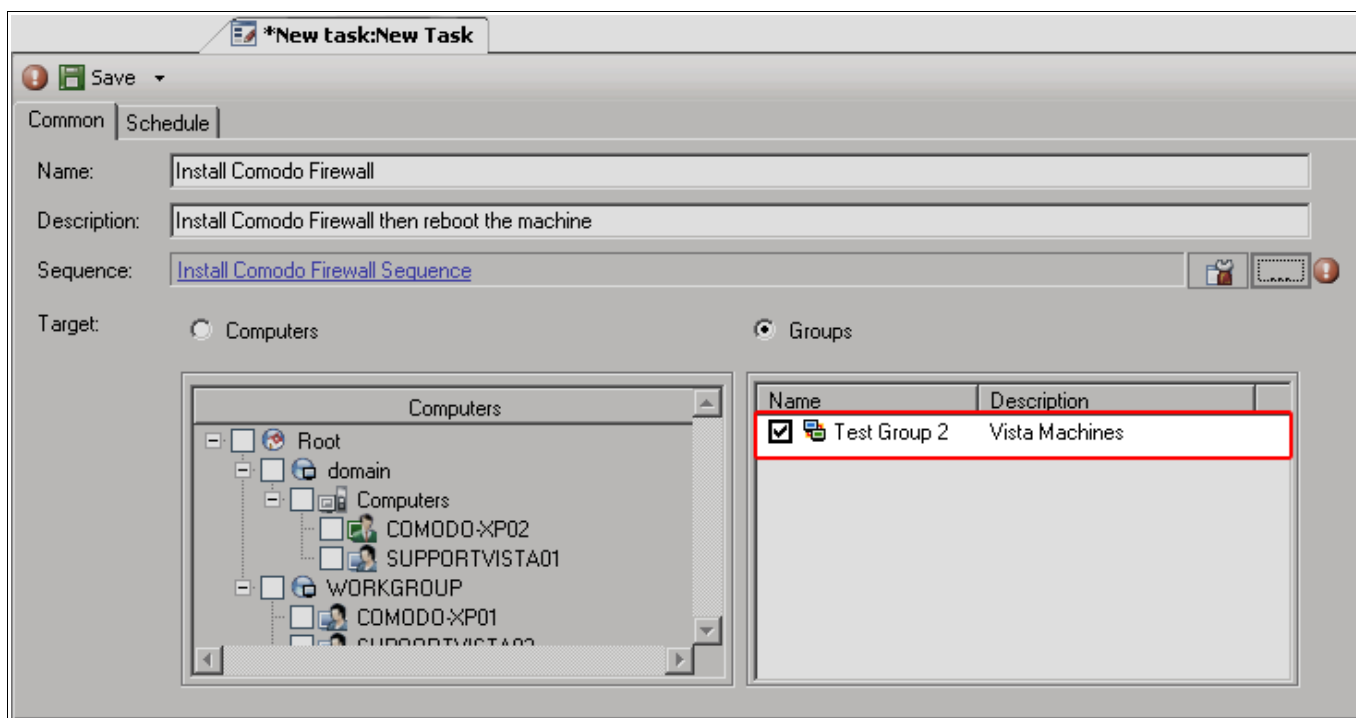
	selected item
Show	Hidden computers can be made visible at Computers' panel again by clicking "Show all" button.
Hide	Hides the selected item so that it is not displayed in the tree. This is handy should, for example, an administrator only wish to view CESH 'Managed' computers. Note: Computers can not be deleted from the display, but in case they are not needed at the moment - they can be hidden.
Open Discovered data	Allows the administrator to view 'discovered' data about the selected item. Discovered data is fetched by running a task that includes a CESH 'Discovery Profile' on the item. The CESH Administrative console presently includes discovery profiles for OS version, Windows service list, Installed product list and Comodo Firewall Pro Configuration (CFP Config.)
Create Task	Allows administrators to start the add new task dialog for the selected workstation, unit or group.
Refresh	Updates the list of computers displayed in the tree by re-polling the network structure.
Details	Allows the user to view details for the selected object such as Name, GUID, SID, Creation date, Date of last modification, DNS (for workstations only), Status (for workstations only)

3.3.3 The 'Group Manager' Window– Functionality and Purpose

The 'Group Manager' window allows the administrator to:

- Define a CESH 'Group' of imported computers for the purposes of rolling out Tasks across multiple computers and/or networks. 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'. For a tutorial explaining how to define a group of imported computers, see section [5.1.3.Managing groups of computers](#)
- Instantly assign or remove 'Managed' status to all computers, Domains, Domain controllers or Workgroups that are members of that group. For more details on the importance of assigning 'Managed Status', see [5.2.Preparing Imported Computers For Remote Management](#)
- Install (or uninstall) the CESH Remote Agent onto all computers in the groups so CESH Central Service can establish or relinquish control of the machine. See [5.2.2.Installing CESH Remote Agent](#) for more details
- Create a new Task to run on all computers in the group (for example, a task to install Comodo Firewall Pro on all computers in the group). Selecting 'Create Task' from the right-click menu will open the 'New Task' dialog with the selected Group already pre-selected as the target. See [3.7.The 'Task Manager' window](#) for more details on the nature, implementation and types of Tasks available .

Once a CESH 'Group' has been created, this group can be specified as the target entity for any new Tasks (or added to the target list of an existing task). The ability to roll out tasks to large numbers of machines will prove itself to be an invaluable time-saver in networks of all sizes:

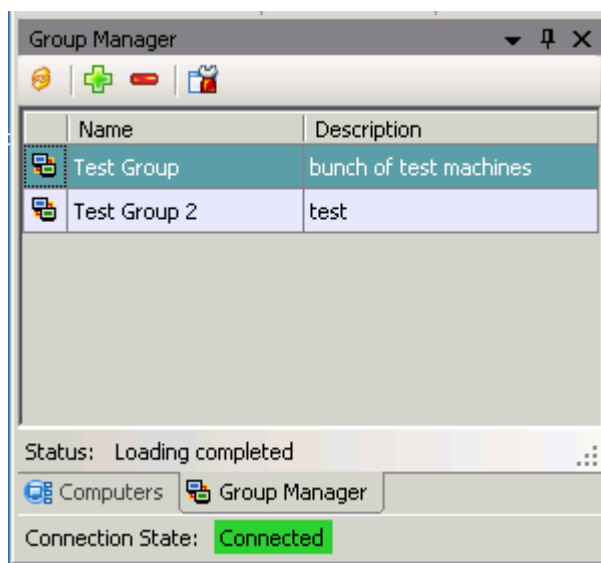


Administrators can open the 'Group Manager' window in the following ways:





- Via the File Menu. Select '**View > Group Manager**' to open the 'Group Manager' window
- Via the shortcut menu button:



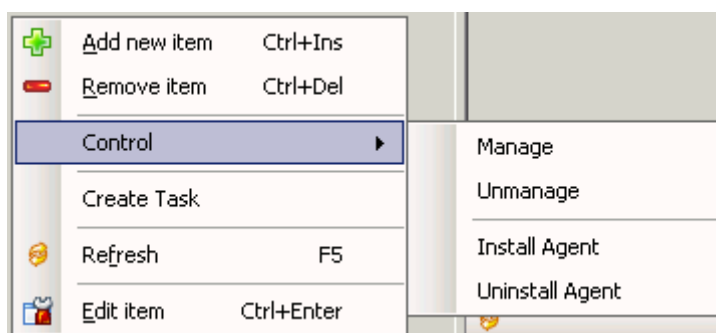
- Via keyboard shortcut. Press '**CTRL + ALT + G**' to open the 'Group Manager' window







The 'Group Manager' window lists all existing, user defined 'Groups' and provides the ability to Add, Remove and reconfigure groups.

Window Specific Controls – Group Manager	
Menu Element	Description
 Refresh	Updates the entire list of groups displayed in the Group Manager tab so that the list incorporates groups which have been recently created, deleted or modified.
 Add	Initiates the 'Add New Group' dialog. More details can be found in 5.1.3.1.Creating groups
 Delete	Deletes the currently selected group
 Edit	Opens the 'Edit Group' dialog – allowing the administrator to alter settings related to this group including Group composition, Name and Description.

Right clicking on any group listed in the 'Group Manager' window will open a context sensitive menu that allows further actions to be carried out on the group:



'Groups' Context sensitive menu - Table of parameters

Action's name	Description
 Add	Initiates the 'Add New Group' dialog. More details can be found in 5.1.3.1.Creating groups
 Delete	Deletes the currently selected group
Control	<p>Manage – Assigns “Managed” Status the selected item</p> <p>Unmanage – Removes Managed status from the selected item.</p> <p>Install Agent – Will initiate the CESM Remote Agent installation procedure on the selected item</p> <p>Uninstall Agent – Will initiate the CESM Remote Agent uninstallation procedure on the selected item</p>
Create Task	Allows administrators to start the add new task process for the selected workstation, unit or group.
 Refresh	Updates the currently selected group so that any recent changes to the group are reflected in the listing.
 Edit	Opens the 'Edit Group' dialog – allowing the administrator to alter settings related to this group including Group composition, Name and Description.

3.4 The Package Management window

3.4.1 Overview

A CESH 'Package' is a file that is used for the installation, maintenance, and removal of software on Microsoft Windows operating systems. CESH 'Packages' are the installer files for Comodo applications such as Comodo Firewall Pro and come in the form of .msi files. You *must* upload the appropriate Package to CESH for the application you wish to manage on networked computers. Once uploaded, this package can be specified as the Parameter' of an 'Install' or 'Uninstall' action. (Note: The 'Uninstall' or 'Install' action may form part or all of a 'Sequence' of 'Actions' that will determine the purpose of any 'Task' you intend to run on a 'Managed' computer or group of computers.) Updated and new Comodo .msi files for use as CESH packages will be provided by Comodo as part of your license agreement.

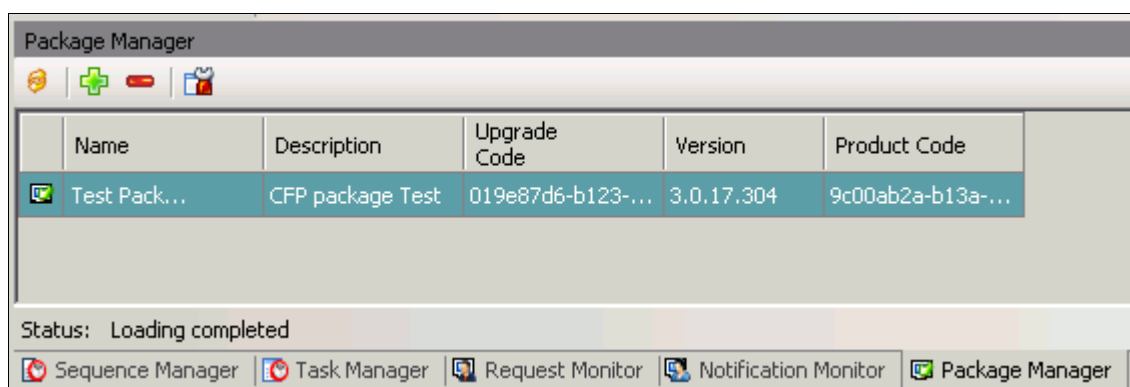
3.4.2 Opening the Package Manager window

Administrators can open the 'Package Manager' window in the following ways:

- Via the File Menu. Select '**View > Package Manager**' to open the 'Package Manager' window
- Via the shortcut menu button:



- Via keyboard shortcut. Press '**CTRL + ALT + P**' to open the 'Package Manager' window



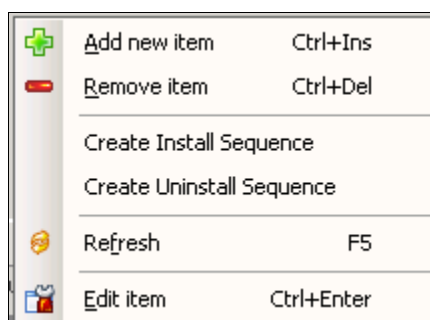
Once opened, the 'Package Manager' window enables administrators to add, view and re-configure CESH 'Packages'.

Window Specific Controls – Package Manager

Control's name	Description
Refresh	Updates list of packages
Add	Enables the user to add a new package to the list. Opens the 'Add New Package' dialog. See 3.4.3.Adding a Package to Comodo Endpoint Security Manager for a short tutorial explaining this process.
Delete	Deletes the selected package

	Edit	Enables the administrator to edit package parameters such as Name and Description and/or to upload an alternative or updated .msi file.
--	------	---

Right clicking on any Package listed in the 'Package Manager' window will open a context sensitive menu that allows further actions to be carried out on the group:



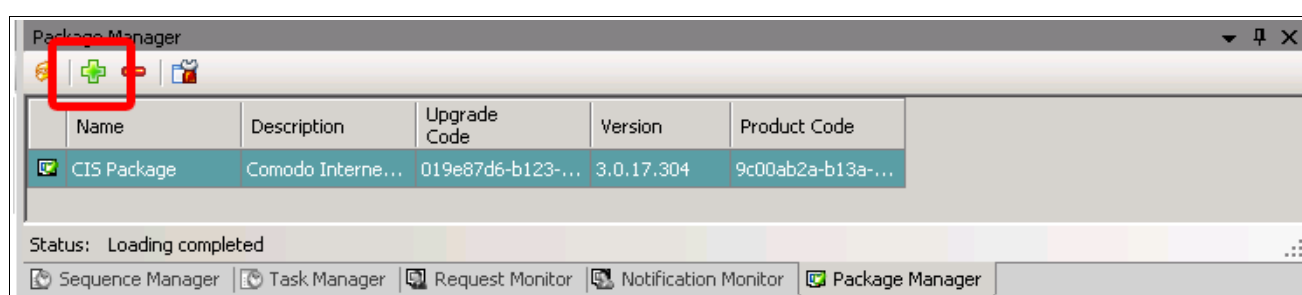
Context management menu - Table of parameters

Action's name	Description
Add new item	Enables the user to add a new package to the list. Opens the 'Add New Package' dialog. See 3.4.3.Adding a Package to Comodo Endpoint Security Manager for a short tutorial explaining this process.
Remove item	Allows the user to delete the package
Create Install Sequence	Allows the user to create Installation Sequence for the package
Create Uninstall Sequence	Allows the user to create Uninstallation Sequence for the package
Refresh	Updates the list of packages.
Edit	Enables the administrator to edit package parameters such as Name and Description and/or to upload an alternative or updated .msi file.

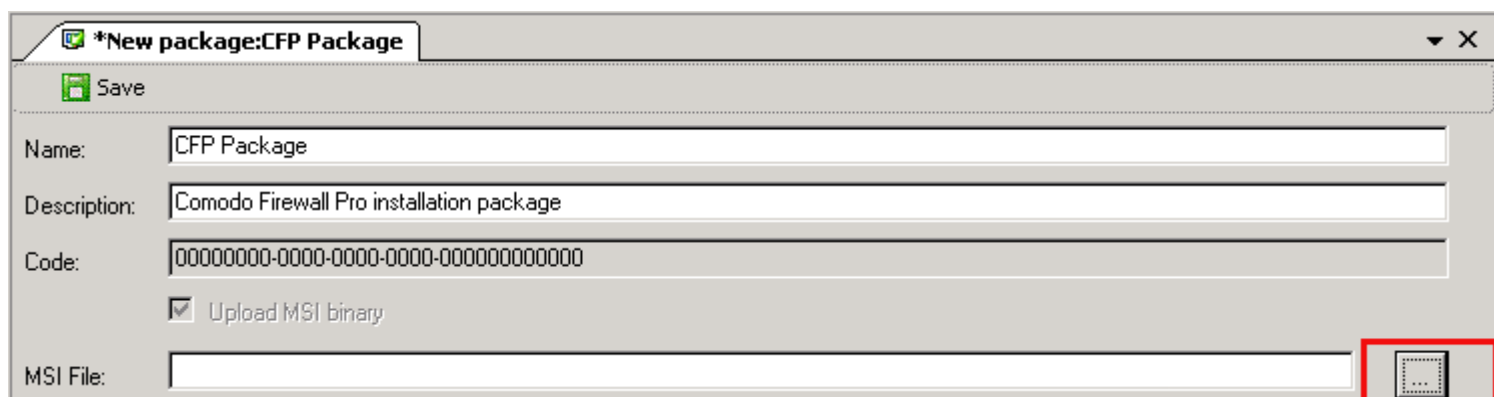
3.4.3 Adding a Package to Comodo Endpoint Security Manager

To add a package to Comodo Endpoint Security Manager:

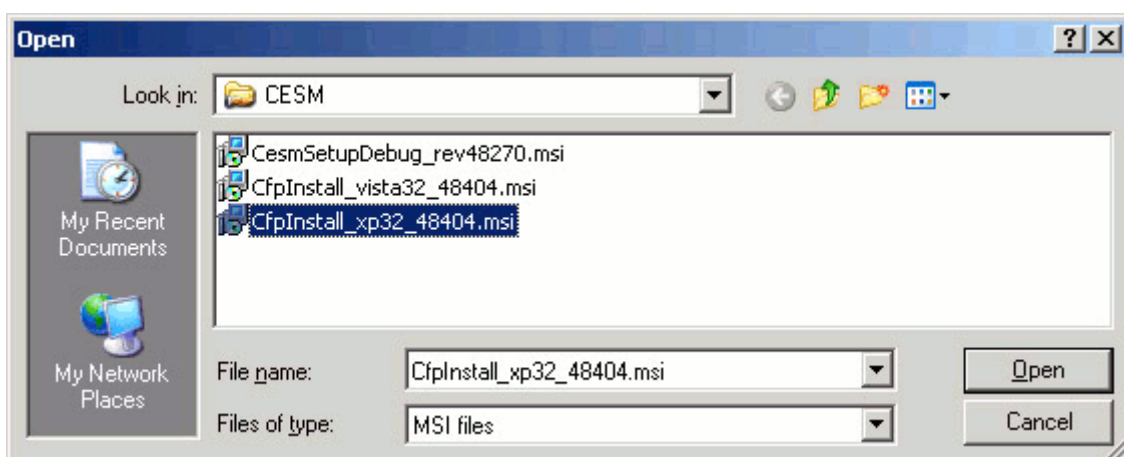
- Open the 'Package Manager' window using any of the methods outlined earlier
- Click the 'Add New Item' Icon (highlighted below)



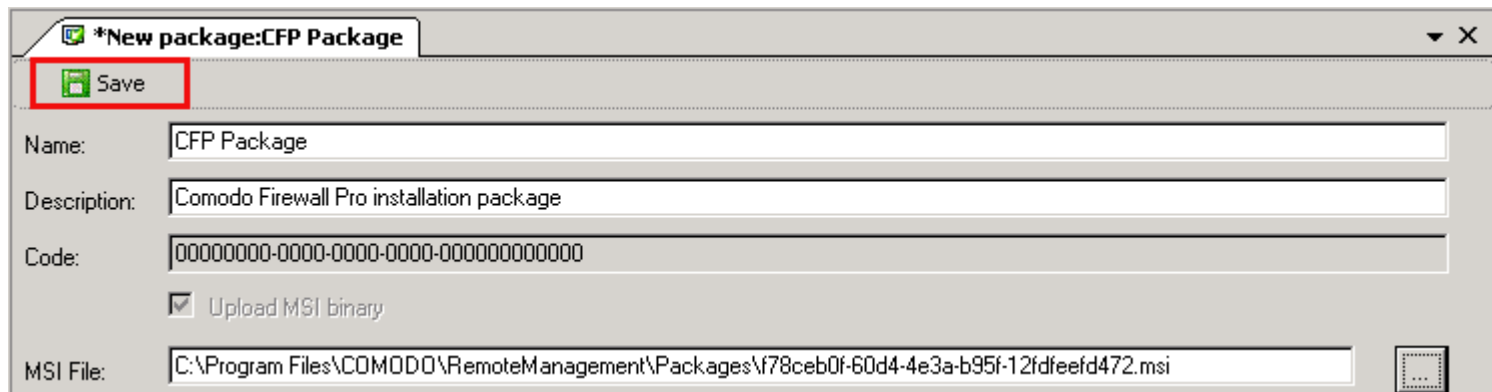
- This will open the 'Add New Package' dialog (shown below). At this stage, you should create an appropriate Name and (optional) Description for the Package you are about to upload.



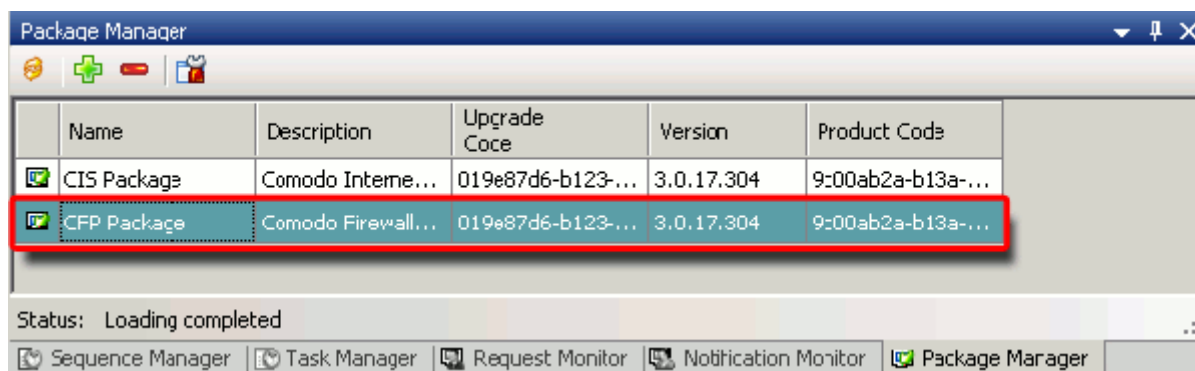
- Next, click the ellipsis button to the right of the 'MSI File:' field (highlighted above). This will open the standard Windows file browser:



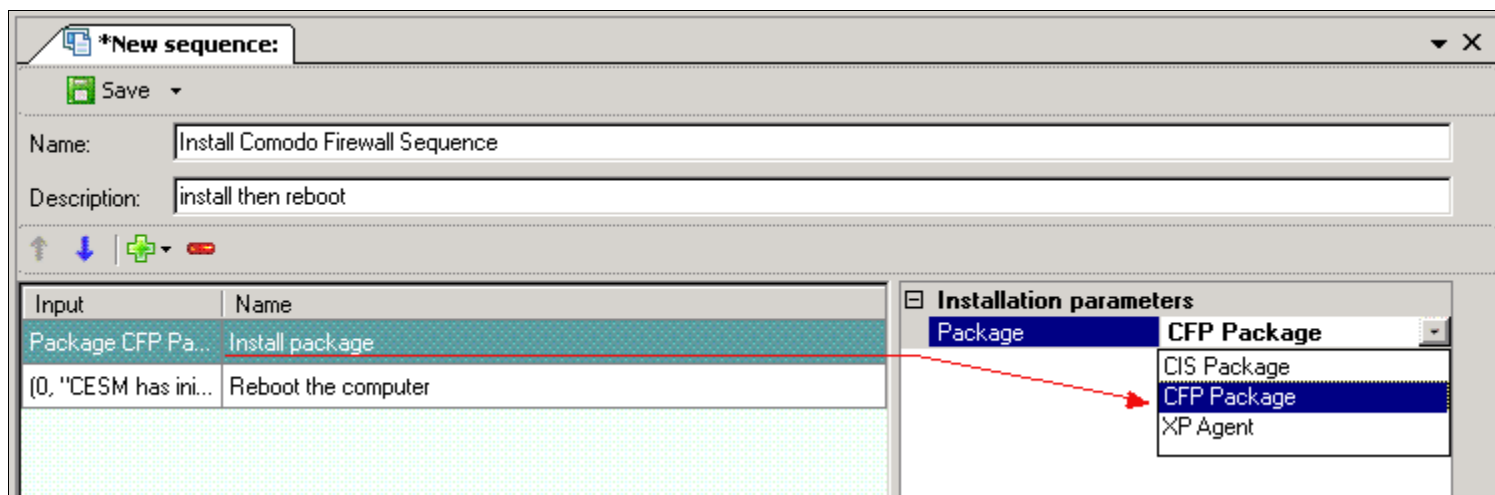
- Browse to the local or network location to which you have saved Comodo .msi files. Select the appropriate file and click 'OK'.
- This will return you to the 'New Package' dialog where the filename of the .msi file will now be displayed in the 'MSI File:' field. Click the 'Save' button to confirm and save your new package:



- The newly created Package will be listed alongside any other packages in the 'Package Manager' window:



- Once the Package has been created, it can be specified as the 'Installation Parameter' of an 'Install' or 'Uninstall' Action in 'Sequence' of Actions using the 'Sequence Manager' dialog:



- It is possible for there to be more than one Package involved in any particular Sequence of Actions. For example, you may want to create a single Sequence of Actions that will 'Uninstall the Comodo Firewall Package' > 'Reboot the Computer' > 'Install the Comodo Internet Security Suite' Package > 'Reboot the Computer'.

3.5 The Discovery Profiles window

3.5.1 Overview

Note: In terms of understanding, 'Discovery Profiles' are heavily dependent on an understanding of CESM 'Actions' and 'Sequences'. If they haven't done so already, Comodo advises administrators to familiarize themselves with Actions and Sequences before reading this section.

A Discovery Profile is an Action that fetches data about Managed computers in a network and returns that information to the CESM console. Armed with this data, administrators can make informed decisions about the configuration policy that they wish to take on those Managed computers - including Windows Service control, the installation or uninstallation of packages and the configuration of Comodo applications such as Comodo Firewall Pro. For example, the "Installed Packages" Discovery Profile will inform the administrator as to which Packages were installed on the machine at the time the Action was run (including any 3rd party .msi packages). The administrator can then quickly uninstall any one of those packages from that machine by right clicking, selecting 'Create Sequence'; saving this Sequence as a Task and running the Task on that machine or multiple machines in the network. The 'OS Version' Discovery Profile could be used to determine which version of a Package the administrator should install on a Managed computer.

Clicking on a specific 'Discovery Profile' listed in the 'Discovery Profiles' window is firstly a convenient way of viewing all Managed computers in the network that have had that Profile executed on them. Secondly, and more importantly, it allows you to quickly access the data recovered by that Profile for the machine in question and use that data as a basis for new Sequences to be implemented on Managed computers.

CESM includes 4 discovery profiles:

Discovery Profile Name	Prerequisites for viewing data	Clicking on this Discovery Profile in the 'Discovery Profiles' Window will show you:
OS Version	A 'Task' must have been run on at least one machine with a 'Sequence' that contained : Action = 'Discover Data' + Discovery Parameter = 'OS Version'	A list of the names of all computers upon which a 'Discover Data' Action with the Discovery Profile 'OS Version' has been run and the time it was run. To the right of this list of computers is the results panel which displays the operating system present on the selected machine at the time the Action was run.
Windows services list	A 'Task' must have been run on at least one machine with a 'Sequence' that contained : Action = 'Discover Data' + Discovery Parameter = 'Windows Services List'	A list of the names of all computers upon which a 'Discover Data' Action with the Discovery Profile 'Windows Services' has been run and the time it was run. To the right of this list of computers is the results panel. Clicking the ellipsis button (...) on the right hand side of this panel will display the Name, State and Type of all services present on the machine at the time the Action was run. Right clicking on any one of these services will allow the administrator to quickly create a new 'Sequence' containing a 'Control Service' Action that can be used to stop, start, pause or continue that service. This Sequence can then be used as part of a Task which can be deployed on that individual machine or across multiple machines.
Installed products	A 'Task' must have been run on at least one machine with a 'Sequence' that contained : Action = 'Discover Data' + Discovery Parameter = 'Installed Product List'	A list of the names of all computers upon which a 'Discover Data' Action with the Discovery Profile 'Installed Product List' has been run and the time it was run. To the right of this list of computers is the results panel. Clicking the ellipsis button (...) on the right hand side of this panel will display the Name, Version, Publisher, Date (of installation) and Location of all Comodo and 3 rd party Packages present on the machine at the time the Action was run. ('Package', in this instance, means 'installed using a

		.msi installer) Right clicking on any one of these Packages will allow the administrator to quickly create a new 'Sequence' containing an 'Uninstall Package' Action that that can be used to remove that Package. This Sequence can then be used as part of a Task which is used to remove the selected Package from that individual machine or multiple machines.
CFP Config	A 'Task' must have been run on at least one machine with a 'Sequence' that contained : Action = 'Discover Data' + Discovery Parameter = 'CFP Config'	A list of the names of all computers upon which a 'Discover Data' Action with the Discovery Profile 'CFP Config' has been run and the time it was run. To the right of this list of computers is the results panel. Clicking the ellipsis button (...) on the right hand side of this panel will open a window which displays the various configuration settings that were in use on that installation of the firewall at the time the Action was run. Clicking 'File > Save As' at the top left of this window will allow the administrator to save this configuration setting as a .xml file. This .xml file can then be loaded as the basis of a new 'Sequence' containing the 'CFP Set Config' Action. This Sequence can then be used as part of a Task to roll out those settings across multiple machines. Alternatively, having decided this discovered profile is a good 'start' point, the administrator may wish to change only one or two of the settings when defining the Sequence and implement the new configuration across the entire network.

3.5.2 Opening the Discovery Profiles window

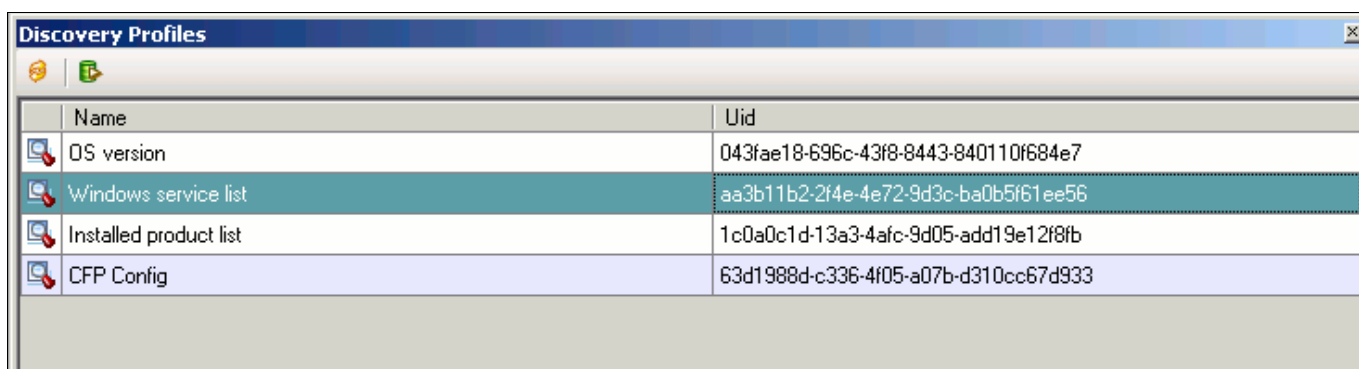
Administrators can open the 'Discovery Profiles' window in the following ways:



- Via the File Menu. Select '**View > Discovery Profiles**' to open the 'Discovery Profiles' window
- Via the shortcut menu button:



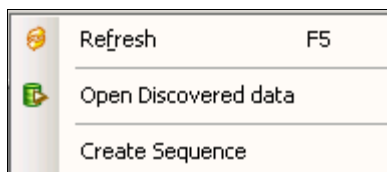
- Via keyboard shortcut. Press '**CTRL + ALT + D**' to open the 'Discovery Profiles' window
- Via context menu or 'Computers' window.

Once opened, the 'Discovery Profiles' window enables administrators to view discovered data for selected type of profile.



Window Specific Controls – Discovery Profiles	
Control's name	Description
 Refresh	Updates profiles' list
 Open Discovered Data	Enables the user to view profiles of the selected Managed workstation.

Right clicking on any of four profiles listed in the 'Discovery Profile' window will open a context sensitive menu that allows further actions to be carried out:

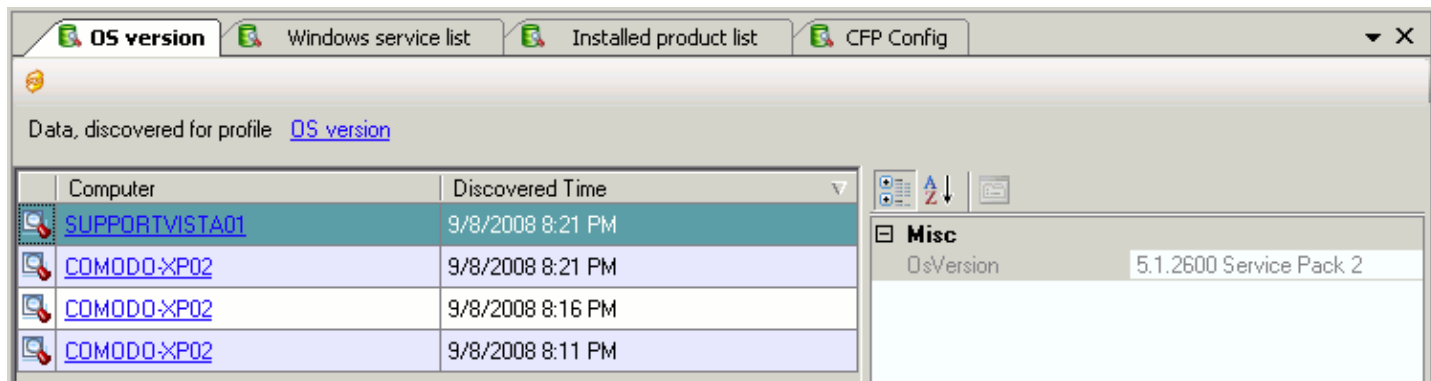


Context management menu - Table of parameters

Action's name	Description
Create Sequence	<p>Allows the administrator to create a new sequence:</p> <ul style="list-style-type: none"> An 'Uninstall Package' sequence can be quickly created from the context sensitive menu if the 'Installed Products List' Discovery Profile is selected. A 'Control Windows Service' sequence can be quickly created from the context sensitive menu if the 'Windows service list' Discover Profile is selected. A 'Set CPF config' sequence can be quickly created from the context sensitive menu if the 'CFP' Discovery Profile is selected.
Refresh	Updates the information about profiles listed.
Open Discovered data	Enables the administrator to view discovered data for selected type of profile.




3.5.2.1 'OS Version' Profile

The 'OS Version' discovery profile allows administrators to establish which operating system is installed on a target computer (or group of computers). Clicking 'OS Version' in the 'Discovery Profiles' window will open a list of the names of all computers upon which a 'Discover Data' Action with the Discovery Profile 'OS Version' has been run and the time it was run.



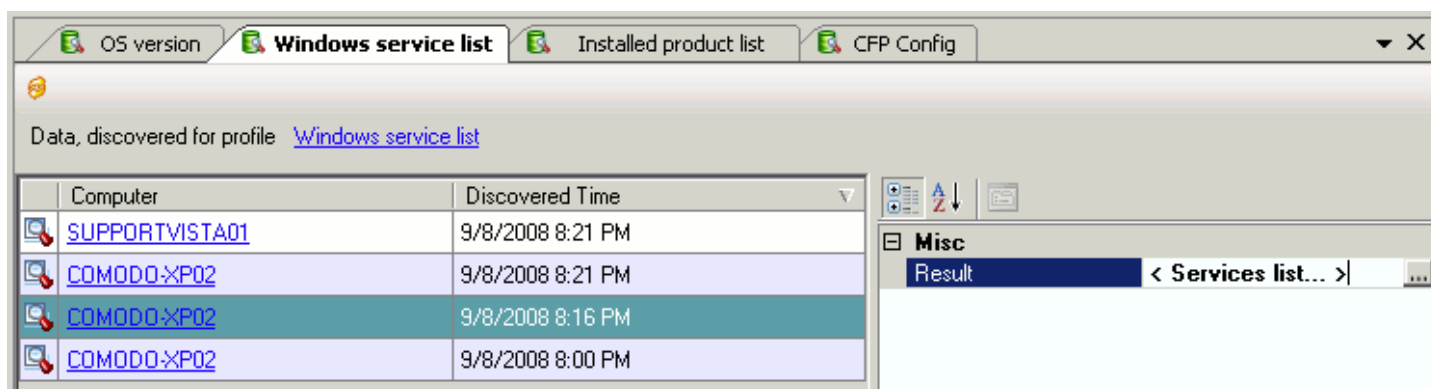
To the right of this list of computers is the results panel which displays the operating system present on the selected machine at the time the Action was run.

The filter buttons allow the administrator to sort discovered data by categories, alphabetically and by property pages.

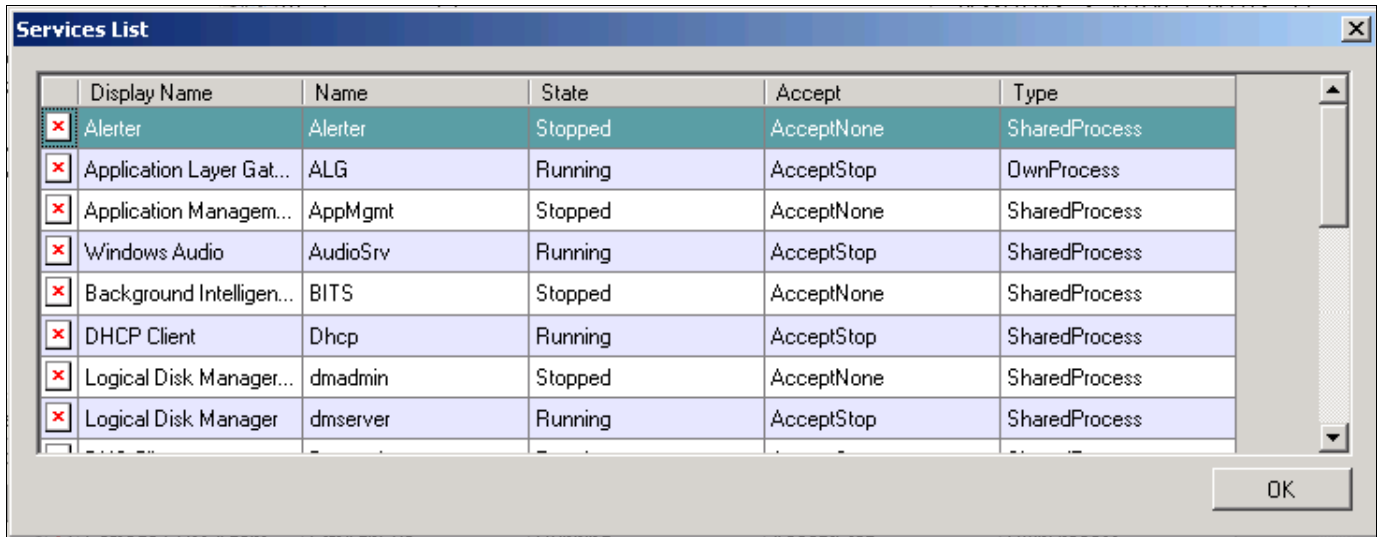
Controls	Description
	Sort by categories.
	Sort alphabetically.
	Sort by property pages.

3.5.2.2 'Windows Services' Profile

The 'Windows Services List' discovery profile allows the administrator to view (and subsequently create a Sequence to control) the list of Windows services registered on a target computer. Clicking on 'Windows Services List' in the 'Discovery Profiles' window will open a list of the names of all computers upon which a 'Discover Data' Action with the Discovery Profile 'Windows Services' has been run and the time it was run. This list contains name, status and control abilities.



To the right of this list of computers is the results panel containing the 'Services List' for that particular machine. Clicking the ellipsis button (...) on the right hand side of this panel will display the Name, State and Type of all services present on the machine at the time the Action was run (see below)



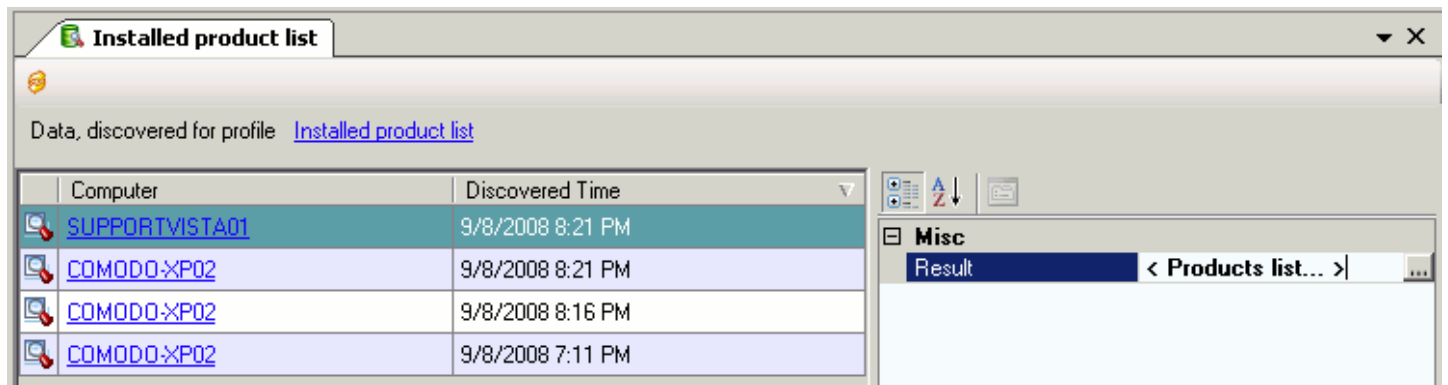
Right clicking on any one of these services will allow the administrator to quickly create a new 'Sequence' containing a 'Control Service' Action that that can be used to stop, start, pause or continue that service. This Sequence can then be used as part of a Task which can be deployed on that individual machine or across multiple machines.

The filter buttons allow the administrator to sort discovered data by categories, alphabetically and by property pages.

Controls	Description
	Sort by categories.
	Sort alphabetically.
	Sort by property pages.
	Allows administrator to view list of Windows services registered on a target computer.

3.5.2.3 'Installed Products' Profile

The "Installed MSI packages" discovery profile allows the administrator to view which programs are present on a target computer or computers that have been installed with the Windows installer (.msi). Clicking on 'Installed Products' in the 'Discovery Profiles' window will show a list of the names of all computers upon which a 'Discover Data' Action with the Discovery Profile 'Installed Product List' has been run and the time it was run.



To the right of this list of computers is the results panel containing the 'Products List' (those .msi packages on that particular machine). Clicking the ellipsis button (...) on the right hand side of this panel will display the Name, Version,

Publisher, Date (of installation) and Location of all Comodo and 3rd party Packages present on the machine at the time the Action was run. ('Package', in this instance, means 'installed using a .msi installer')

Name	Version	Publisher	Installed	Location
Comodo Firewall Pro	3.0.17.304	Comodo	9/8/2008	
VMware Tools	3.1.0000	VMware, Inc.	8/14/2008	C:\Program Files\VMw...
WebFldrs XP	9.50.7523	Microsoft Corporation	8/13/2008	
Comodo CRM Agent	1.0.0.0	Comodo	8/14/2008	

Right clicking on any one of these Packages will allow the administrator to quickly create a new 'Sequence' containing an 'Uninstall Package' Action that can be used to remove that Package. This Sequence can then be used as part of a Task which is used to remove the selected Package from that individual machine or multiple machines.

The filter buttons allow the administrator to sort discovered data by categories, alphabetically and by property pages.

Controls	Description
	Sort by categories.
	Sort alphabetically.
	Sort by property pages.
	Allows administrator to view list of Windows services registered on a target computer.

3.5.2.4 'CFP Config' Profile

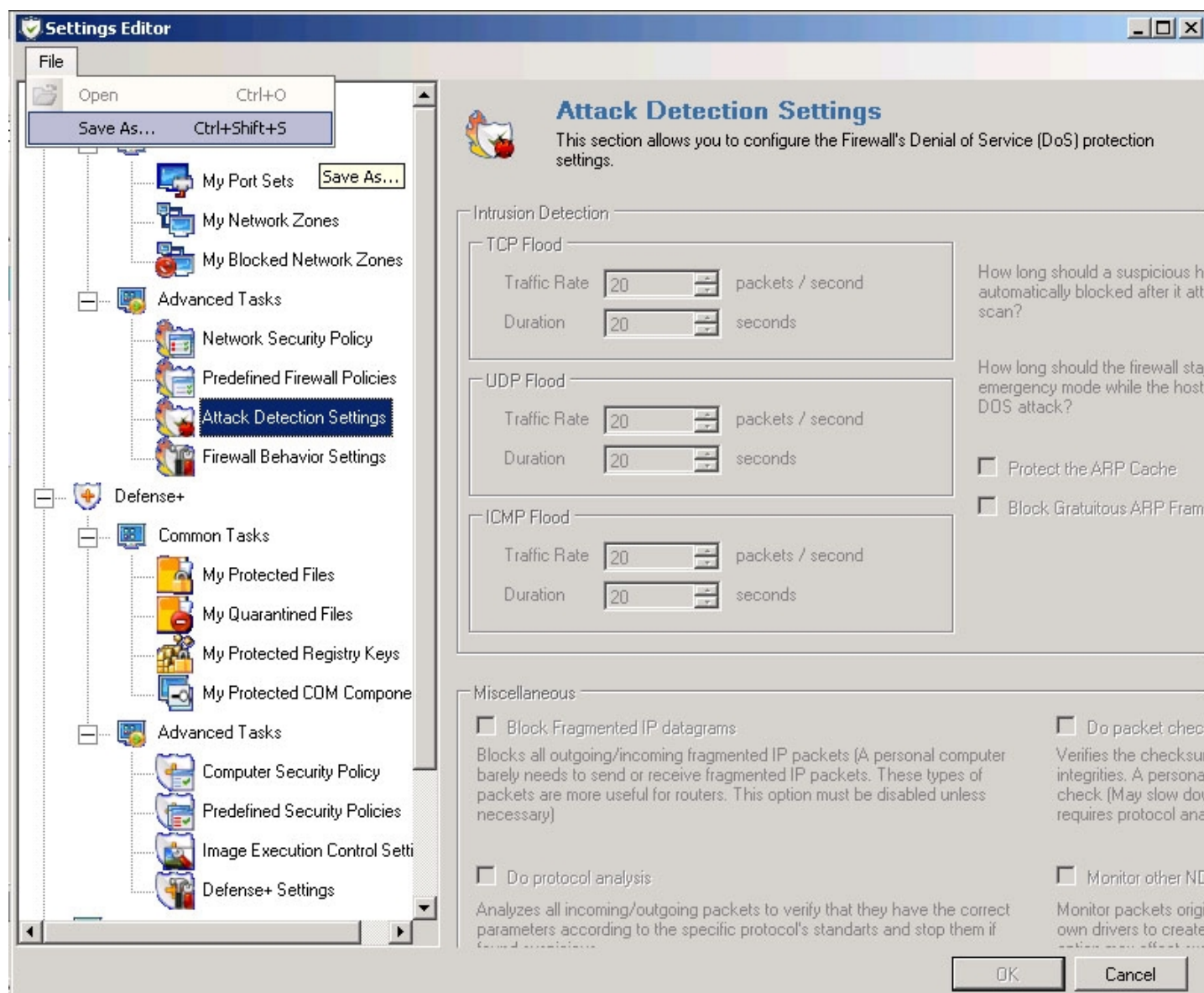
The 'CFP Config' Profile allows the administrator to view the current configuration settings of Comodo Firewall Pro on a particular machine. Clicking 'CFP Config' in the 'Discovery Profiles' window will display a list of the names of all computers upon which a 'Discover Data' Action with the Discovery Profile 'CFP Config' has been run and the time it was run.

Computer	Discovered Time
COMODO-XP02	9/12/2008 1:41 AM
COMODO-XP02	9/12/2008 1:45 AM
COMODO-XP02	9/12/2008 7:47 AM
COMODO-XP02	9/12/2008 7:47 AM
COMODO-XP02	9/12/2008 9:50 AM
COMODO-XP02	9/15/2008 8:32 AM

Discovery data
Result: <CFP Config... >



Result
Comodo Firewall Pro discovered individual configuration data



To the right of this list of computers is the results panel. Clicking the ellipsis button (...) on the right hand side of this panel will open the 'Settings Editor' which displays the various configuration settings that were in use on that installation of the firewall at the time the Action was run:



Clicking 'File > Save As' at the top left of this window will allow the administrator to save this configuration setting as a .xml file. This .xml file can then be loaded as the basis of a new 'Sequence' containing the 'CFP Set Config' Action. This Sequence can then be used as part of a Task to roll out those settings across multiple machines. Alternatively, having decided this discovered profile is a good 'start' point but is in need of tweaking, the administrator change one or two of the settings when defining the Sequence and implement the new configuration across the entire network.

The filter buttons allow the administrator to sort discovered data by categories, alphabetically and by property pages.

Controls	Description
	Sort by categories.
	Sort alphabetically.

	Sort by property pages.
	Allows administrator to view list of Windows services registered on a target computer.

3.5.2.5 Example: Using 'CFP Config' Discovery Profile to roll out an existing CFP configuration onto other machines

(Note: The process outlined below describes a specific situation whereby the administrator needs to copy and re-deploy a pre-existing CFP configuration (or copy it in large but with minor tweaks). To set and deploy a brand new CFP configuration on networked computers, administrators should skip straight to step 3.)

If you currently have a computer with CFP installed and wish to copy and re-deploy that CFP configuration on other computers in the network:

1. Open the "Discovery profiles" window, select the "CFP Config" profile. Choose the machine that has the CFP configuration you wish to use and click the ellipsis (...) button to the right of the 'Discovery Data' panel.
2. This will open the CFP 'Settings Editor' which displays the configuration settings in use on that machine at the time the Discovery Profile Action was run. Click 'File > Save As...' from the file menu in this window and save these configuration settings to a local or network drive as a .xml file. Note – you cannot alter the configuration of these settings yet. If you desire to reconfigure these settings, then this is done during the next stage – creating a 'Set CFP Config' Sequence.
3. Next, open the 'Sequence Manager' and click the "+" icon to create a new Sequence. Select 'CFP Set Config' as the 'Action' and click 'Add'.
4. At the 'Config Parameters' panel, click the ellipsis (...) button. This will open the CFP 'Settings Editor' window. As you wish to roll out the settings from the computer whose 'CFP Config' discovery profile you saved in step 2., you should now click 'File > Open' at the file menu and browse to this saved .xml file. At this stage, administrators should make any configuration changes they wish to implement. Click 'OK' at the bottom of the 'Settings Editor' when finished.
5. You will now be returned to the 'Sequence' configuration dialog. The 'Config Parameters' for CFP have been set in step 4. Supply a Name and Description for the Sequence and Save the sequence.
6. To roll the configuration out to network computers, you now need to create a task that includes the Sequence you created in steps 3 and 4. Open the "Tasks manager" window and click the "+" icon to create a new Task. To the right of the 'Sequence' field there is an ellipsis button (...) which will allow you to choose the Sequence you saved in step 4. After providing a Name and Description for the sequence, choose the target computers using the 'Computer' or 'Groups' selection windows in the lower half of the Task editing dialog. If you want to run this task at a later time, configure your preferences in the 'Schedule' tab. Save the task.
7. Open 'Task Manager'. You can run this task immediately by right clicking on the Task name and selection 'Execute' from the context sensitive menu. Alternatively, you may wish to schedule this task to run at a later time.

3.6 The Sequence Manager window

3.6.1 Overview

A Sequence is one of the most important concepts in CESM. A Sequence is a set of Actions that will be executed in a Task. Once created, a Sequence (of Actions) is added to a Task and the Task is executed on a list of Managed computers or group of Managed computers. The Administrator can create, manage, delete, edit Sequences via the 'Sequence Manager'.

- A Task cannot be created or executed without a Sequence being added to that Task.
- A Sequence is composed of one or more Actions. Actions are the commands that are carried out on Managed Computers.
- Multiple Actions can be chained sequentially in a Sequence in order to carry out complex task sets.
- Actions in a Sequence are executed consecutively from the top of the list down. If any Action in a Sequence fails then this acts as a roadblock and all subsequently listed Actions will not be performed.
- Once a Sequence has been created it can be added to a Task. Tasks are then deployed on the target computer or groups of computers
- Any Sequence can be used in more than one Task should the administrator require.

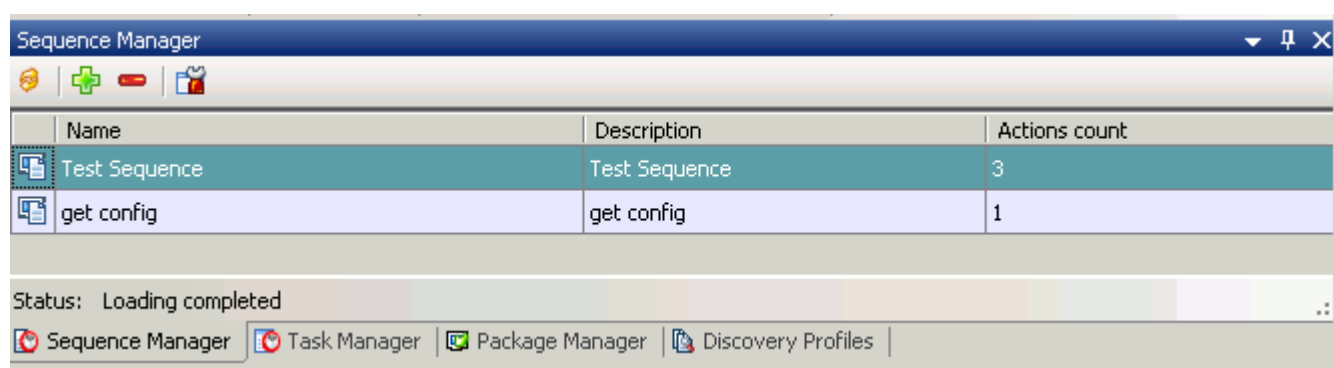
3.6.2 Opening the Sequence Manager window

Administrators can open the 'Sequence Manager' window in the following ways:


- Via the File Menu. Select '**View > Sequence Manager**' to open the 'Sequence Manager' window
- Via the shortcut menu button:






- Via keyboard shortcut. Press '**CTRL + ALT + S**' to open the 'Sequence Manager' window:

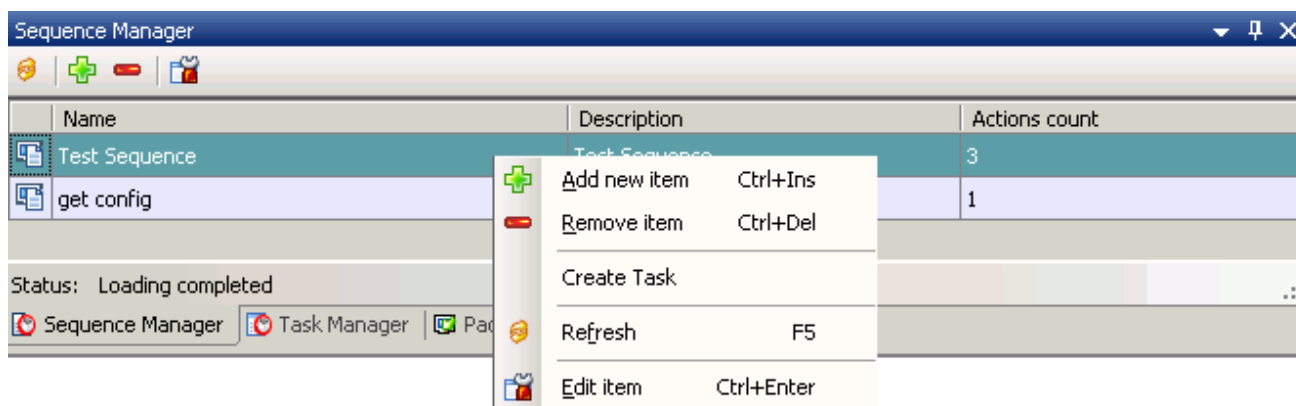


Sequence Manager – Window Specific controls:

Control's name	Description
 Refresh	Updates the list of displayed Sequences to reflect changes such as newly added sequences; removed sequences or modifications to existing Sequences.

	Add	Enables the user to add a new Sequence to the list. Opens the 'Add New Sequence' dialog.
	Delete	Deletes the selected Sequence
	Edit	Enables the administrator to edit the Sequence's parameters such as Name and Description and/or component Actions.

Right clicking on any sequence listed in the 'Sequence Manager' window will open a context sensitive menu that allows further configuration:



Context sensitive menu - Table of parameters

Action's name	Description
Add new item	Enables the user to add a new Sequence to the list. Opens the 'Add New Sequence' dialog.
Remove item	Allows the user to delete the Sequence.
Create Task	Allows the user to create a CESH 'Task' based on the selected 'Sequence.'
Refresh	Updates the list of displayed Sequences to reflect changes such as newly added sequences; removed sequences or modifications to existing Sequences.
Edit item	Enables the administrator to edit the Sequence's parameters such as Name and Description and/or component Actions.

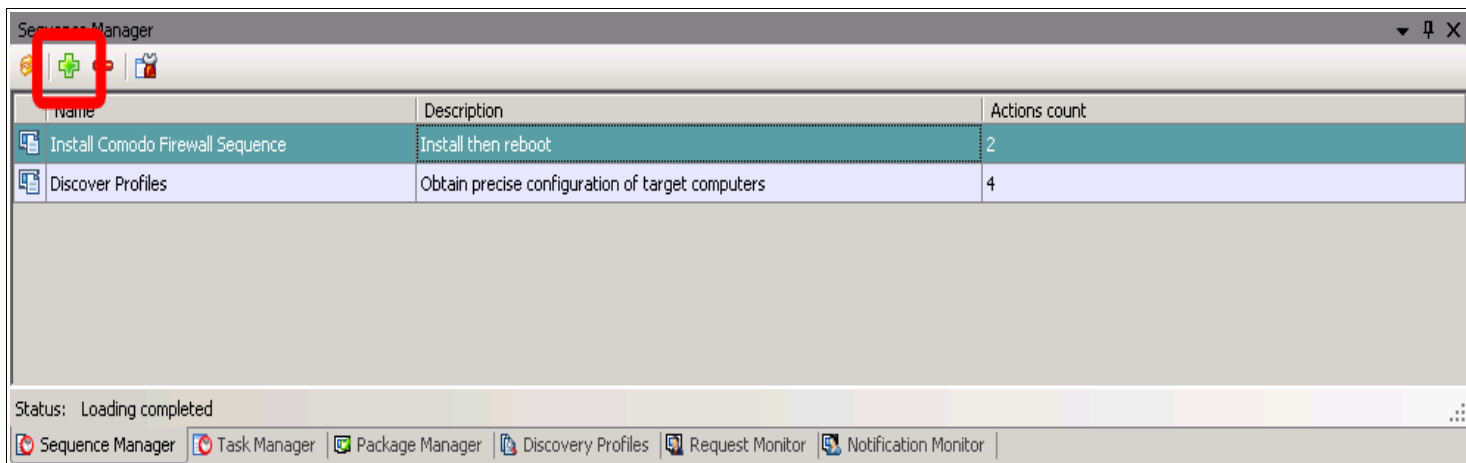
3.6.3 Creating a Sequence and Adding Actions to that Sequence

- **Prerequisites.** Because all Sequences of Actions are ultimately deployed onto networked computers via a CESH Task, administrators are advised to first:
 - Ensure that all Network Structures have been imported and that target computers have 'Managed' status *and* have the CESH Remote Agent Installed. For a tutorial explaining how to import network structures, see [Importing Network Structures](#). For more details on managing computers using the administrative console, see [The Computers and Group Manager Windows](#). For more details on assigning managed status to computer, see [Preparing Imported Computers for Remote Management](#).

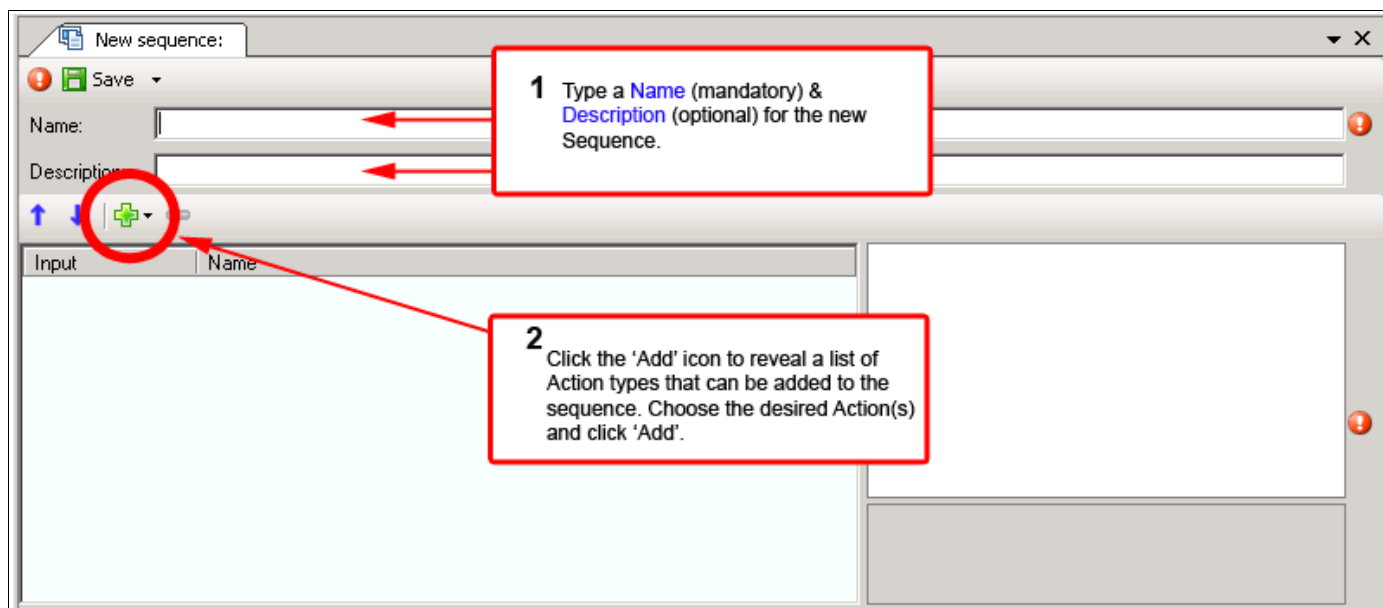
- The appropriate Comodo Packages (or third party packages) have been uploaded to the CESM Administrative interface.

To create a new Sequence:

- Open the 'Sequence Manager' window using one of the methods outlined earlier. At the Sequence Manager window, click the green 'Add' symbol (shown below).



- This will open the 'New Sequence' tab:



The following table contains more detailed descriptions of each of the Actions available within a Sequence.

3.6.3.1 Table of Actions – Definitions and Usage

Action Name	Description
Reboot the computer	Adding this Action to a sequence will reboot the target computer or group of computers. If the 'Reboot...' Action is part of a chain of Actions in a Sequence, then typically it is the final Action in that Sequence (for example Action 1 = Install Package. Action 2 = Reboot)

	<p><i>Required Parameters:</i> Shutdown Timeout. You should set actual reboot delay in seconds.</p>
Install package	<p>This Action enables the administrator to install a Comodo (or 3rd party) .msi package onto the target computers or group of computers (for example, this Action would be used to install Comodo Firewall Pro). This Action can only be executed if the appropriate CISM 'Package' has been uploaded to the interface. See section 3.4.The Package Management Window for more details.</p> <p><i>Required Parameters:</i> MSI package name to be selected by the administrator. See 'Adding a new package' for more details.</p> <p>Note: Some .msi packages may require the machine to be rebooted in order to complete the installation. Where this is the case, administrators should add the 'Reboot the Computer' as the last Action in the Sequence).</p>
Uninstall package	<p>Enables the administrator to uninstall Comodo (or 3rd party) .msi packages from a target computer or group of computers (for example, this command would be used to uninstall Comodo Firewall Pro prior to installation of an updated package. Alternatively, it could also be used to uninstall other, 3rd party, applications that are deemed surplus to requirements.)</p> <p>Note: Before running this Action, it is <i>advisable</i> that the administrator first establish which version of the package(s) are installed on target machine by running a Task containing a Sequence with an 'Installed Packages Discovery Profile' on the machine. For more details, see 'Discover Data' Action and section 3.5.The Discovery Profiles Window</p> <p><i>Required Parameters:</i> Behavior of the uninstallation action</p>
Control Windows service	<p>The 'Control Windows Service' Action enables the administrator to remotely stop, start, pause or continue a Windows service that is registered as present on a target computer.</p> <p>Note: Before running this Action, It is <i>advisable</i> that the administrator first establish which Windows services are running on the target machine by first running a Task containing a Sequence with a 'Windows Services List Discovery Profile' on the machine. For more details, see 'Discover Data' Action and section 3.5.The Discovery Profiles Window</p> <p><i>Required Parameters:</i></p> <ul style="list-style-type: none"> - Specification of Control Command to be issued to the Windows Service – either 'Start', 'Stop', 'Pause' or 'Continue') - Specification of the Name of the Windows service to be controlled by the command.
Discover data	<p>The 'Discover Data' Action allows administrators to collect system information about Managed computers in a network. Once in possession of this data, administrators can make informed decisions about the configuration policy that they wish to take on those Managed computers. There are four types of 'Discover Data' known as 'Discovery Profiles' – one of which must be selected as a parameter of the Action when creating the Sequence:</p> <ul style="list-style-type: none"> • OS Version – Fetches Operating System information from target computers • Windows Services List – Collects a list detailing the Name and State of Windows services on a target machine • Installed Product List – Fetches a list of all Comodo and 3rd party packages installed on a target machine (specifically, those applications that were installed with a .msi installer) • CFP Config – Collects the current configuration settings for Comodo Firewall Pro on target machines <p>Once a 'Discover Data' Action has been run, the information is returned to the CISM console and can be viewed (i) By selecting the specific Discovery Profile in the 'Discovery Profiles' window (ii) By right clicking on an individual Managed computer or CISM Group in the 'Computers' or 'Group Manager' window and selecting 'Open Discovered Data'.</p>

	<i>Required Parameters:</i> Specification of type of Discovery Profile (OS version, Windows service list, Installed product list, CFP Config)
CFP Set Config	<p>The 'CFP Set Config' Action allows the administrator to roll out a specific configuration of Comodo Firewall Pro settings to individual or multiple computers in a network. These settings can be deployed at any point after the CFP package has been installed on those target machines.</p> <p><i>Required Parameters:</i> Administrator must specify the CFP configuration settings in the 'Settings Editor'</p>

- Select the Action or Actions you wish to include in the Sequence. In the example below we have chosen to add four 'Discover Data' Actions to the Sequence. For each of these 'Discover Data' Actions, we have selected a different 'Discovery Profile' by modifying the control in the 'Discovery Parameters' control to the right.

1 After choosing the Action 'Discover Data' you need to choose the 'Discovery Profile' from the 'Discovery Parameters' panel.

2 The chosen 'Discovery Profile' will appear as the 'Input' for the 'Discover Data' Action. Actions can be re-ordered using the blue arrows above the 'Input' header

Input	Name
(Installed products list)	Discover data
(Windows services list)	Discover data
(OS version)	Discover data
(CFP Config)	Discover data

Discovery parameters
Discovery Profile: **Installed products list**

- Click 'Save' to confirm your choices. This new Sequence can be viewed and/or modified via the 'Sequence Manager' Window:

Name, Description and Action Count of the Sequence that has just been created. This Sequence can now be called upon by a Task

Name	Description	Actions count
Install Comodo Firewall Sequence	Install then reboot	2
Discover Profiles	Obtain precise configuration of target computers	4
All Discover Profiles Sequence	Installed Products - Services - OS - CFP Config	4

- This Sequence is now available to be used as a Sequence (of Actions) in a Task . It is during the creation of a Task that the target computers for the Actions specified in the Sequence are chosen. Please see the next section [3.7.The 'Task Manager' window](#) for more details.

3.7 The 'Task Manager' window

3.7.1 Overview

A CESM 'Task' is comprised of a Sequence of Action(s) that is executed on a Managed Computer. The Task Manager window allows the administrator to execute any Task – thereby deploying the Actions defined in the Sequence in that Task (including sequences designed to install Comodo packages; install 3rd party .msi packages; implement Comodo Firewall configuration settings on all Managed network items; discover and control Windows services on those computers and more.)

- A Task cannot be created or executed without a Sequence first being added to that Task. Before attempting to create a task, please ensure that you have created at *least one* Sequence.
- Executing a Task on a computer or group of computers means executing the Action or Actions that are contained in that Task's 'Sequence'.
- Tasks can be executed immediately or can be scheduled to run at a predetermined time (Daily, Weekly, Monthly, Once)
- A Task can only be executed on a Managed Computer which has the CESM Remote Agent installed upon it.
- A single Task may be executed on any Imported Network item - including individual computers; entire Active Directory Domains; entire Workgroups or all computers in a CESM 'Group' (of computers)
- The success or failure of a Task can be viewed in real-time from the Task Result Manager window. This window also contains a history of the results of all Tasks run in the past.

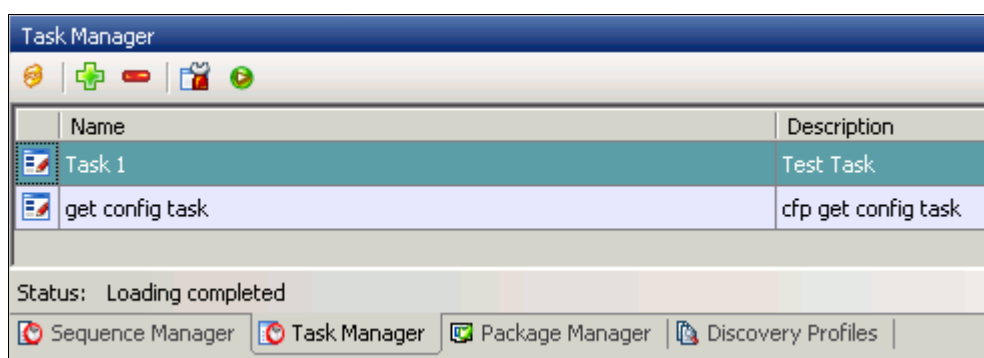
3.7.2 Opening the Task Manager Window

Administrators can open the 'Task Manager' window in the following ways:






- Via the File Menu. Select '**View > Task Manager**' to open the 'Task Manager' window
- Via the shortcut menu button:



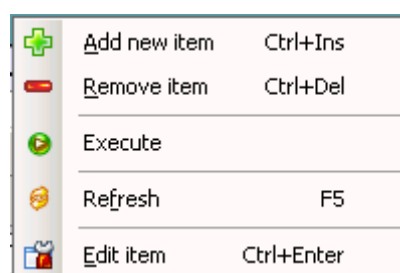
- Via keyboard shortcut. Press '**CTRL + ALT + T**' to open the 'Task Manager' window



Task Manager – Window Specific controls:

Control's name	Description
 Refresh	Updates the list of displayed Tasks to reflect changes such as newly added Task; removed Tasks or modifications to existing Tasks.
 Add	Enables the user to add a new task to the list. Opens the 'Add New task' dialog.
 Delete	Deletes the selected Task.
 Edit	Enables the administrator to edit task's parameters such as Name and Description and/or action, schedule.
 Execute	Runs the Task on the network items that were specified during the creation of the Task.

Right clicking on any selected Task in the 'Task Manager' window will open a context sensitive menu that contains the same controls as outlined above:



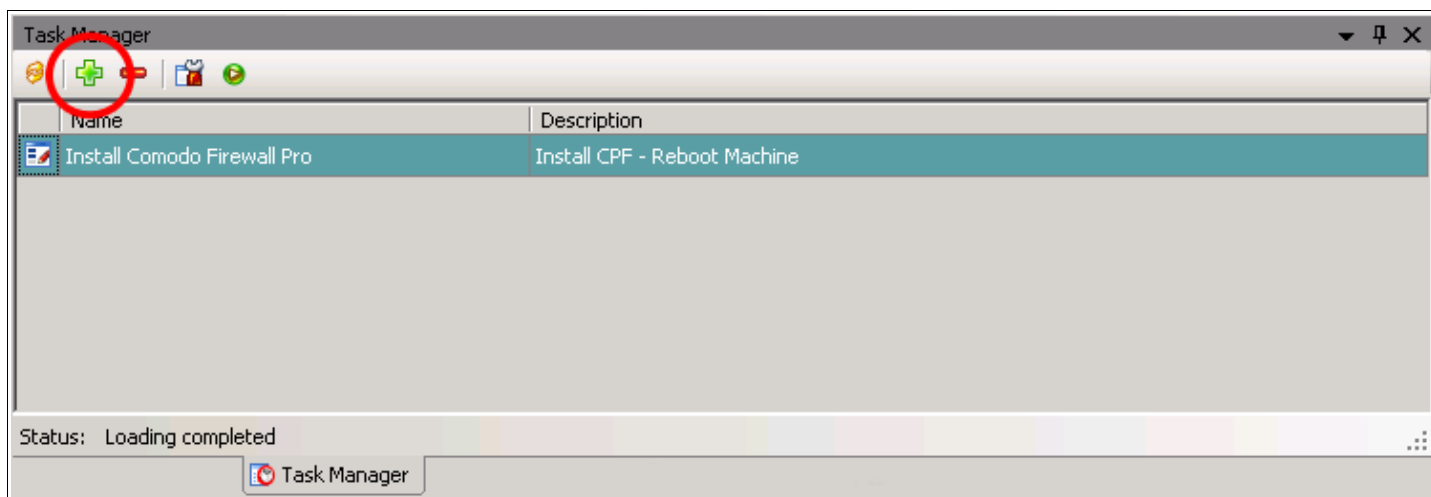
3.7.3 Creating and Executing a Task

Prerequisites. Before creating a CESM Task, administrators are advised to first:

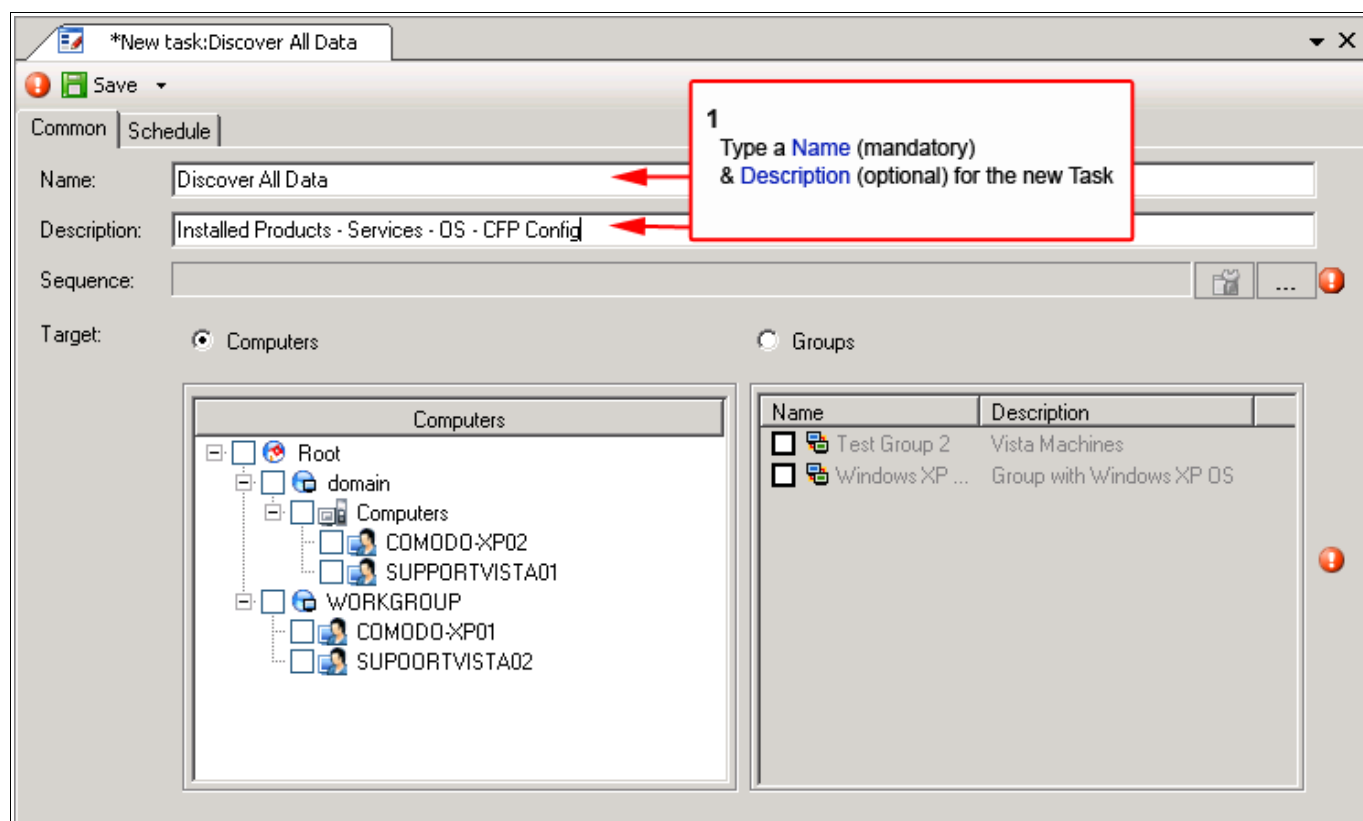
- Ensure that all Network Structures have been imported and that target computers have 'Managed' status **and** have the CESM Remote Agent Installed. A Task can only be executed on Managed computers that are connected to the CESM Central Service via the CESM Remote Agent. For a tutorial explaining how to import network structures, see [Importing Network Structures](#). For more details on managing computers using the administrative console, see [The Computers and Group Manager Windows](#). For more details on assigning managed status to computer, see [Preparing Imported Computers for Remote Management](#).
- Ensure the appropriate Comodo [Packages](#) (or third party packages) have been uploaded to the CESM Administrative interface. (This is required for certain Actions such as "Install Package")
- Ensure they have defined at least one [Sequence](#) containing at least one [Action](#) to be deployed on the imported, Managed Computers.

To create a new Task:

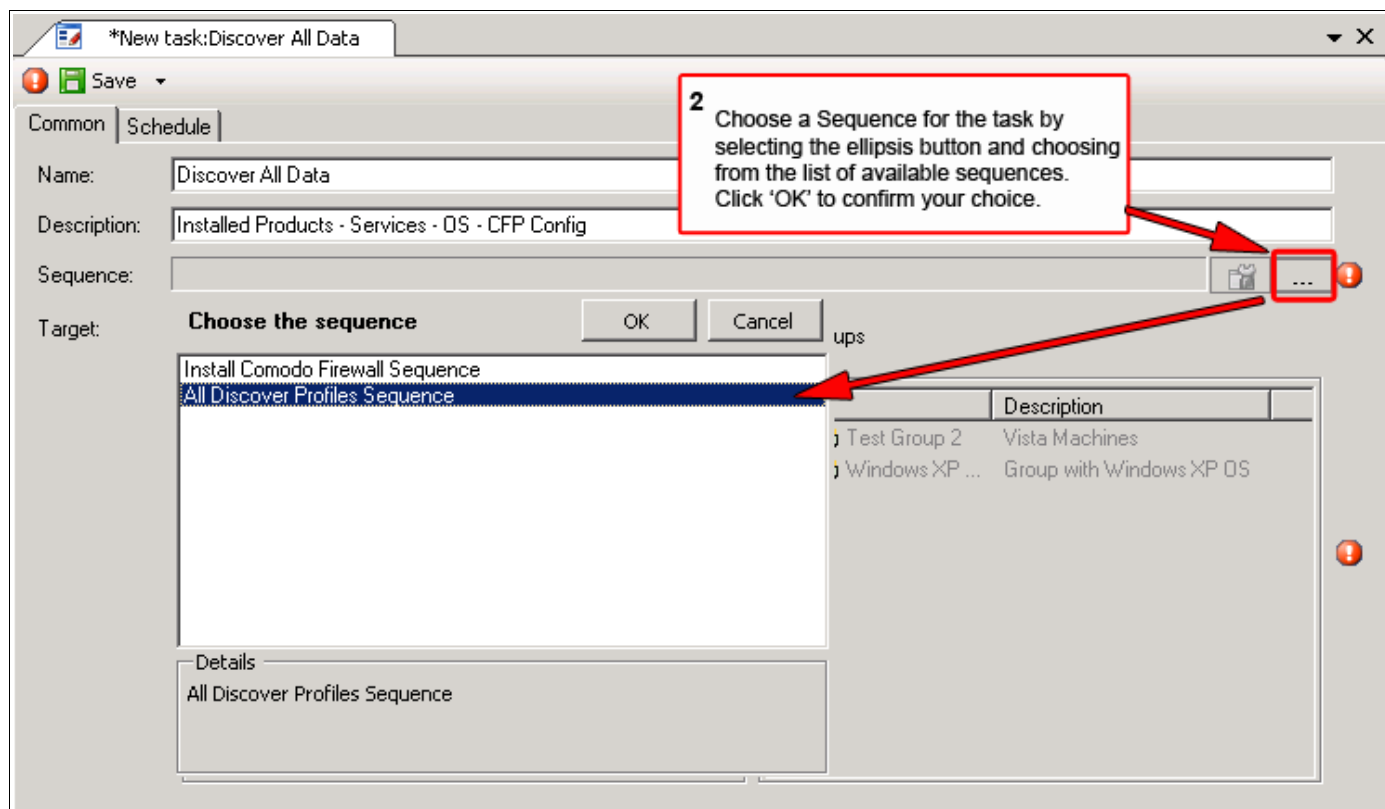
- Open the 'Task Manager' window using [one of the methods outlined earlier](#). This will open the Task Manager window. This windows displays all existing Tasks that have been created. To begin adding a new Task, click the green 'Add' symbol (shown below).



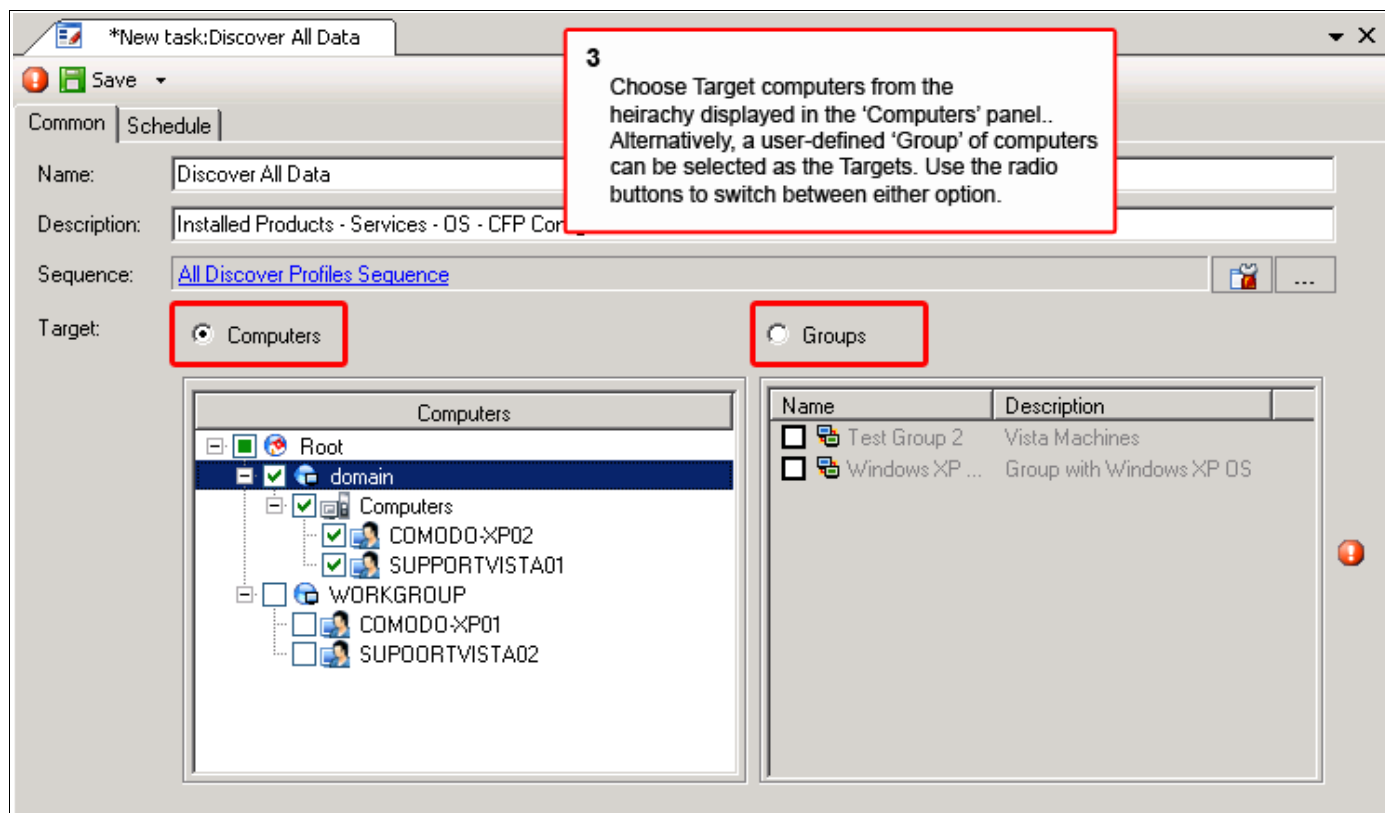
- This will open the 'New Task' dialog. Firstly create a Name and Description for the Task. Task 'Name's are mandatory – Descriptions are optional. It is good practice to choose Task Names that accurately describe the purpose of the Task (or more accurately, the purpose of the Action(s) within the sequence of that Task.)



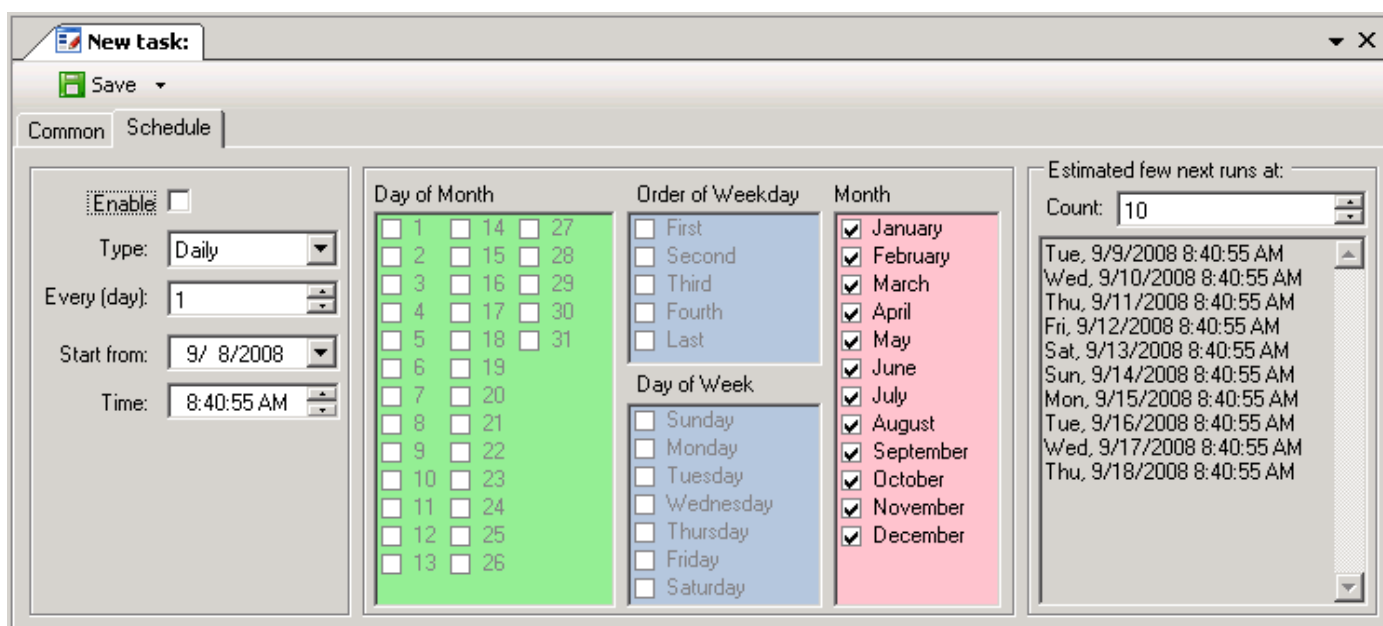
- Secondly, add the Sequence (of Actions) that this Task should implement. (If you haven't done so already, you should first create a Sequence and define Actions within that Sequence.) To select a Sequence, click the ellipsis button (...) at the end of the 'Sequence' field. This will open a list of existing Sequences:



- Next, choose the Target computers for the Task. Target computers can be selected using the 'Computers' panel at the lower left of the 'New Task' dialog. Alternatively, administrators can select a predefined CESM 'Group' of machines as the target for the task:



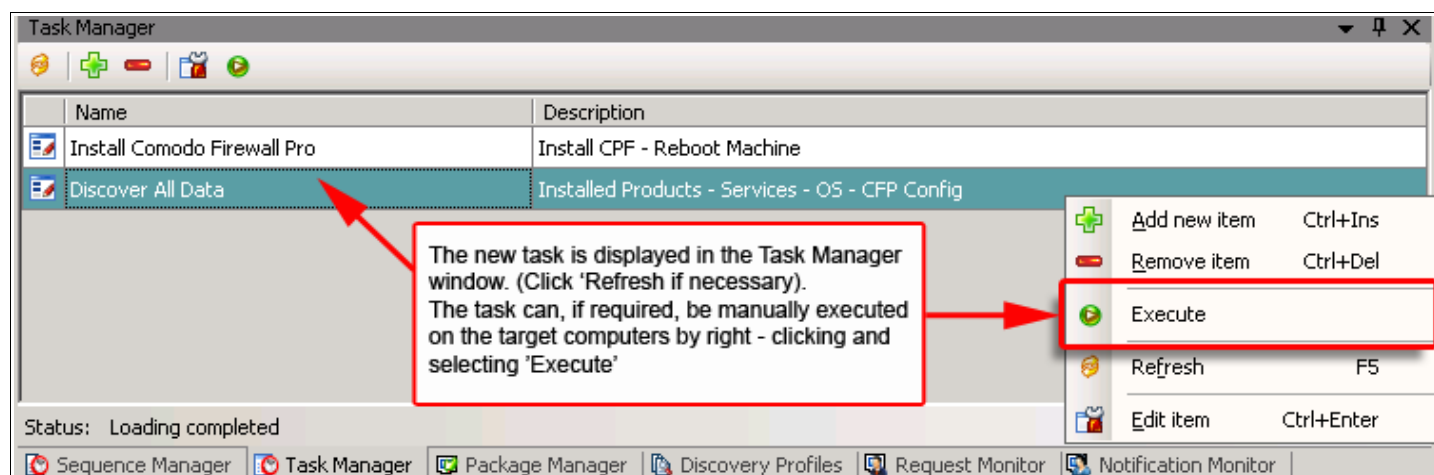
- Schedule the Task (**optional**). Administrators have the option to schedule a time and date for the execution of the Task by accessing the 'Schedule' tab of the 'New Task' dialog:



Form element	Type additional information	Description
Enable	Check-box	Enables scheduling of the task. Administrators must select this box in order to implement the Scheduling feature for the Task.
Type	Drop-down list	Tasks can be scheduled to execute: Daily – task is executed daily Weekly - task is executed weekly Monthly - task is executed monthly Once – task is executed single time at specific time and date.
Every (day):		The Task is executed between once every specified number of days. For example, if '2' is chosen then the Task is performed every 2 days at the specified time.
Start from:		Task execution start date.
Time:		Task execution time.
Day of Month	Check-box	Task is executed at specified day of a month.
Order of Weekday	Check-box	Task is executed at specified week of a month.
Day of Week	Check-box	Task is executed at specified day of a week.

Month	Check-box	Task is executed at specified months of year.
Estimated few next runs at:		Shows the timetable of the estimated next runs of the task. Default amount: 10

Once the administrator has successfully created and saved the new task, it becomes available in the Task Manager window:



After executing a Task, Administrators can check it's success or failure by opening the 'Task Result Manager'. Please see the next section for more details.

3.8 The Task Result Manager window

3.8.1 Overview

The 'Task Result Manager' window enables the administrator to view whether a Task executed on a target computer, network or CESM group was successful or not. If a Task failed for any reason, then the administrator can use this window to identify which particular Actions have failed and on which specific computers the fails occurred. Furthermore, administrators can quickly create a custom Task to re-run only those failed actions on the affected computers. The current status of any 'in-progress' tasks can be updated by clicking the "Refresh" button – allowing administrators to check the ongoing progress of a task and to estimate how much time remains before task completion.

3.8.2 Opening the Task Result window

Administrators can open the 'Task Result' window in the following ways:

- Via the File Menu. Select ' **History > Task Result**' to open the 'Task Result' viewer.
- Via the shortcut menu button:














- Via keyboard shortcut. Press '**CTRL + SHIFT + T**' to open the 'Task Result' viewer.

Result	Started	Completed	Status	Result Code	Message
Discover Profiles	9/15/2008 8:32:32 AM	9/15/2008 8:32:32 AM	Failed		
COMODO-XP02	9/15/2008 8:32:32 AM	9/15/2008 8:32:32 AM	Succeeded		
Discover data,(OS version)	9/15/2008 8:32:32 AM	9/15/2008 8:32:32 AM	Succeeded	0x00000000	
Discover data,(Windows services list)	9/15/2008 8:32:32 AM	9/15/2008 8:32:32 AM	Succeeded	0x00000000	
Discover data,(Installed products list)	9/15/2008 8:32:32 AM	9/15/2008 8:32:32 AM	Succeeded	0x00000000	
Discover data,(CFP Config)	9/15/2008 8:32:32 AM	9/15/2008 8:32:32 AM	Succeeded	0x00000000	
SUPPORTVISTA01	9/15/2008 8:32:32 AM	9/15/2008 8:32:32 AM	Failed		Target computer SUPPORTVISTA01
Discover data,(OS version)	9/15/2008 8:32:32 AM	9/15/2008 8:32:32 AM	Failed	0xFFFFFFFF	
Discover data,(Windows services list)	9/15/2008 8:32:32 AM	9/15/2008 8:32:32 AM	Pending	0x00000000	
Discover data,(Installed products list)	9/15/2008 8:32:32 AM	9/15/2008 8:32:32 AM	Pending	0x00000000	
Discover data,(CFP Config)	9/15/2008 8:32:32 AM	9/15/2008 8:32:32 AM	Pending	0x00000000	
COMODO-XP01	9/15/2008 8:32:32 AM	9/15/2008 8:32:32 AM	Failed		
SUPPORTVISTA02	9/15/2008 8:32:32 AM	9/15/2008 8:32:32 AM	Failed		
Install Comodo Firewall	9/9/2008 10:34:02 PM	9/9/2008 10:34:02 PM	Succeeded		
SUPPORTVISTA01	9/9/2008 10:34:02 PM	9/9/2008 10:34:02 PM	Succeeded		
Install package,Package CIS Pack...	9/9/2008 10:34:02 PM	9/9/2008 10:34:02 PM	Succeeded	0x00000000	
Reboot the computer,(0, "CESM ha...	9/9/2008 10:34:02 PM	9/9/2008 10:34:02 PM	Succeeded	0x00000000	

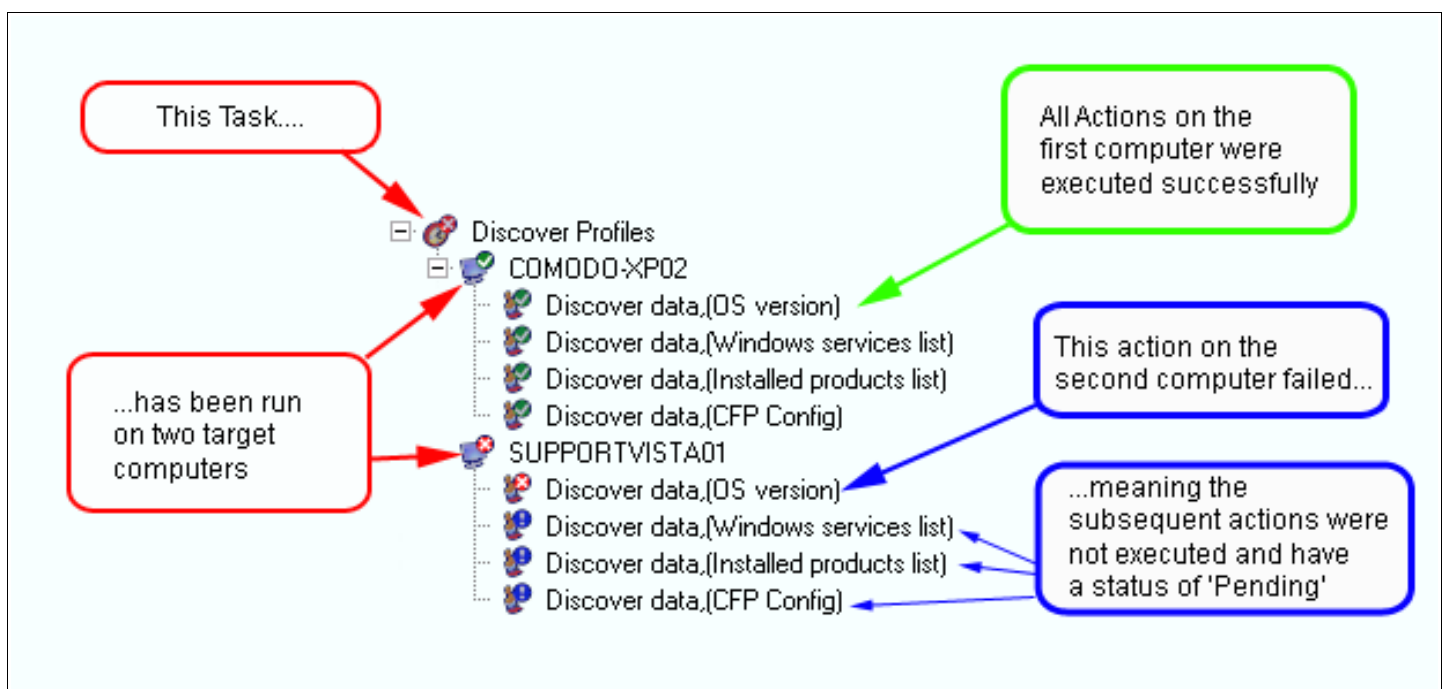
Every Task is represented as a row with the Task name, its success or failure status, its start and end time and other details. Expanding the Tree hierarchy will reveal the target computers within the Task and the Actions that have been, are being or will be executed on those target computers. To view the very latest status of any task, administrators should click the 'Refresh' button.

3.8.3 Task Result Manager – Table of Columns, Controls and Icons:

Control name	Description
 Refresh	Updates the list of executed and in-progress Tasks.
Results Column Icon	Description
	Task Status = Succeeded. Entire Task, including all component Actions in the Task's Sequence, were executed successfully on all target machines .
	Task Status = Executing. Task is currently being executed. This means at least one component Action on at least one target Machine in the Task has yet to be completed.
	Task Status = Failed. At least one Action on one target computer was not executed successfully
	Target Computer Status = Succeeded. All Actions on the named target computer were successfully executed
	Target Computer Status = Executing. At least one Action on the named target computer is currently being executed.
	Target Computer Status = Failed. At least one Action on the named target computer has failed to execute successfully.
	Action Status = Succeeded. The named Action has been executed successfully on the target computer.

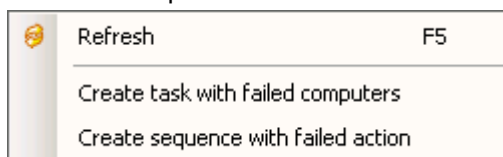
	Action Status = Pending. Can have two meanings. (1) CESH has not attempted to execute this action on the target computer because of the failure of an Action that preceded it. (2) This action is currently queued and will be executed after successful execution of the Action(s) that precede it in the Sequence
	Action Status = Executing. This Action is currently being executed on the target computer.
	Action Status = Failed. This Action has failed to execute successfully on the target computer. CESH will not attempt to execute any subsequent Actions that may have been listed in this task. All subsequent Actions will Automatically be given a status of 'Pending'.
Column Name	Description
Started	Displays the time that CESH began executing the Task or Action named in the 'Result' column.
Completed	Displays the time that CESH completed execution of the Task or Action named in the 'Result' column.
Status	Displays the status of the Task, Target Computer or Action listed in the results column Actions that were successfully completed have a status of 'Succeeded' Actions finished with an error have a status of 'Failed' Actions that are currently being executed have a status of 'Executing' Actions awaiting execution in a queue have a status of 'Pending'.
Result Code	Actions that failed to successfully execute will generate a specific error code. The administrator can reference this result code to help diagnose the problem. Actions that successfully executed always generate the code '0x00000000'
Message	An explanatory message associated with the Result Code described above.

The following graphic shows a simple example of a Task result as viewed through the Task Result Manager window:





As can be seen in the example above, the failure of a single Action on one target computer will mean that Task is given a status of 'Failed'.

Right clicking on any Task, Target Computer or Action listed in the 'Task Result Manager' window will open a context sensitive menu that provides further administrative options.



This context sensitive menu shown above allows the administrator to create a custom Task that is designed to (1) Run only on those machines that failed the original Task and (2) Run only those Actions that originally failed on those machines.

Task Result Manager – Context Sensitive Menu

Menu Option	Right Click on:	Description
Create task with failed computers	Any Task with a status of 'Failed' 	Enables the user to create a new Task with only the target computers for which Task execution was not successful. Opens the 'Add New task' dialog, with the 'failed' computers automatically pre-selected as the target machines. The new Task will not include any computers that passed the original task. Having addressed the issue causing the error, administrators can use this functionality to quickly roll out the same Sequence of actions to only those computers that were affected by the original issue without having to re-deploy to the entire network.
Create sequence with failed action	Any Target Computer with a status of 'Failed' 	Enables the user to create a new Sequence consisting of only those Actions from the original Task that returned a status of 'Failed' or 'Pending'. Selecting this option will open a new Sequence with those Actions already populated. The new sequence will not include any Actions which were successfully executed during the original Task. This feature can be used in combination with 'Create task with failed computers' to create a highly targeted Task that implements only those Actions that failed and only on those computers in the network which were affected by those fails. For example: An administrator wishes to deploy a Task on an Active Directory network containing 150 workstations. This Task contains a Sequence which consists of four actions. The first three are 'Install Package' Actions whilst the fourth is a 'Reboot' Action. On 145 of the workstations the Task is executed successfully. However, on the remaining 5, only the first two Actions successfully executed while the third failed (thus also preventing the execution of the fourth Action). Once the administrator has identified * and fixed the issue causing the error he or she can, using the 'Create Sequence with failed Action' feature, create a sequence consisting of just those third and fourth actions. This Sequence can then be added to a Task that was created using the 'Create Task with failed computers' feature. This task can then be deployed to execute only the previously 'failed' actions on only the 5 affected computers (out of the 150 in the network). This can be a great time saver in large networks. * To help identify problems on the target workstation, the administrator may wish to consider running one or more <u>Discovery Profile</u> Actions on those machines.
Refresh	Anywhere in the window	Updates the list of executed tasks.

3.9 The Notification Monitor window

3.9.1 Overview

The 'Notification Monitor' enables the administrator to view (and react to) all service status messages sent by CESM Central Service. 'Notifications' are messages sent to the CESM Administrative Console by the CESM Central Service in response to service related commands issued by the Administrative Console. A service related command issued by the CESM Administrative Console includes items such as installing or uninstalling the CESM Remote Agent on a target machine.

- The Notification Monitor window enables the administrator to view messages regarding the success or failure of commands issued to the CESM Central Service such as Install/Uninstall CESM Remote Agent
- The Monitor also displays warnings and critical messages sent by the Central Service regarding issues such as service connection status and service crashes.
- Administrators should take care to differentiate the Notification Monitor from the Task Result window (which is used to monitor the success or failure of user-defined Tasks such as the installation of Comodo Firewall Pro on target computers)
- Administrators will find the Notification Monitor especially useful when troubleshooting any issues relating to the installation of the CESM Remote Agent on target computers.
- The Notification Monitor is intended to quickly inform the administrator of the latest events. Once individual Notifications have been viewed/and or dealt with, the administrator has the option to clear them from the list.
- The Notification History window is a permanent archive of all Notification messages and can be referenced should the administrator wish to view messages that were removed from the Notification Monitor.

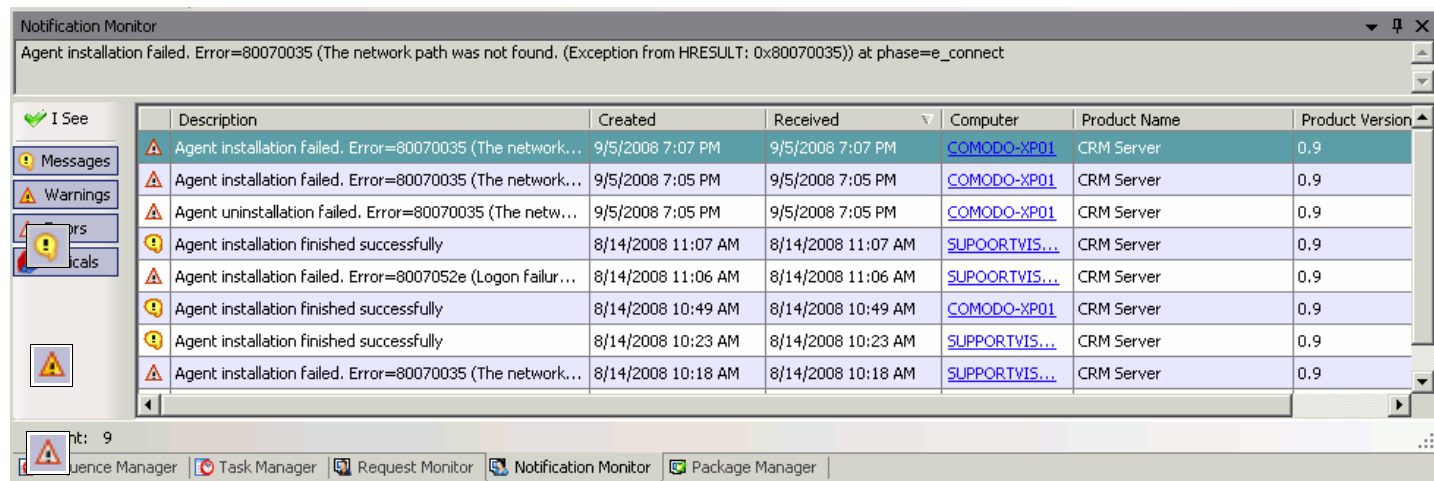
3.9.2 Opening the Notification Monitor

Administrators can open the 'Notification Monitor' window in the following ways:

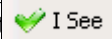
- Via the File Menu. Select '**View > Notification Monitor**' to open the 'Notification Monitor' viewer.
- Via the shortcut menu button:



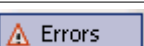



- Via keyboard shortcut. Press '**CTRL + ALT + N**' to open the 'Notification Monitor' viewer.



Notification Monitor – Table of Columns, Controls and Icons

Item Name	Type	Description
<i>(Message)</i>	Icon	Notifications that are classified as 'Messages' typically inform the administrator of the successful completion of a command on a target machine. For example, the successful installation of the Comodo Remote Agent on the computer that is named in the 'Computer' column.
<i>(Warning)</i>	Icon	Notifications that are classified as 'Warnings' alert the administrator to potential network issues that may impair CESH's ability to deploy Tasks and monitor Requests.
<i>(Error)</i>	Icon	Notifications that are classified as 'Errors' inform the administrator of the failure of CESH Central Service to execute a command on a target computer. For example, an 'Error' notification will be generated if CESH Central Service was not able to complete the installation of the CESH Remote Agent on the computer that is named in the 'Computer' column.
<i>(Critical)</i>	Icon	Notifications that are classified as 'Critical' alert the administrator to high severity errors that may or have already prevented CESH from functioning normally. For example, a critical application crash.
Description	Column header	A text description of the specific notification. In the case of notifications classified as 'Error' or 'Critical' (error), the description will also contain an error code and a precise description of the reason for the error.
Created 	Column header	Shows the time and date that the notification was generated by the CESH Central Service.
Received	Column header	Shows the time and date that the CESH Administrative Console received the notification from the CESH Central Service
Computer	Column header	The name of the workstation to which the notification pertains. Clicking on the target computer's name will open the 'Computers' window – allowing the administrator to quickly view details about the computer in question and/or issue further commands to that computer.
Product Name	Column header	Displays the name of the CESH product or service that generated the notification. In most cases this will be the CESH Central Service.
Product Version	Column header	Displays the version number of the product named in the 'Product Name' column.
	Control	The 'I See' button allows the administrator to mark the selected notification as 'viewed' and will remove the notification from the list. Notifications that are removed from the 'Notification Monitor' can, if needed, be accessed via the 'Notification History' window (which keeps a permanent record of all notifications).

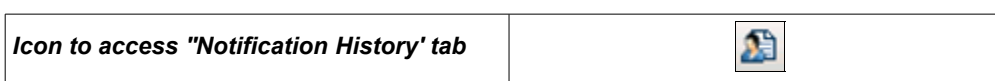
 Messages	Filter	Clicking the 'Messages' button enables the administrator to add all 'Message' notifications to the list of displayed notifications
 Warnings	Filter	Clicking the 'Warnings' button enables the administrator to add all 'Warning' notifications to the list of displayed notifications
 Errors	Filter	Clicking the 'Errors' button enables the administrator to add all 'Error' notifications to the list of displayed notifications
 Criticals	Filter	Clicking the 'Criticals' button enables the administrator to add all 'Critical' notifications to the list of displayed notifications

3.9.3 The Notification History Window

The Notification History window is a permanent record of all notifications that have been received by the CESM Administrative Console. Messages removed from the Notification Monitor can still be viewed using the Notification History window.

Administrators can open the 'Notification History' window in the following ways:

- Via the File Menu. Select '**View > Notification History**' to open the 'Notification History' viewer.
- Via the shortcut menu button:



- Via keyboard shortcut. Press '**CTRL + SHIFT + N**' to open the 'Notification Monitor' viewer.

3.10 The Request Monitor

3.10.1 Overview

The 'Request Monitor' window enables administrator to view and react to alerts from Comodo Packages that have been installed and are running on Managed computers. (Packages include CESM controlled Comodo applications such as Comodo Firewall Pro). Each request contains information sent by a Comodo product which requires the administrator's attention. Administrators can simply allow or block an activity or choose a predefined policy for the application which generated the activity. All answers supplied by the administrator are saved as rules on the target computer that originally generated the request – meaning there is no need to answer the same request many times. The administrator can also deal with requests in 'batches' by providing the same answer simultaneously to multiple requests. If a request is missed for any reason then the request will expire and the default answer will be automatically deployed to the computer. However, this answer will not be saved as the default behavior and a request of the same nature on the same computer will be reported to the administrative console as another request

- Each request has an expiration period. If administrators do not respond to a request before that request expires then the 'Default Answer' will be applied.
- An archive of all requests can be viewed in the 'Request History' window.

3.10.2 Opening the Request Monitor window

Administrators can open the 'Request Monitor' window in the following ways:

- Via the File Menu. Select '**View >Request Monitor**' to open the 'Request Monitor' viewer.
- Via the shortcut menu button:

Icon to access "Request Monitor" tab



- Via keyboard shortcut. Press '**CTRL + ALT + R**' to open the 'Request Monitor' viewer.

Request Monitor


AgeintID=8429; WinWord is trying to open TCP connection to 123.123.123.123 port 123

Description	Computer	Created	Expired At	Received	Product Name	Product Version
AgeintID=84...	WORKSTATION 1	11.09.2008 ...	11.09.2008 ...	11.09.2008 ...	CFP	3.0
AgeintID=84...	WORKSTATION 2	11.09.2008 ...	11.09.2008 ...	11.09.2008 ...	CFP	3.0
AgeintID=84...	WORKSTATION 1	11.09.2008 ...	11.09.2008 ...	11.09.2008 ...	CFP	3.0
AgeintID=84...	WORKSTATION 3	11.09.2008 ...	11.09.2008 ...	11.09.2008 ...	CFP	3.0
AgeintID=84...	WORKSTATION 3	11.09.2008 ...	11.09.2008 ...	11.09.2008 ...	CFP	3.0
AgeintID=84...	WORKSTATION 6	11.09.2008 ...	11.09.2008 ...	11.09.2008 ...	CFP	3.0
AgeintID=84...	WORKSTATION 4	11.09.2008 ...	11.09.2008 ...	11.09.2008 ...	CFP	3.0

Count: 363

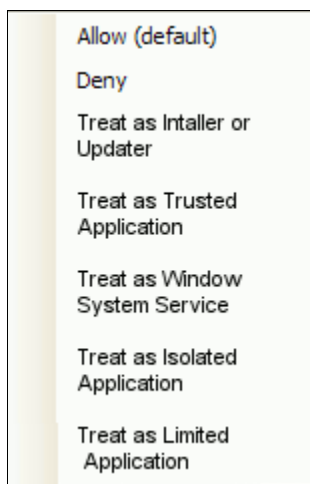
Notification Monitor Request Monitor

Request Monitor – Table of parameters

Column Name	Description
Description 	Enables the administrator to view detailed information about the request.
Computer	Enables the administrator to view the computer from which the request was received.
Created	Enables the administrator to view the date and time that the request was propagated on the computer listed in the 'Computer' column.
Expired At	Enables the administrator to view the time at which the request expired.
Received	Enables the administrator to view the date and time that the request was received by the CESM Administrative Console
Product Name	Enables the administrator to view the name of product that sent the request. (for example, Comodo Firewall Pro)
Product Version	Enables the administrator to view the version of product that sent the request.
Control	Description
Clear Expired	Enables the administrator to remove expired requests from the list by selecting the 'Clear Expired' button. (note – Requests that are removed from the Request Monitor can still be viewed in the 'Request History' window.
Response pane	Enables the administrator to react to the received request by selecting a preset response. The 'Allow' and 'Block' responses are always available for any request. There may also be additional response choices listed under the

default 'Allow' and 'Block' responses. The additional responses that are available for any one request are dependent on the nature of the request and on the product that propagated the request.

Right clicking on any Request listed in the 'Request Monitor' window will open a context sensitive menu that allows the administrator to select a response to an individual request or a batch of requests. Again, the contents of the context sensitive menu are dependent on the product that generated the request and the nature of that request. The example below shows the context sensitive menu for a particular type of request generated by Comodo Firewall Pro:



Context Sensitive Menu - default Options

Action's name	Description
Allow	Allows the request from the Comodo package running on the source computer
Deny	Blocks the request from the Comodo package running on the source computer

All remaining responses listed in the context sensitive menu are product specific. For example, 'Treat as Installer or Updater' is a response that is specific to Comodo Firewall Pro. It usually occurs when the user of the computer is attempting to install a new program that the Firewall does not recognize. It is, however, beyond the remit of this document to explain the nature of all possible product specific response options. In order to respond in an informed manner to such product specific requests, administrators are advised to familiarize themselves with the specific Comodo product and the user guide associated with that product. Guides for all products are available through the Comodo website or will be supplied upon request.

3.10.3 The Request History Window

The 'Request History' window is an archive of all received requests including all requests that the administrator has removed from the Request Monitor window.

Administrators can open the 'Request History' window in the following ways:

- Via the File Menu. Select ' **History >Request History**' to open the 'Request History' viewer.
- Via the shortcut menu button:

Icon to access "Request History" tab



- Via keyboard shortcut. Press 'CTRL + SHIFT + R' to open the 'Request History' viewer.

Answer	Answered	Status	Description	Computer	Created	Expired	Received
		Expired	AgeintID=842...	WORKSTATION 6	11.09.2008 5:21	11.09.2008 5:31	11.09.2008 5:21
		Expired	AgeintID=842...	WORKSTATION 2	11.09.2008 5:21	11.09.2008 5:31	11.09.2008 5:21
		Expired	AgeintID=842...	WORKSTATION 1	11.09.2008 5:21	11.09.2008 5:31	11.09.2008 5:21
		Expired	AgeintID=842...	WORKSTATION 3	11.09.2008 5:21	11.09.2008 5:31	11.09.2008 5:21
		Expired	AgeintID=842...	WORKSTATION 3	11.09.2008 5:21	11.09.2008 5:31	11.09.2008 5:21

Count: 54971

Request History – Table of parameters

The column structure and information available in the Request History window are similar to those in the [Request Monitor window](#) with the following two additions:

Column Name	Description
Answer	Enables the administrator to view the response that the administrator supplied in the Request Notification window. If the Request expired before a response was supplied then this cell will be blank.
Answered	Enables the administrator to view the time and date that the response identified in the 'Answer' column. If the Request expired before a response was supplied then this cell will be blank.

Administrators can update the list of currently displayed requests by right clicking anywhere in the 'Request History' window and selecting 'Refresh'.

4 Importing Network Structure

4.1 Section Overview

This section outlines the preliminary steps required to establish control of networked computers under Comodo End-Point Security Manager. Ultimately, any computer (or group of computers) must be designated as a CESM 'Managed' computer in order for an administrator to define and schedule tasks for the Comodo applications installed upon it. To complete this process, you will need to carry out the following steps:

- i. [Import networked computers into the CESM Administrative Console](#)
- ii. [\(Optional\) Create computer 'Groups' within CESM Administrative Console to simplify management](#)
- iii. [Assign 'Managed' status to those computers that you wish to control](#)
- iv. [Install the CESM Remote Agent on those Managed computers](#)

After completing steps (i) through (iv) you will have successfully finished the initial setup of your CESM configuration and can begin to set tasks for the Comodo applications installed on your chosen Managed machines. (Full details on each aspect of creating and setting Tasks can be found in 'The Administrative Console'. A walk through example can be found in 'Managing Computers using the CESM Administrative Console'

4.1.1 Initiating the import

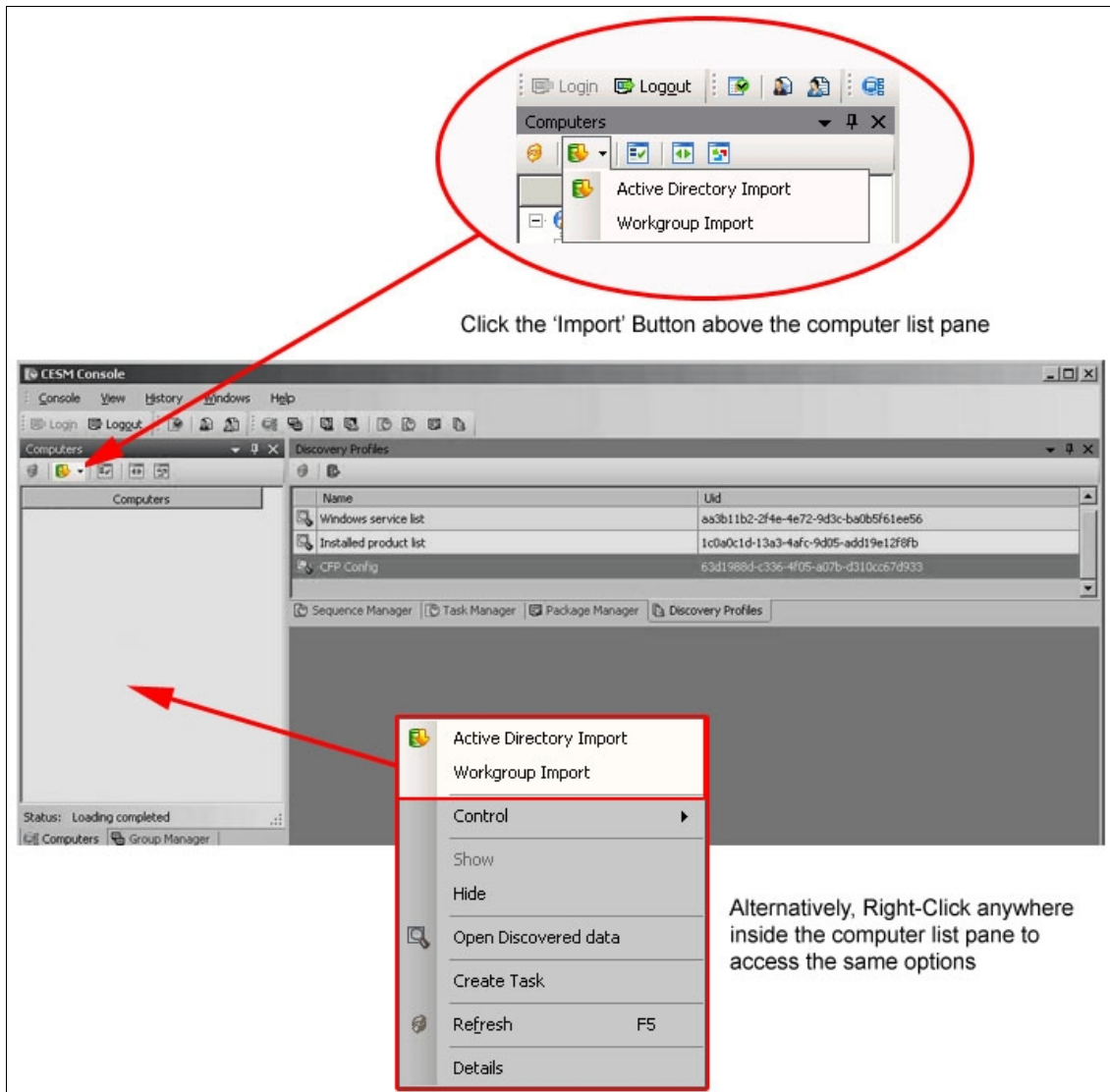
After successfully installing and logging into the CESM Administrative Console the first task an administrator should complete is to import their network structure. CESM allows administrators to import computers from two sources: Active Directory or from a Windows Workgroup.

To begin importing a network structure:

- Click the 'Import' button on the 'Computers' task bar above the Computer list pane

OR

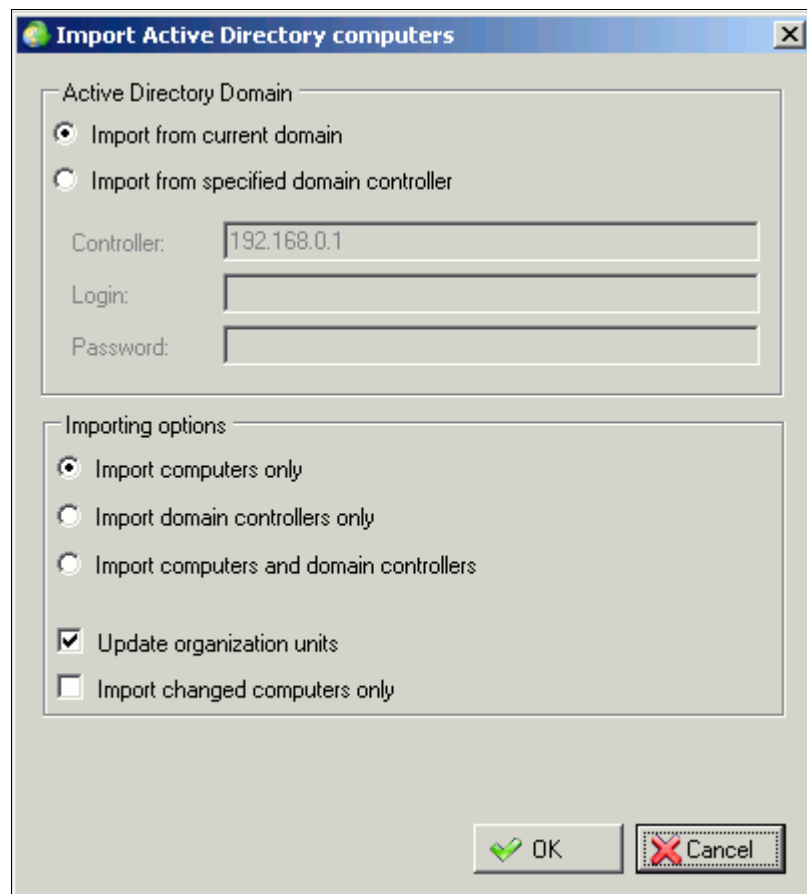
- Right-Click anywhere inside the Computer list pane to open the context sensitive menu
- Select a source from which to import a list of networked computers – either 'Active Directory Import' or 'Workgroup Import'



CESM can manage an unlimited number of networked computers so, administrators should repeat this process until all computers for which management is required have been successfully imported. Full explanations of importing using either source can be found in the following sections: [Importing from Active Directory](#) and [Importing from a Workgroup](#).

4.1.2 Importing from Active Directory

Choosing to [import computers](#) from Active Directory will open up the following preferences dialog:



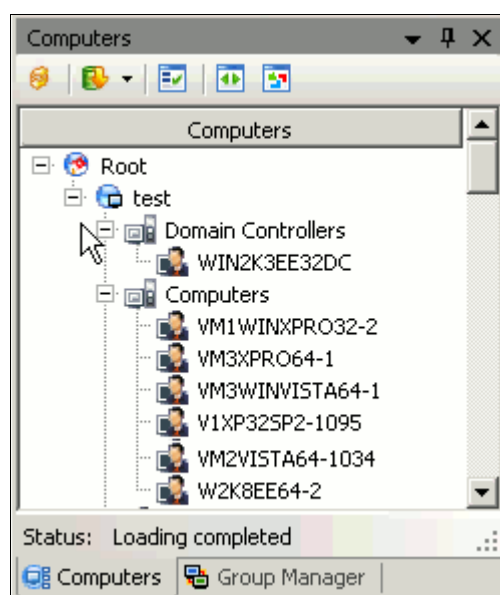
Active Directory Import – Table of Parameters

Active Directory Domain

Import from current domain (Checked by default)	Selecting this option will import all computers from the Active Directory domain that the administrator is currently logged into.
Import from specified 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:
Controller:	Administrators should enter the internal IP address of the Active Directory domain controller from which they wish to import.
Login:	Enter the user-name of a user with administrative rights to domain controller from which they wish to import.

Active Directory Import – Table of Parameters	
Password:	Enter the password of the user specified in the 'Login' field
Importing Options	
Import Computers Only	Selecting this option means that only computers will be imported from the domain specified in the 'Active Directory Domain' section. Domain controllers belonging to that domain will not be imported.
Import Domain Controllers Only	Selecting this option means that only domain controllers will be imported from the domain specified in the 'Active Directory Domain' section. Computers belonging to that domain will not be imported.
Import Computers and Domain Controllers	Selecting this option means that both computers and domain controllers will be imported from the domain specified in the 'Active Directory Domain' section.
Update Organizational Units (Checked by default)	Selecting this option means that organizational units' names (tree folders names) will be updated automatically.
Import Changed Computers only	Selecting this option means that only computers whose configuration has been modified will be imported.

When the Active Directory import process is finished, the full list of imported items will be displayed in a tree in the Computers pane of CESM manager:



Administrators now have the following broad options:

- **Add More Computers:** Administrators can add further computers to the list by repeating the Active Directory Import Process and/or using by using the Workgroup import process.

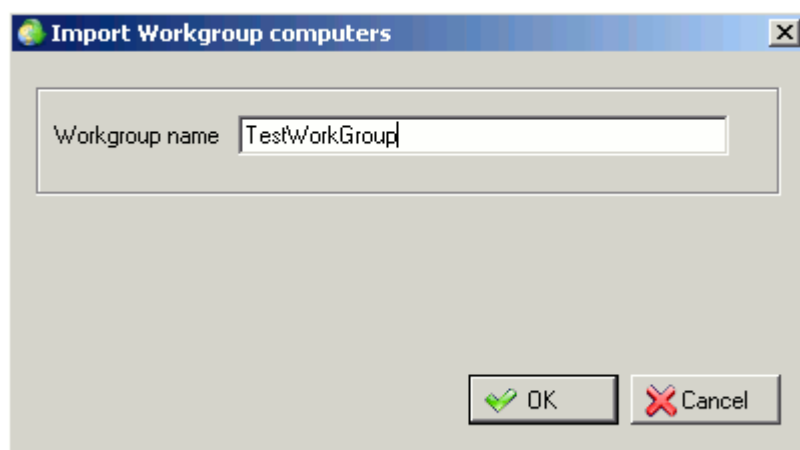
- **Create Groups from these Computers:** Creating user-defined groups of computers is perhaps the easiest and fastest way to roll out tasks to multiple machines or entire networks. Please refer to the section '[Managing Groups of Computers](#)' for more details on the steps involved in this process.
- **Manage these computers:** At this stage, all computers and/or domain controllers in the Domain have 'Unmanaged' status (Unmanaged status is indicated by the Grey color of the icon next to the computer's name). In order for CESM to establish control of these computers, two further actions must be taken:

(1) Assign 'Managed' Status to the computer(s). Full instructions on how to create Managed computers can be found in section [Assigning Managed Status to Imported Computers](#)

(2) Install CESM Remote Agent on the computers. Full instructions on installing Agents onto computers can be found in section [Installing CESM Remote Agent](#)

4.1.3 [Importing from a Workgroup](#)

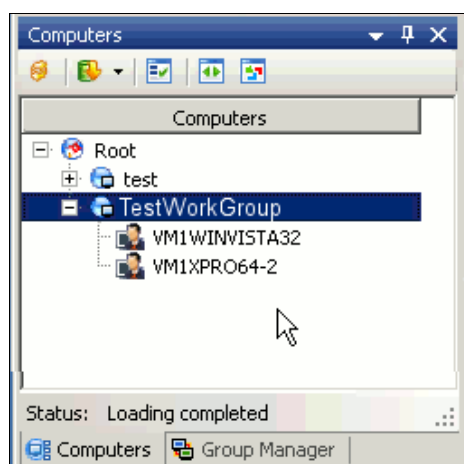
Choosing to [import computers](#) as Workgroup will open up the following preferences dialog:



Workgroup Import – Table of Parameters

Workgroup name	Administrators should enter the name of a network Workgroup which they wish to import. Clicking OK will import the computers belonging to that Workgroup into the Computer list pane.
-----------------------	---

When the Workgroup import process is finished, the full list of imported items will be displayed in a tree in the Computers pane of CESM manager:



Administrators now have the following broad options:

- **Add More Computers:** Administrators can add further computers to the list by repeating the [Active Directory Import Process](#) and/or using by using the [Workgroup import process](#).
- **Create Groups from these Computers:** Creating user-defined groups of computers is perhaps the easiest and fastest way to roll out tasks to multiple machines or entire networks. Please refer to the section '[Managing Groups of Computers](#)' for more details on the steps involved in this process.
- **Manage these computers:** At this stage, all computers and/or domain controllers in the Workgroup have 'Unmanaged' status (Unmanaged status is indicated by the Grey color of the icon next to the computer's name). In order for CESM to establish control of these computers, two further actions must be taken:

(1) Assign 'Managed' Status to the computer(s). Full instructions on how to create managed computers can be found in section [5.2.1.Assigning Managed Status to Imported Computers](#)

(2) Install CESM Remote Agent on the computers. Full instructions on installing Agents onto computers can be found in section [5.2.2.Installing CESM Remote Agent](#)

4.1.4 **Additional Information**



Work-group computers will not be imported if they are not powered on. Any Workgroup computers that were previously powered-off can be imported by re-running the 'Workgroup Import' process.

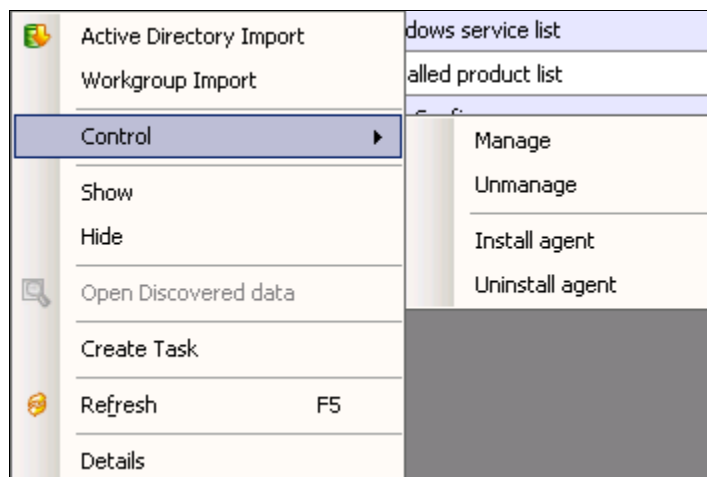


Any newly added computers can be imported into the list by re-running 'Active Directory Import' or 'Workgroup Import' using either of the two methods outlined above. (The list of computers displayed in the tree can also be refreshed by right clicking in the Computer List pane and selecting 'Refresh' from the context sensitive menu.

5 Workstation/Workgroup Management

5.1.1 Managing Computer tree items

Right-clicking on any computer or Workgroup in the Computer or Group Manager Windows will open a context sensitive menu that allows the administrator to directly manage that item:



5.1.2 Context management menu - Table of parameters

Action's name	Description
Active Directory Import	Imports the list of computers you want to manage from Active Directory. More...
Workgroup Import	Imports the Workgroup of computers you want to manage. More...
Control	<p>Manage – Assigns 'Managed' Status to the selected item</p> <p>Unmanage – Removes 'Managed' status from the selected item.</p> <p>Install Agent – Will initiate the CESM Remote Agent installation procedure on the selected item</p> <p>Uninstall Agent – Will initiate the CESM Remote Agent uninstallation procedure on the selected item</p>
Show	Hidden computers can be made visible at Computers' panel again by clicking the 'Show all' button.
Hide	Hides the selected item so that it is not displayed in the tree. This is handy, for example, should an administrator wish to hide unmanaged computers and only view 'Managed' computers. Note: Computers can not be deleted from the display, but in case they are not needed at the moment - they can be hidden.
Open Discovered data	Allow the administrator to view 'discovered' data about the selected item. Discovered data includes OS version, Windows service list, Installed product list, CFP Config.
Create Task	Allows administrators to start the New Task process for the selected workstation, unit or group.
Refresh	Updates the list of computers displayed in the tree from the CESM server.

Details	Allows the administrator to view details for the selected object such as Name, GUID, SID, Creation date, Date of last modification, DNS (for workstations only), Status (for workstations only)
---------	---


Most of the actions in the table above are also available for tree nodes, which means that the Action will be applied to every computer in the branch below.

The number of simultaneously managed computers is limited by CESM License.

Usage of 'Expand all' and 'Collapse all' buttons makes exploring the Computers tree even more convenient.

5.1.3 Managing groups of computers

If you need to perform any actions on a set of workstations, especially if you need this set more than once – the best way is to create a group.

 Note, if a group of computers is changed it will be reflected in existing tasks scheduled for this group.

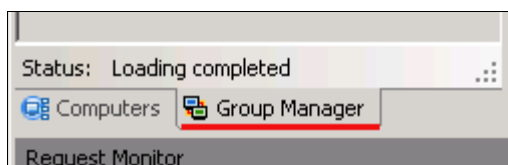
5.1.3.1 Creating groups

You can create your own groups of desired computers and assign them as a target for:

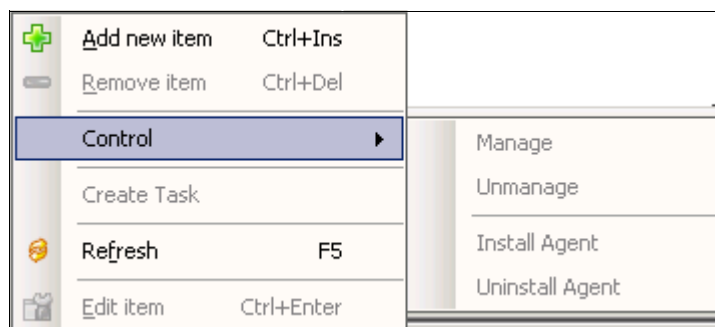
- Execution of tasks
- Setting status of computers to “managed”
- Installation of CESM Agent.

To create new group:

- Switch to Group Manager tab.



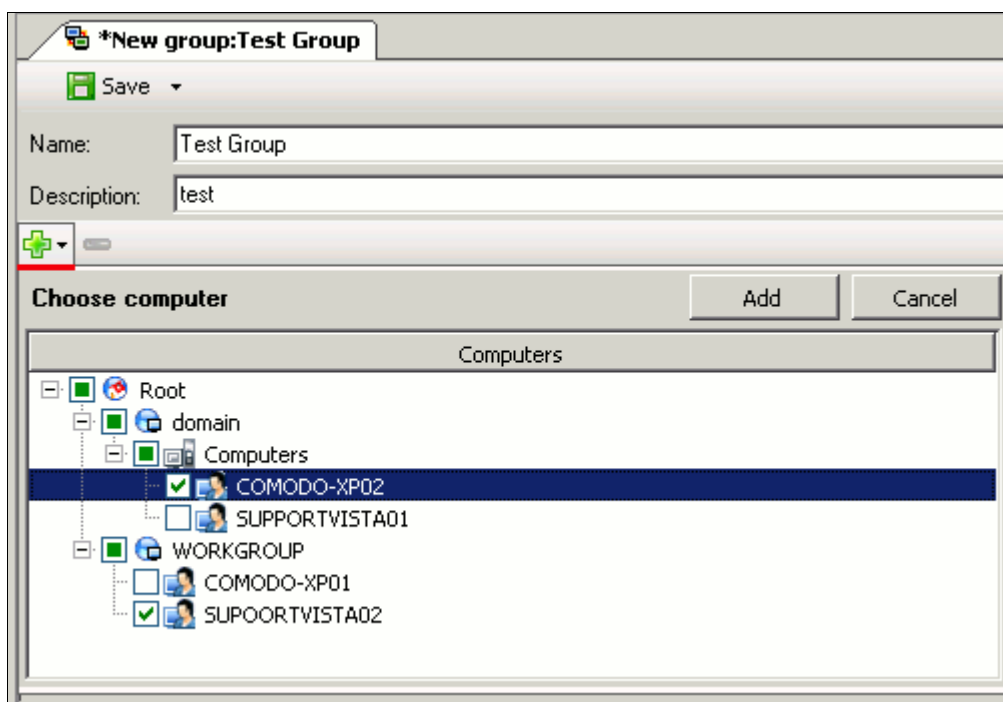
- Right-click to open the context sensitive actions menu:



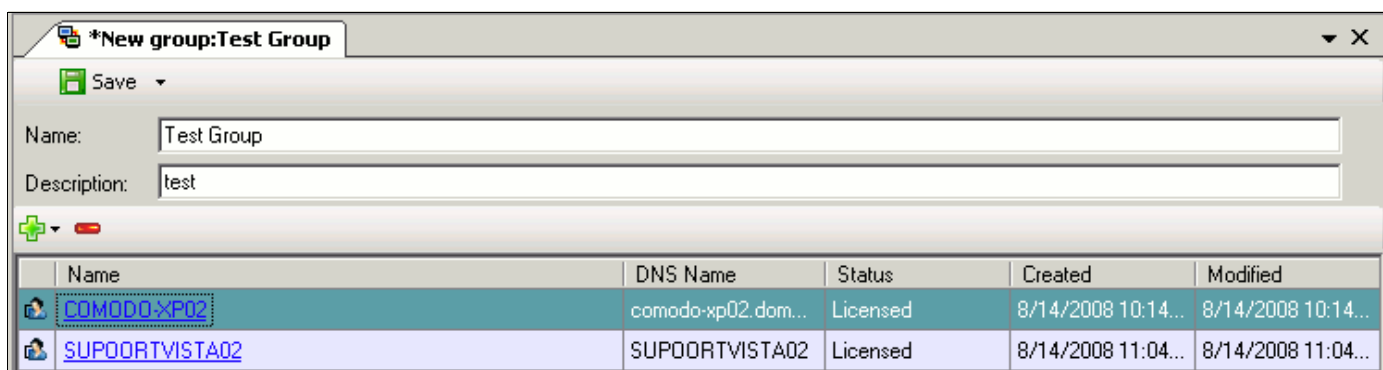
- Point to and click 'Add new item'.
- This will open the 'New Group' dialog box. Fill out the form that appears, specifying the new group's name and description.:



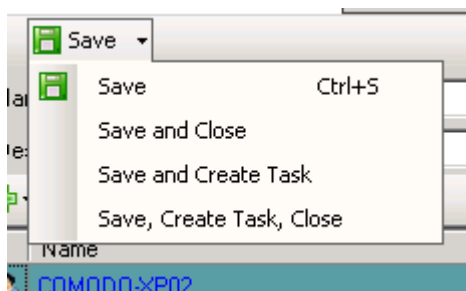
v. To begin adding computers to this new group, click the green 'Add Computer' symbol as shown:



vi. Check off those workstations, controllers, domains and/or Workgroups you want to combine in this group then click the 'Add' button to the right. The list of computers you selected as members of this group will be displayed in the list of group members:

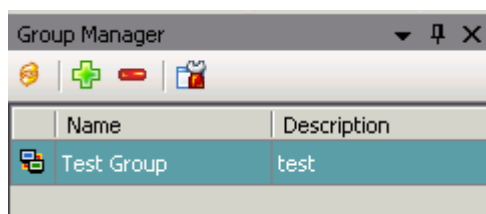


vii. Next, click the 'Save' button or select one of the following Save options:



Tip: The 'Save' button has “smart saving” ability. Administrators that are familiar with the Administrative Console can select 'Save, Create Task, Close' to immediately begin the Task creation process with this Group pre-selected as the target.

viii. This new group appears in the Group Manager pane. It can now be referenced as the target of new tasks when creating or editing new tasks.

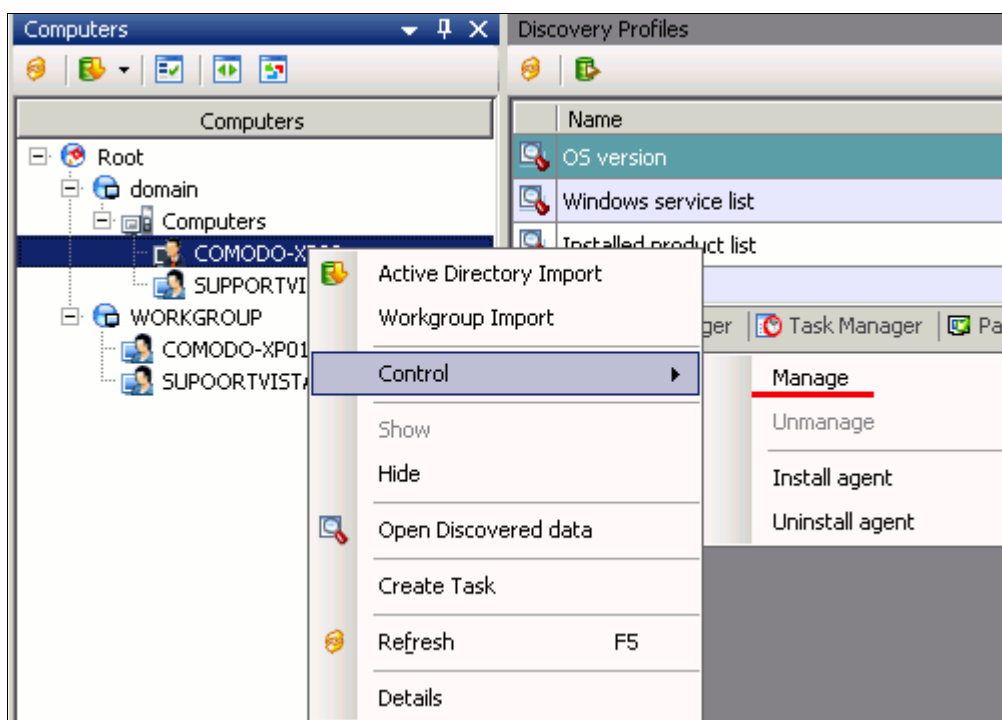


5.2 Preparing Imported Computers For Remote Management

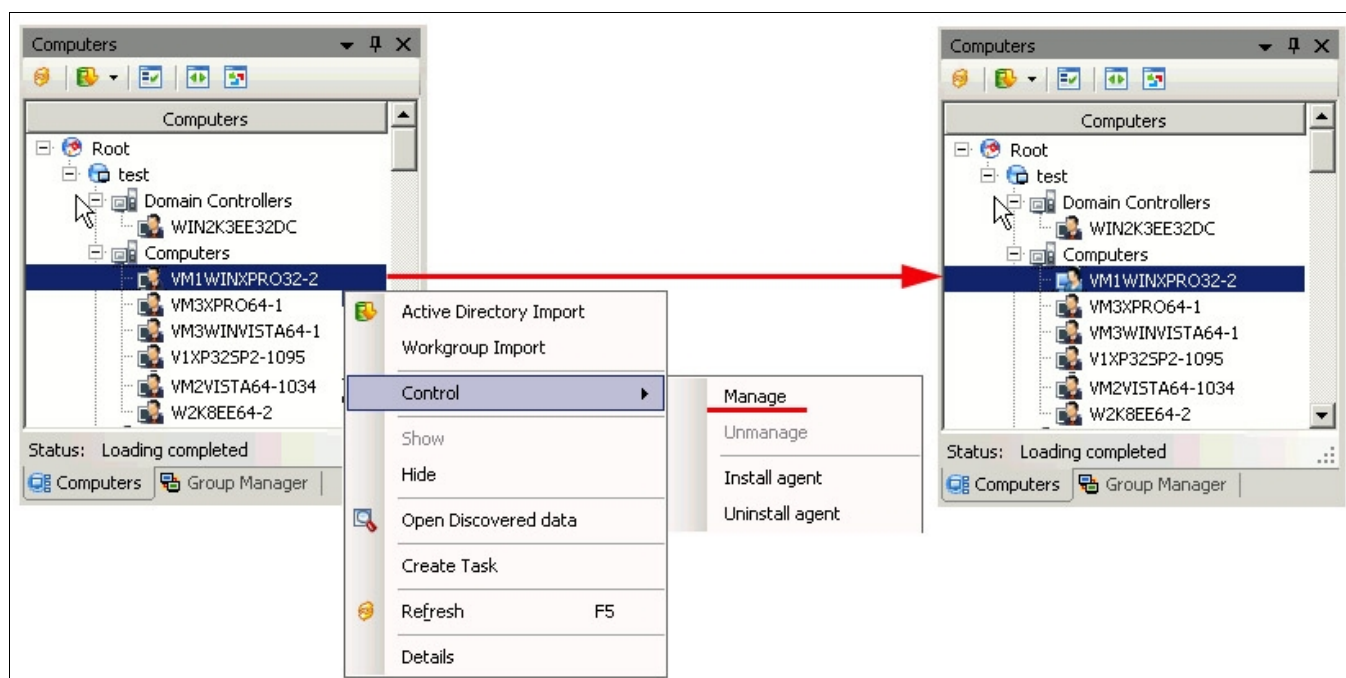
In order to manage remote computers from the CESM Administrative Console, each computer must be assigned 'Managed' status and have the CESM Remote Agent Installed upon it. A CESM 'Managed' computer means that Central Service can send and receive data to and from the CESM Agent installed on it.

5.2.1 Assigning Managed Status to Imported Computers

Once imported, assigning Managed status to a computer, Domain, Workgroup or user-defined CESM Group of computers is simply a case of right-clicking on the item you wish to manage and selecting 'Control > Manage':



Assigning 'Managed' status to a machine will change the color of the icon representing that machine from Grey to Light Blue:



- Entire Domains / Workgroups or user-defined groups of computers can be assigned 'Managed' status by selecting the name of the domain or Workgroup at the top of the tree, right-clicking and selecting 'Manage'.
- Similarly, Managed items can be stripped of their status by right clicking on the item(s) and selecting 'Unmanage'

- It is only possible to manage as many computers as are specified by your license agreement. CESM will warn and prevent you if you attempt to manage more items than are permitted by your license.
- **Important:** After assigning 'Managed' status to a computer, Administrators still need to ensure that they have installed the Comodo Remote Agent on that computer to establish control of the item. See [Installing Remote Agents](#) for more details

5.2.2 Installing CESM Remote Agent

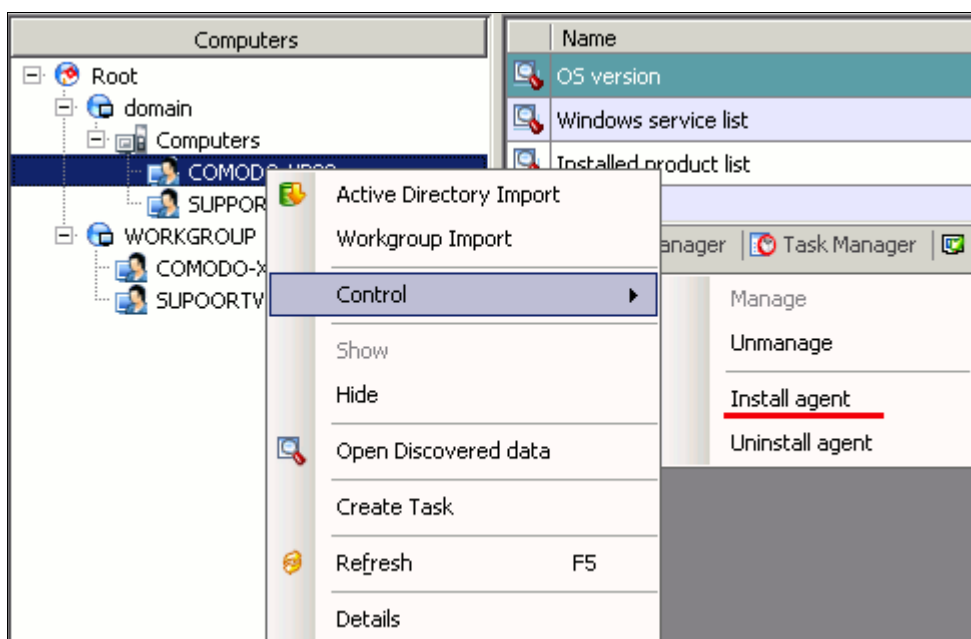
Installing the CESM remote agent is the second step towards managing a remote computer using the Administrator interface (the first being to designate that computer as a Managed Computer). The CESM Agent component must be installed on every remote computer that you wish to manage. This section describes how to install the agents onto managed PC's directly from the Administrator interface.



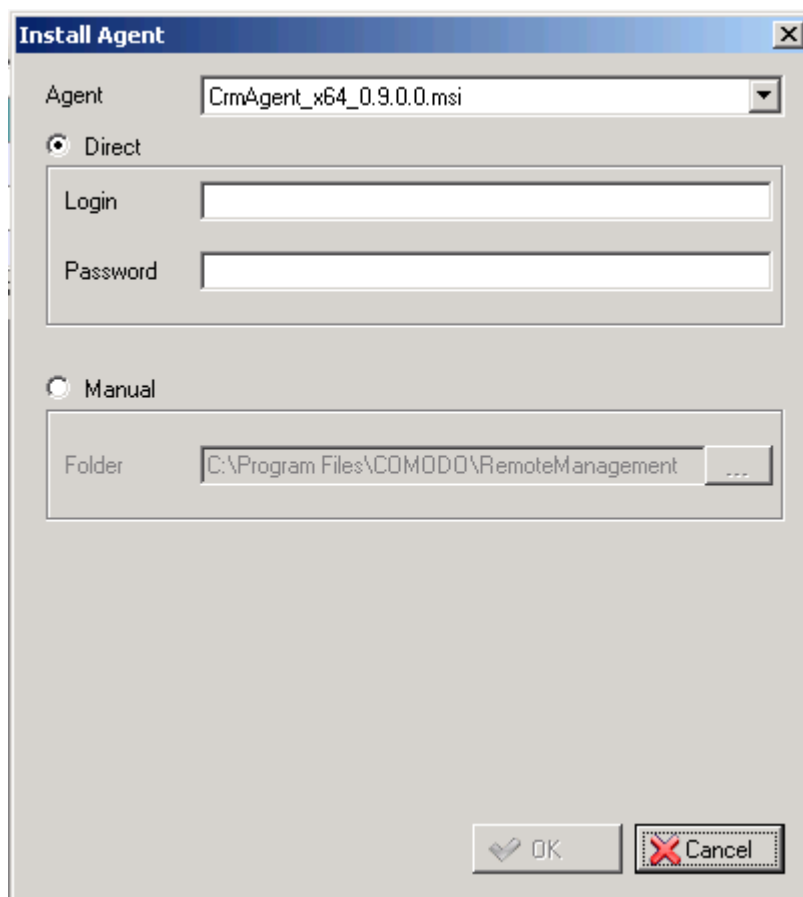
Another Reminder: CESM Remote Agent should only be installed only on computers that have been successfully designated as a 'Managed Computer' in the CESM Administrative Console. If you haven't done so already, you first need to assign 'Managed' status to the computer(s) you wish to control. For more details, please refer to section [5.2.1. Assigning Managed Status to Imported Computers](#)

To install the CESM Remote Agent on a Managed computer:

- Open the CESM Administrative Console.
- Right-click on the Managed Computer (or group) that you wish to install the agent on
- From the context sensitive menu, select Control > Install Agent.



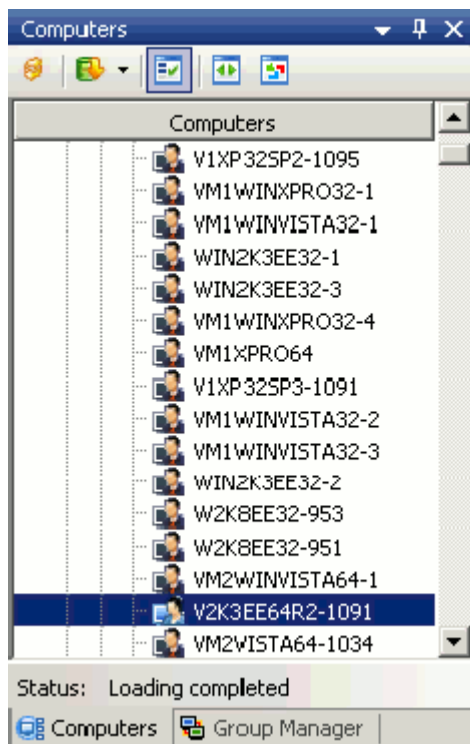
iv. Selecting 'Install Agent' from the context sensitive menu will open the 'Install Agent' configuration dialog:



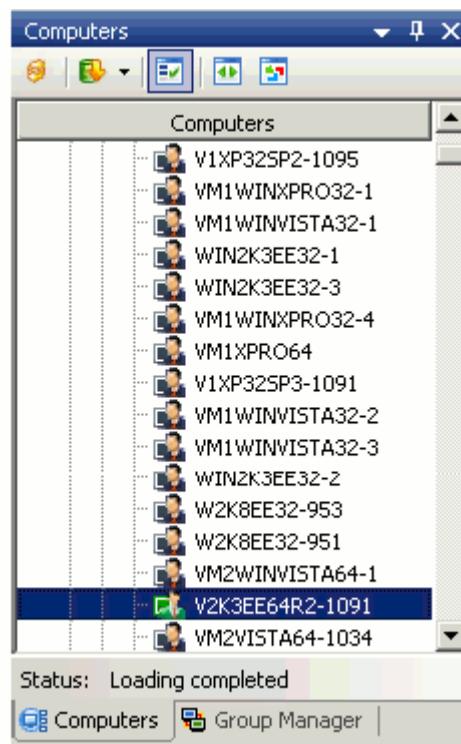
At the 'Install Agent' configuration dialog:

- Select the version of the agent you wish to install from the Agent drop down menu (see [5.2.2.1.About Agent Versions](#) should you need more details)
- Enter the local administrator login name and password for the target Managed Computer (use the format 'user@domain' in the 'user' field for computers imported with Active Directory).
- Click 'OK' to connect to the Managed PC and install the agent
 - For successful installation of the Agent, the user (whose user name and password were entered in the dialog shown above) should have administrator privileges on the remote Managed computer.
 - Each Agent is bound to the Central Service that executed its installation. It is not possible to manage computers through Agents that were installed by another instance of CESM Central Service.

After the CESM Agent has been installed onto the target machine(s), the Agent will attempt to establish connectivity with the CESM Central Service. If the connection attempt is successful then the color of the icon representing that machine will change from Light Blue (Managed but not connected to Central Service) to Green (Managed and successfully connected to CESM Central Service) :



Managed. Agent not installed or not connected

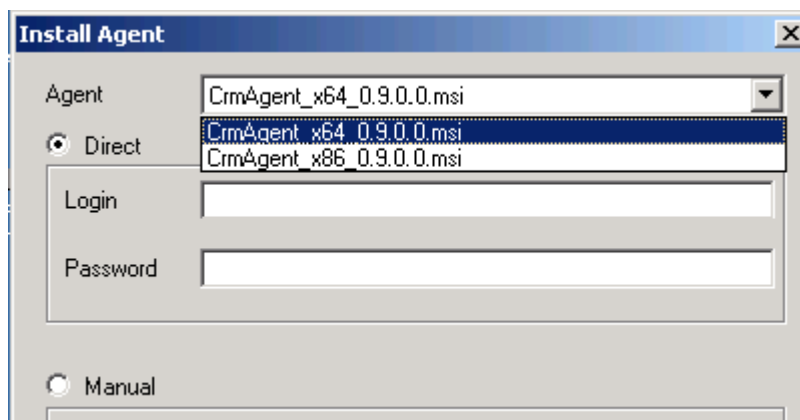


Managed. Agent installed and connected

Administrators can also check the “Notification monitor” window in the Administrator Console interface to make sure Agent installation has been successfully completed.

5.2.2.1 About Agent Versions

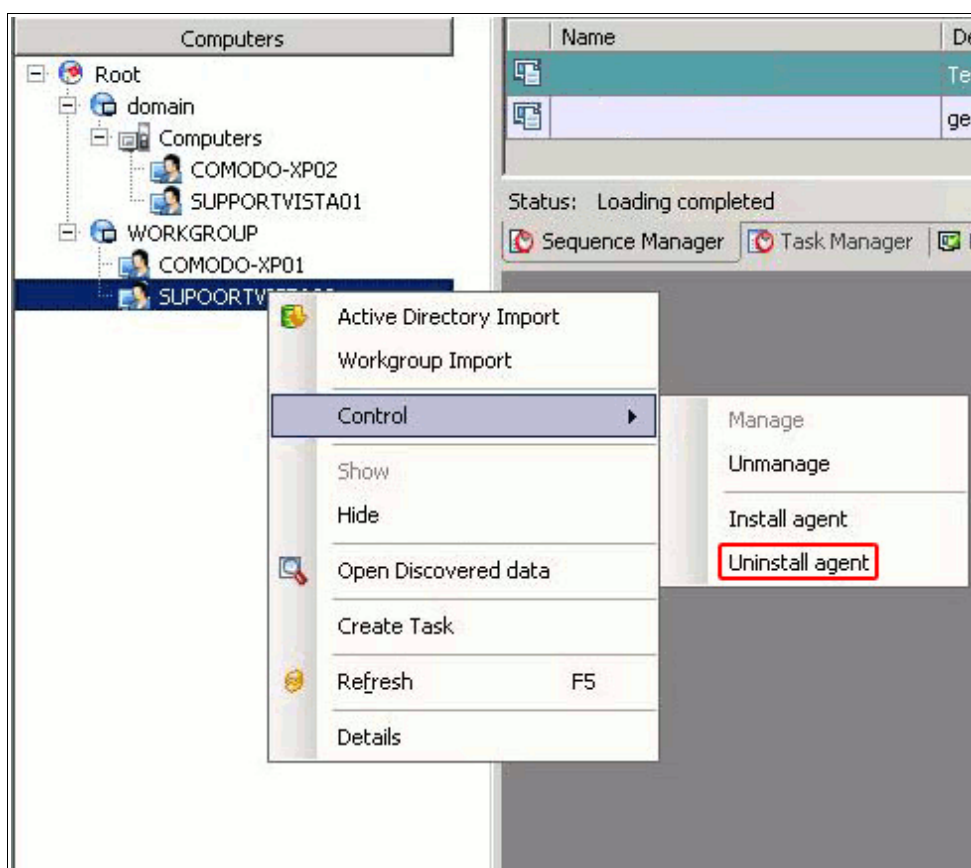
Comodo provides 32 bit and 64 bit versions of the Agent. Administrators should choose the appropriate version for the target Managed PC from the 'Agent' drop-down menu:



- For target Managed Computers with 32 bit operating systems select 'CrmAgent_x86_X.X.X.X.msi'
- For target Managed Computers with 64 bit operating systems select 'CrmAgent_x64_X.X.X.X.msi'

5.2.2.2 Uninstalling CESM Remote Agents

CESM Agents can be uninstalled by right clicking on the computer (or group of computers) and selecting 'Control > Uninstall Agent' :



- Uninstalling the Agent from a computer will mean Comodo products installed on that computer will no longer be manageable from the CESM Administrative Console – even if the computer retains it's 'Managed' status. All tasks scheduled to that computer will also fail. The CESM Administrator Console will, however, continue to attempt to run any tasks scheduled to that computer until such time as those tasks are deactivated.

6 Managing computers using the CESM Administrative Console

This section takes the form of a tutorial explaining how an administrator can install then monitor installations of Comodo Firewall Pro on networked computers. The step-by-step walk-through is intentionally high level and is intended as a complement to the more detailed explanations provided in section 3.

6.1 Prerequisites

- The Central Service and the Administrative Console have been installed. (See [Installing Comodo End Point Security Manager](#) for more details).
- The Network structure has been imported. (See [Importing Network Structure](#) for more details).
- To imported computers has been assigned status 'Managed'. (See [Assigning Managed Status to Imported Computers](#) for more details).

- The remote Agent on target workstations has been installed. (See [Installing CESM Remote Agent](#) for more details).
- All target computers have been powered on.
- Any versions of Comodo products, that were not designed to be managed by Comodo End Point Security Manager have been manually uninstalled from target machines. (This includes the .exe versions available for download from, for example, <http://www.personalfirewall.comodo.com>). CESM is designed to manage Comodo packages that have been installed using a .msi installer

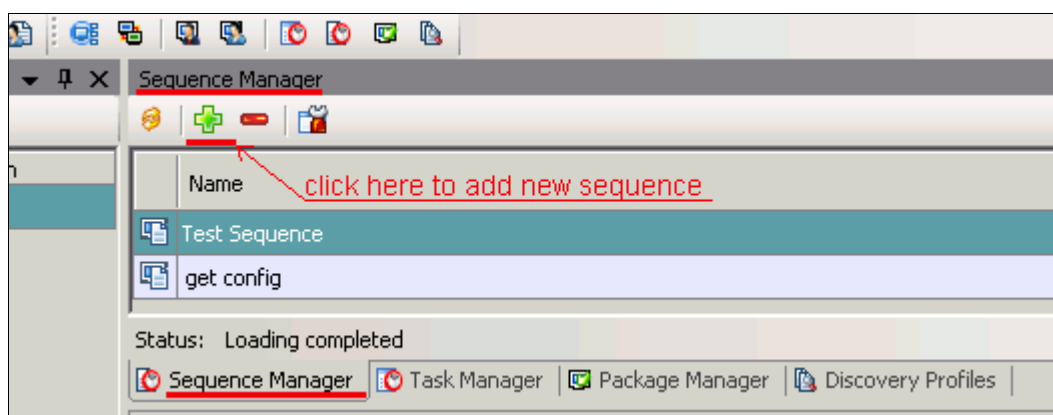
6.2 Installation and Management of Comodo Firewall Pro using CESM

6.2.1 Step 1. Run a full set of Discovery Profiles on the Managed Computers

While not essential to the deployment of Comodo Firewall, running a Discovery Profile Sequence on imported, Managed computers will provide administrators with very important configuration information about the computers they are about to manage using CESM. For a full description of Discovery Profiles, see section [3.5.The Discovery Profiles window](#)

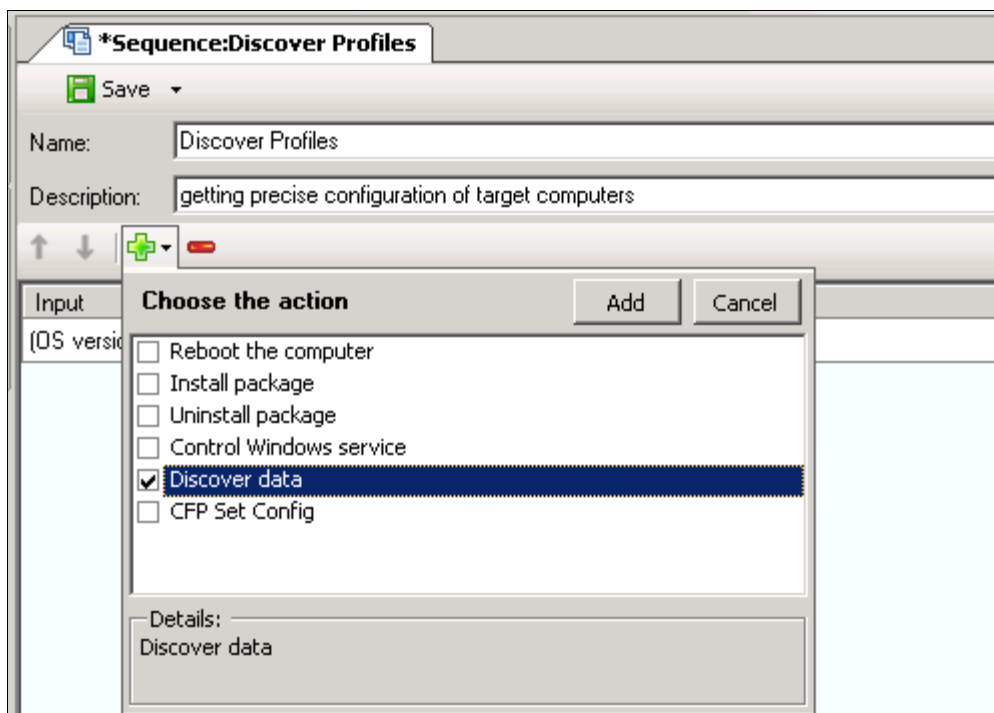
To run a set of Discovery Profiles:

- Open the 'Sequence Manager' window by selecting ' View > Sequence Manager'
- Click the 'Add New Sequence' Icon (highlighted below).

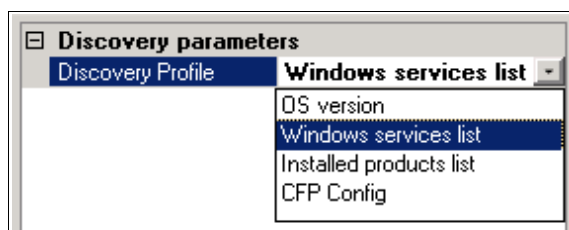
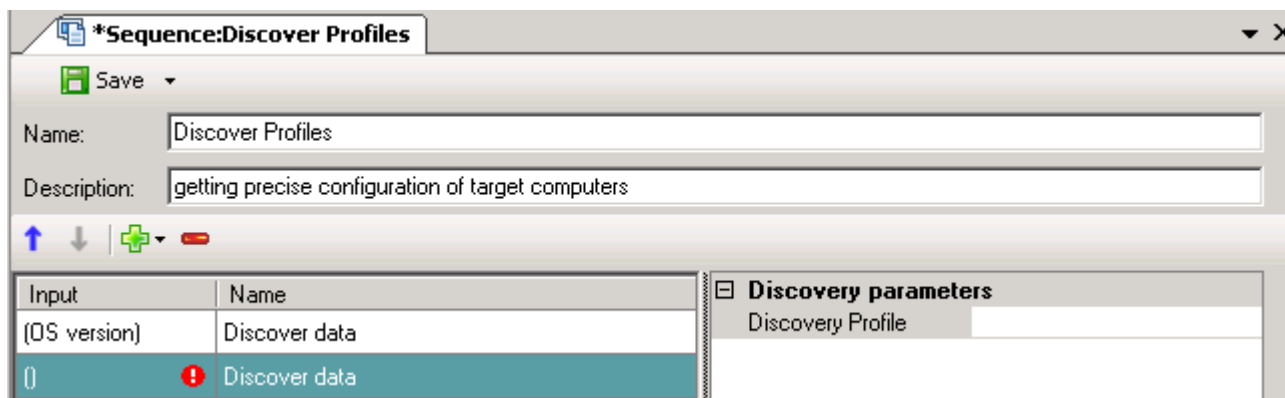


- This will open the 'Add New Sequence' dialog. At this stage, you should create an appropriate Name and Description for the sequence you are about to create. In the example shown below, we have chosen to name the Sequence 'Discover Profiles'

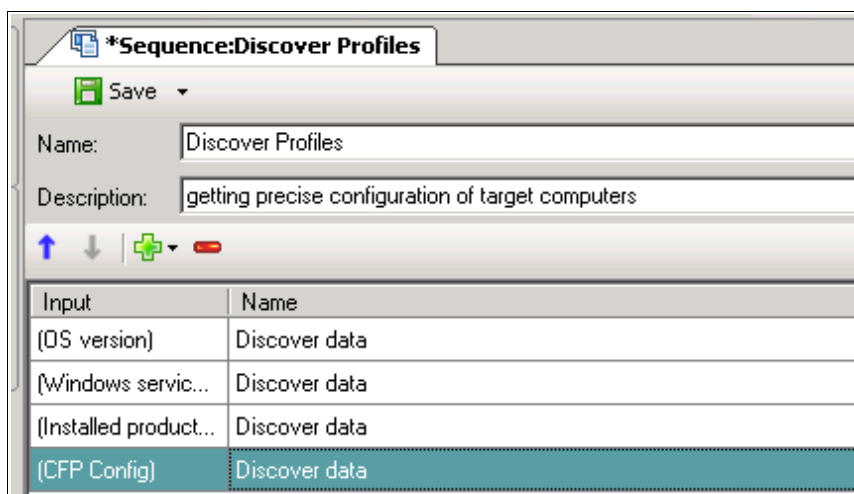
Next, you need to choose the Actions that will be executed in this Sequence. Select the 'Discover data' Action by checking the box alongside it's name and clicking the 'Add' button.



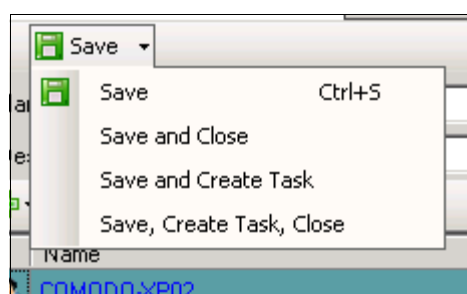
- Next, choose the type of Discovery Profile. (The red exclamation mark indicates that you cannot save this Sequence until a 'Discovery Parameter' has been chosen.) Select a Discovery Profile type from the drop-down list by clicking the ellipsis button (...) at the Discovery Parameter panel on the right (as shown below).



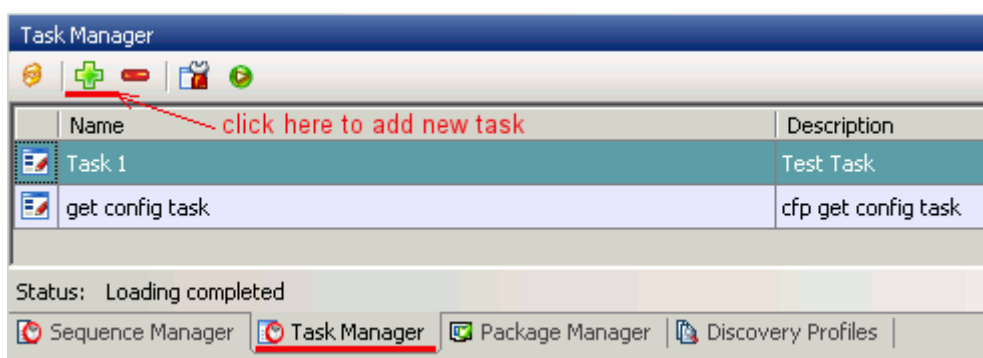
- The 'Windows Service list' Discovery Data Action has now been added to the Sequence. Repeat this procedure for the other three types of Discovery Profile. The completed Sequence containing four Discover Data Actions should look similar to the graphic below:



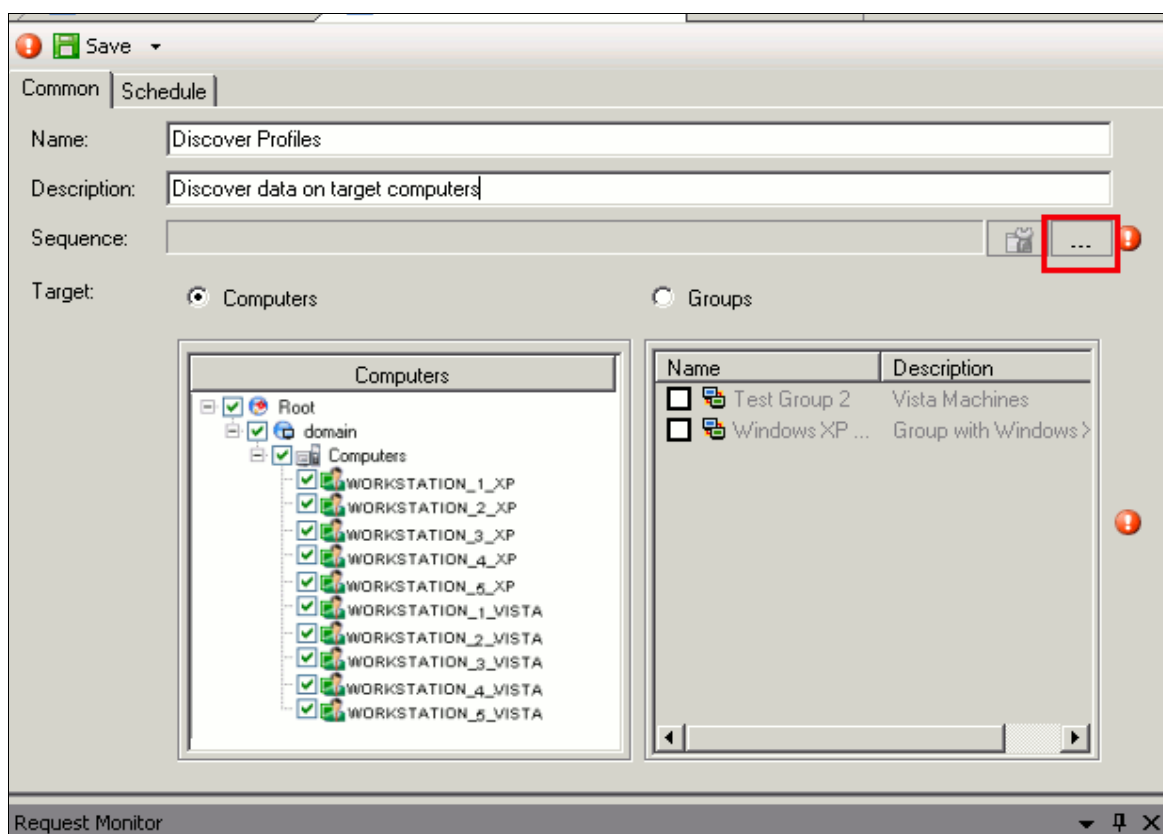
- Click 'Save':



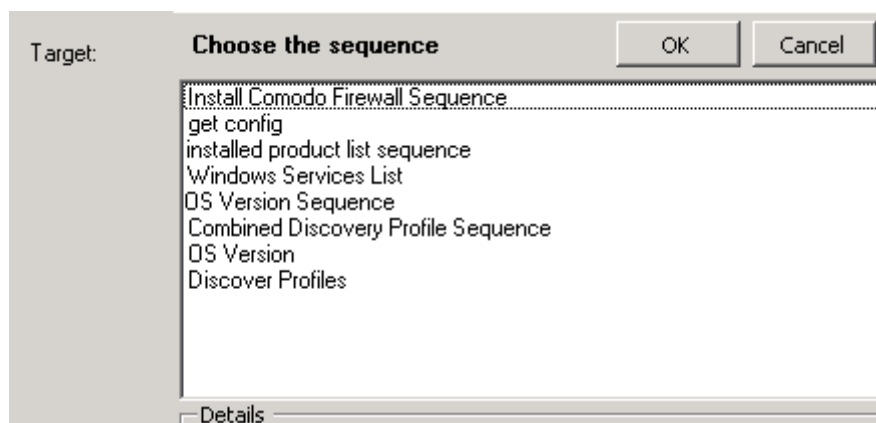
- Next we need to add this Sequence to a Task that will execute the Discovery Profile Actions on the Target Computers. Open the 'Task Manager' tab by selecting 'View > Task Manager'
- Click the 'Add New Task' Icon (highlighted below)



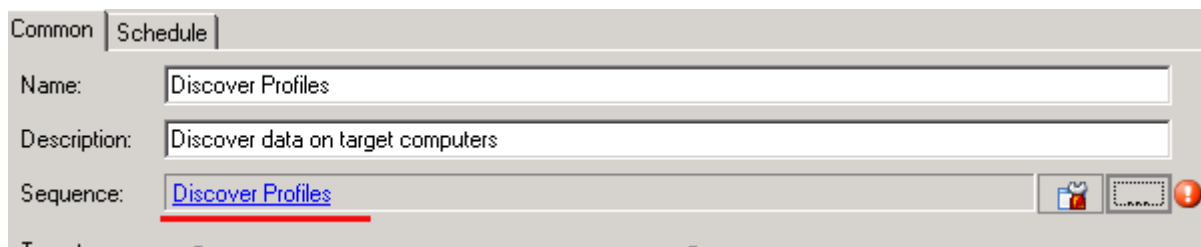
- This will open the 'Add New Task' dialog (shown below). At this stage, you should create an appropriate Name and (optional) Description for the Task you are about to create.



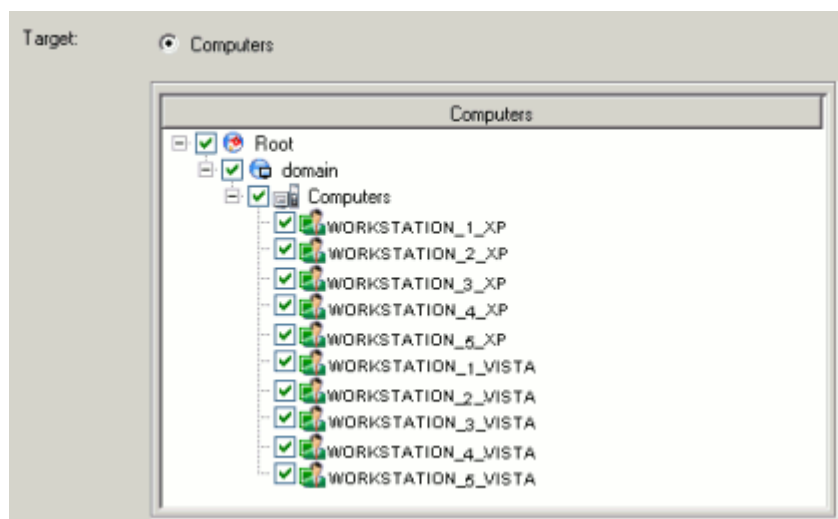
- Next, click the ellipsis button to the right of the 'Sequence' field (highlighted above). This will open the 'Choose Sequence' dialog. Choose the 'Discover Profiles' Sequence you created earlier and click 'OK' :



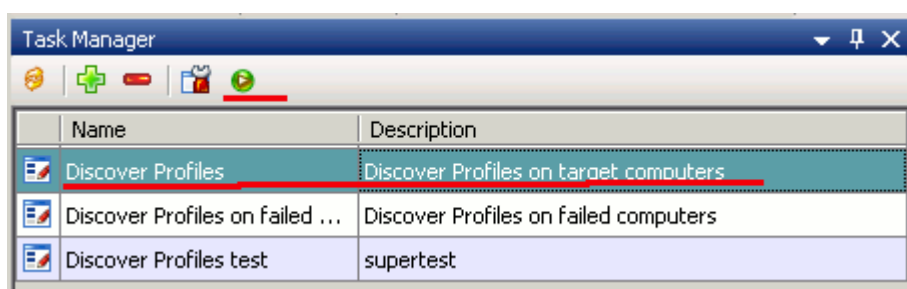
- This will return you to the 'New Task' dialog where the name of the Sequence will now be displayed in the 'Sequence' field:



- Select the target Managed workstations, controllers, domains and/or Workgroups you want to discover data for.

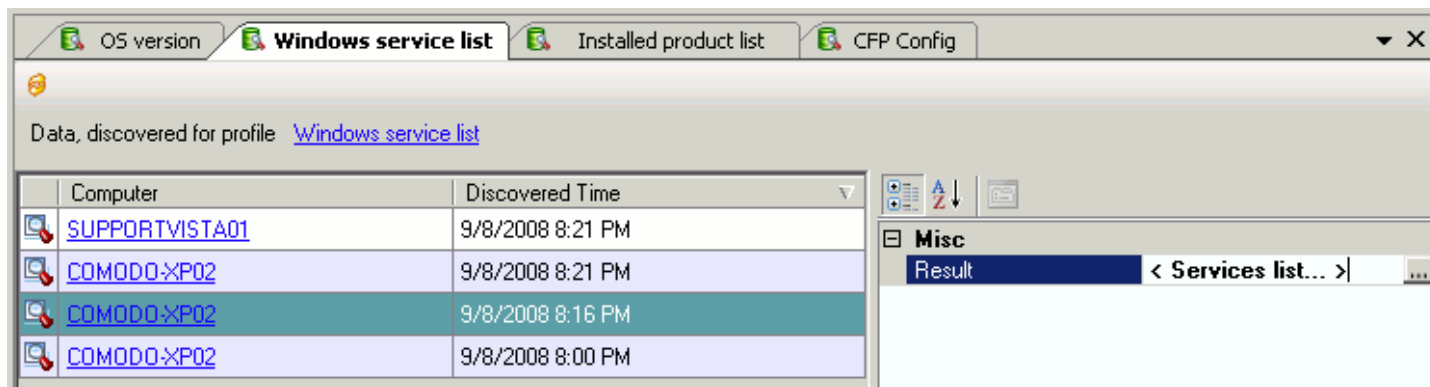


- Click the 'Save' button to confirm and save the new Task.
- Open the 'Task Manager' window (View > Task Manger). Select the task you have just created and click the 'Execute' icon as shown below:



- This will execute the Task on the target computers. Open the 'Task Result Manager' (History > Task Results) to check whether the Task executed successfully or not. (More details on the Task Result window can be found in section [3.8.The Task Result Manager window](#))

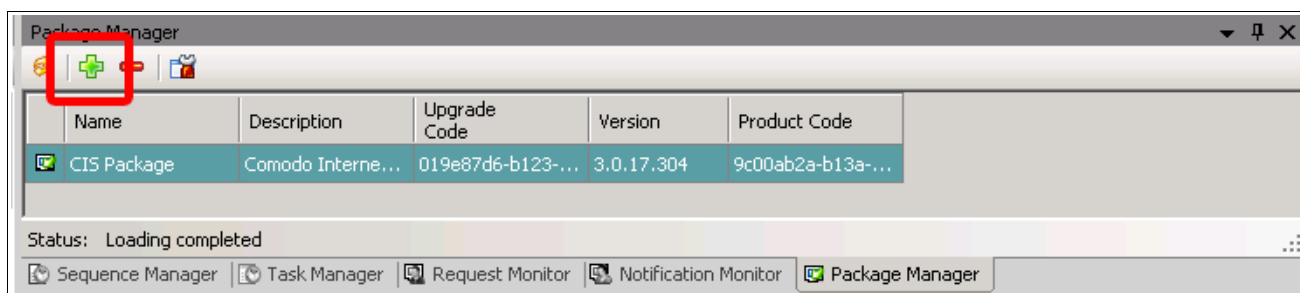
To view the discovered data about the target machines you need to open the 'Discovery Profiles' window (View > Discovery Profiles). The Discovery Profiles window lists the four types of profile. Clicking any of the profiles will open a list of computers upon which that profile has been run. The graphic below shows a typical 'Windows Services' list:



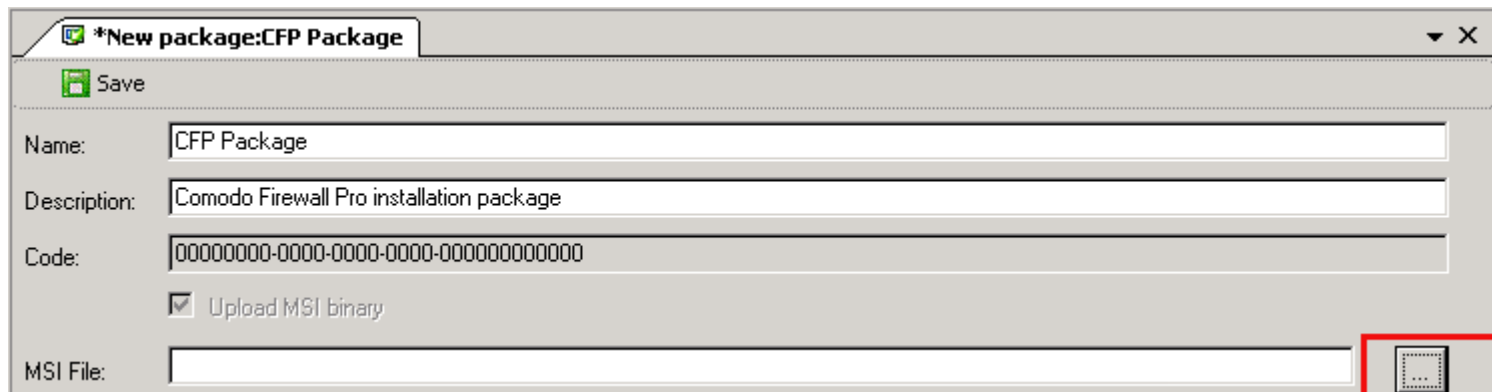
- To the right of this list of computers is the results panel for the selected machine. Clicking the ellipsis button (...) on the right hand side of this panel will display those details. In the case of the 'Windows Service list' profile shown above, it will display the Name, Version, Publisher, Date (of installation) and Location of all Comodo and 3rd party Packages present on the machine at the time the Action was run. Similarly, the OS Version profile will inform the administrator of the exact version of Windows that is running on the target computer.
- For more details on the functionality, operation and uses of Discovery Profiles, see section [3.5.The Discovery Profiles window](#)

6.2.2 Step 2. Upload the Comodo Firewall installation Package to the CESM Console

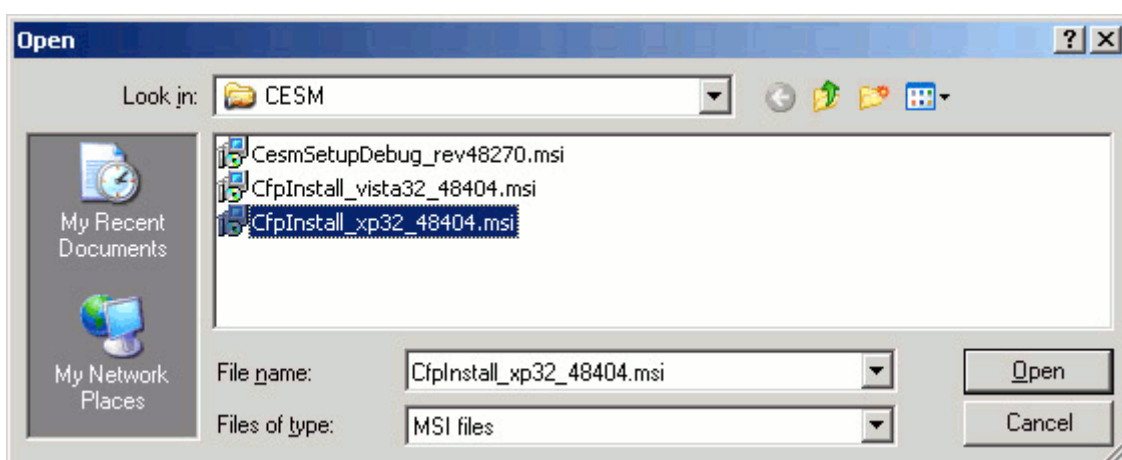
The next step is to upload the Comodo Firewall installation .msi package to the CESM Administrative console so that it can be installed on target computers. Switch to the 'Package Manager' window (View > Package Manager) and click the 'Create a new package' icon.



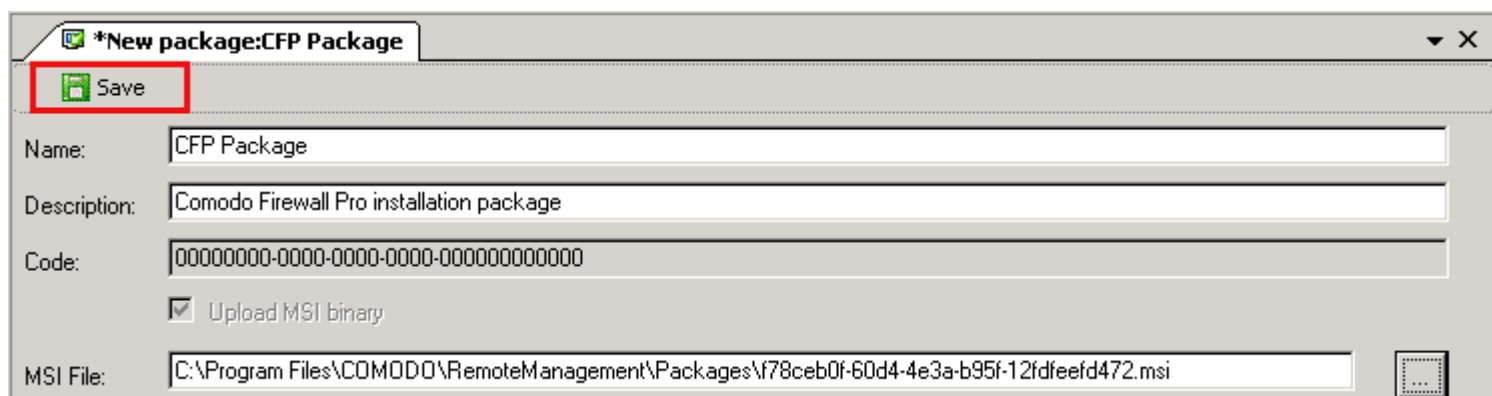
- This will open the 'Add New Package' dialog (shown below). At this stage, you should create an appropriate Name and (optional) Description for the Package you are about to upload.



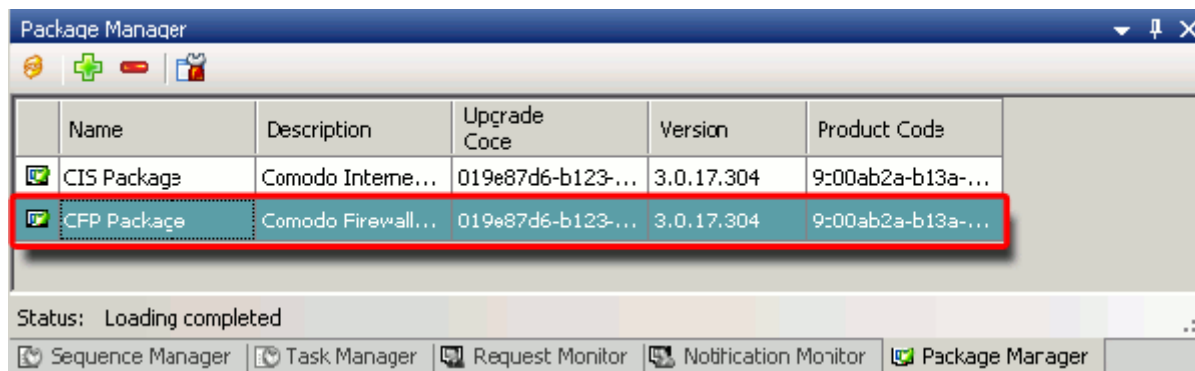
- Next, click the ellipsis button to the right of the 'MSI File:' field (highlighted above). This will open the standard Windows file browser:



- Browse to the local or network location to which you have saved Comodo .msi files. Select the appropriate file and click 'OK'.
- This will return you to the 'New Package' dialog where the filename of the .msi file will now be displayed in the 'MSI File:' field. Click the 'Save' button to confirm and save your new package:



- The newly created Package will be listed alongside any other packages in the 'Package Manager' window:

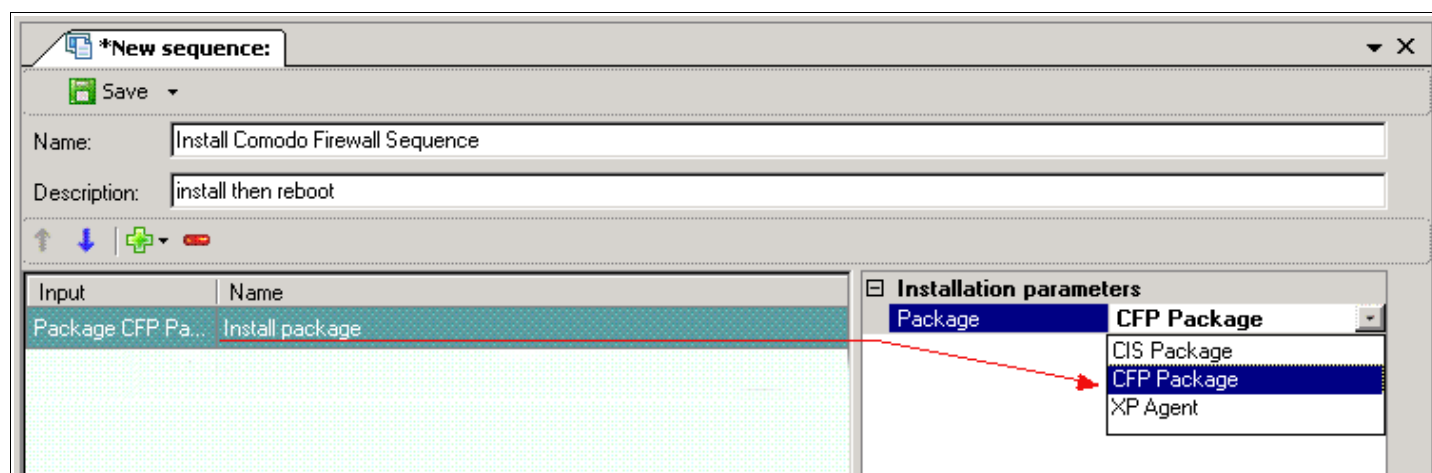


- Once the Package' has been created, it can be specified as the Parameter of an 'Install package' Action or an 'Uninstall package' Action in a Sequence (see Step 3, below).

For more details on the Package Manager, see section [3.4.The Package Management window](#)

6.2.3 Step 3: Create a Sequence of Actions to install the Comodo Firewall Package on Managed computers

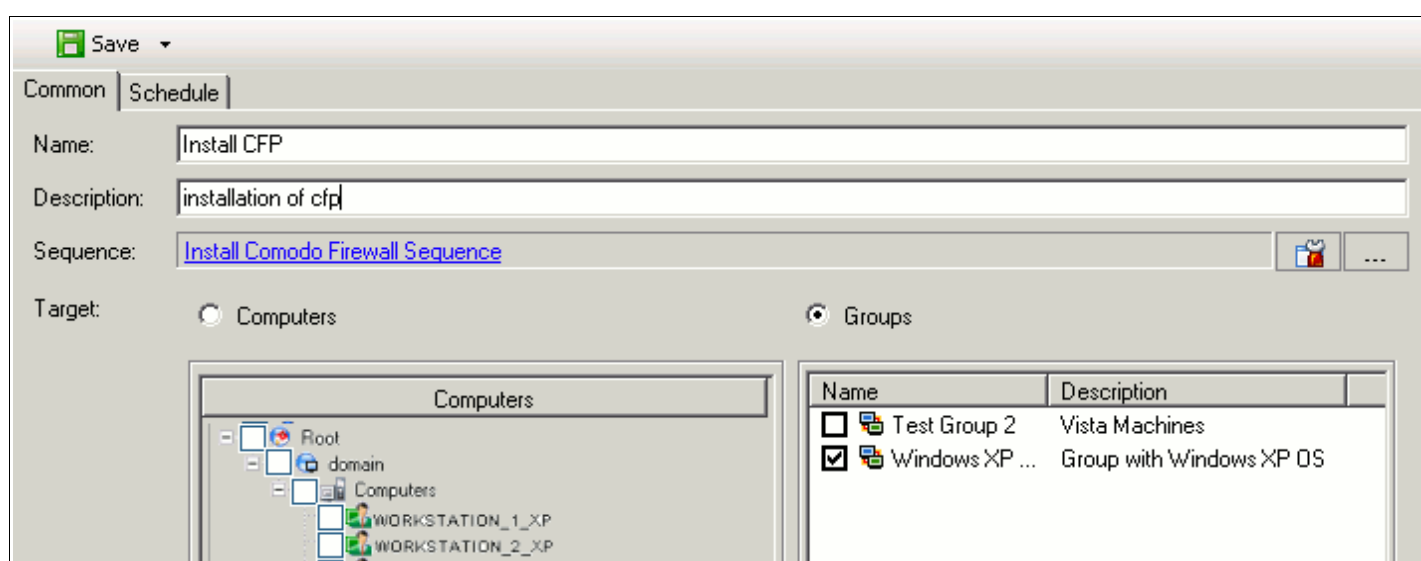
- Open the 'Sequence Manager' window (View > Sequence Manager)
- Click the 'Add New Sequence' Icon
- This will open the 'Add New Sequence' dialog. At this stage, you should create an appropriate Name and (optional) Description for the Sequence you are about to create (for example, 'Install CFP').
- Click the 'Add New Item' icon and select the Actions - 'Install package'. Click 'Add'. You now need to specify the parameters of this Actions from the panel to the right.
 - 'Install package' – select the CFP .msi package you have uploaded:



- Click 'Save'. This Sequence of Actions can now be added to a Task to be deployed on the target machines. (In fact it can be re-used in as many Tasks as required)

6.2.4 Step 4: Add the Sequence to a Task and execute that Task on Managed Computers

- Open the 'Task Manager' window (View > Task Manager)
- Click the 'Add New Task' Icon
- This will open the 'Add New Task' dialog. At this stage, you should create an appropriate Name and (optional) Description for the Task you are about to create.
- Select the desired target computers in the 'Targets' field editor and save the Task. (Alternatively, select a predefined CISM 'Group' of computers as the target of the Action.)



- You can execute the Task:
 - Immediately by selecting 'Save and Execute'
 - Manually at any time in the future by first saving then selecting the Task in the 'Task Manager' window then clicking the 'Execute' icon
 - At a scheduled time by configuring your preferences using the 'Schedule' tab
- The progress (success or failure) of the Task can be checked using by viewing the [Task Result Manager](#).
- If required, the administrator can now specify and deploy a precise Comodo Firewall Pro settings configuration to be implemented by running a 'Set CFP config' Action on those computers. For more details, see section [3.5.2.5.Example: Using 'CFP Config' Discovery Profile to roll out an existing CFP configuration onto other machines](#) and section [3.6.3.1.Table of Actions – Definitions and Usage](#)

More details about Tasks can be found in section [3.7.The 'Task Manager' window](#)

6.2.5 Step 5: Managing Requests (Alerts) from Comodo Firewall Pro on Managed Computers

Comodo Firewall Pro is designed to protect computers from internal and external threats by combining a powerful packet filtering firewall and a host intrusion prevention system. Both these components will generate alerts on the target PC whenever software attempts to perform an action that is not permitted by the firewalls configuration settings. Comodo Endpoint Security Manager is designed to allow administrators to centrally manage these alerts using the 'Request Monitor'. Instead of the end user seeing the alerts, they are relayed to the CESM Administrative Console as 'Requests'. From here the administrator can allow or block the Request or respond with a product specific answer. If multiple computers generate the same request then the administrator has the option of applying his response to all those machines in a single action. This feature, in combination with the ability to quickly specify and roll out a secure firewall configuration policy across an entire distributed network, makes CESM one of the most powerful end-point security management tools available.

To view and react to requests from Managed Computers, first open the 'Request Monitor' by selecting 'File > Request Monitor'.

The screenshot shows the 'Request Monitor' window. At the top, it displays the text: 'Request Monitor' and 'AgeintID=8429; WinWord is trying to open TCP connection to 123.123.123.123 port 123'. Below this is a table with the following columns: Description, Computer, Created, Expired At, Received, Product Name, and Product Version. The table contains 8 rows of data, all with 'AgeintID=84...' in the Description column and 'CFP' in the Product Name column. The 'Computer' column lists various workstation names like 'WORKSTATION 1', 'WORKSTATION 2', etc. To the left of the table is a control panel with 'Allow (default)' and 'Deny' options. At the bottom left, it shows 'Count: 363'. At the bottom right, there are tabs for 'Notification Monitor' and 'Request Monitor'.

Description	Computer	Created	Expired At	Received	Product Name	Product Version
AgeintID=84...	WORKSTATION 1	11.09.2008 ...	11.09.2008 ...	11.09.2008 ...	CFP	3.0
AgeintID=84...	WORKSTATION 2	11.09.2008 ...	11.09.2008 ...	11.09.2008 ...	CFP	3.0
AgeintID=84...	WORKSTATION 1	11.09.2008 ...	11.09.2008 ...	11.09.2008 ...	CFP	3.0
AgeintID=84...	WORKSTATION 3	11.09.2008 ...	11.09.2008 ...	11.09.2008 ...	CFP	3.0
AgeintID=84...	WORKSTATION 3	11.09.2008 ...	11.09.2008 ...	11.09.2008 ...	CFP	3.0
AgeintID=84...	WORKSTATION 6	11.09.2008 ...	11.09.2008 ...	11.09.2008 ...	CFP	3.0
AgeintID=84...	WORKSTATION 4	11.09.2008 ...	11.09.2008 ...	11.09.2008 ...	CFP	3.0

The Request Monitor will display a list of all Requests generated by the computers upon which Comodo Firewall Pro has been installed. Having selected a particular Request, the administrator can provide his Response either from the pane to the left or by right-clicking and selecting a Response from the context sensitive menu. Alternatively, the administrator can group-select multiple Requests and issue the same response to all selected computers at once. Full details on using the Request Monitor can be found in section [3.10.The Request Monitor](#)

7 About Comodo

Comodo is a leading global provider of Identity and Trust Assurance services on the Internet, with over 200,000 customers worldwide. Headquartered in Jersey City, NJ with global offices in the UK, Ukraine and India, the company offers businesses and consumers the intelligent security, authentication and assurance services necessary to ensure trust in online transactions.

As a leading Certification Authority, and in combination with the Digital Trust Lab (DTL), Comodo helps enterprises address digital ecommerce and infrastructure needs with reliable, third generation solutions that improve customer relationships, enhance customer trust and create efficiencies across digital ecommerce operations. Comodo's solutions include SSL certificates, integrated Web hosting management solutions, web content authentication, infrastructure services, digital e-commerce services, digital certification, identity assurance, customer privacy and vulnerability management solutions.

For additional information on Comodo – Creating Trust Online™ please visit www.comodo.com

Comodo Group Inc

**US Headquarters,
525 Washington Blvd.,
Jersey City, NJ 07310
Tel: +1.888.COMODO.1**

Comodo C.A.

**3rd Floor, Office Village,
Exchange Quay, Trafford Road,
Salford, Manchester M5 3EQ,
United Kingdom.
Tel Sales: +44 (0) 161 874 7070
Fax Sales: +44 (0) 161 877 7025**

www.comodo.com sales@comodo.com