COMODO
Creating Trust Online®

Comodo
Endpoint Security Manager
SME

Software Version 2.1

Quick Start Guide

Guide Version 2.1.111114

Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

Endpoint Security Manager - SME

Quick Start Guide

This tutorial briefly explains how an administrator can setup Endpoint Security Manager - SME then install and monitor installations of Comodo Internet Security (CIS) on networked computers.

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

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

- **Step 1 - Install ESM SME**
- **Step 2 - Login to the Admin Console**
- **Step 3 - Install Agents (and optionally Comodo Internet Security) on Target Machines**
- **Step 4 - Open the dashboard - check that target endpoints are reporting correctly**
- **Step 5 - Create Groups of Computers**
- **Step 6 - Import security policy from an endpoint and apply to groups**
- **Step 7 - Viewing Reports**

Important: Do NOT use the 'Back' button on your browser to navigate the interface as this will return you to the login screen. Navigate backwards and forwards between screens using the arrows in the left and right of the interface OR left-click and hold then drag to swipe between screens.

ESM requires installation of the Central Service and the Administrative Console. They can either be installed on separate machines or both on the same machine.

Step 1 - Install ESM SME *(see* **Installing and Configuring the Service** *if you need more help with this)*

1. Download and run the ESM setup file from the Comodo website. This file will install the central service on the machine you intend to use as the ESM server. Supported Operating Systems are Win XP, Win Vista, Win 7 and Windows Server 2003/2008.

   There is a choice of two setup files. The '..._FULL.exe' file contains all additional, required software (.net Framework 4, SQL Server compact 4.0 and Microsoft Report Viewer 10.0). The other is a lightweight web installer that does not contain this additional software but will download it from the Internet if it is not detected on your server.

2. Run the setup file. Any missing software components will be automatically installed (ESM requires .NET, SQL server compact and Microsoft report viewer).

3. Select 'Typical' as the installation type for fastest setup experience; after installation you will need to provide a valid license key by clicking the License tile using the Console interface. Select 'Custom' if you wish to change install location or select which components are installed; you will be required to provide your license during setup.

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

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

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

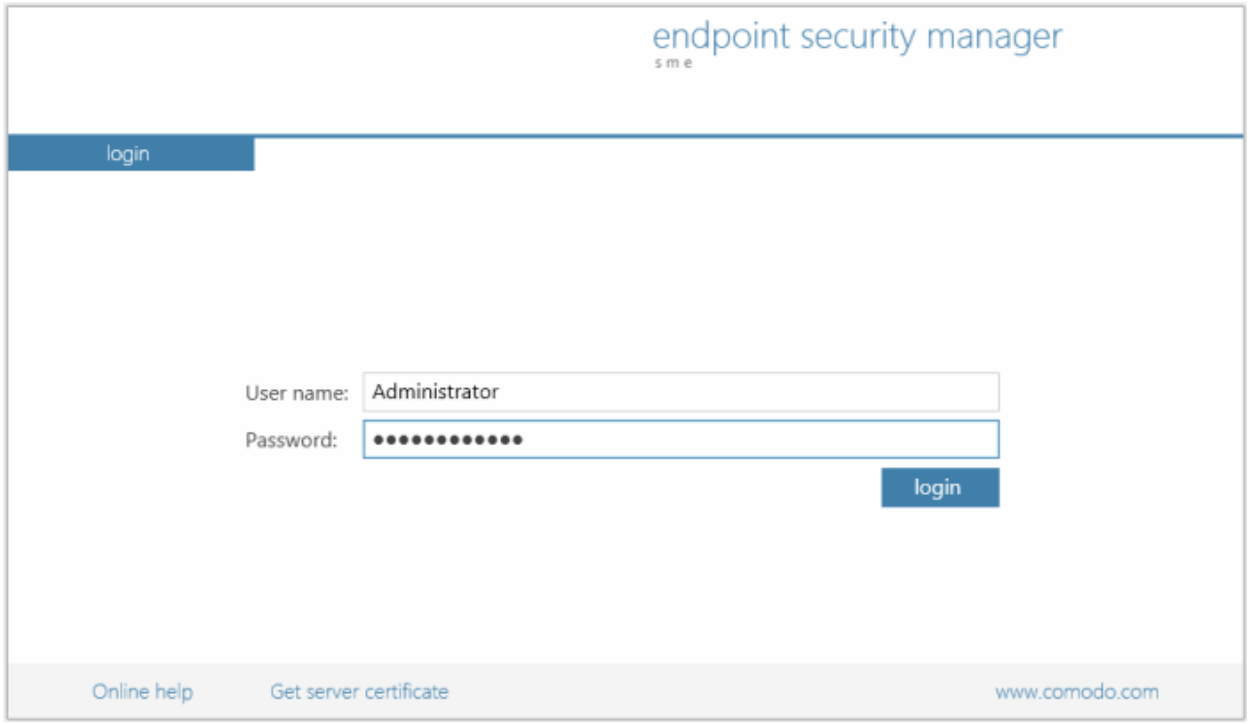
7. Since the ESM console can be accessed via the Internet, you may desire to obtain an SSL certificate and apply it using the Configuration Tool or you can distribute the self-signed certificate already installed to computers that you will use to administer ESM.

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

1. After setup is complete, there are two ways that you can access the admin console:
    - On the server itself - open the console by clicking 'Start > All Programs > Comodo > Endpoint Security Manager > ESM Console'
    - From remote machines via Internet browser - use the following address format to access the console:
      https://<your server hostname or IP address>:57194

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

2. Login to the console using the Windows administrator user ID and password of the system that ESM was installed on to begin using your software.



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

Note on using the interface

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

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

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

A third alternative is to click the plain arrows in the middle on the left and right of the interface.

Please do not use the 'back' button on your browser as this will return you to the login screen.

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

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

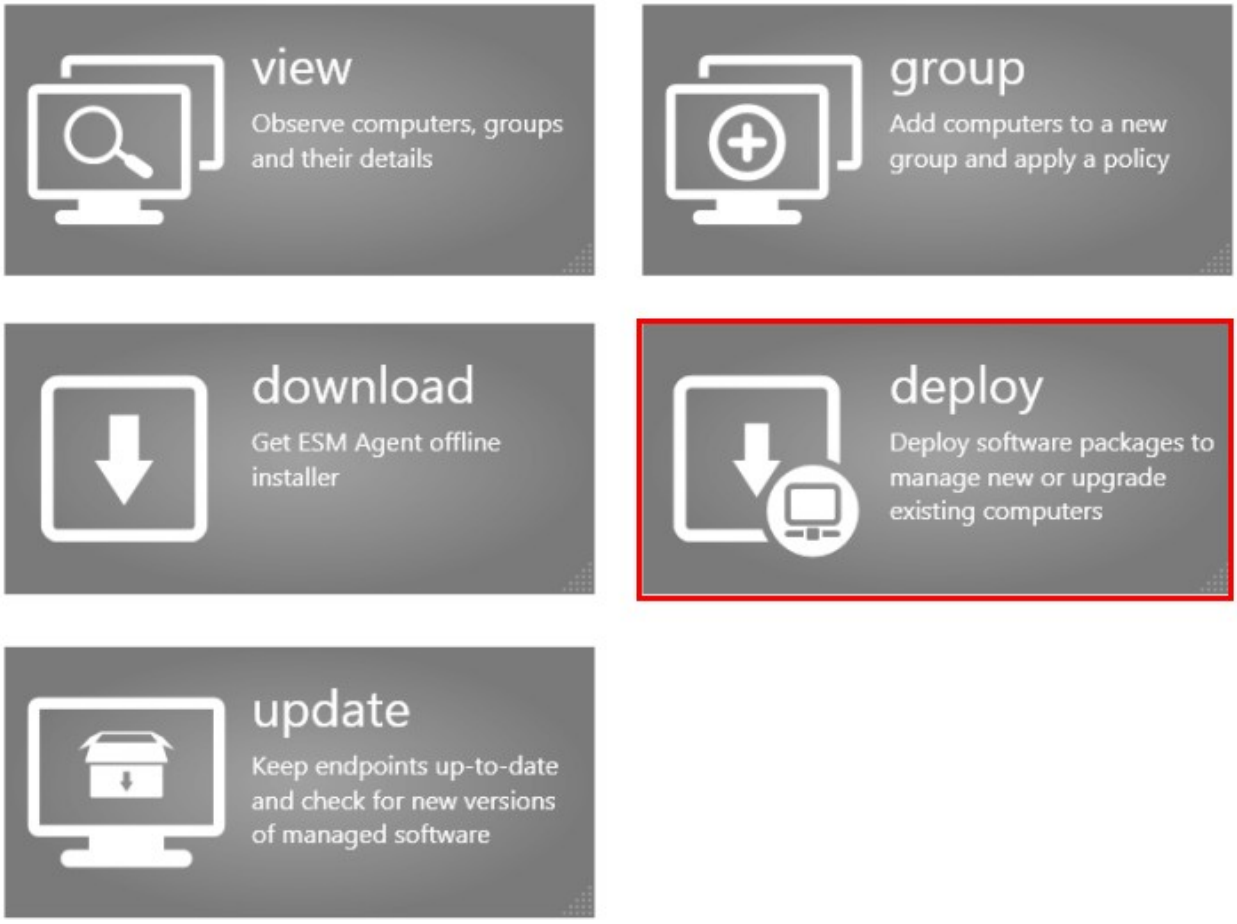
ESM server. The next stage of setup is to install this agent.

There are three methods to accomplish this:

- Remotely, using a console wizard to automatically push the agent and (optionally) CIS onto target machines. This wizard is started by clicking the 'deploy ' tile in the 'Computers' section of the console.
- Locally. You can install the agent and bring endpoints under central management by clicking the 'Manage this endpoint' link in the CIS interface. A walk-through using this method can be found at **How to Connect CIS to ESM at the Local Endpoint**.
- Locally. You can download the agent setup file from the admin console, transfer the file to the endpoints to be managed through any media like DVD, CD, USB memory and install the agent at the endpoints. Detailed explanation on using this method can be found in **Adding Computers by Manual Installation of Agent and CIS**.

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

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



3. The first stage is to choose how you want to import (Target Type). Computers can be imported using one of three methods: Active Directory, Workgroup or by Network Address. Administrators should, of course, repeat this wizard until they have imported all computers in their network.
4. Select the appropriate import method then *swipe* the screen to the move to the next stage. '*Swiping*' is done by holding left-click button down in white space and dragging the mouse to the left. If you have a touch-sensitive screen then you can swipe between screens with your finger. A third alternative is to click the plain black arrows in the middle on the left and right side of the interface.
    - If you chose 'Active Directory', you next have to choose whether to import from the current domain or a custom domain. The 'current' domain means whichever domain the ESM *server* is a member of - not the current domain of the endpoint being used to manage the server. If you choose 'custom domain' then you will need to enter the IP or name of the domain controller and the administrator UN/PW for that domain.

- If you chose 'Workgroup', you next have to specify which workgroup to import from. You can specify manually by typing the workgroup name or use the 'Find workgroups' option to have the wizard present you with a choice of detected workgroups. You can only import from one workgroup at a time so you may have to repeat this wizard.
- If you chose 'Network Addresses', you next have to specify the IP, IP range, host name or subnet of the target machines. Click the 'add' button to confirm your choice. Repeat until you have added all IP addresses or ranges that you wish to import.

Swipe left (or click the right arrow button) to continue.

5. The next stage, 'Select Targets', allows you to choose those imported computers onto which you want to install the Agent and Comodo Internet Security. Select the check-boxes next to your intended targets and swipe the screen left to continue (or click the right arrow button).
6. The next step 'Target Summary' provides you the summary such as status, IP address of the endpoint(s) that you want to install the agent or CIS. Select the check box beside the computer that you want to install the packages. If you want to select all the computers, select the check box beside the 'target computer'. Swipe left (or click the right arrow button) to move onto the next step.
7. Credentials. Next up is to choose whether the agent has to be installed under the currently logged in user account or the network administrator account. If you choose 'Custom Credentials', enter the user name and password of an account with administrative privileges on the machine - such as Administrator, machinename/administrator, domain/administrator as the login ID. Swipe left (or click the right arrow button) to move onto the next step.
8. The next stage 'Packages' displays the version details of ESM Agent and CIS. You can also check for updates of these applications and download it in your server for deployment on to the endpoints.
9. The final step prior to deployment is to decide whether you *also* want to install Comodo Internet Security (CIS) at this time.

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

      (1) Click 'Check for updates' then If any newer versions are available, you can choose to download them to the ESM server by clicking 'download'.

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

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

      (4) Check 'Suppress Reboot' if you do not want the target endpoint to automatically restart after installation. Reboot is required to complete installation, but you may want to postpone this until later.

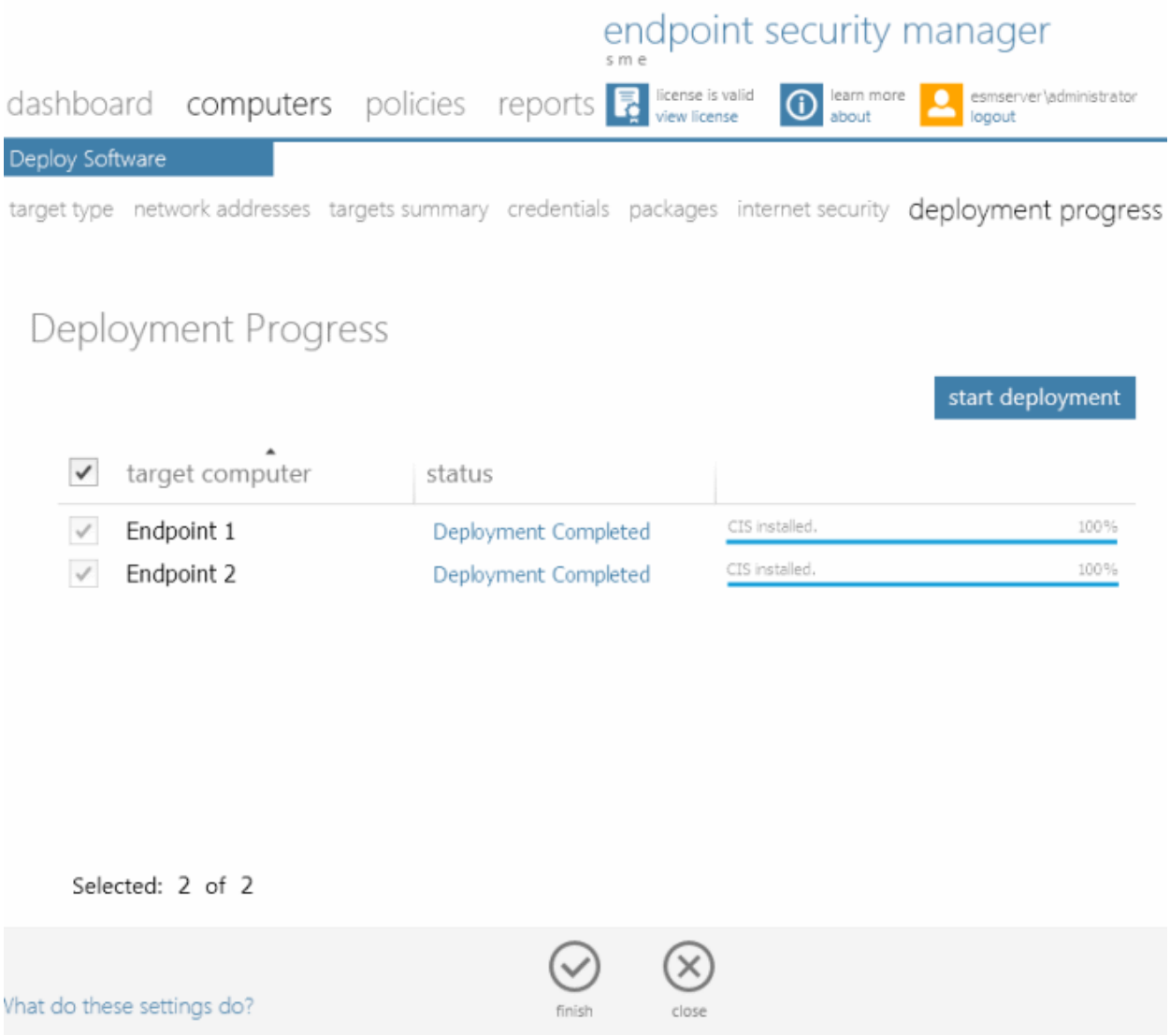
      (5) 'Uninstall all incompatible third-party products' - Check this option to uninstall select third party antivirus, firewall and other desktop security software from the endpoints, prior to the installation of CIS. Performing this step will remove potentially incompatible products and thus enable CIS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

      Click Here to see the full list of incompatible products.

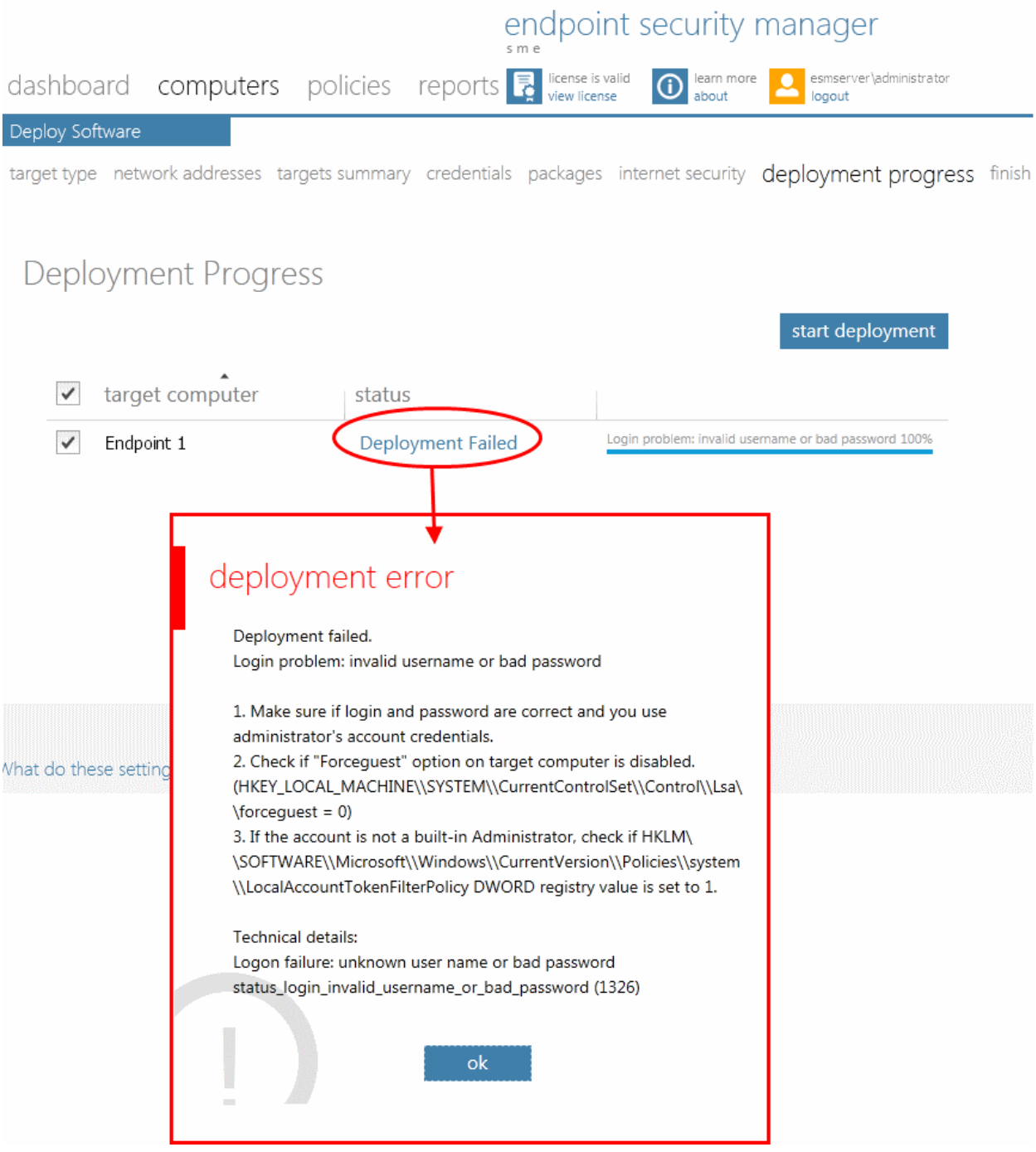
      However the following steps will help most Windows users:

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

    - To move onto the deployment stage, click 'start deployment'. You will see installation progress per-endpoint. Once installation is complete, you should see a results screen similar to the following screenshot.



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



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

Step 4 - Check that Target Endpoints are Reporting Correctly

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

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

    - After checking that all computers are reporting correctly, it is a good idea to make sure the latest virus databases are installed. Click the 'Outdated' tile to begin this process.
    - After updating, we advise running a virus scan on target computers. Click the 'Antivirus Scan' tile to do this. Note - real-time AV protection is already running on all endpoints. If any malware is discovered, it will be brought to your attention via the 'Malware Found' tile.
    - A full description of the dashboard interface. the meaning of each tile and how to add more tiles can be found in **The Dashboard Area**.
    - General advice regarding navigation and other functional areas can be found in the **The Administrative Console**.

Step 5 - Create Groups of Computers

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

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

- We advise admins to create groups corresponding to the structure of their organization THEN import policy (from an endpoint) and apply it to selected groups.
- To start, click the 'computers' link from the top navigation followed by the 'group' tile. Select required computers, leave policy as (Locally Configured), type a name for the group then finish.
- If you wish to create multiple groups, repeat the previous step until all computers have been assigned.
- See '**Creating Endpoint Groups**' if you need help with this wizard. See '**The Computers area**' for an overview of functionality.

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

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

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

- To set the parameters of a particular security policy, you need to place the endpoint in 'locally managed' mode by selecting 'Manage Locally' in CIS settings on the endpoint itself - either by physically sitting at the machine or by a remote connection. See **How to Configure CIS Policies - An Introduction** for general advice with this.
- Once you have set and tested the policy at the endpoint, you should return to the ESM console and prepare to import this policy. Note - leave the endpoint in local management mode while doing this.
- At the console, click 'policies' then the 'create' tile to start the policy import and deployment wizard. Select 'A computer' as source type then choose the specific computer from which you want to import. Modify 'Settings' and 'Agent Settings' if required.
- For 'targets', choose which groups you want to apply the policy to and how you want it applied. 'for local policy' and 'for Internet policy' are the policies to be used depending on whether the machine connects from inside or outside of the VPN. Also, select 'Override individual computer's policy' to make sure this policy is applied correctly.
- Selecting 'Force target computers to be managed remotely upon policy assignment' means ESM will engage 'Remote Mode' and thus enforce policy compliance on the selected endpoint. if the policy becomes altered, ESM will automatically re-apply it. If not selected, the endpoints will remain in 'Local Mode' (although your policy will still be applied, it could become changed over time at the local level).
- Finally, give the policy a name and description and select 'Apply policy after finish' to immediately implement. Do not select this if you wish to deploy later.

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

Step 7 - Viewing Reports

The reports area contains a wealth of valuable information for administrators. Each report is an 'Active Report' that also allows admins to launch relevant tasks. Reports can be exported, printed and cover the following categories:

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

Click here to read more about reports.

About Comodo

The Comodo companies are leading global providers of Security, Identity and Trust Assurance services on the Internet. Comodo CA offers a comprehensive array of PKI Digital Certificates and Management Services, Identity and Content Authentication (Two-Factor - Multi-Factor) software, and Network Vulnerability Scanning and PCI compliance solutions. In addition, with over 10,000,000 installations of its threat prevention products, Comodo Security Solutions maintains an extensive suite of endpoint security software and services for businesses and consumers.

Continual innovation, a core competence in PKI and a commitment to reversing the growth of Internet-crime distinguish the Comodo companies as vital players in the Internet's ongoing development. Comodo, with offices in the US, UK, China, India, Romania and the Ukraine, secures and authenticates the online transactions and communications for over 200,000 business customers and millions of consumers, providing the intelligent security, authentication and assurance services necessary for trust in on-line transactions.

Comodo Security Solutions, Inc.

1255 Broad Street

Clifton, NJ 07013

United States

Tel: +1.888.256.2608

Tel: +1.703.637.9361

Email: **EnterpriseSolutions@Comodo.com**

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