Symantec Network Access Control ensures that a company's client computers are compliant with the company's security policies before the computers are allowed to access the network. Symantec Network Access Control uses a Host Integrity Policy and an optional Symantec Enforcer to discover and evaluate which computers are compliant.

Components of Symantec Network Access Control

- **Symantec Endpoint Protection Manager (with SQL Database)**
- **Symantec Endpoint Protection client** or **Symantec Network Access Control client**
- **NAC Enforcer** (optional)

NAC Enforcement Options

The available enforcement options in Symantec Network Access Control are:
- **Self Enforcement**
- **Symantec Enforcer Appliances**
- **Symantec NAC Integrated Enforcer for Microsoft DHCP Servers**
- **Symantec NAC Integrated Enforcer for Microsoft Network Access Protection**
- **Universal enforcement API**
- **Enforcement by using Cisco NAC**

Self-Enforcement

Enforcement is done by the (SNAC) Client itself. No Enforcer hardware is required. Self enforcement by the SEP client firewall has no effect on the systems without SEP clients in the network.

With Self Enforcement, the client can quarantine its system if it falls out of compliance. Quarantine policies have to be defined on SEPM. The client can quarantine itself by switching to a quarantine firewall policy, a Firewall that restricts access to specific IP addresses or segments.

This allows for rapid deployment of basic endpoint security. No network-level systems or configuration is needed.

Please check the link for more information—

http://www.symantec.com/docs/TECH102534

**Install Symantec Network Access Control when SEPM is already installed and Running**

How to enable: There are two methods to enable SNAC on already running SEPM...

Method 1:Manually copy the License file (SNAC.XML) from SNAC CD and add the packages to Client Install packages under SEPM.
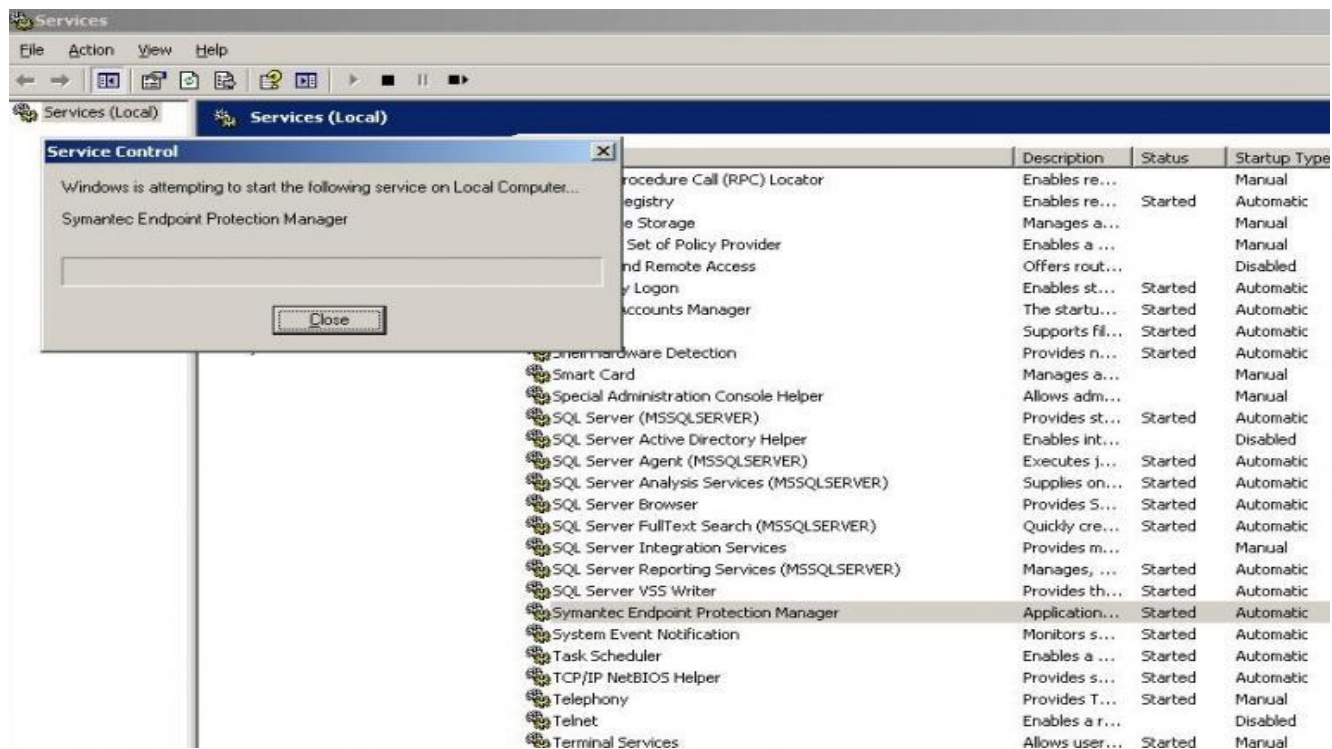
a. Go to SEPM folder on SNAC CD and copy the snac.xml file.


Caption: License file for SNAC
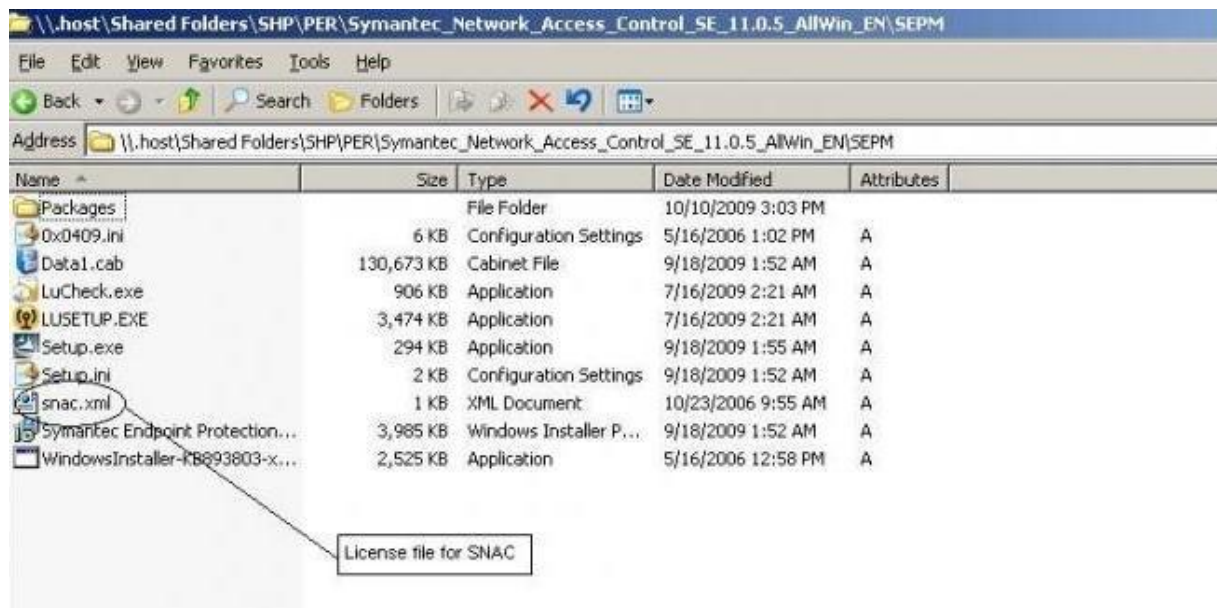
b. Paste the snac.xml file inside "Program Files\Symantec\Symantec Endpoint Protection Manager\tomcat\etc\license" folder.
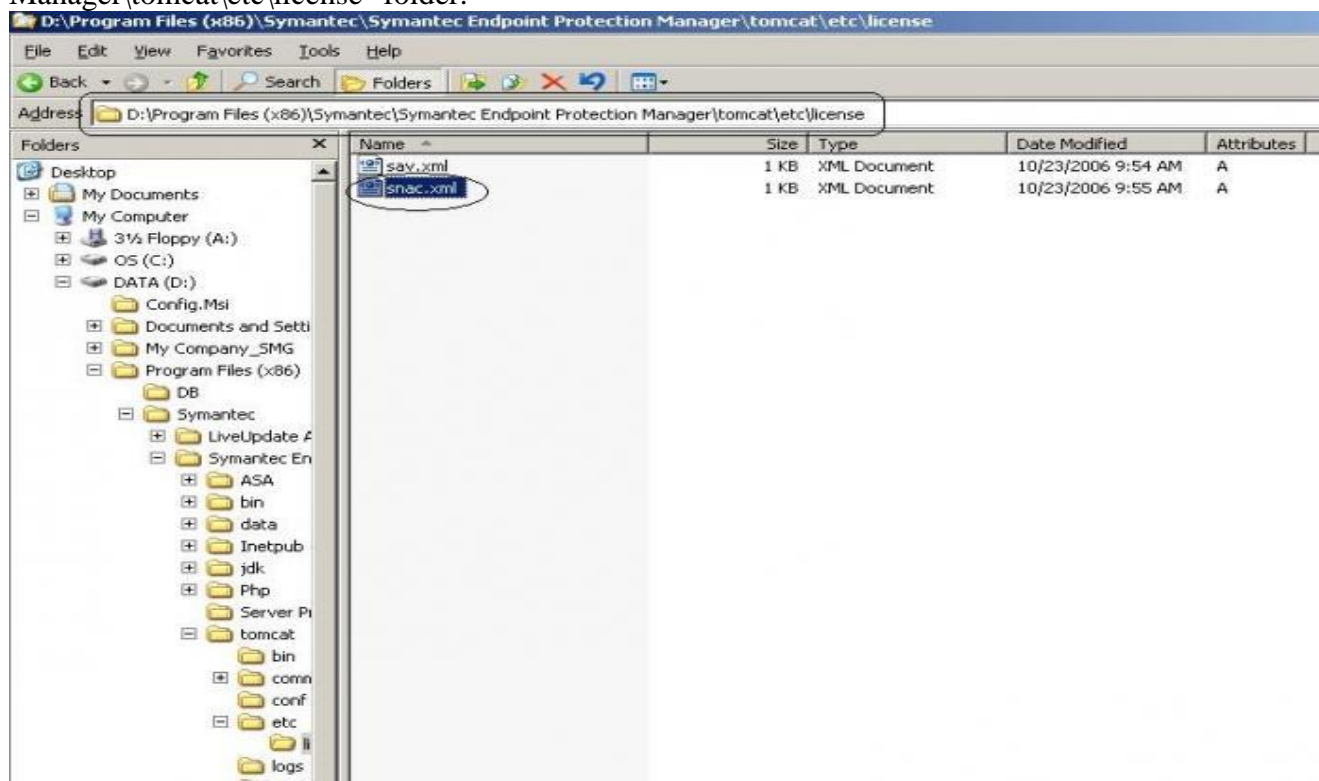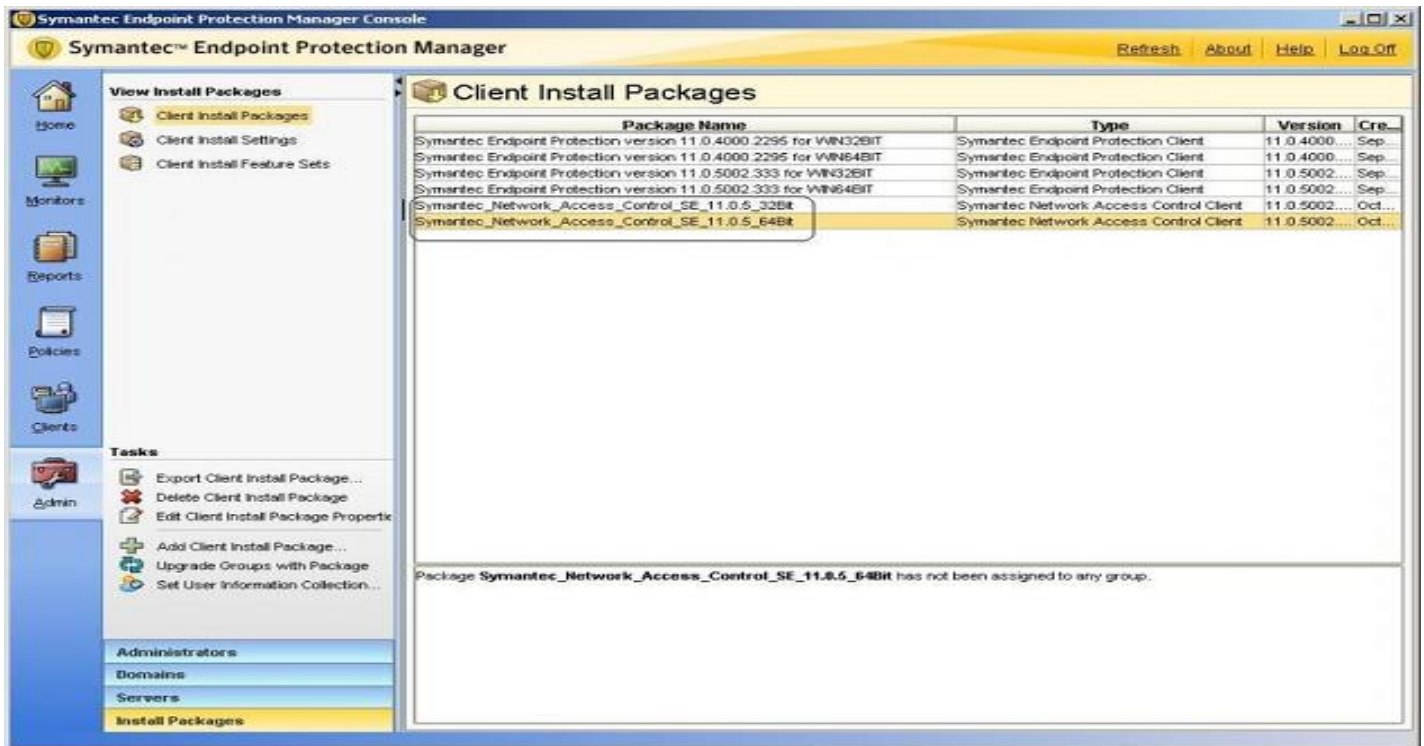
c. Restart the "Symantec Endpoint Protection Manger".

d. After completing the above steps SNAC will be enabled on your SEPM. Now you can add SNAC packages to "Client install packages". Go to Admin-->Install Packages-->Add Client install package. browse the SNAC folder in the CD and select setup.exe file.
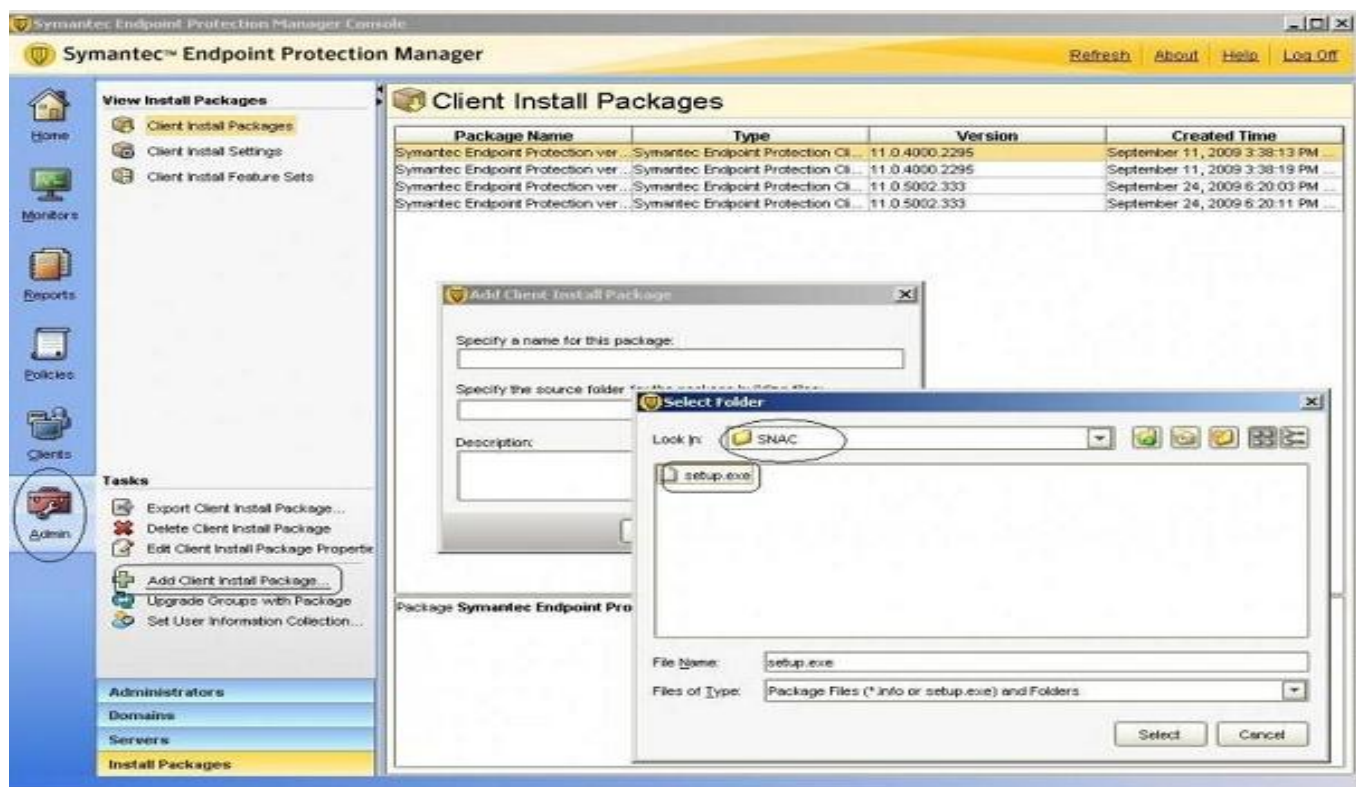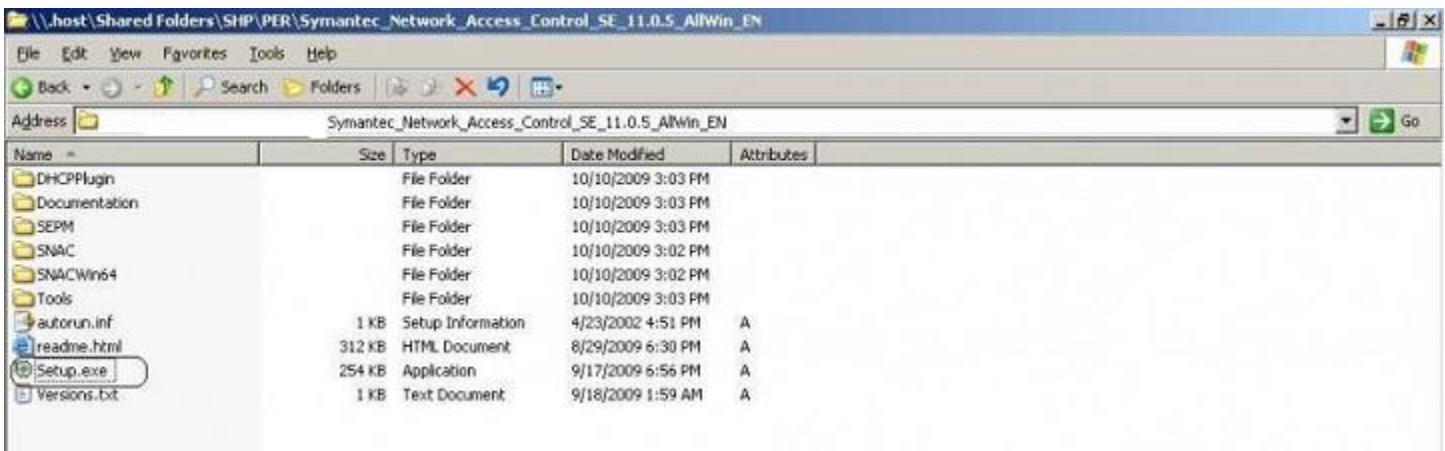
e. Same procedure can be followed for 64 bit package also. Folder name is SNACWin64.
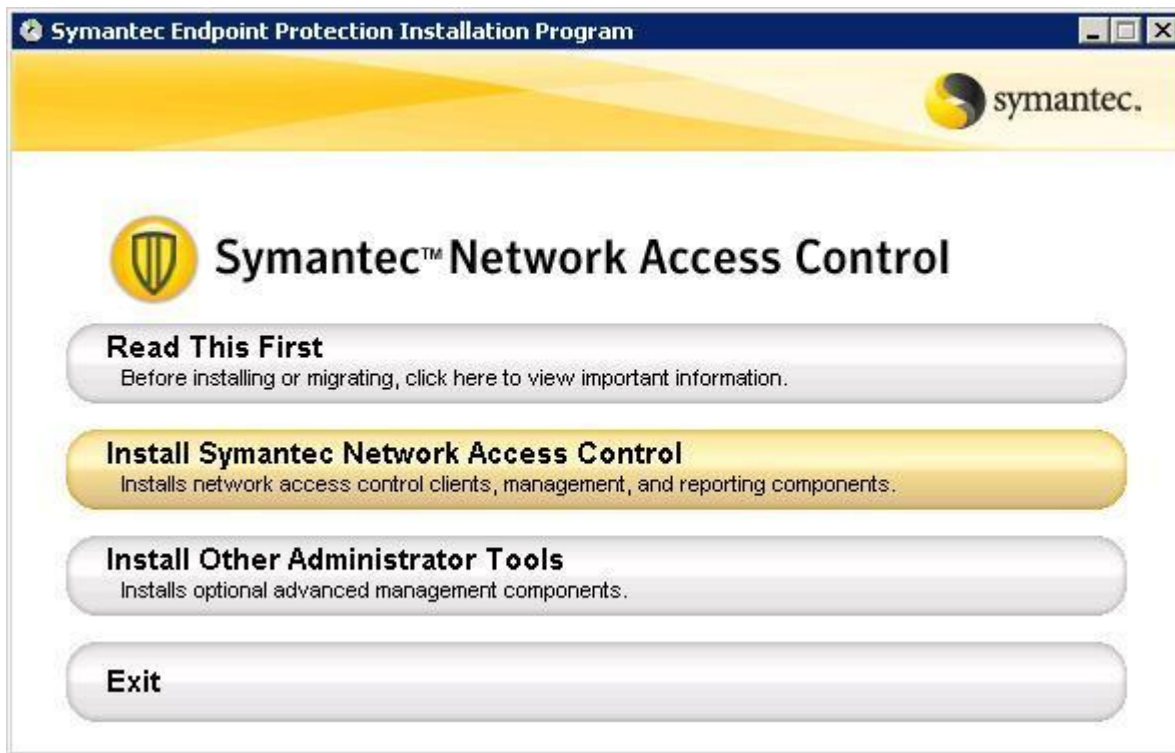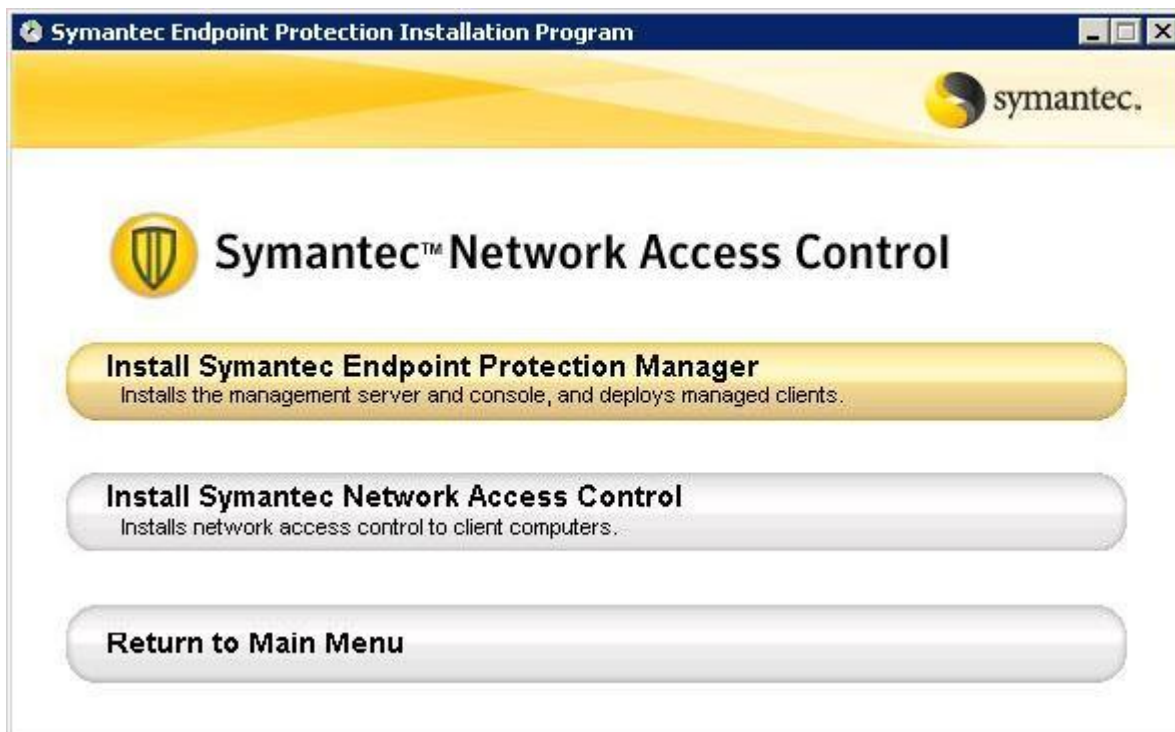

Method 2: Upgrade from CD.

a. When you put the cd "Symantec endpoint protect installation program" menu will appear. If its not coming open the CD and run setup.exe
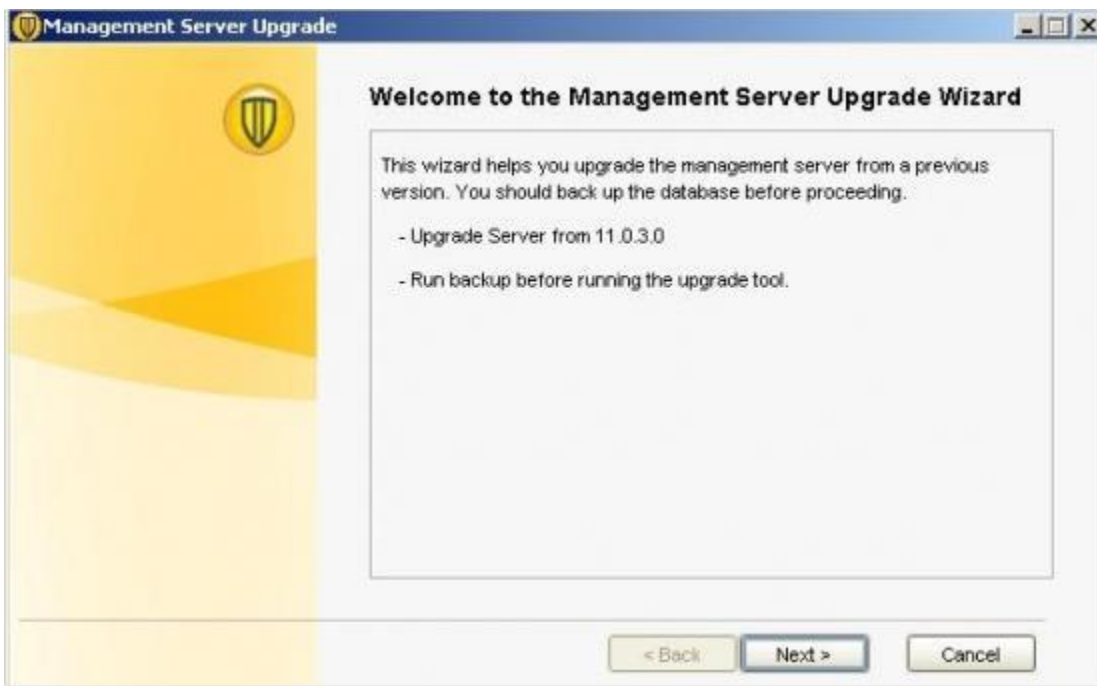
b. Select Install Symantec Network Access Control.

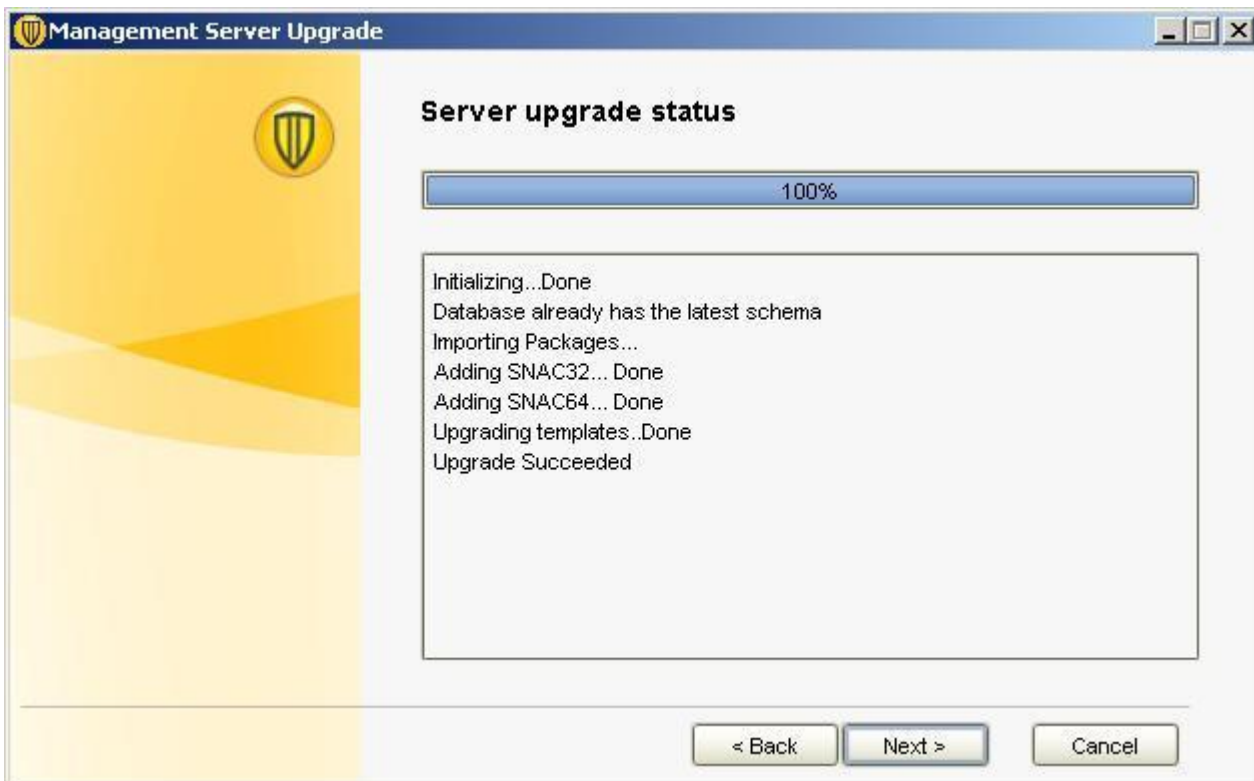**c**. Select Install Symantec Endpoint protection Manger. Now it copies the License file and starts configuring SEPM.

d. Once the "Management server upgrade wizard" starts click Next.

e. Once Wizard is complete click "Next" and "Finish".

f. After the upgrade wizard SEPM configuration wizard appears.. Provide the appropriate values and complete the configuration.
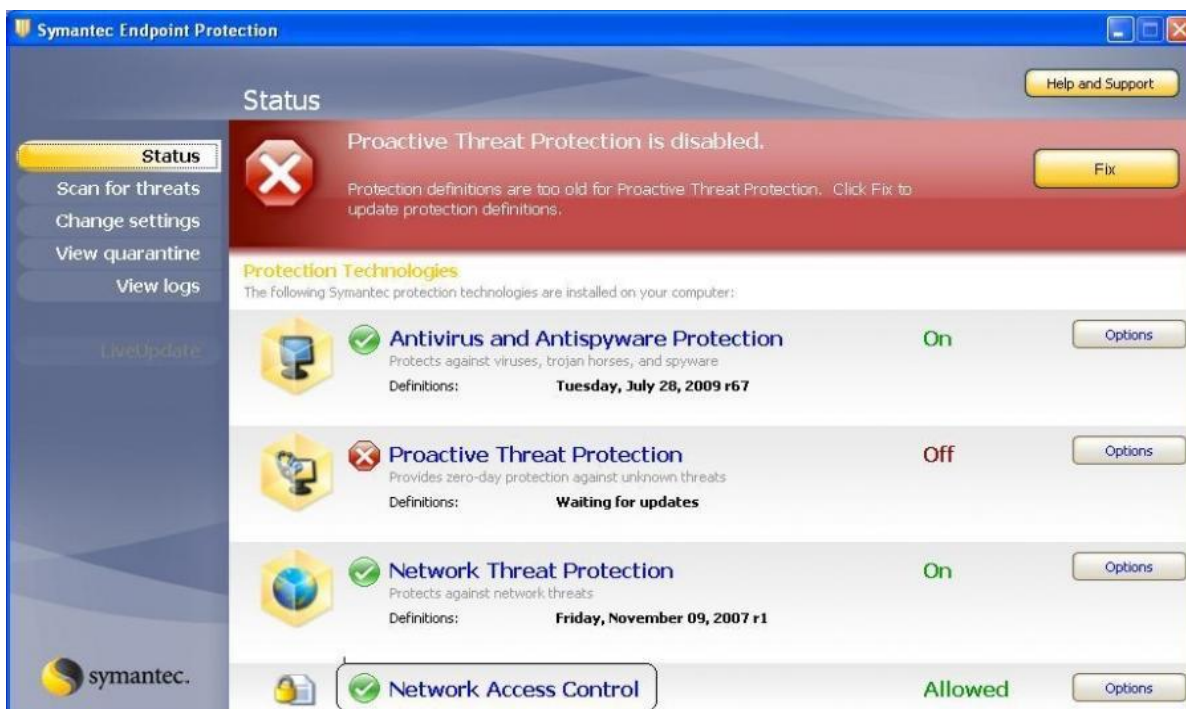

SNAC installation is complete.

How to see SNAC component on SEPM and Clients:

After the installation of SNAC "Host Integrity" policy will appear under Policies tab. Now you can modify and assign it to any group.

Once client's get the policy you will see Network Access Control on Client UI.

Symantec Enforcer Appliances

The following Linux-based Symantec Enforcer appliances work with managed clients, such as Symantec Endpoint Protection clients, and Symantec Network Access Control clients to protect the enterprise network:

■ Symantec Network Access Control **Gateway Enforcer appliance**
Gateway Enforcer appliances perform one-way checking. They check the clients that try to connect through the Gateway Enforcer appliance's external NIC to the company's network.
Please check the link for more information—
http://service1.symantec.com/SUPPORT/ent-security.nsf/docid/2008120314183848

■ Symantec Network Access Control **DHCP Enforcer appliance**
The DHCP Enforcer enforces security policies on the clients that try to access a DHCP server. Please check the link for more information—
http://service1.symantec.com/SUPPORT/ent-security.nsf/docid/2008120314183448

■ Symantec Network Access Control **LAN Enforcer appliance**
The LAN Enforcer appliance acts as a Remote Authentication Dial-In User Service (RADIUS) proxy. A LAN Enforcer appliance communicates with a switch or wireless access point that supports EAP/802.1x authentication. Please check the link for more information—
http://service1.symantec.com/SUPPORT/ent-security.nsf/docid/2008120314023148

Symantec NAC Integrated Enforcer for Microsoft DHCP Servers

The Integrated Enforcer for Microsoft DHCP Servers checks for either Symantec Endpoint Protection or Symantec Network Access Control client installations on all the DHCP clients that the DHCP server manages. It then enforces policies for those clients as configured on the Symantec Endpoint Security Manager.

Installation and configuration of the Symantec Network Access Control (NAC) integrated enforcer plug-in for Microsoft DHCP servers can be found in below link----
http://service1.symantec.com/SUPPORT/ent-security.nsf/docid/2008101315503848

Symantec NAC Integrated Enforcer for Microsoft Network Access Protection

The Integrated Enforcer for Microsoft Network Access Protection (NAP) works in concert with the Microsoft Windows Network Policy Server (NPS) on a Microsoft Windows Server 2008. The Symantec Integrated NAP Enforcer ensures that the clients that try to connect to the network comply with configured security policies.

Universal enforcement API

Universal Enforcement API Symantec has developed the Universal Enforcement API to allow other vendors with related technology to integrate their solutions with the Symantec software.

Enforcement by using Cisco NAC

Cisco Network Admissions Control Symantec clients can support the Cisco Network Admissions Control enforcement solution.