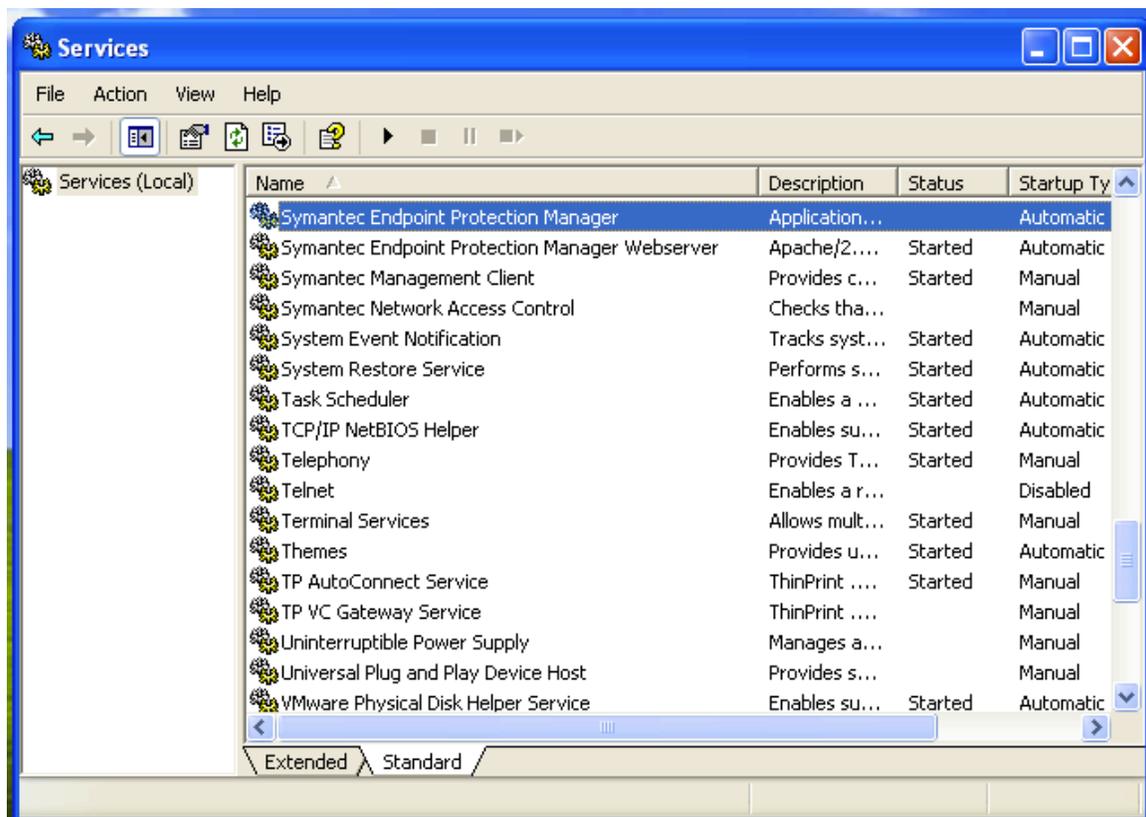


Symantec Network Access Control

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.

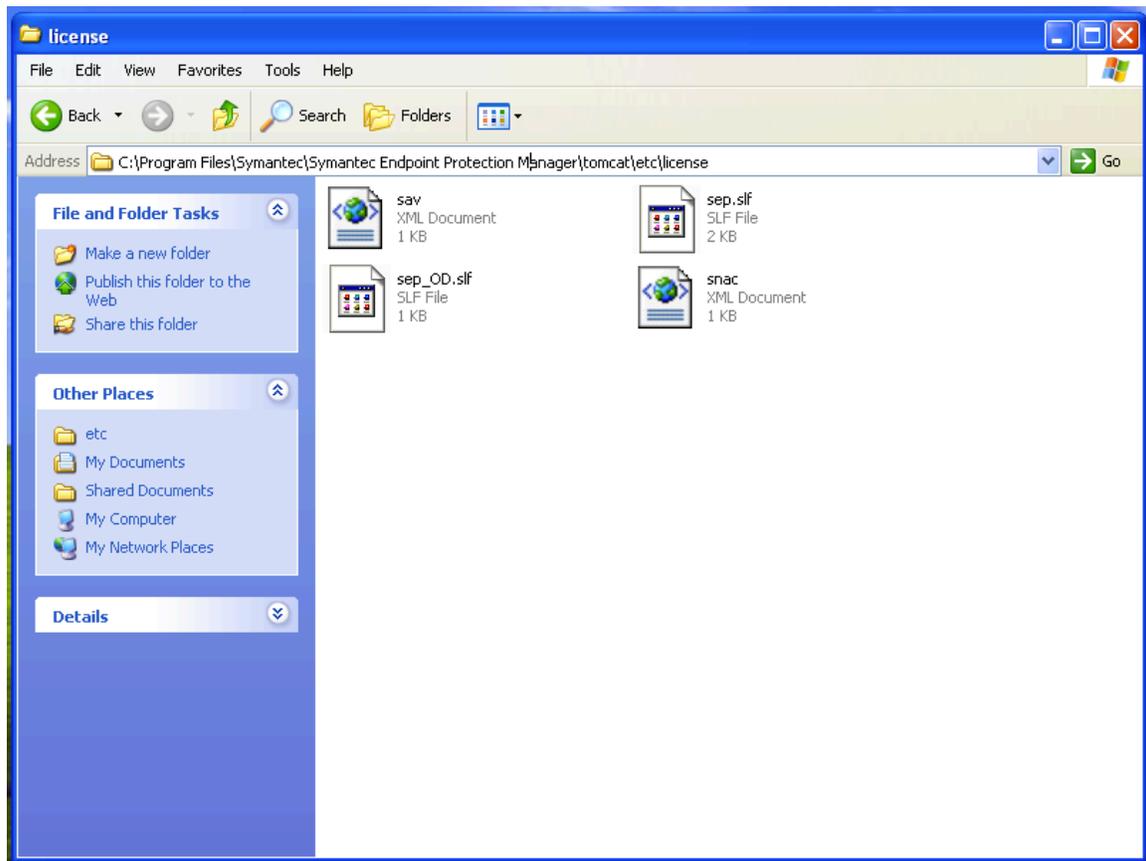
To enable the SNAC please follow the steps

Goto Services.msc and Stop the Symantec Endpoint Protection Manager Service

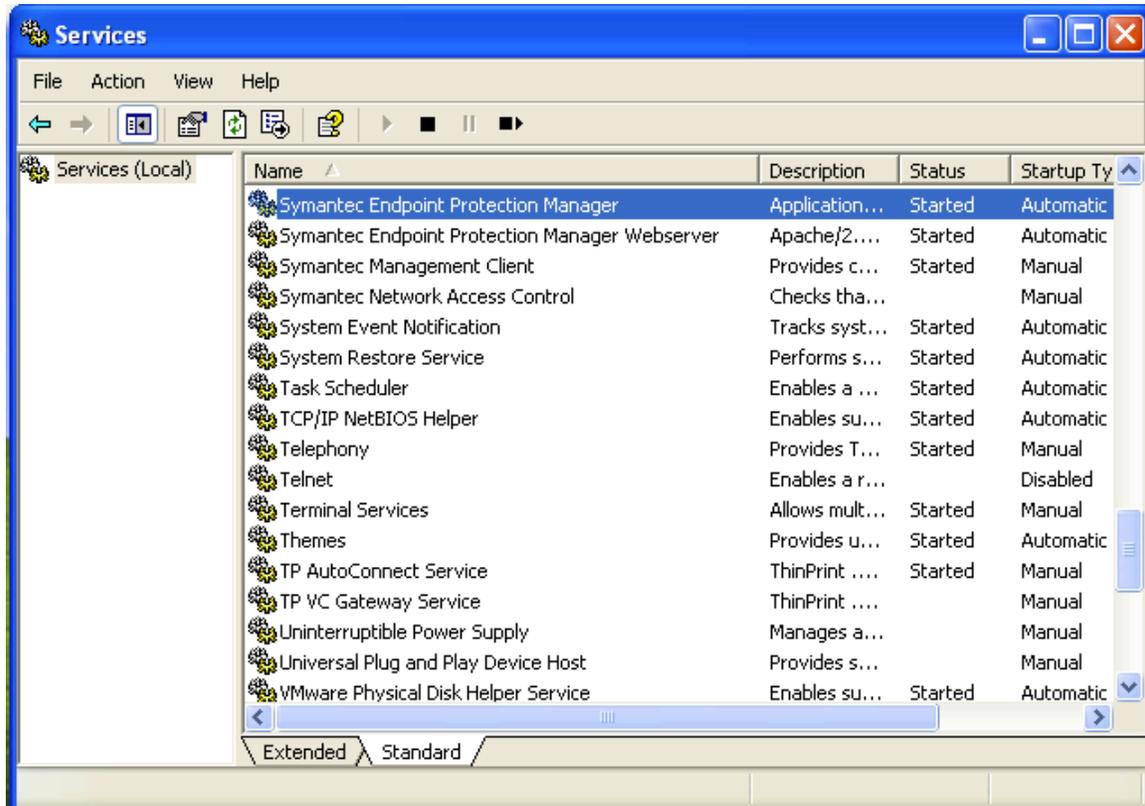


Goto C:\Program Files \Symantec \Symantec Endpoint Protection Manager \tomcat\etc\license

Paste the snac.xml files in the following location



Goto Services.msc and start the Symantec Endpoint Protection Manager Services



Logon to Symantec Endpoint Protection Manager and confirm that Host Integrity Policy is available in the Policies Tab

The screenshot displays the Symantec Endpoint Protection Manager web interface. The main content area is titled "Host Integrity Policies" and contains a table with the following data:

Name	Description	Location Use Count
Host Integrity policy	Created automatically during product installation.	0

Below the table, there is a section titled "Recent changes appear below:" with a table showing the following entry:

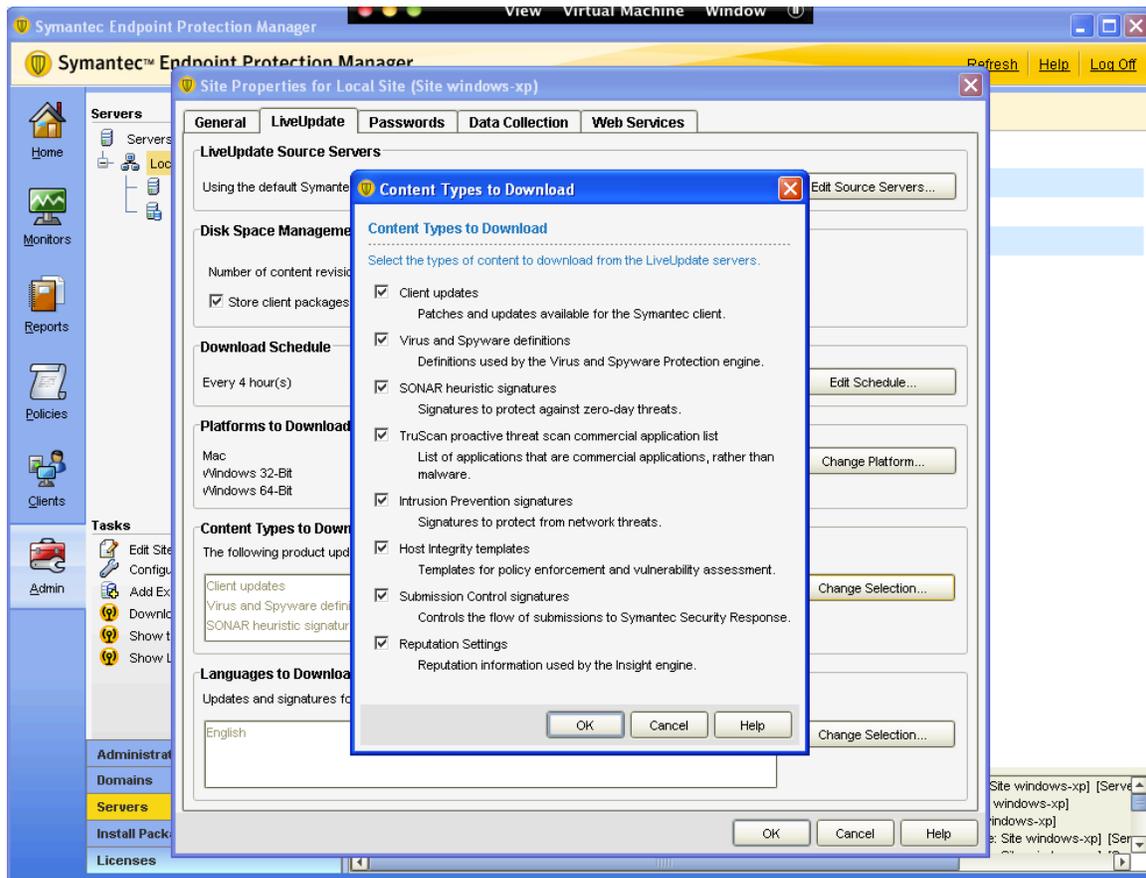
Description	Time	Administrator
Added shared policy upon system install	February 16, 2012 10:15:56 AM IST	admin

The interface also features a left-hand navigation pane with icons for Home, Monitors, Reports, Policies, Clients, and Admin. The Policies section is expanded, showing options like Virus and Spyware Protection, Firewall, Intrusion Prevention, Application and Device Control, Host Integrity, LiveUpdate, Exceptions, and Policy Components. The Admin section includes tasks such as "Add a Host Integrity policy", "Import a Host Integrity policy", and "Search for Applications".

Goto Admin => Under Tasks => Select Servers

Select Local Site => Goto Live Update tab

Under Content Type Downloads Check whether Host Integrity Templates is checked
if not checked mark it as checked

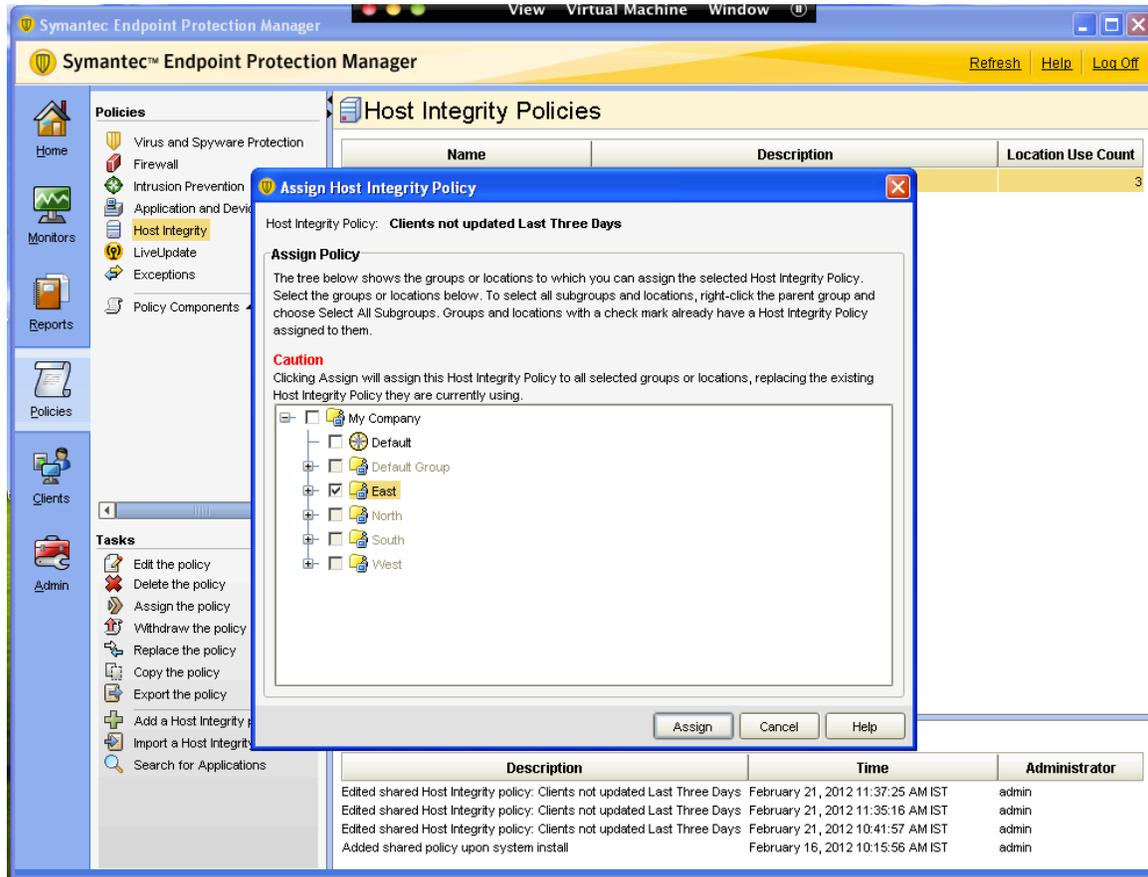


Click OK

Do a manual live update so the Host Integrity templates are available in SEPM

Goto to Start => Run => and type Luall and
Run Luall

After successful live update Host Integrity template would be downloaded in SEPM
 Assign the Host Integrity Policy to the Groups



Policy Creation for Clients, which are not updated for 3 days through NAC

Logon to Symantec Endpoint Protection Manager Console

Goto to the Clients Tab => Select the Group to which you have applied the Host Integrity Policy

The screenshot displays the Symantec Endpoint Protection Manager console. The left sidebar contains navigation options: Home, Monitors, Reports, Policies, Clients, and Admin. The 'Clients' section is expanded to show a tree view with 'My Company' as the root, containing 'Default Group', 'East', 'North', 'South', and 'West'. The 'East' client group is selected, and its configuration is shown in the main pane. The 'Policy inheritance is OFF' checkbox is checked, indicating that policies are not inherited from the parent group. The 'Location-independent Policies and Settings' section lists several policies, all of which are currently set to 'Off'. The 'Location-specific Policies and Settings' section shows a list of policies for the 'East' location, including Virus and Spyware Protection, Firewall, Intrusion Prevention, Application and Device Control, Host Integrity, LiveUpdate Settings, and Exceptions. The 'Quarantine Policies when Host Integrity Fails' section is currently empty. The 'Recent changes appear below:' section shows a log of recent actions, including editing the LiveUpdate Settings policy, changing the console mode, and adding a non-shared Virus and Spyware Protection policy.

Description	Time	Administrator
Edited shared LiveUpdate Settings policy: LiveUpdate Settings policy	February 20, 2012 1:02:49 PM IST	admin
Changed Console mode at [Default]	February 16, 2012 10:51:27 AM IST	admin
Add a non-shared [Virus and Spyware Protection Policy],<Virus an...	February 16, 2012 10:50:28 AM IST	admin

Goto Host Integrity Policy and Click Edit Shared

The screenshot shows a software window titled "Host Integrity Policy" with a blue header bar. On the left is a sidebar with a "Host Integrity Policy" icon and three menu items: "Overview" (highlighted in orange), "Requirements", and "Advanced Settings". The main area is titled "Overview" and contains two tabs: "Policy Name" (selected) and "Used By". Below the tabs, there is a section for "Policy Name" with a sub-header "Type a name and description for the policy." This section includes a "Policy name:" label and a text box containing "Host Integrity policy", and a "Description:" label and a larger text box containing "Created automatically during product installation." Below these fields is a checked checkbox labeled "Enable this policy". At the bottom of the main area, the "Created:" field shows "admin" and the "Last modified:" field shows "February 16, 2012 10:14:18 AM IST". At the very bottom of the window are three buttons: "OK", "Cancel", and "Help".

Give the name of the Policy as per your requirement

Host Integrity Policy

Host Integrity Policy

Overview

Requirements

Advanced Settings

Overview

Policy Name Used By

Policy Name

Type a name and description for the policy.

Policy name: Clients not updated Last Three Days

Description: Created automatically during product installation.

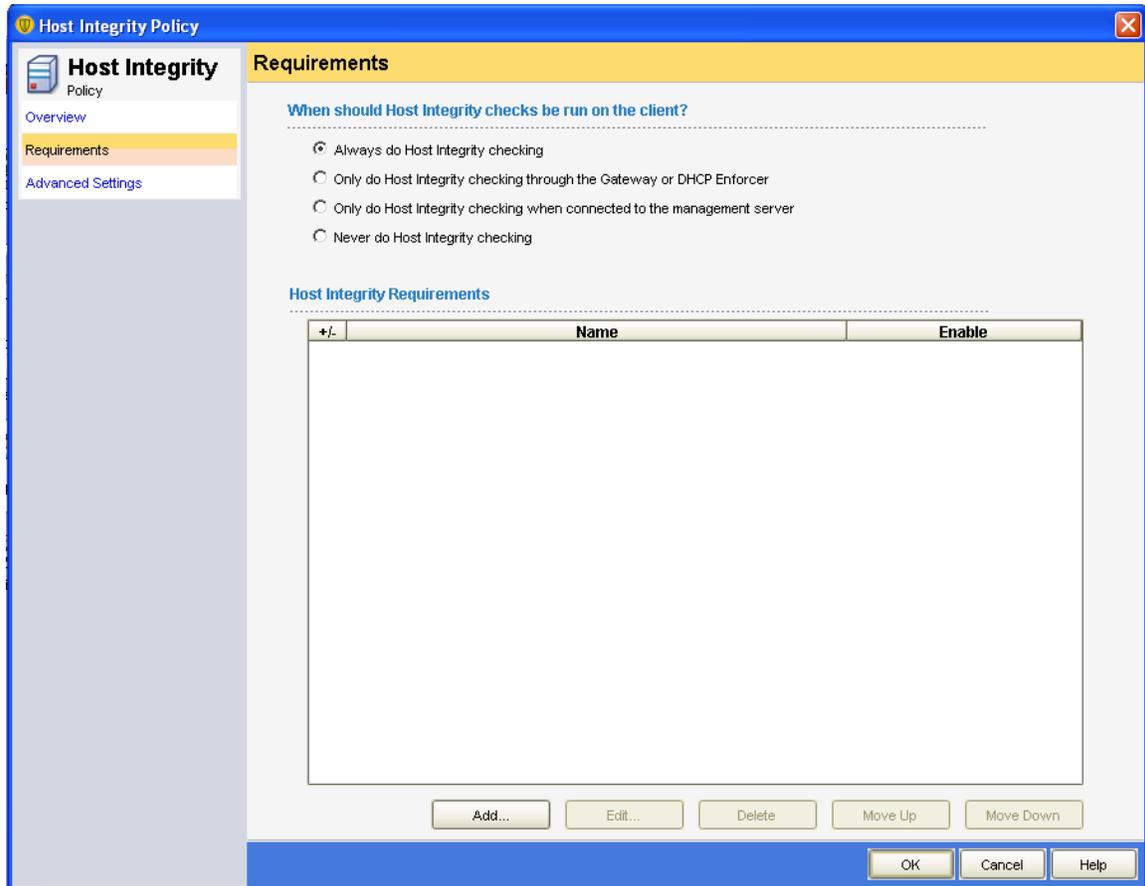
Enable this policy

Created: admin

Last modified: February 16, 2012 10:14:18 AM IST

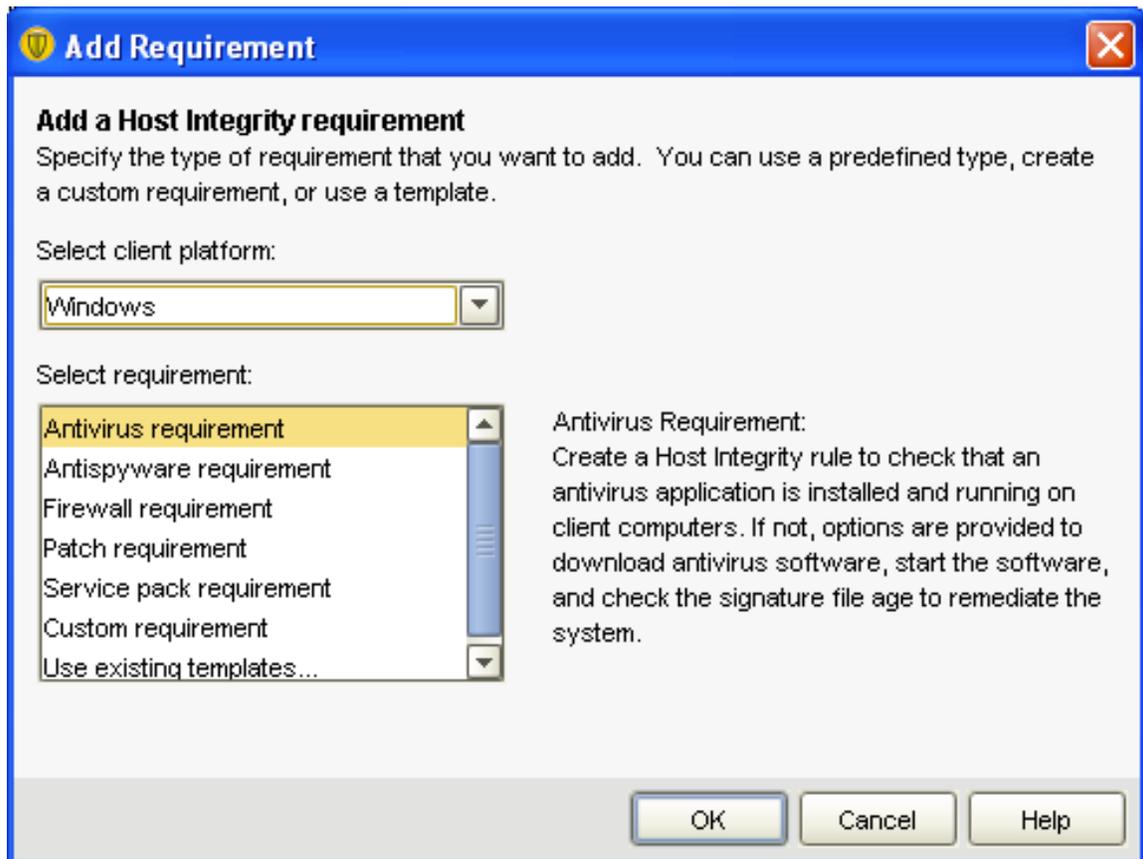
OK Cancel Help

Goto Requirements and Select Always do Host Integrity Checking



Click Add

After Clicking Add the following window will be opened



In Select Client Platform Select the OS in this scenario we have selected Windows

In Select Requirement we would select Antivirus Requirement

Click OK

In Add Requirement

Type the Name of the Requirement

Select the Antivirus application that must be installed and running: Select Symantec Endpoint Protection

Add Requirement

Name:

Client Type:

Antivirus application that must be installed and running:

Install antivirus if it has not been installed on the client

Download the installation package

Download URL:

Execute the command (use %F% to specify the downloaded file if it is available):

Start antivirus if it is not running on the client

Execute the command:

Antivirus Signature File Checking

Specify the oldest age of the signature file:

Check the signature file date

Ensure signature file date is not equal to

Ensure signature file date is equal to

Ensure signature file date is before

Ensure signature file date is after

If not, update the signature file

Download the signature file

Download URL:

Execute the command (use %F% to specify the downloaded file if it is available):

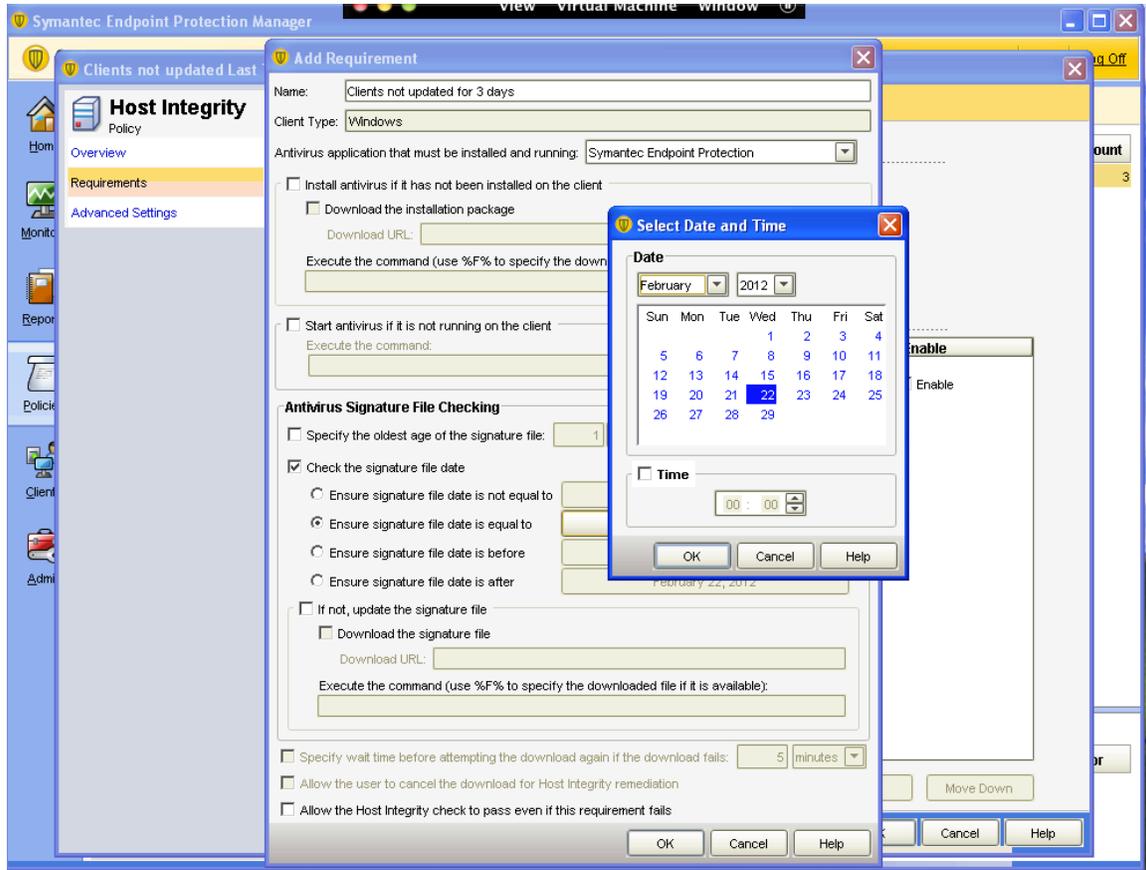
Specify wait time before attempting the download again if the download fails:

Allow the user to cancel the download for Host Integrity remediation

Allow the Host Integrity check to pass even if this requirement fails

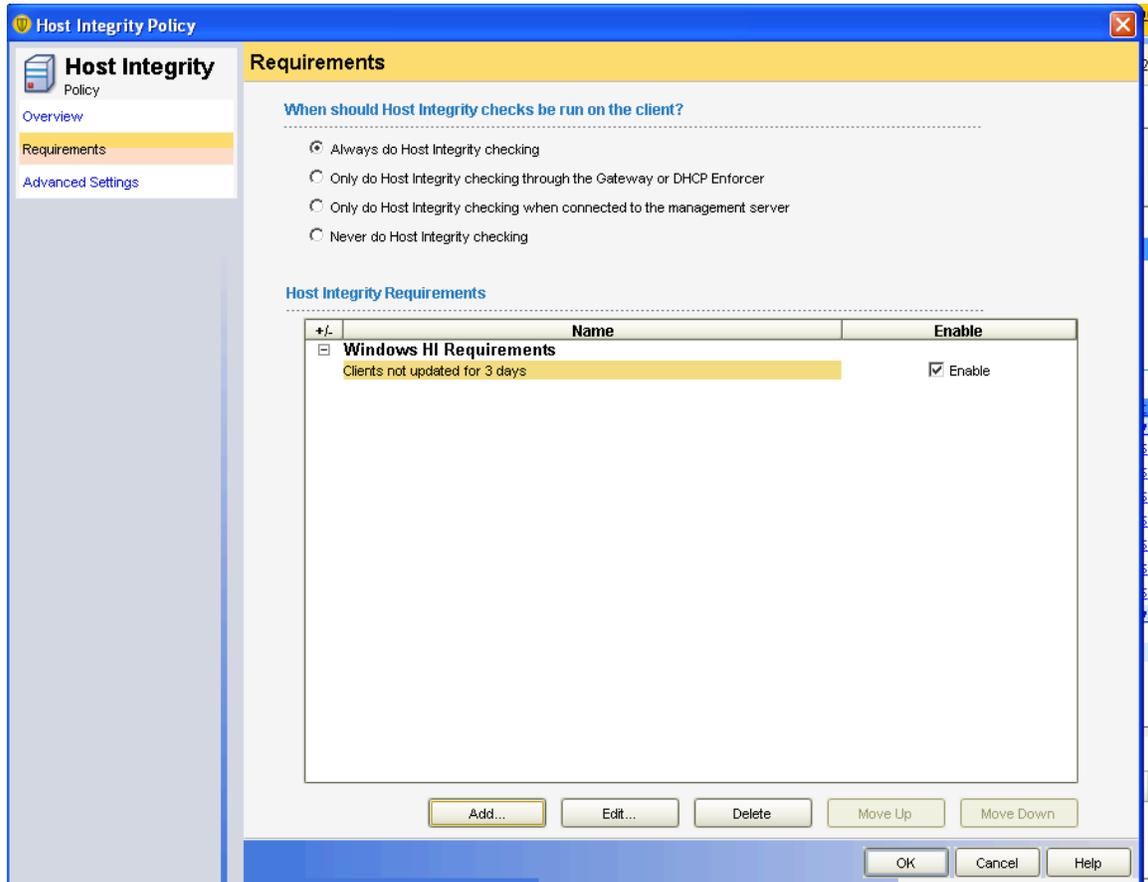
Put Check mark on “Check the signature file date

Under the Same Window Check Ensure signature date is equal to February 22 2012 and Select the date 22 (Note its only for Testing Purpose)



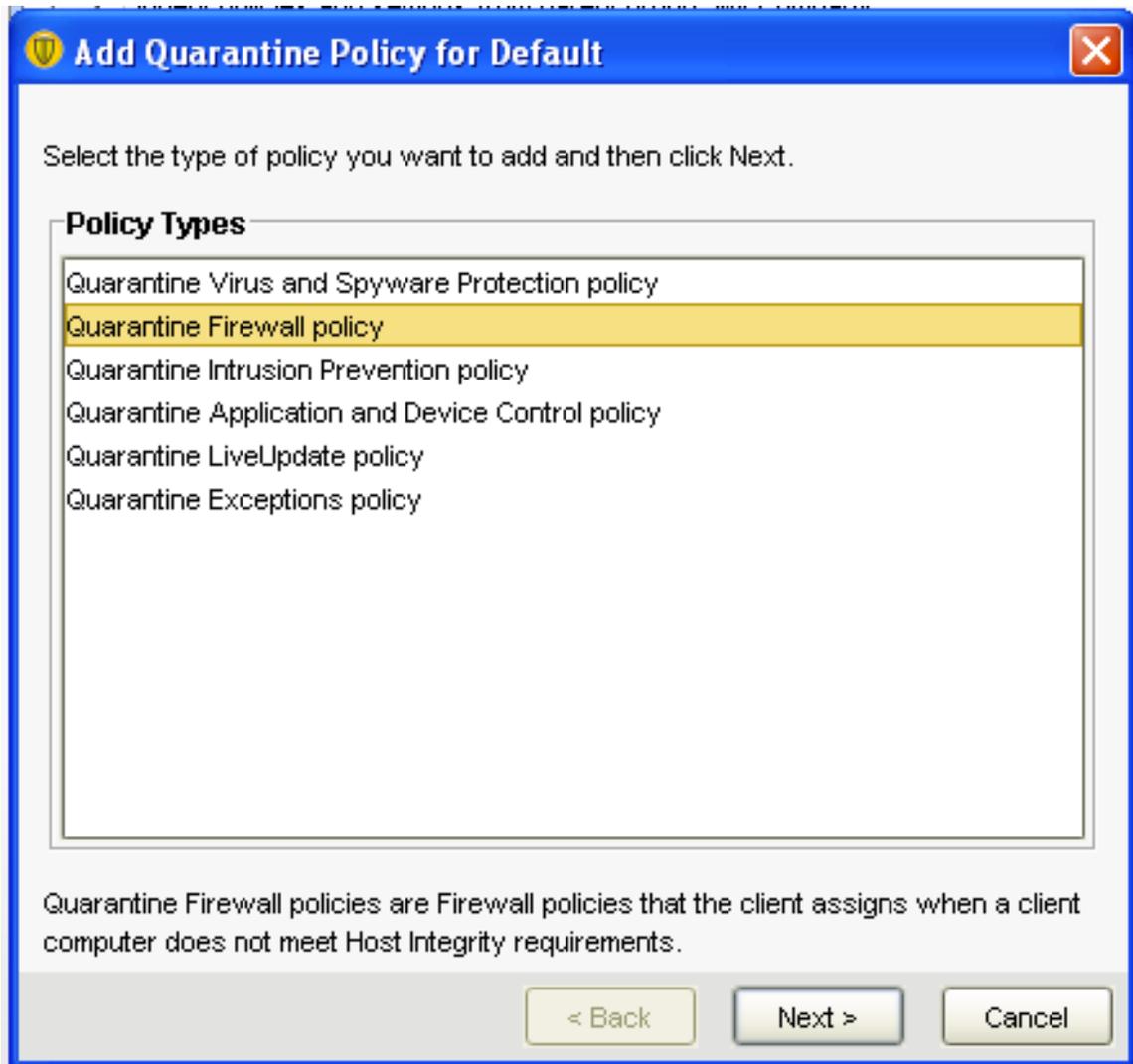
Click OK

The following window will appear
Click OK



Add Quarantine Policy for Default

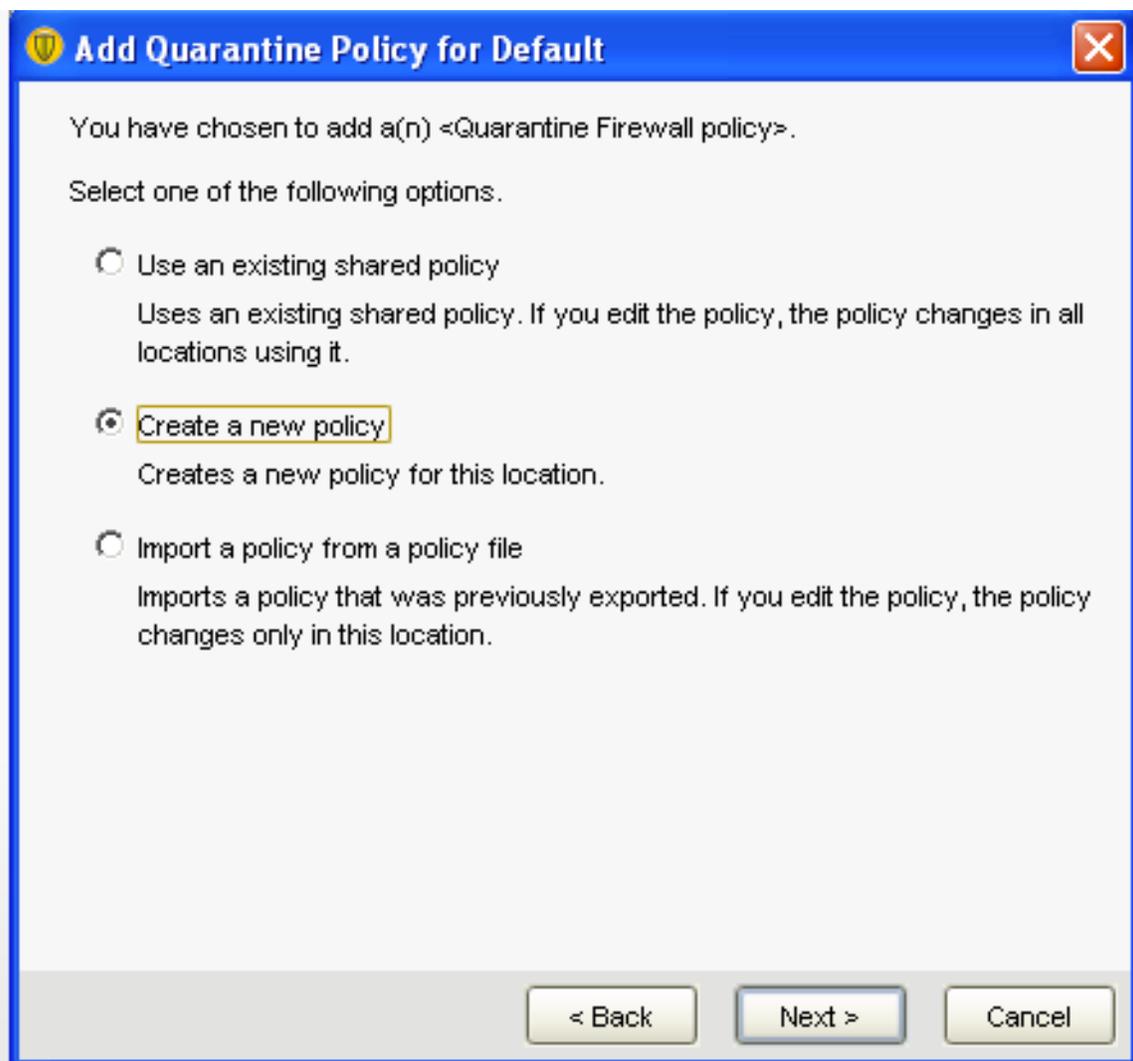
Select Quarantine Firewall Policy and Click Next



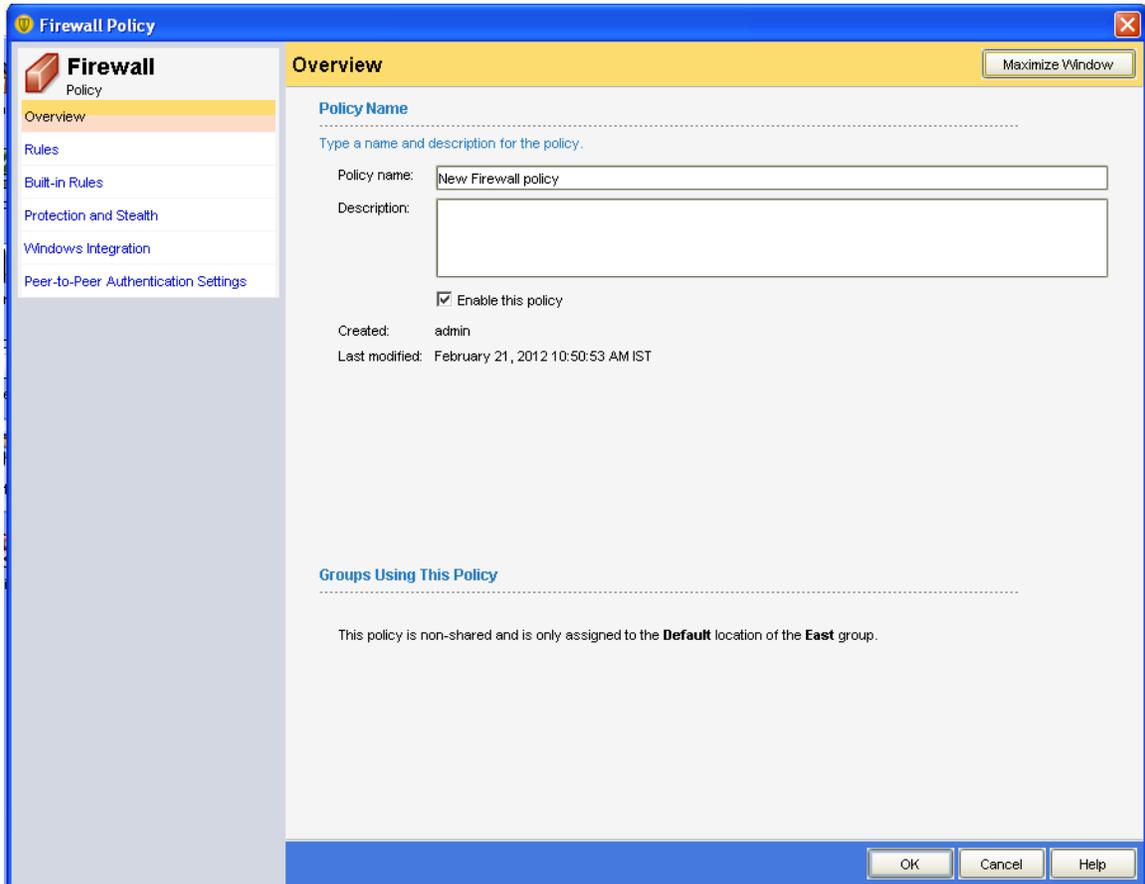
In Add Quarantine Policy for Default

Select Create a New Policy

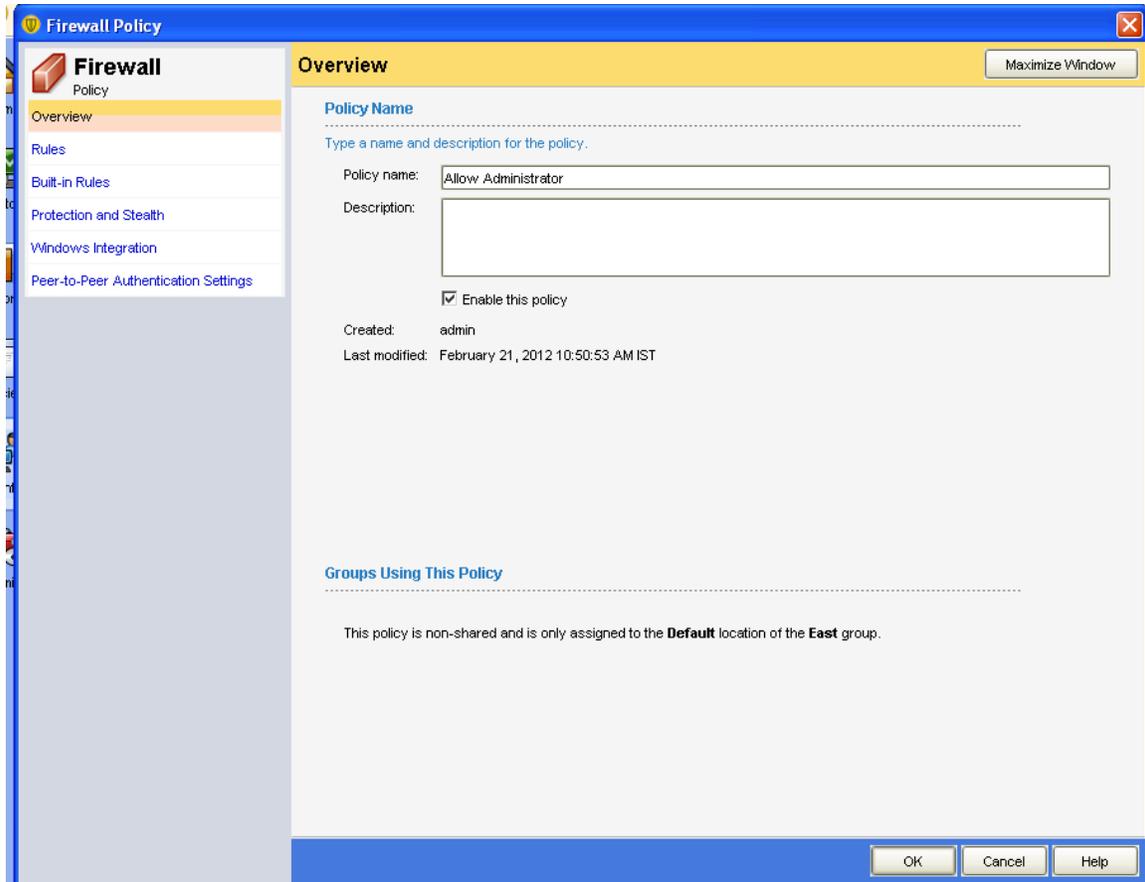
Click Next



After Clicking Next Firewall Policy window will get opened



In Overview Add the name of the Policy



In Rules Window Add Blank Rule

The screenshot shows the Windows Firewall Policy Rules window. The left sidebar contains navigation options: Overview, Rules (selected), Built-in Rules, Protection and Stealth, Windows Integration, and Peer-to-Peer Authentication Settings. The main area is titled 'Rules' and contains a table of firewall rules. Below the table are buttons for 'Add Rule...', 'Add Blank Rule', 'Delete Rule', 'Move Up', and 'Move Down'. At the bottom are 'OK', 'Cancel', and 'Help' buttons.

Firewall Policy

Firewall Policy

Overview

Rules

Built-in Rules

Protection and Stealth

Windows Integration

Peer-to-Peer Authentication Settings

Rules Notifications

Maximize Window

Firewall Rules

Firewall rules allow, block and log network traffic. You can add higher priority rules in the table below.

Inherit Firewall Rules from Parent Group

No	En...	Name	Action	Application	Host	Service	Log	Severity
1	<input checked="" type="checkbox"/>	Rule 0	Allow	* Any	* Any	* Any	None	5-Major
2	<input type="checkbox"/>	Block IPv6	Block	* Any	* Any	Ethe...	None	10-Minor
3	<input checked="" type="checkbox"/>	Block IPv6 over IPv4 (Ter...	Block	* Any	* Any	UDP:...	None	10-Minor
4	<input checked="" type="checkbox"/>	Block IPv6 over IPv4 (ISA...	Block	* Any	* Any	IP:[41]	None	10-Minor
5	<input checked="" type="checkbox"/>	Allow fragmented packets	Allow	* Any	* Any	IP:[fr...	None	10-Minor
6	<input checked="" type="checkbox"/>	Allow wireless EAPOL	Allow	* Any	* Any	Ethe...	None	10-Minor
7	<input checked="" type="checkbox"/>	Allow Local File Sharing t...	Allow	* Any	Remot...	TCP:...	None	10-Minor
8	<input checked="" type="checkbox"/>	Block Local File Sharing	Block	* Any	* Any	TCP:..., UDP:...	Write t...	10-Minor
9	<input checked="" type="checkbox"/>	Allow Bootp	Allow	* Any	* Any	UDP:...	None	10-Minor
10	<input checked="" type="checkbox"/>	Allow UPnP Discovery fr...	Allow	* Any	Remot...	UDP:...	None	10-Minor
11	<input checked="" type="checkbox"/>	Block UPnP Discovery	Block	* Any	* Any	UDP:...	Write t...	10-Minor
12	<input checked="" type="checkbox"/>	Allow Web Service requ...	Allow	* Any	Remot...	TCP:...	None	10-Minor
13	<input checked="" type="checkbox"/>	Block Web Service requ...	Block	* Any	* Any	TCP:..., UDP:...	Write t...	10-Minor
14	<input checked="" type="checkbox"/>	Allow LLMNR from privat...	Allow	* Any	Remot..., Remot...	UDP:...	None	10-Minor

Add Rule... Add Blank Rule Delete Rule Move Up Move Down

OK Cancel Help

In Rule Select Host and Double Click on Host

Firewall Policy

Firewall Policy

Overview

Rules

Built-in Rules

Protection and Stealth

Windows Integration

Peer-to-Peer Authentication Settings

Rules Notifications

Firewall Rules

Firewall rules allow, block and log network traffic. You can add higher priority rules in the table below.

Inherit Firewall Rules from Parent Group

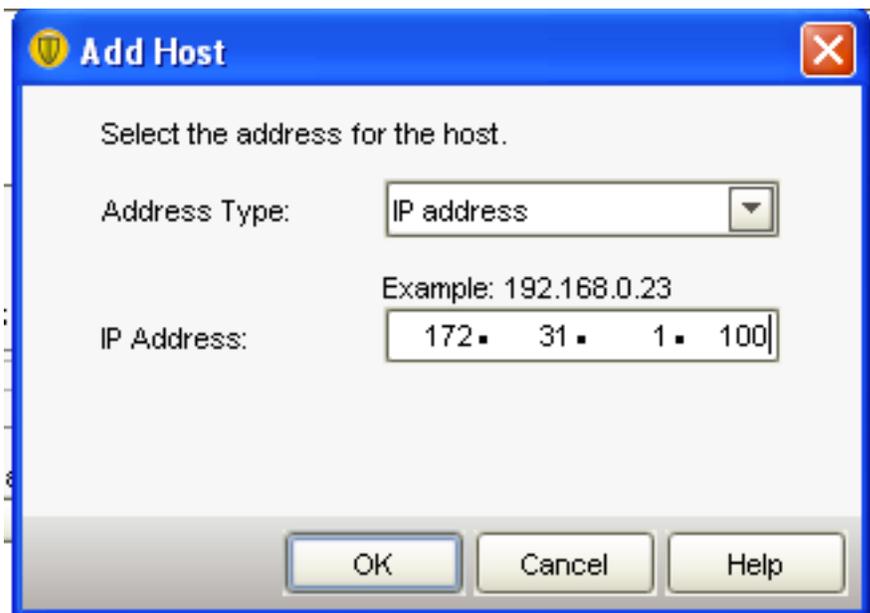
No	En...	Name	Action	Application	Host	Service	Log	Severity
1	<input checked="" type="checkbox"/>	Rule 0	Allow	* Any	* Any	* Any	None	5-Major
2	<input type="checkbox"/>	Block IPv6	Block	* Any	* Any	Ethe...	None	10-Minor
3	<input checked="" type="checkbox"/>	Block IPv6 over IPv4 (Ter...	Block	* Any	* Any	UDP:...	None	10-Minor
4	<input checked="" type="checkbox"/>	Block IPv6 over IPv4 (ISA...	Block	* Any	* Any	IP:[41]	None	10-Minor
5	<input checked="" type="checkbox"/>	Allow fragmented packets	Allow	* Any	* Any	IP:[fr...	None	10-Minor
6	<input checked="" type="checkbox"/>	Allow wireless EAPOL	Allow	* Any	* Any	Ethe...	None	10-Minor
7	<input checked="" type="checkbox"/>	Allow Local File Sharing t...	Allow	* Any	Remot...	TCP:...	None	10-Minor
8	<input checked="" type="checkbox"/>	Block Local File Sharing	Block	* Any	* Any	TCP:...	Write t...	10-Minor
9	<input checked="" type="checkbox"/>	Allow Bootp	Allow	* Any	* Any	UDP:...	None	10-Minor
10	<input checked="" type="checkbox"/>	Allow UPnP Discovery fr...	Allow	* Any	Remot...	UDP:...	None	10-Minor
11	<input checked="" type="checkbox"/>	Block UPnP Discovery	Block	* Any	* Any	UDP:...	Write t...	10-Minor
12	<input checked="" type="checkbox"/>	Allow Web Service requ...	Allow	* Any	Remot...	TCP:...	None	10-Minor
13	<input checked="" type="checkbox"/>	Block Web Service requ...	Block	* Any	* Any	TCP:...	Write t...	10-Minor
14	<input checked="" type="checkbox"/>	Allow LLMNR from privat...	Allow	* Any	Remot...	UDP:...	None	10-Minor

Add Rule... Add Blank Rule Delete Rule Move Up Move Down

OK Cancel Help

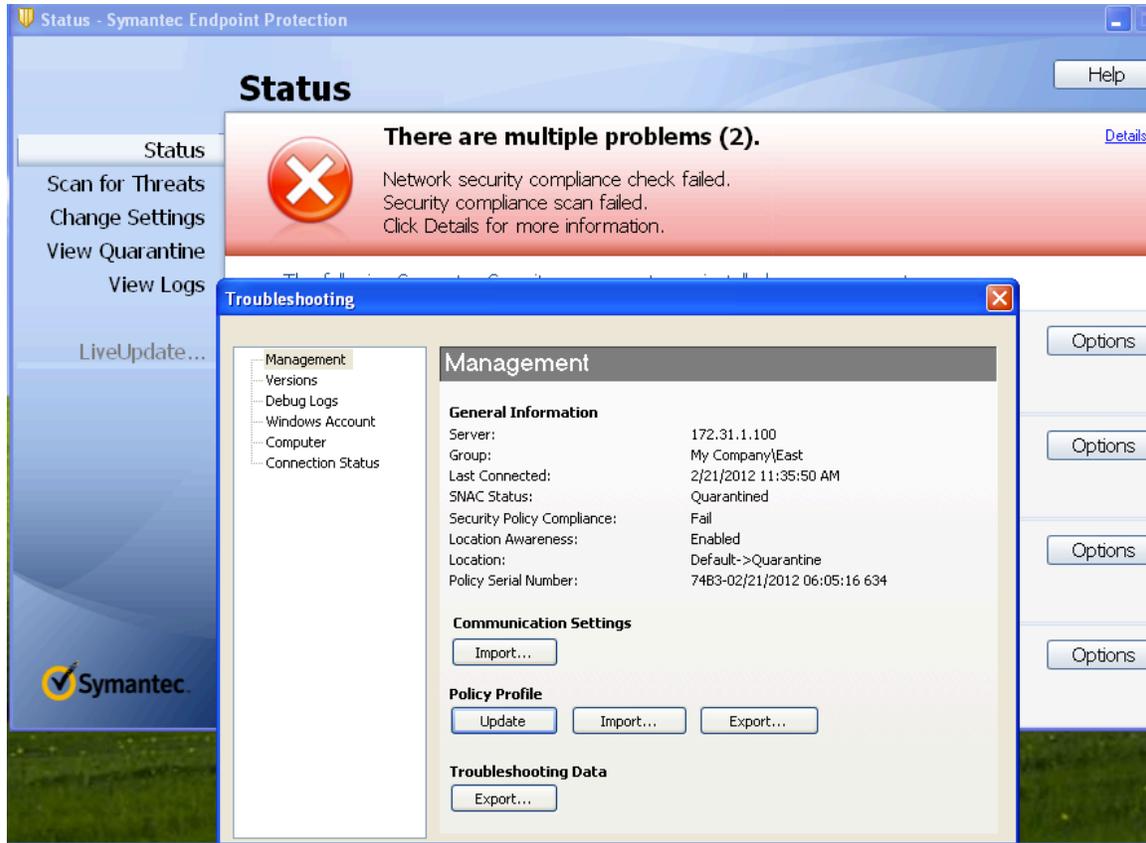
After Double Clicking following Windows will be opened

In Remote Add the IP Address of the System in case the any system fails host integrity test the system IP Address Added can access the Host Integrity Failed to Access the System



Click OK and Once Again Click OK

Host Integrity as the definition was not latest and the System will be disconnected from Network



Again Add Blank Rule in Firewall and Name it as Block

Firewall Policy Maximize Window

Firewall Policy

- Overview
- Rules**
- Built-in Rules
- Protection and Stealth
- Windows Integration
- Peer-to-Peer Authentication Settings

Rules Notifications

Firewall Rules

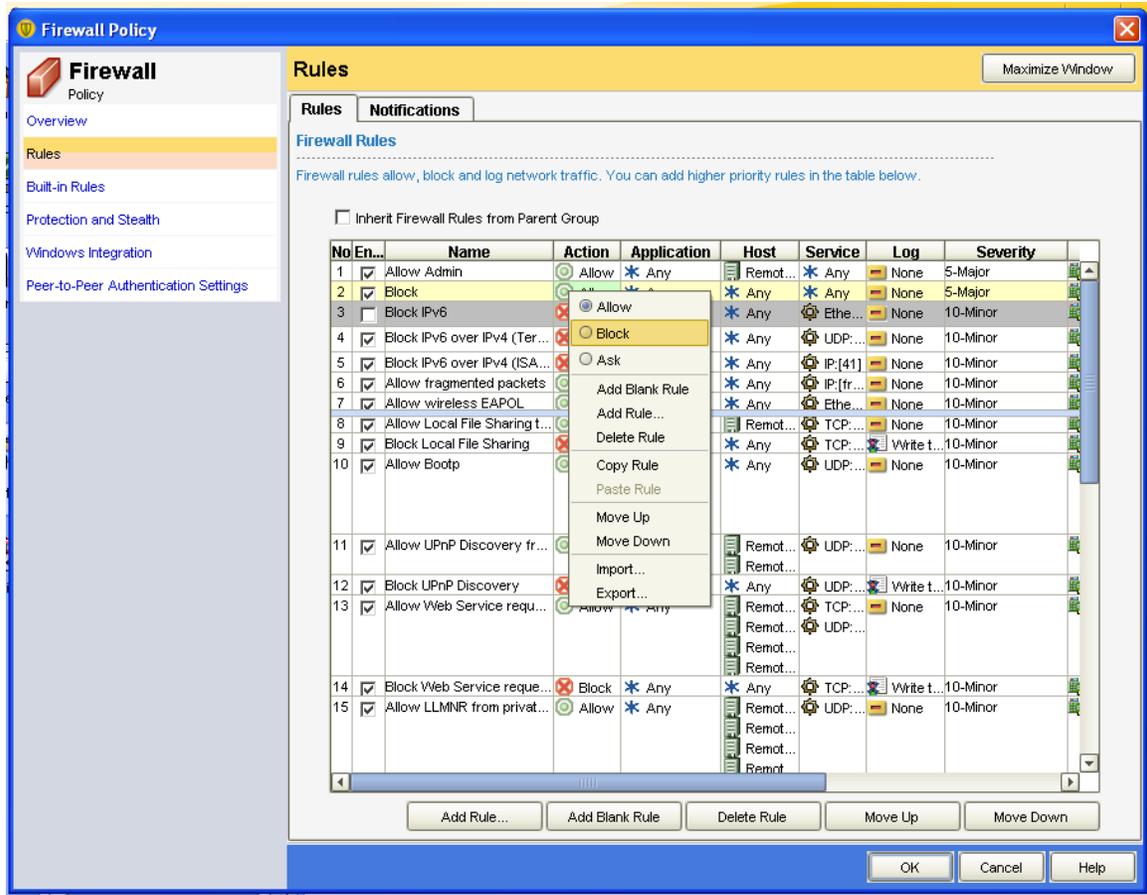
Firewall rules allow, block and log network traffic. You can add higher priority rules in the table below.

Inherit Firewall Rules from Parent Group

No	En...	Name	Action	Application	Host	Service	Log	Severity
1	<input checked="" type="checkbox"/>	Allow Admin	Allow	* Any	Remot...	* Any	None	5-Major
2	<input checked="" type="checkbox"/>	Block	Allow	* Any	* Any	* Any	None	5-Major
3	<input type="checkbox"/>	Block IPv6	Block	* Any	* Any	Ethe...	None	10-Minor
4	<input checked="" type="checkbox"/>	Block IPv6 over IPv4 (Ter...	Block	* Any	* Any	UDP:...	None	10-Minor
5	<input checked="" type="checkbox"/>	Block IPv6 over IPv4 (ISA...	Block	* Any	* Any	IP:[41]	None	10-Minor
6	<input checked="" type="checkbox"/>	Allow fragmented packets	Allow	* Any	* Any	IP:[fr...	None	10-Minor
7	<input checked="" type="checkbox"/>	Allow wireless EAPOL	Allow	* Any	* Any	Ethe...	None	10-Minor
8	<input checked="" type="checkbox"/>	Allow Local File Sharing t...	Allow	* Any	Remot...	TCP:...	None	10-Minor
9	<input checked="" type="checkbox"/>	Block Local File Sharing	Block	* Any	* Any	TCP:...	Write t...	10-Minor
10	<input checked="" type="checkbox"/>	Allow Bootp	Allow	* Any	* Any	UDP:...	None	10-Minor
11	<input checked="" type="checkbox"/>	Allow UPnP Discovery fr...	Allow	* Any	Remot...	UDP:...	None	10-Minor
12	<input checked="" type="checkbox"/>	Block UPnP Discovery	Block	* Any	* Any	UDP:...	Write t...	10-Minor
13	<input checked="" type="checkbox"/>	Allow Web Service requ...	Allow	* Any	Remot...	TCP:...	None	10-Minor
14	<input checked="" type="checkbox"/>	Block Web Service requ...	Block	* Any	* Any	TCP:...	Write t...	10-Minor
15	<input checked="" type="checkbox"/>	Allow LLNMR from privat...	Allow	* Any	Remot...	UDP:...	None	10-Minor

Select the Block Rule Right and in Action Select Block

Click OK



Click OK