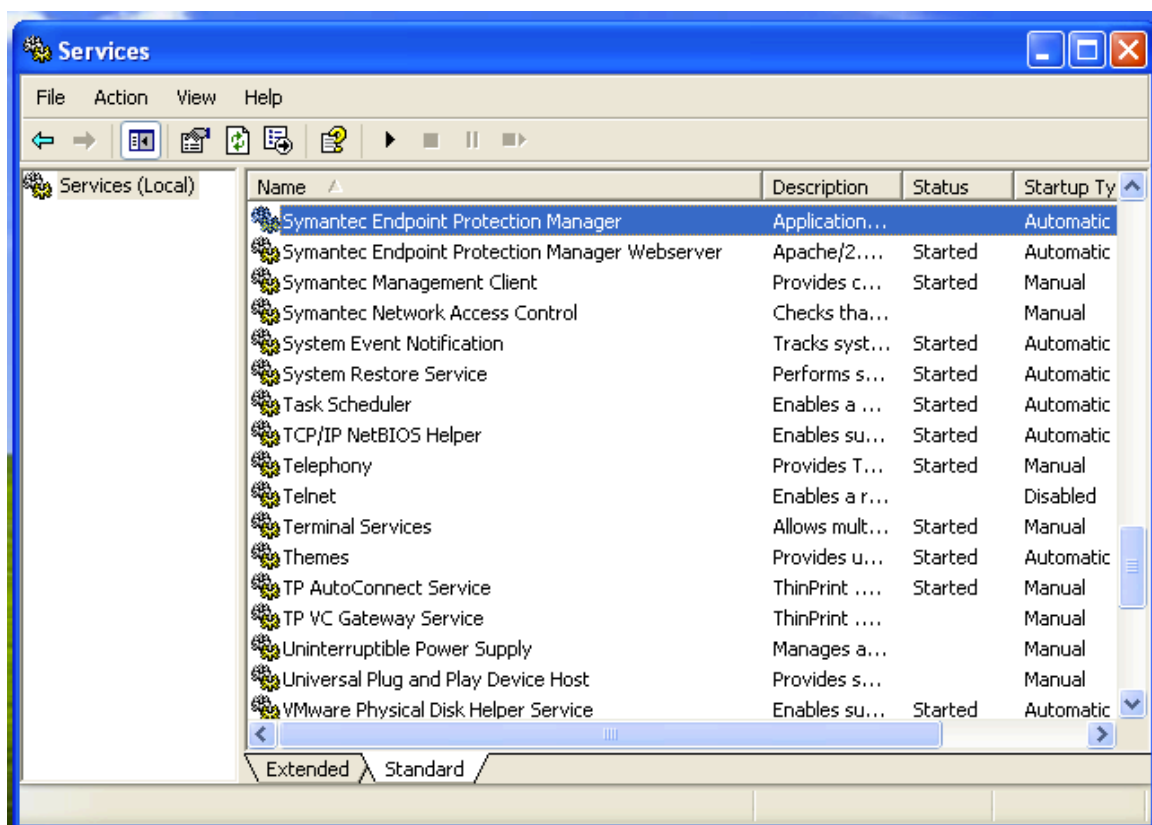


## Symantec Network Access Control

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.

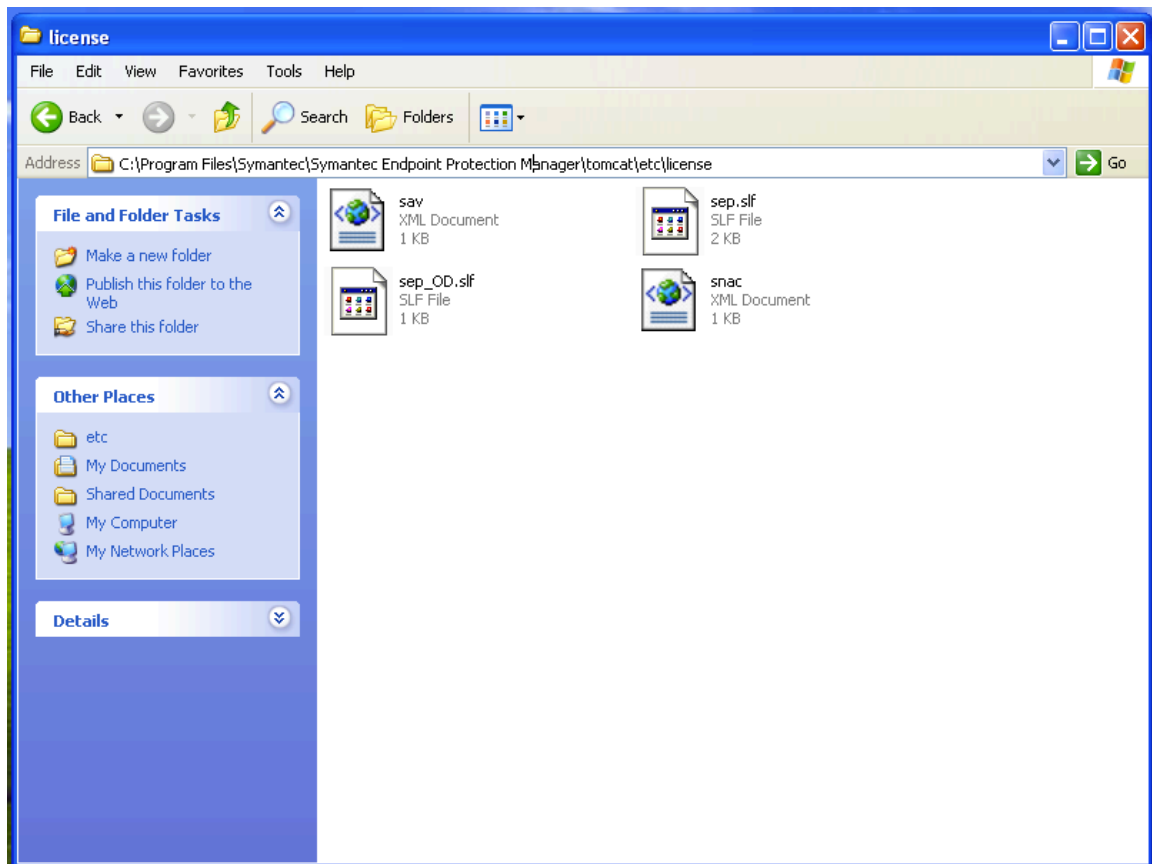
To enable the SNAC please follow the steps

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

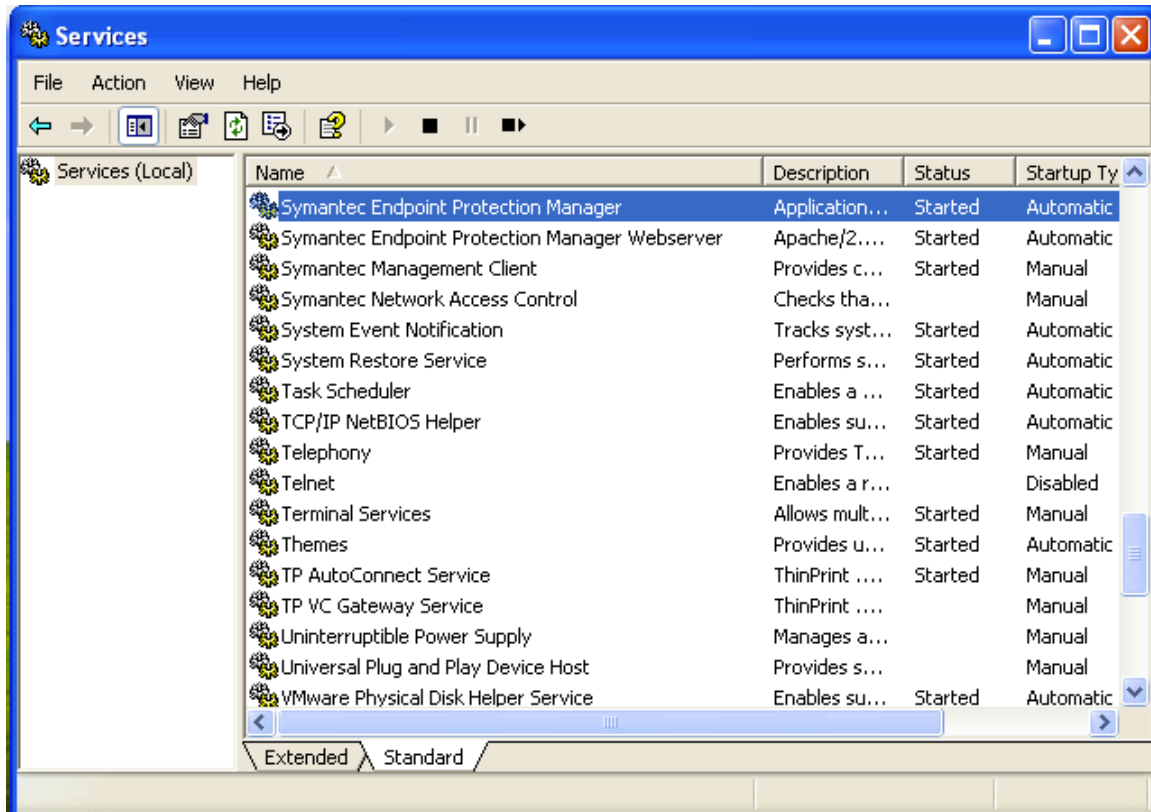


Goto C:\Program Files \Symantec \Symantec Endpoint Protection Manager \tomcat\etc\license

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 left sidebar contains navigation links: Home, Monitors, Reports, Policies (selected), Clients, and Admin. The 'Policies' section is expanded, showing a list of policy components: Virus and Spyware Protection, Firewall, Intrusion Prevention, Application and Device Control, Host Integrity (highlighted), LiveUpdate, Exceptions, and Policy Components. The main content area is titled 'Host Integrity Policies' and features a table with the following data:

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

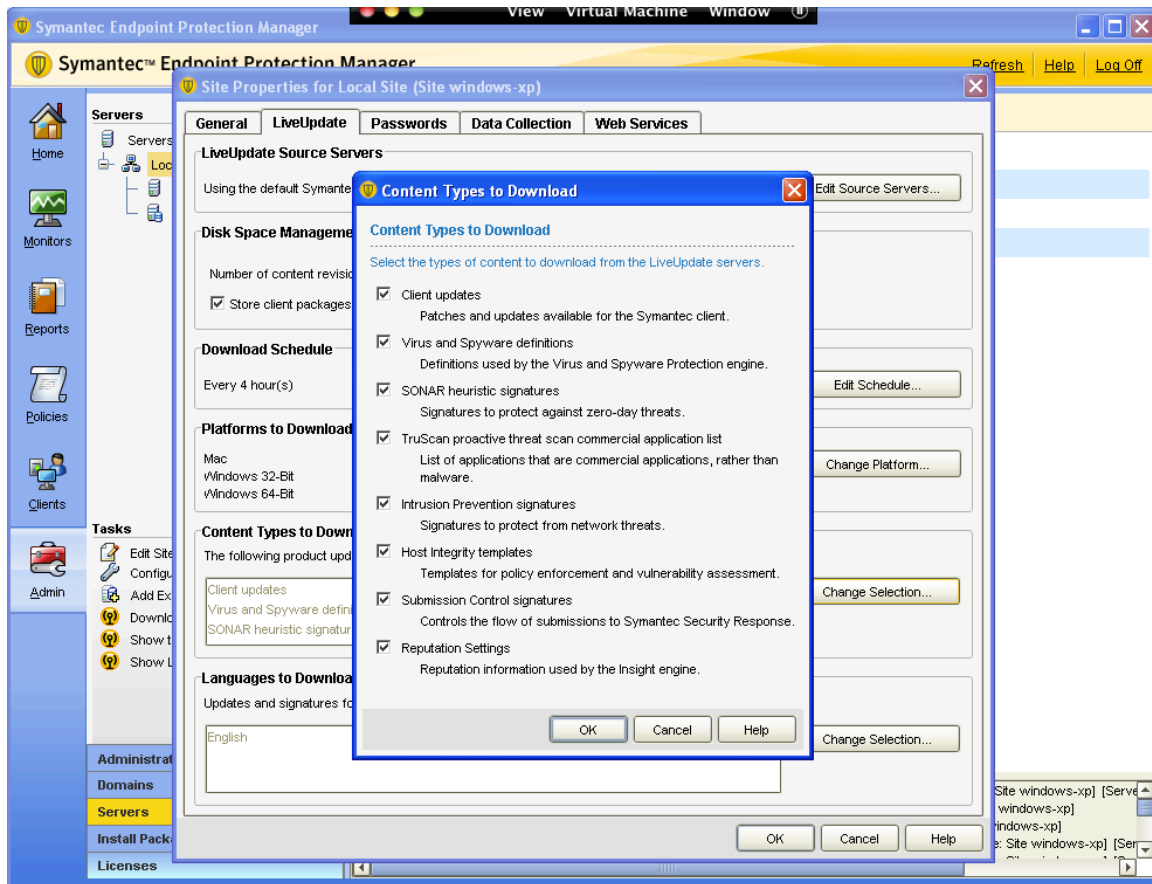
Below the table, a section titled 'Recent changes appear below:' contains another table:

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

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

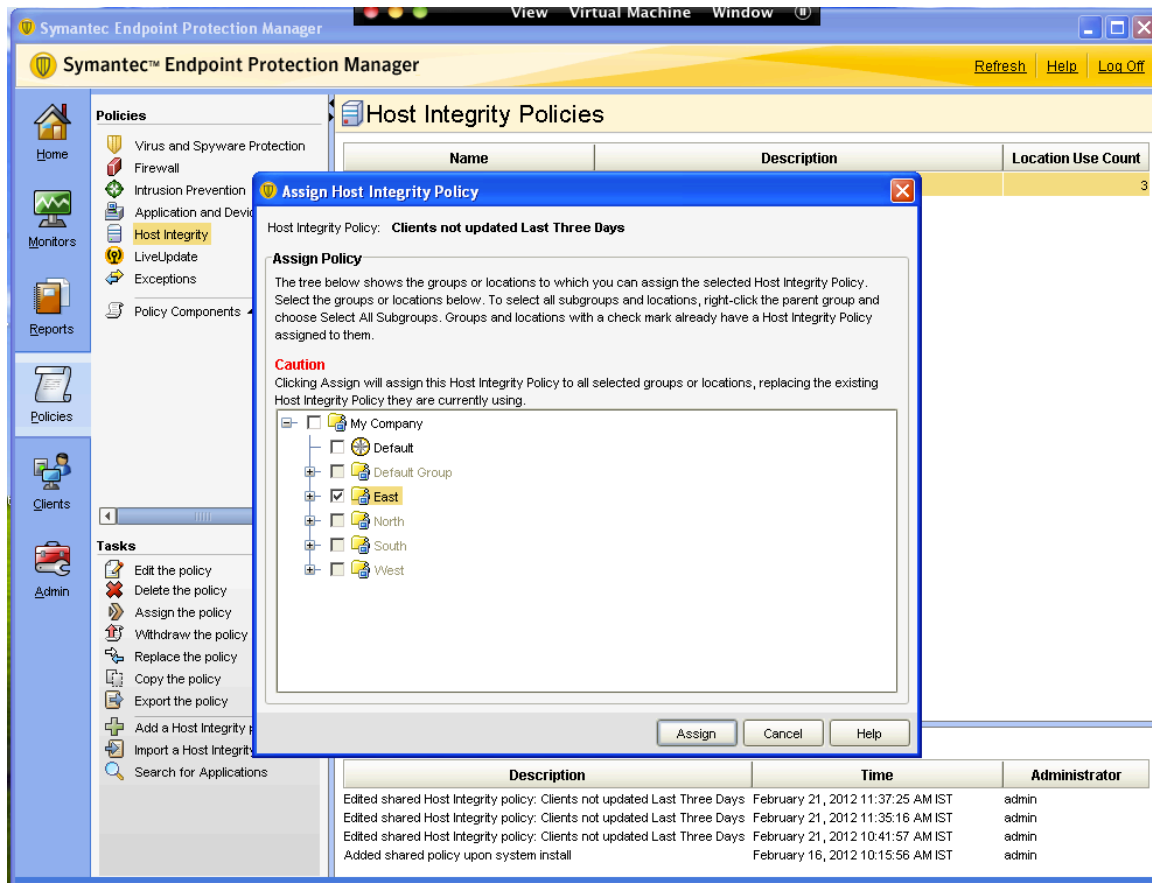


Click OK

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

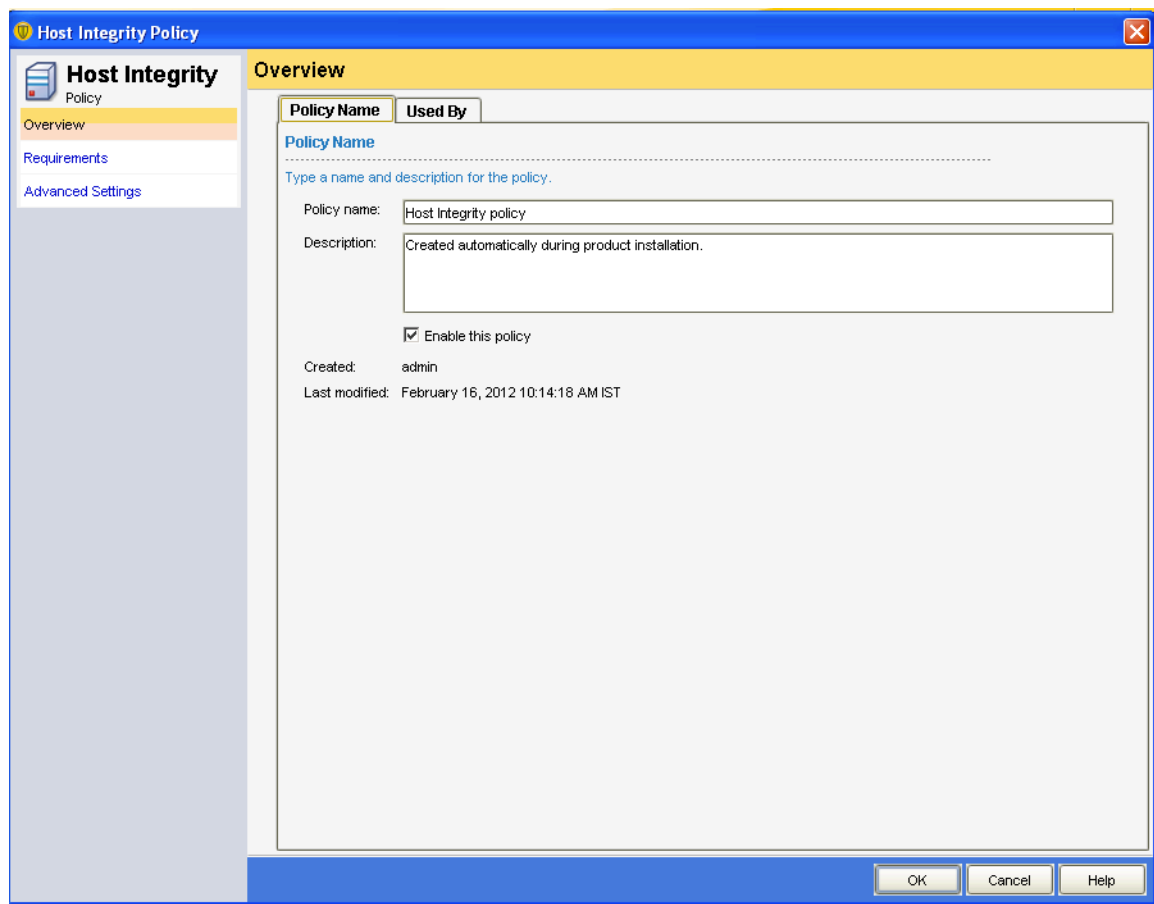
Logon to Symantec Endpoint Protection Manager Console

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 icons for Home, Monitors, Reports, Policies, Clients, and Admin. The 'Clients' tab is selected, showing a tree view with 'My Company' as the root, containing 'Default Group', 'East', 'North', 'South', and 'West'. The 'East' group is highlighted. The main pane shows the configuration for the 'East' client group. At the top, it says 'Policy serial number: 74B3-02/21/2012 04:30:26 034'. Below this are tabs for 'Clients', 'Policies', 'Details', and 'Install Packages'. The 'Policies' tab is active, showing 'Policy inheritance is OFF' and a checkbox to 'Inherit policies and settings from parent group "My Company"'. The main content area is divided into two sections: 'Location-independent Policies and Settings' and 'Location-specific Policies and Settings'. The 'Location-independent' section has a table with columns 'Policies' and 'Settings'. The 'Location-specific' section shows 'Settings for Location: Default' and a list of policies for 'East', including 'Virus and Spyware Protection policy - Balanced [non-shared]', 'Firewall policy [shared]', 'Intrusion Prevention policy [shared]', 'Application and Device Control policy [shared]', 'Host Integrity policy [shared]', 'LiveUpdate Settings policy [shared]', and 'Exceptions policy [shared]'. Each policy has a 'Tasks' link. Below this is a section for 'Quarantine Policies when Host Integrity Fails' with a link to 'Add a policy...'. At the bottom, a table shows 'Recent changes appear below:' with columns for 'Description', 'Time', and 'Administrator'.

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 image shows a software window titled "Host Integrity Policy" with a standard Windows-style title bar (blue background, yellow close button). On the left is a sidebar with a "Host Integrity" header and three sub-items: "Policy" (selected), "Overview", "Requirements", and "Advanced Settings". The main area is titled "Overview" and contains a tabbed interface with "Policy Name" and "Used By" tabs. The "Policy Name" tab is active, showing a form with the following fields:

- Policy name:** A text box containing "Host Integrity policy".
- Description:** A text box containing "Created automatically during product installation."
- Enable this policy:** A checked checkbox.
- Created:** A label with the value "admin".
- Last modified:** A label with the value "February 16, 2012 10:14:18 AM IST".

At the bottom right of the window are three buttons: "OK", "Cancel", and "Help".



Give the name of the Policy as per your requirement

The screenshot shows a software window titled "Host Integrity Policy" with a standard Windows-style title bar (blue with a close button). 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" (active) and "Used By". Below the tabs, there is a section for defining the policy. It starts with a blue link "Policy Name" followed by a dotted line and the instruction "Type a name and description for the policy.". There are two input fields: "Policy name:" with the text "Clients not updated Last Three Days" and "Description:" with the text "Created automatically during product installation.". Below these fields is a checkbox labeled "Enable this policy" which is checked. At the bottom left of the main area, it shows "Created: admin" and "Last modified: February 16, 2012 10:14:18 AM IST". At the bottom right of the window are three buttons: "OK", "Cancel", and "Help".

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.

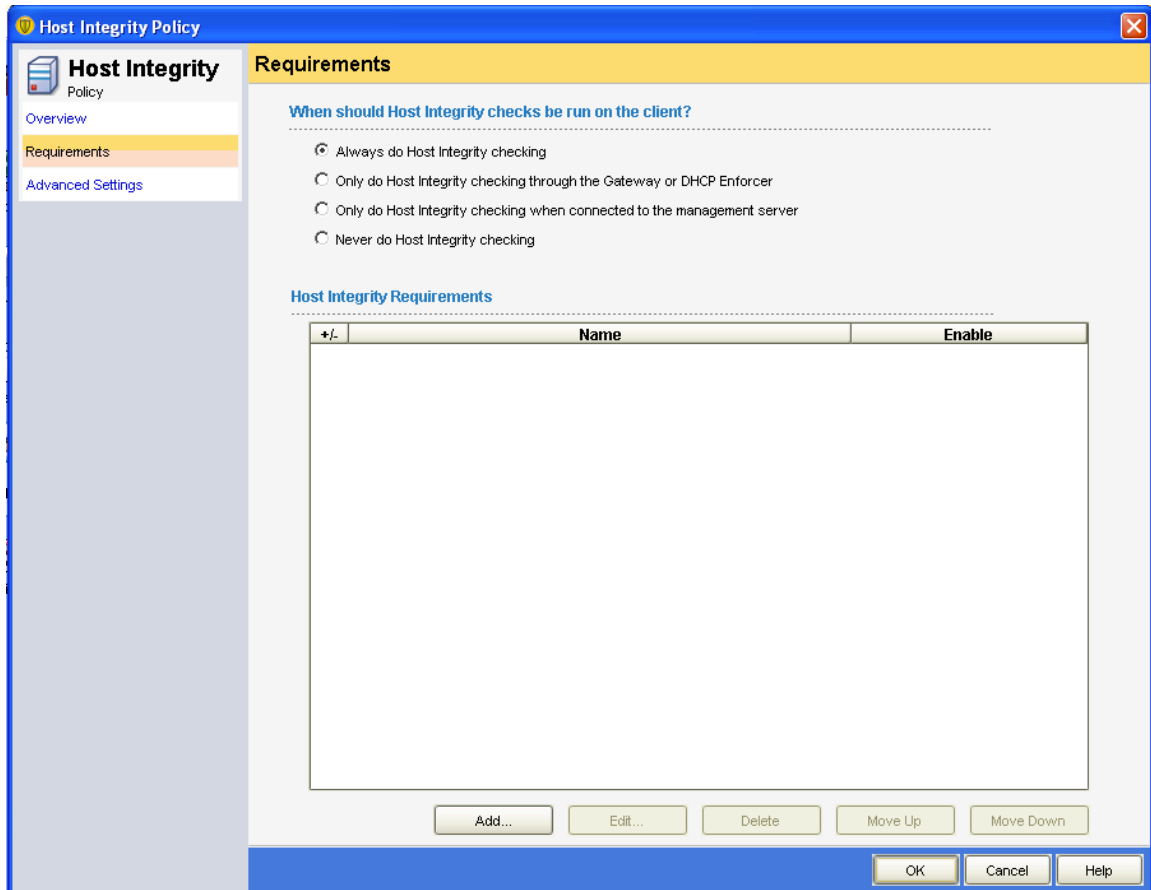
☒ Enable this policy

Created: admin

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

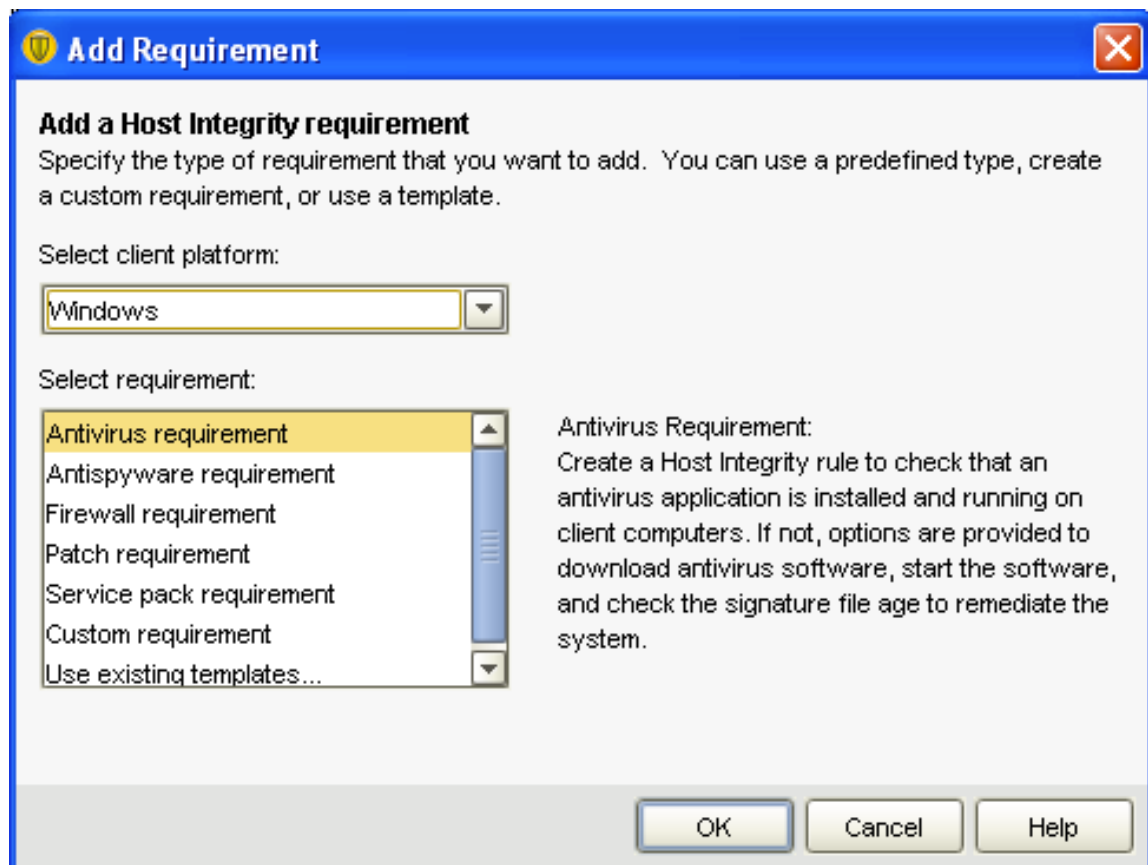
OK Cancel Help

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:

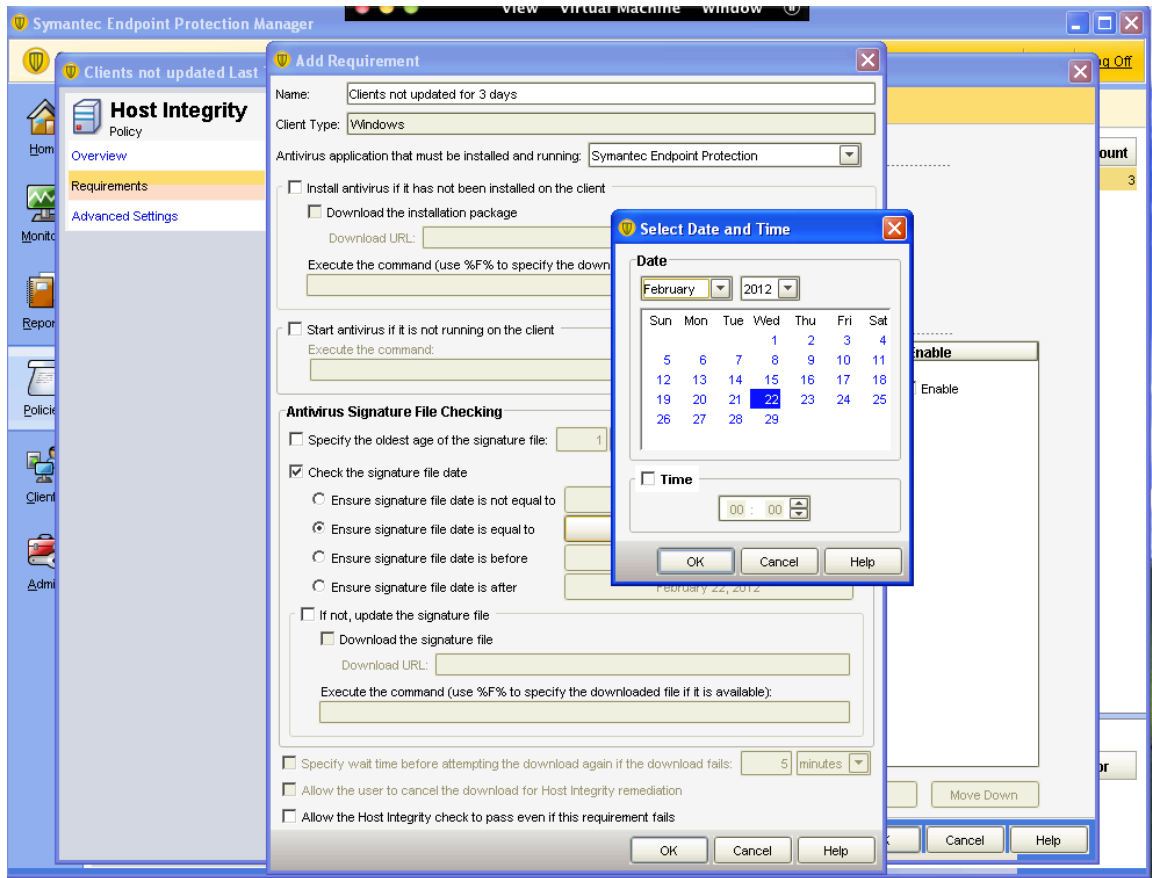
☐ Allow the user to cancel the download for Host Integrity remediation

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

OK Cancel Help

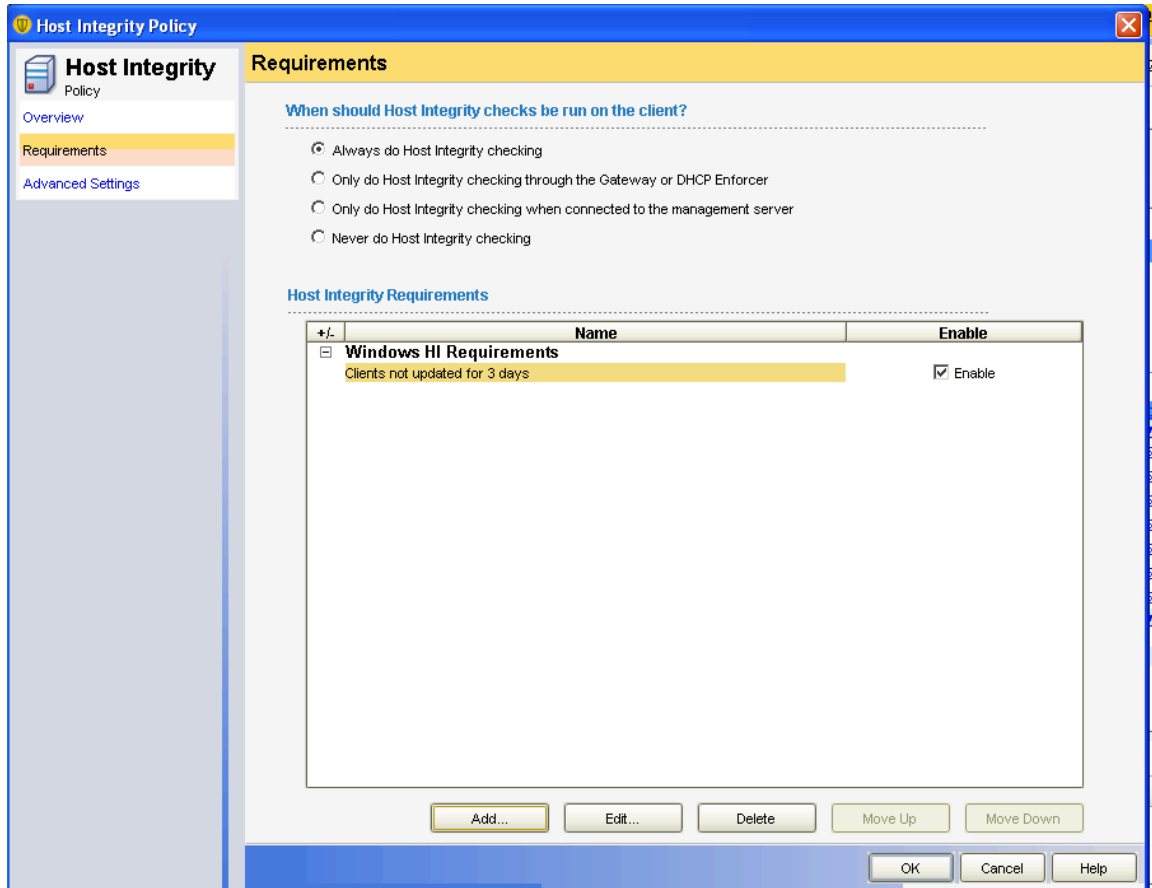
Put Check mark on “Check the signature file date

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)



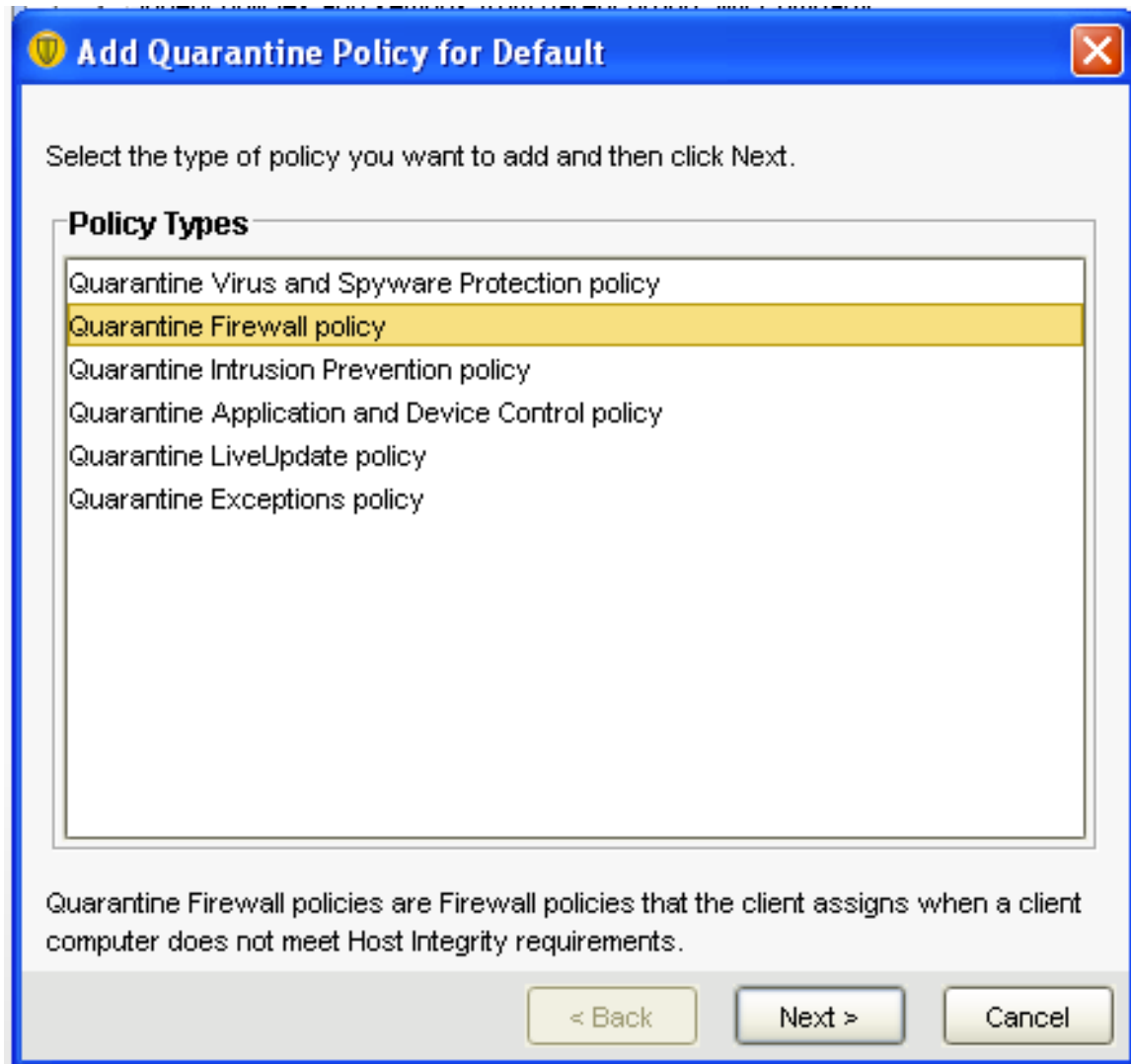
Click OK

The following window will appear  
Click OK



Add Quarantine Policy for Default

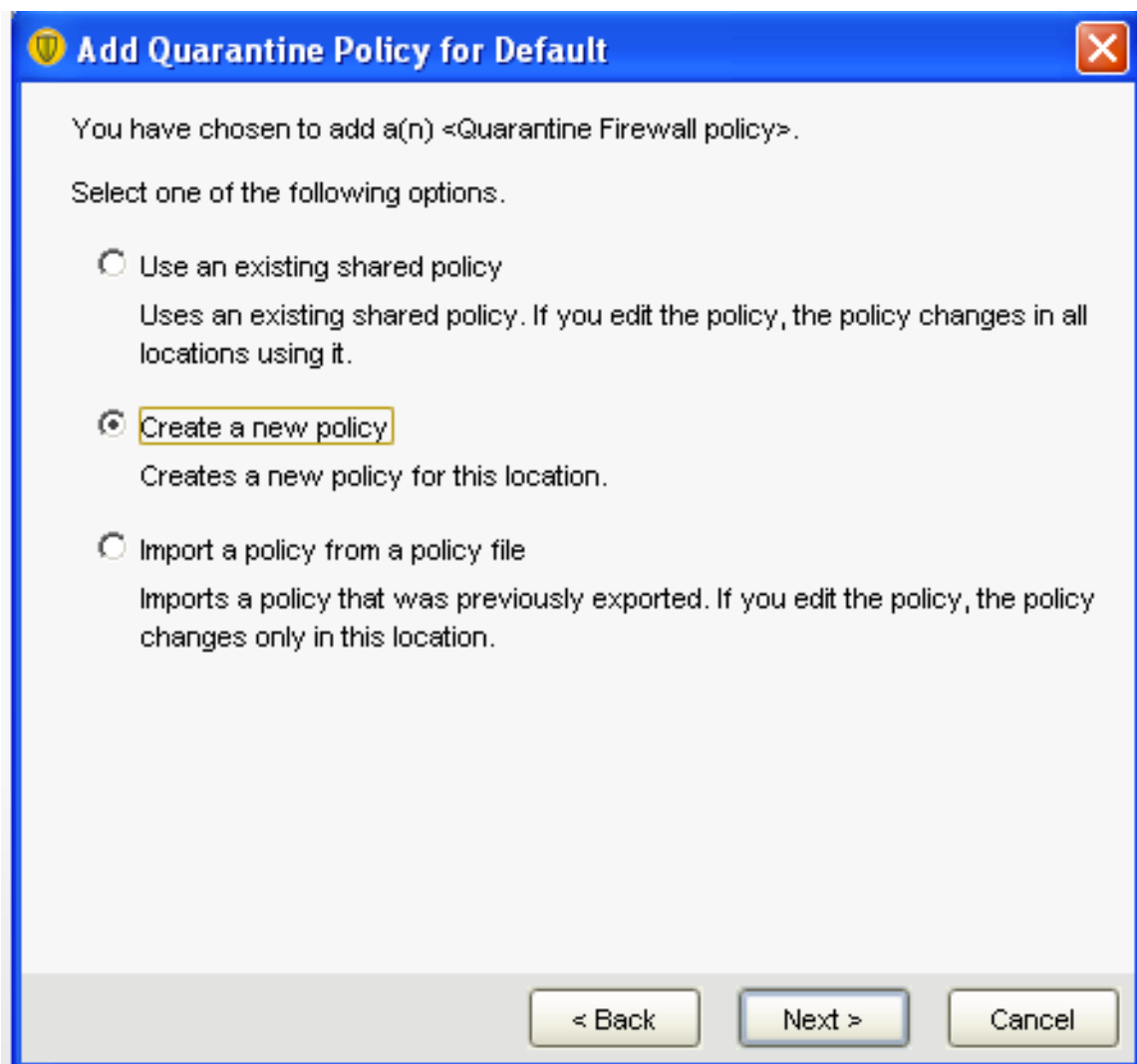
Select Quarantine Firewall Policy and Click Next



In Add Quarantine Policy for Default

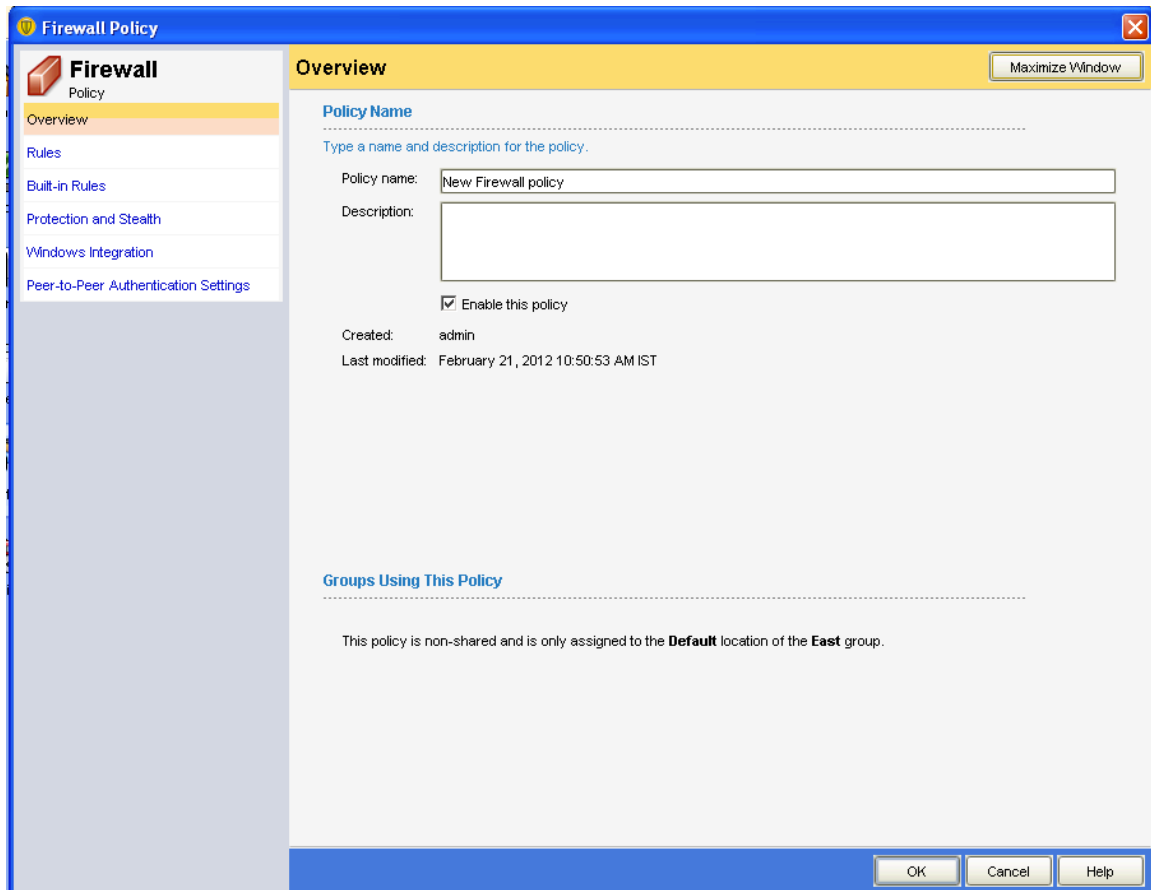
Select Create a New Policy

Click Next





After Clicking Next Firewall Policy window will get opened



In Overview Add the name of the Policy

The screenshot shows the 'Firewall Policy' window in Windows Firewall with Advanced Security. The 'Overview' tab is selected in the left-hand navigation pane. The main area displays the 'Policy Name' section with a text box containing 'Allow Administrator'. Below this is a larger text box for the 'Description'. A checkbox labeled 'Enable this policy' is checked. The 'Created' field shows 'admin' and the 'Last modified' field shows 'February 21, 2012 10:50:53 AM IST'. The 'Groups Using This Policy' section indicates that the policy is non-shared and assigned to the 'Default' location of the 'East' group. At the bottom right, there are 'OK', 'Cancel', and 'Help' buttons.

**Firewall Policy**

**Overview**

**Policy Name**

Type a name and description for the policy.

Policy name:

Description:

☒ Enable this policy

Created: admin

Last modified: February 21, 2012 10:50:53 AM IST

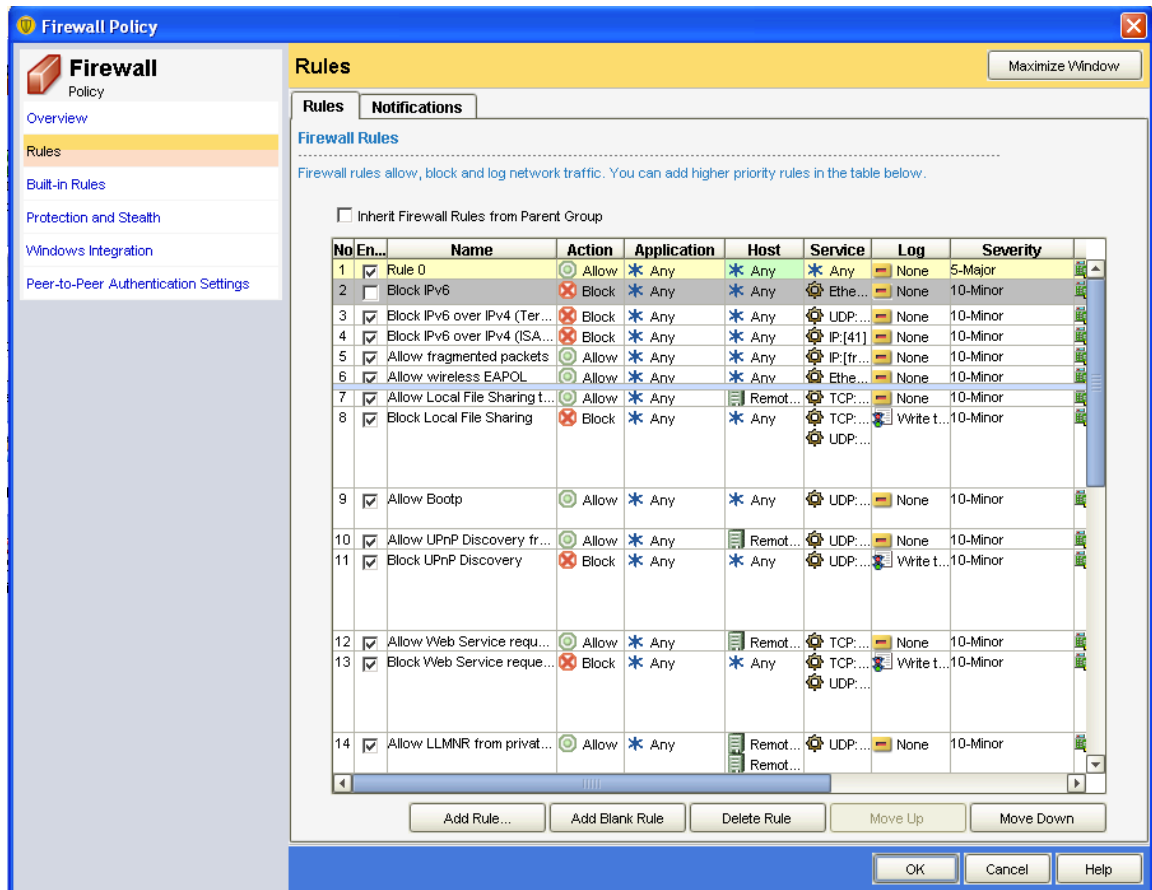
**Groups Using This Policy**

.....

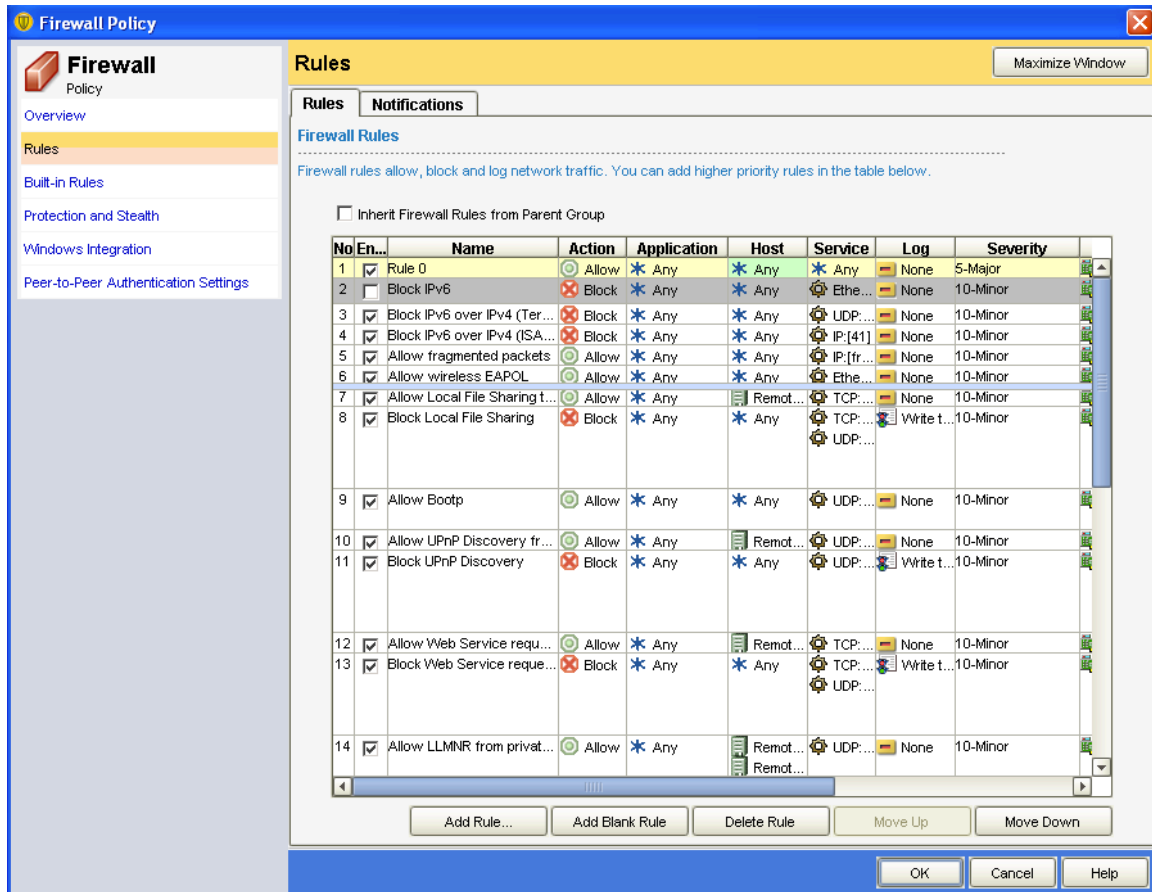
This policy is non-shared and is only assigned to the **Default** location of the **East** group.

OK Cancel Help

## In Rules Window Add Blank Rule

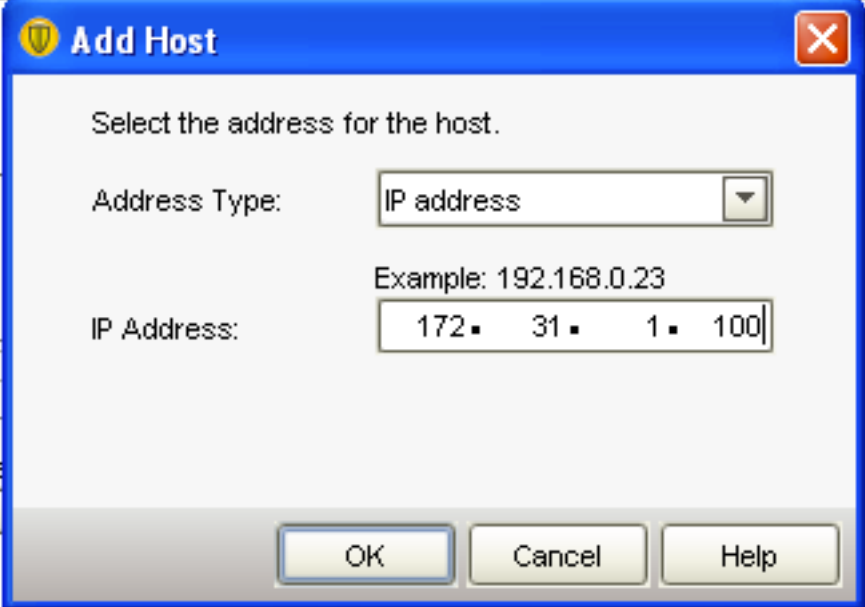


In Rule Select Host and Double Click on Host



After Double Clicking following Windows will be opened

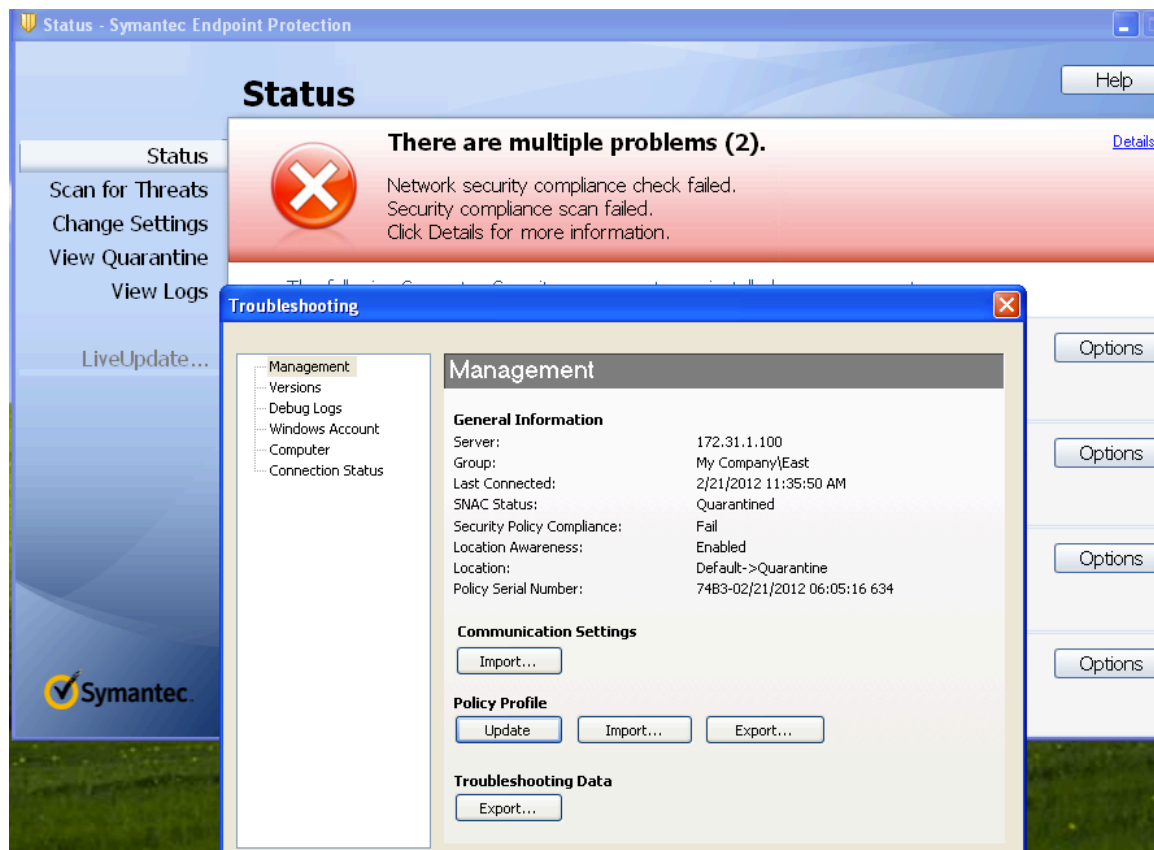
In Remote Add the IP Address of the System in case the any system fails host integrity test the system IP Address Added can access the Host Integrity Failed to Access the System



The image shows a Windows-style dialog box titled "Add Host" with a blue header bar. Inside the dialog, the text "Select the address for the host." is displayed. Below this, there is a label "Address Type:" followed by a dropdown menu currently showing "IP address". Underneath the dropdown is the text "Example: 192.168.0.23". Below that is a label "IP Address:" followed by a text input field containing the IP address "172.31.1.100" with dots separating the octets. At the bottom of the dialog are three buttons: "OK", "Cancel", and "Help".

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

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 LLMNR from privat...	Allow	* Any	Remot...	UDP:...	None	10-Minor

Add Rule...

Add Blank Rule

Delete Rule

Move Up

Move Down

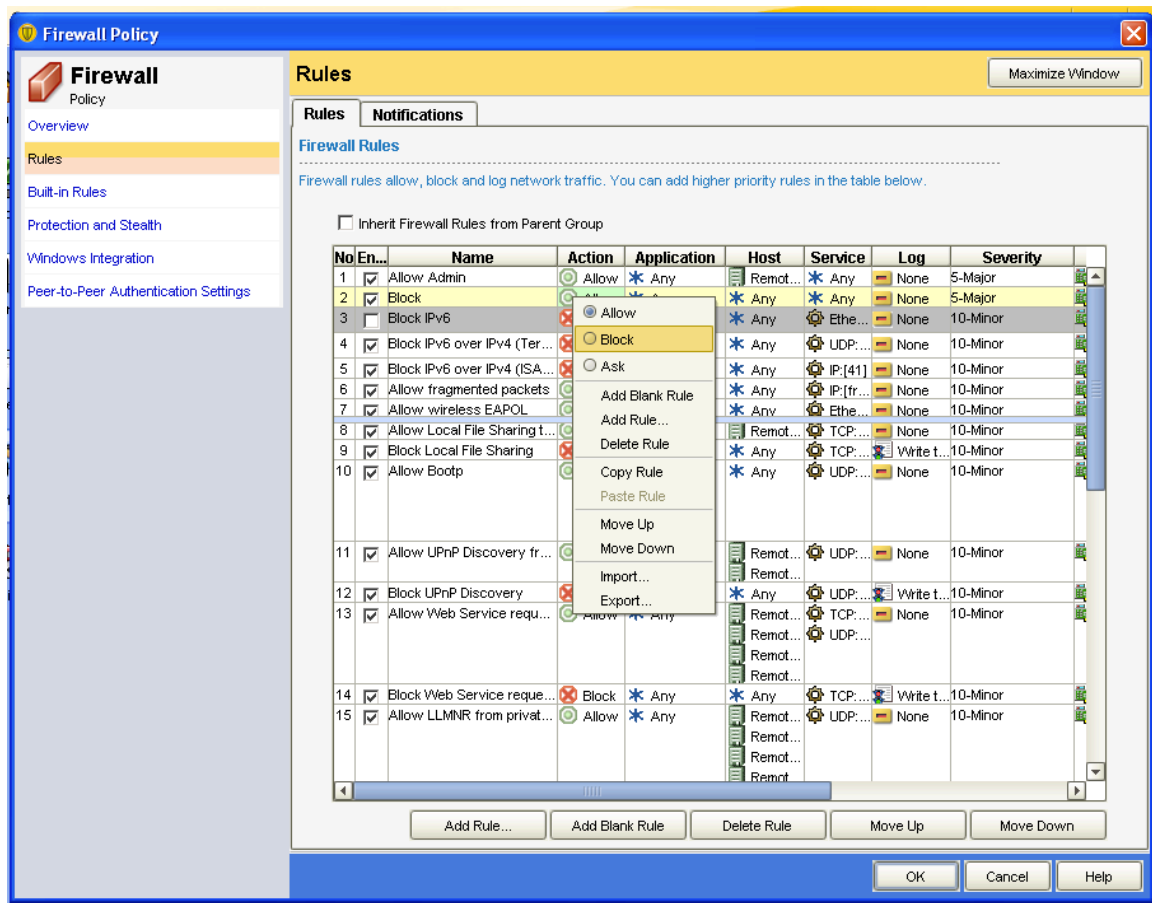
OK

Cancel

Help

Select the Block Rule Right and in Action Select Block

Click OK



Click OK