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

Services				
File Action View	Help			
⇔ → 🔳 🖀 🕻) 🖪 😫 🕨 = 🗉 =>			
🆏 Services (Local)	Name A	Description	Status	Startup Ty 🔼
	Symantec Endpoint Protection Manager	Application		Automatic
	Symantec Endpoint Protection Manager Webserver	Apache/2	Started	Automatic
	Symantec Management Client	Provides c	Started	Manual
	Symantec Network Access Control	Checks tha		Manual
	System Event Notification	Tracks syst	Started	Automatic
	System Restore Service	Performs s	Started	Automatic
	🖏 Task Scheduler	Enables a	Started	Automatic
	TCP/IP NetBIOS Helper	Enables su	Started	Automatic
	See Telephony	Provides T	Started	Manual
	wa Telnet	Enables a r		Disabled
	Terminal Services	Allows mult	Started	Manual 🔤
	when the mes	Provides u	Started	Automatic 🗧
	TP AutoConnect Service	ThinPrint	Started	Manual
	TP VC Gateway Service	ThinPrint		Manual
	WyUninterruptible Power Supply	Manages a		Manual
	W Universal Plug and Play Device Host	Provides s		Manual
	🦓 VMware Physical Disk Helper Service	Enables su	Started	Automatic 👱
	<			>
	Extended Standard			

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

Services				
File Action View	Help			
⇔ → 💽 😭 🔮	〕 💀 😫 ▶ ■ 🗉 ■>			
🍓 Services (Local)	Name A	Description	Status	Startup Ty 木
	Symantec Endpoint Protection Manager	Application	Started	Automatic
	Symantec Endpoint Protection Manager Webserver	Apache/2	Started	Automatic
	Symantec Management Client	Provides c	Started	Manual
	Symantec Network Access Control	Checks tha		Manual
	System Event Notification	Tracks syst	Started	Automatic
	System Restore Service	Performs s	Started	Automatic
	🖏 Task Scheduler	Enables a	Started	Automatic
	TCP/IP NetBIOS Helper	Enables su	Started	Automatic
	Relephony Contract Co	Provides T	Started	Manual
	Renet Contract Contra	Enables a r		Disabled
	Terminal Services	Allows mult	Started	Manual
	Strengtheres	Provides u	Started	Automatic 🗧
	TP AutoConnect Service	ThinPrint	Started	Manual
	n VC Gateway Service	ThinPrint		Manual
	We Uninterruptible Power Supply	Manages a		Manual
	www.Universal Plug and Play Device Host	Provides s		Manual
	🤹 VMware Physical Disk Helper Service	Enables su	Started	Automatic 👱
				>
	Extended Standard			

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

🛡 Syman	tec Endpoint Protection Manager	View View View View View View View View	rtual Machine Wind	ow U	
🔘 Syr	mantec™ Endpoint Protectio	n Manager		Ret	resh Help Log Off
	Policies	Host Integrity Policie	s		
Home	Virus and Spyware Protection Firewall	Name		Description	Location Use Count
Monitors	 Intrusion Prevention Application and Device Control Host Integrity LiveUpdate Exceptions Policy Components 	Host Integrity policy	Created automatically during	g product installation.	0
Policies					
Clients	4				
Admin	Tasks Add a Host Integrity policy Import a Host Integrity policy Search for Applications				
		Recent changes appear below:			
		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

🔘 Symant	tec Endpoint Protection Manager	View Virtual Machine Win	low 🔳
🔘 Syr	nantec™ Endpoint Protection	Manager	Refresh Help Log Off
Home Home Monitors Reports	Clients My Company Carlor Corup Carlor Co	Clients Policies Details Install Packages Policy inheritance is OFF Inherit policies and settings from parent group "My Company" Location-independent Policies and Settings Policies Custom Intrusion Prevention Off System Lockdown Off Network Application Monitoring Off	Policy serial number: 74B3-02/21/2012 04:30:26 034 Settings UveUpdate Content Policy Settings Client Log Settings Communications Settings External Communications External Co
Clerts Clerts	Tasks Add Location Manage Locations Export Communications Settings. Copy the group policies Add a group	Location-specific Policies and Settings Settings for Location: Default Location-specific Policies: Virus and Spyware Protection policy - Balanced [nor Firewall policy [shared] Application and Device Control policy [shared] Application and Device Control policy [shared] Kot Integrity policy [shared] Cueupdate Settings policy [shared] Cueurantine Policies when Host Integrity Fails: No policy assigned to this location. Location-specific Settings:	Serieral securities Add a policy -shared] Tasks >>
		Recent changes appear below:	
		Description Edited shared Livel Indete Settings policy: Livel Indete Settings policy	Eebruary 20, 2012 1:02:49 PM IST admin
		Changed Console mode at [Default] Add a non-shared [Virus and Spyware Protection Policy], <virus an.<="" th=""><th>February 16, 2012 10:50:28 AM IST admin</th></virus>	February 16, 2012 10:50:28 AM IST admin

Goto Host Integrity Policy and Click Edit Shared

Host Integrity Policy		×
Host Integrity	Overview	
Overview	Policy Name Used By	
Requirements	Policy Name	
Requirements Advanced Settings	Policy Name Type a name and description for the policy. Policy name: Host Integrity policy Description: Created automatically during product installation. ✓ Enable this policy Created: admin Last modified: February 16, 2012 10:14:18 AM IST	
	OK Cancel Help	

Give the name of the Policy as per your requirement

Host Integrity Policy		
🗐 Host Integrity	Overview	
Policy	Policy Name Used By	
Requirements	Policy Name	
Advanced Settings	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

Host Integrity Policy		X	
🗐 Host Integrity	Requirements		
Overview	When should Host Integrity checks be run on the client?		
Requirements	C Always do Host Integrity checking		
Advanced Settings	C Only do Host Integrity checking through the Gateway or DHCP Enforcer		
	$\ensuremath{\mathbb{C}}$ Only do Host Integrity checking when connected to the management server		
	O Never do Host Integrity checking		
	Host Integrity Requirements		
	+/- Name	Enable	
	Add Edit Delete Move Up	Move Down	
	ОК	Cancel Help	

Click Add

After Clicking Add the following window will be opened

🛡 Add Requirement	
Add a Host Integrity requirement Specify the type of requirement that you was a custom requirement, or use a template. Select client platform: Vindows Select requirement Select requirement Antispyware requirement Firewall requirement Patch requirement Service pack requirement Custom requirement Use existing templates	ant to add. You can use a predefined type, create Antivirus Requirement: Create a Host Integrity rule to check that an antivirus application is installed and running on client computers. If not, options are provided to download antivirus software, start the software, and check the signature file age to remediate the system.
	OK Cancel Help

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 Re	equirement 🔀				
Name:	Clients not updated for 3 days				
Client Type:	ent Type: Windows				
Antivirus ap	plication that must be installed and running: Symantec Endpoint Protection				
r 🔲 Install :	antivirus if it has not been installed on the client				
🔽 Doʻ	wnload the installation package				
Do	wnload URL:				
Execu	te the command (use %F% to specify the downloaded file if it is available):				
r 🗖 Start a	ntivirus if it is not running on the client				
Execu	te the command:				
Antivirus	Signature File Checking				
🗌 🔲 Specif	y the oldest age of the signature file: 1 weeks				
Check	the signature file date				
⊙ En	nsure signature file date is not equal to February 21, 2012				
O En	nsure signature file date is equal to February 21, 2012				
O En	nsure signature file date is before February 21, 2012				
O En	sure signature file date is after February 21, 2012				
r 🗖 lf no	t, update the signature file				
	Download the signature file				
	Download URL:				
Exe	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: 5 minutes					
Allow the user to cancel the download for Host Integrity remediation					
🗖 Allow tł	he 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)

🛡 Sym	antec Endpoint Protection M	anager	
0	Clients not updated Last	🖤 Add Requirement	<mark>na Off</mark>
	🗇 Heat Integrity	Name: Clients not updated for 3 days	
1		Client Type: Windows	
Hom	Overview	Antivirus application that must be installed and running: Symantec Endpoint Protection	ount
	Requirements	r 🗖 Install antivirus if it has not been installed on the client	3
- 22	Advanced Settings	Download the installation package	
<u>M</u> onitc		Download URL:	
. 5		Execute the command (use %F% to specify the down	
		February 2012	
Repor		Sun Mon Tue Wed Thu Fri Sat	
Æ		Execute the command: 5 6 7 8 9 10 11 mable	
		12 13 14 15 16 17 18 19 20 21 23 24 25	
Policie		Antivirus Signature File Checking	
		Specify the oldest age of the signature file:	
- '		Check the signature file date	
Client		C Ensure signature file date is not equal to	
		Ensure signature file date is equal to	
		C Ensure signature file date is before OK Cancel Help	
<u>A</u> dmi		C 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: 5 minutes	pr
		Allow the user to cancel the download for Host Integrity remediation Move Down	
		Allow the Host Integrity check to pass even if this requirement fails	1
		OK Cancel Help Cancel Help	

Click OK

The following window will appear Click OK

🔍 Host Integrity Policy			X
🗐 Host Integrity	Requirements		
Policy Overview	When should Host Integrity checks be run on the client?		
Requirements	Always do Host Integrity checking		
Advanced Settings	$\mathbb C$ Only do Host Integrity checking through the Gateway or DHCP Enforcer		
	O Only do Host Integrity checking when connected to the management server		
	C Never do Host Integrity checking		
	Host Integrity Requirements		
	+/- Name	Enable	
	Windows HI Requirements Clients not updated for 3 days	I Enable	
	Add Edit Delete	Move Up Move Down	q

Add Quarantine Policy for Default

Select Quarantine Firewall Policy and Click Next

Add Quarantine Policy for Default	×
Select the type of policy you want to add and then click Next.	
Policy Types	٦
Quarantine Virus and Spyware Protection policy]
Quarantine Firewall policy	
Quarantine Intrusion Prevention policy	
Quarantine Application and Device Control policy	
Quarantine LiveUpdate policy	
Quarantine Exceptions policy	
Quarantine Firewall policies are Firewall policies that the client assigns when a client computer does not meet Host Integrity requirements.	Ł
< Back Next > Cancel	

In Add Quarantine Policy for Default

Select Create a New Policy

Click Next

Add Quarantine Policy for Default	×
You have chosen to add a(n) <quarantine firewall="" policy="">.</quarantine>	
Select one of the following options.	
O Use an existing shared policy Uses an existing shared policy. If you edit the policy, the policy changes in all	11
locations using it.	
Create a new policy Creates a new policy for this location.	
O Import a policy from a policy file	
Imports a policy that was previously exported. If you edit the policy, the polic changes only in this location.	у
< Back Next > Cancel	

After Clicking Next Firewall Policy window will get opened

🔍 Firewall Policy					
	Overview			Maximi	ze Window
Overview	Policy Name				
Rules	Type a name and descripti	on for the policy.			
Built-in Rules	Policy name: New Fi	rewall policy			
Protection and Stealth	Description:				
Windows Integration					
Peer-to-Peer Authentication Settings					
	J⊻ Ena	ble this policy			
	Created: admin	v 21 2012 10:50:53 AM IST			
	Groups Using This Poli	cy			
	This policy is non-share	ed and is only assigned to the Default location of the East group.			
			ок	Cancel	Help

In Overview Add the name of the Policy

Firewall Policy					×
	Overview			Maximiz	ze Window
n Overview	Policy Name				
Rules	Type a name and c	lescription for the policy.			
Built-in Rules	Policy name:	Allow Administrator			
Protection and Stealth	Description:				
Windows Integration					
Peer-to-Peer Authentication Settings		_			
70		Enable this policy			
	Created: Last modified:	admin February 21, 2012 10:50:53 AM IST			
2	East mounta.	1001001 y 21, 2012 10:00:00 Am Of			
16					
¢.					
1					
	Groups Using Th	nis Policy			
n					
	This policy is no	n-shared and is only assigned to the Default location of the East group	p.		
			ок	Cancel	Help

In Rules Window Add Blank Rule

Firewall	Rules								Maximiz	e Wind
Policy	Rules	<u> </u>	otifications							
view										
;	Firewal	Rul	es							
in Rules	Firewall	rules	allow, block and log networ	k traffic. Ye	ou can add highe	er priority rule	es in the table	e below.		
ction and Stealth	Inherit Firewall Rules from Parent Group									
ows Integration	No	En	. Name	Action	Application	Host	Service	Log	Severity	
to Door Automatication Cottinue	1		Rule 0	Allow	≭ Any	≭ Any	🗶 Any 🛛	📃 None	5-Major	Ē.
to-Peer Authentication Settings	2		Block IPv6	😢 Block	≭ Any	≭ Any	🍄 Ethe	🔜 None	10-Minor	重
	3	N	Block IPv6 over IPv4 (Ter	😢 Block	🗶 Any	🗰 Any	🙆 UDP:	- None	10-Minor	Ē
	4		Block IPv6 over IPv4 (ISA	😣 Block	* Any	🗰 Any	🙆 IP:[41]	None	10-Minor	iii ii
	5		Allow fragmented packets	Allow	🗶 Any	🗶 Any	🖗 IP:[fr	🔜 None	10-Minor	Ē.
	6		Allow wireless EAPOL	Allow	* Anv	* Anv	Ethe	- None	10-Minor	
	7	N	Allow Local File Sharing t	🔘 Allow	🔭 Any	Remot	. 🗭 TCP:	🔜 None	10-Minor	E
	8	V	Block Local File Sharing	😒 Block	Any	🛪 Any	ф тср: ф UDP:	🛐 Write t	.10-Minor	<u></u>
	9		Allow Bootp	Allow	🗶 Any	🔭 Any	UDP:	= None	10-Minor	Ē
	10		Allow LIPoP Discovery fr		👻 Anu	E Remot		None	10-Minor	
	11		Block LIPpP Discovery	Block	Any Any	😭 Kemot		VANTe t	10-Minor	-
		IV		S DIOCK	T OU	τ ου γ	a obr	• vvite t	10-1110	
	12	5	Allow Web Service requ		🗶 Anv	E Remot	O TOP	- None	10-Minor	嚴
	13	V	Block Web Service reque	8 Block	* Any	* Any	Ф́ ТСР: Ф́ UDP:	Vvrite t	.10-Minor	<u> </u>
	14	V	Allow LLMNR from privat	i Allow	🔭 Any	Remot	🏟 UDP:	None	10-Minor	i i i i i i i i i i i i i i i i i i i
	I ■			11111						•
			Add Rule	Add Blar	nk Rule	Delete Rule	N	/love Up	Move Dov	٧n

In Rule Select Host and Double Click on Host

Policy Rules Notifications Rules Firewall Rules Built-in Rules Firewall Rules alow, block and log network traffic. You can add higher priority rules in the table below. Protection and Steath Inherit Firewall Rules from Parent Group Windows Integration Inherit Firewall Rules from Parent Group Peer-to-Peer Authentication Settings Inherit Firewall Rules from Parent Group None 0.000 W Any & Any & Any & Any & None 5-Migor 2 Block IPv6 over IPv4 (Ter & Block & Any & Any & Any & None 10-Minor 3 Ø Block IPv6 over IPv4 (Ter & Block & Any & Any & Any & None 10-Minor 5 Ø Allow V fragmerted packets & Allow & Any & Any & Mone 10-Minor 6 Ø Allow V fragmerted packets & Allow & Any & Any & Term. 7 Ø Allow V fragmerted packets & Allow & Any & Any & Diff	Firewall	Rules					Maximize Wind
Diverview Rules Rules Firewall Rules Built-In Rules Firewall Rules allow, block and log network traffic. You can add higher priority rules in the table below. Protection and Steath Inherit Firewall Rules from Parent Group Windows Integration Inherit Firewall Rules from Parent Group None for Authentication Settings Inherit Firewall Rules from Parent Group None for Authentication Settings Image: State S	Policy	Pulae Notifications	- -				
Ides Firewall Rules ait-in Rules it-in Rules otection and Steath Inhert Firewall Rules from Parent Group Indows Integration Inhert Firewall Rules from Parent Group NoE n Name Action Application Host Service Log Severity 1 V Rule 0 Allow X Any X Any None 10-Minor 3 V Block IPv6 over IPv4 (Ter © Block X Any X Any © Inherit None 10-Minor 3 V Block IPv6 over IPv4 (Ter © Block X Any X Any © Inhom 10-Minor 3 V Block IPv6 over IPv4 (Ter © Block X Any X Any © IP(1) None 10-Minor 4 V Block IPv6 over IPv4 (Ter © Block X Any X Any © IP(1) None 10-Minor 5 V Allow Wored Starting © Allow X Any X Any © IP(1) None 10-Minor 6 V Allow Uscal File Sharing © Allow X Any X Any © UDP None 10-Minor 9 V </td <td>iew</td> <td>Nules Nouncauons</td> <td>1</td> <td></td> <td></td> <td></td> <td></td>	iew	Nules Nouncauons	1				
iii. In Rules Firewall rules allow, block and log network traffic. You can add higher priority rules in the table below. indows Integration Inherit Firewall Rules from Parent Group Image: Proper Authentication Settings No En Name Action Application Host Service Log Severity Image: Proper Authentication Settings Image: Proper Authentication Settings Rule 0 Allow Any Any Any Any Any Proper Any None 10-Minor Image: Proper Authentication Settings Image: Proper Authentication Proper Authenting Proper Proper Authentication Proper Authentication		Firewall Rules					
tection and Steath Inherit Firewall Rules from Parent Group ndows Integration Prote 0 Allow 1 Any Any Any Any None 5-Major arto-Peer Authentication Settings Prote 0 Allow 1 Any X Any X Any None 5-Major 2 Block IPv6 Stock IPv6 Stock X Any X Any X Any None 10-Minor 3 Ø Block IPv6 over IPv4 (Ter Stock X Any X Any X Any Y DiP None 10-Minor 4 Ø Block IPv6 over IPv4 (Ter Stock X Any X Any X Any Y DiP None 10-Minor 5 Ø Allow Vireless EAPOL Ø Allow X Any X Any Y DiP None 10-Minor 6 Ø Allow Uccal File Sharing Ø Block X Any X Any Y DiP None 10-Minor 7 Ø Allow Uccal File Sharing Ø Block X Any X Any Y DiP None 10-Minor 10 Ø Allow UpiP Discovery fr Ø Allow X Any X Any Y UDP None 10-Minor 11 Ø Block UPiP Discovery	n Rules	Firewall rules allow, block a	nd log network traffic. Y	ou can add higher	priority rules in the	table below.	
No En Name Action Application Host Service Log Severity ar-to-Peer Authentication Settings 1 V Rule 0 0 Allow X Any X Any <td< td=""><td>tion and Stealth</td><td>🗌 Inherit Firewall Ru</td><td>les from Parent Group</td><td></td><td></td><td></td><td></td></td<>	tion and Stealth	🗌 Inherit Firewall Ru	les from Parent Group				
Image: Construction Settings Image: Constructing Settings <td< th=""><th>ws Integration</th><th>No En Na</th><th>me Action</th><th>Application</th><th>Host Serv</th><th>ice Log</th><th>Severity</th></td<>	ws Integration	No En Na	me Action	Application	Host Serv	ice Log	Severity
Proceed Admentionation Settings 2 Block IPv6 Block * Any Any Any Block * Any None 10-Minor 3 Ø Block IPv6 over IPv4 (Ter Block * Any Any Any Dip-(m) None 10-Minor 4 Ø Block IPv6 over IPv4 (Ter Block * Any Any Any Dip-(m) None 10-Minor 5 Ø Block IPv6 over IPv4 (Ter Block * Any Any Any None 10-Minor 5 Ø Allow tragmented packets Allow Any Any None 10-Minor 6 Ø Allow turbless EAPOL Allow Any Any Any None 10-Minor 7 Ø Allow Local File Sharing Ø Allow Any Any Y Writet 10-Minor 9 Ø Allow Bootp Ø Allow Any Any Ø UDP None 10-Minor 10 Ø Allow UPP Discovery Ø Allow Any Any Ø UDP None 10-Minor	- Deep Authorities Cotting	1 🔽 Rule 0	Allow	🖈 Any 🔰	🗶 Any 🛛 🗶 Ar	ny 📃 None 5-1	Major 🙀 🕯
3 Image: Block IPv6 over IPv4 (Ter Block Image: Any Any Dep None 10-Minor 4 Image: Block IPv6 over IPv4 (Ter Block Image: B	o-Peer Authentication Settings	2 🔲 Block IPv6	😣 Block	🛪 Any 💦	🗱 Any 🛛 🏟 Eti	ne 💻 None 🛛 10	I-Minor 🙀
4 Image: Block IPv6 over IPv4 (ISA Solick X Any X Any PI(41) None 10-Minor 5 Image: Allow fragmented packets Allow X Any X Any Y Any PI(17 None 10-Minor 6 Image: Allow fragmented packets Allow X Any X Any Y Any PI(17 None 10-Minor 7 Image: Allow fragmented packets Allow X Any X Any None 10-Minor 7 Image: Allow Local File Sharing Allow X Any X Any None 10-Minor 7 Image: Allow Local File Sharing Block X Any X Any Image: Allow Collabor Allow X Any Image: Allow Collabor Image: Allow X Any Image: Allow Collabor Image: Allow X Any Image: Allow Collabor Image: Allow X Any Image: Allow <		3 🔽 Block IPv6 ov	er IPv4 (Ter 🔀 Block	🗰 Any 🔰	🗱 Any 🛛 🏟 UE	P: 💻 None 🛛 10)-Minor 🛛 🙀 -
S ✓ Allow fragmented packets △ Allow ** Any × Any ↓ P:[fr None 10-Minor B ✓ Allow wireless EAPOL △ Allow ** Any × Any © Effe None 10-Minor 7 ✓ Allow Local File Sharing △ Allow × Any △ Effe None 10-Minor 8 ✓ △ Allow Local File Sharing △ Allow × Any △ TCP None 10-Minor 9 △ Allow Bootp △ Allow △ Allow × Any △ UDP None 10-Minor 10 △ Allow UPnP Discovery △ Allow ▲ Any △ UDP None 10-Minor 11 △ Allow UPnP Discovery △ Allow × Any △ UDP △ UDP		4 🔽 Block IPv6 ov	er IPv4 (ISA 🔀 Block	🗰 Any 🔰	🖈 Any 🛛 🏟 IP:	(41) 💻 None 🛛 10)-Minor 🙀 -
6 ✓ Allow wireless EAPOL Allow ★ Any ★ Any ♣ Ete ➡ None ▲ Minor 7 ✓ Allow Local File Sharing ± Allow ★ Any ➡ Remot ➡ TCP ■ None 10-Minor 8 ✓ Block Local File Sharing ➡ Block ★ Any ➡ Any ➡ TCP ■ None 10-Minor 9 ✓ Allow Bootp ➡ Allow ★ Any ★ Any ➡ UDP ■ None 10-Minor 10 ✓ Allow Bootp ➡ Allow ★ Any ★ Any ➡ UDP ■ None 10-Minor 10 ✓ Allow UPP Discovery fr ➡ Allow ★ Any ➡ LDP ■ None 10-Minor 11 ✓ Block UPNP Discovery ♠ Block ★ Any ➡ Any ➡ UDP ■ None 10-Minor 12 ✓ Allow Web Service reque ♠ Block ★ Any ➡ Any ➡ TCP ■ None 10-Minor 13 ✓ Block Web Service reque ♠ Block ★ Any ➡ Any ➡ UDP <t< td=""><td></td><td>5 🔽 Allow fragme</td><td>inted packets 🤘 Allow</td><td>🖈 Any 🔰</td><td>🗱 Any 🛛 🏟 IP:</td><td>(fr 💻 None 🛛 10</td><td>)-Minor 🛛 📓 -</td></t<>		5 🔽 Allow fragme	inted packets 🤘 Allow	🖈 Any 🔰	🗱 Any 🛛 🏟 IP:	(fr 💻 None 🛛 10)-Minor 🛛 📓 -
7 Image: Allow Lucal File Sharing to Allow the Any image: Any im		6 🔽 Allow wirele:	ss EAPOL 🛛 🔘 Allow	🖈 Anv 💦	🖈 Anv 🛛 🏠 Eti	ne 르 None 🛛 10)-Minor 📓
8 ✓ Block Local File Sharing Selock ★ Any ★ Any ↓ TCP: ↓ Write t 10-Minor 9 ✓ Allow Bootp ④ Allow ★ Any ★ Any ↓ UDP: ● None 10-Minor 10 ✓ Allow UPP Discovery fr ⑤ Allow ★ Any ↓ UDP: ● None 10-Minor 11 ✓ Block UPP Discovery ⊗ Block ★ Any ♥ UDP: ● None 10-Minor 12 ✓ Allow Web Service requ ⑥ Allow ★ Any ♥ UDP: ● None 10-Minor 12 ✓ Allow Web Service requ ⑧ Allow ★ Any ♥ UDP: ● None 10-Minor 13 ✓ Block Web Service reque ⑨ Block ★ Any ♥ UDP: ● None 10-Minor 14 ✓ Allow LLMNR from privat ⑨ Allow ★ Any ♥ UDP: ● None 10-Minor		7 🔽 Allow Local F	file Sharing t 🧿 Allow	🖈 Any	🗐 Remot 🗭 TO	:P: 💻 None 🛛 10)-Minor 🛛 🧝
9 Image: Allow Bootp Allow Allow Any Image: Any Image: LDP None 10-Minor 10 Image: Allow UPP Discovery Allow Any Image: Any Image: LDP None 10-Minor 11 Image: Allow UPP Discovery Allow Any Image: Any Image: LDP None 10-Minor 11 Image: Allow UPP Discovery Block Any Image: LDP None 10-Minor 12 Image: Allow Web Service reque Allow Any Image: Remot Image: CP None 10-Minor 12 Image: Allow Web Service reque Allow Any Image: Remot Image: CP None 10-Minor 13 Image: Block Web Service reque Image: Block X Any X Any Image: CP None 10-Minor 14 Image: Allow LLMNR from privat Image: Allow X Any Image: Remot Image: UPP None 10-Minor		8 🔽 Block Local F	ile Sharing 🛛 🔀 Block	* Any >	🖈 Any 🏟 TC 🏟 UE	:P: 🐉 Write t10 :P:	I-Minor 🛱
10 ✓ Allow UPNP Discovery fr O Allow ★ Any Remot [®] UDP None 10-Minor 11 ✓ Block UPNP Discovery S Block ★ Any ★ Any UDP Virite t 10-Minor 12 ✓ Allow Web Service requ O Allow ★ Any ▼ TCP None 10-Minor 13 ✓ Block Web Service reque Ø Block ★ Any ★ Any ♥ TCP None 10-Minor 14 ✓ Allow LLMNR from privat Ø Allow ★ Any ■ Remot ♥ UDP None 10-Minor		9 🔽 Allow Bootp	Allow	🖈 Any	🖈 Any 🗳 UE	P: 🗾 None 10)-Minor 🛱
11 Image: Block UPnP Discovery Image: Block Image: Anny <		10 🔽 Allow UPnP D	scovery fr 🔘 Allow	🖈 Any	🗐 Remot 🙆 UD	P: = None 10)-Minor 📓
12 Image: Allow Web Service requ Allow Allow Any Image: Remot Image: TCP: None 10-Minor 13 Image: Block Web Service reque Image: Block Image: Any Image: Any Image: TCP: Image: None 10-Minor 14 Image: Allow LLMNR from privat Image: Allow Image: Any		11 🔽 Block UPnP D	iscovery 😵 Block	* Any	🖈 Any 🛱 UE	0P: 😵 Vvirite t10	/-Minor 🛱
13		12 🔽 Allow Web S	ervice requ 🗿 Allow	× Anv	Remot 🏟 TO	P = None 10)-Minor 🛍
14 🔽 Allow LLMNR from privat 💿 Allow 🔭 Any 📑 Remot 🍄 UDP: 🚍 None 10-Minor		13 🔽 Block Web St	wice reque 🔀 Block	* Any	🖈 Any 🏟 TC 🏟 UE	:P: 😵 Write t10 :P:	J-Minor 🚊
		14 🔽 Allow LLMNF	from privat 💿 Allow	* Any	Remot 🏟 UI	P: <mark>=</mark> None 10)-Minor 🛱
			1111				•
Add Rule Add Blank Rule Delete Rule Move Up Move Dow		Add	Rule Add Bla	ink Rule D	elete Rule	Move Up	Move Down

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

	🔍 Add Host	\mathbf{X}
	Select the address for the host.	
	Address Type: IP address	
1 w 1 1 1 w 1	Example: 192.168.0.23 IP Address: 172• 31• 1• 100	
	OK Cancel Help	

Click OK and Once Again Click OK

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

🛡 Status - Symantec Endj	point Protection			
	Status			Help
Status	The	ere are multiple prob	olems (2).	Details
Scan for Threats Change Settings	Netw Secu Click	ork security compliance che rity compliance scan failed. Details for more information	eck failed. n.	
View Quaranune View Logs				
LiveUpdate	Troubleshooting Management Versions Debug Logs Windows Account Computer Connection Status	Management General Information Server: Group: Last Connected: SNAC Status: Security Policy Compliance: Location Awareness: Location: Policy Serial Number:	172.31.1.100 My Company\East 2/21/2012 11:35:50 AM Quarantined Fail Enabled Default->Quarantine 7483-02/21/2012 06:05:16 634	Options Options Options
Symantec.		Communication Settings Import Policy Profile Update Import	. Export	Options
and the second second		Troubleshooting Data		

Again Add Blank Rule in Firewall and Name it as Block

Firewall Policy									
💋 Firewall	Rules							Maximiz	e Window
Policy		latifications							
Overview		NUMICATIONS							
Rules	Firewall Rules								
Built-in Rules	Firewall rules allow, block and log network traffic. You can add higher priority rules in the table below.								
Protection and Stealth	🗖 Inhe	erit Firewall Rules from Parer	it Group						
Windows Integration	No En.	Name	Action	Application	Host	Service	Log	Severity	
Deau to Deau Authoritization Cattions	1 🔽	Allow Admin	Allow	≭ Any	🗐 Remot	≭ Апу	💻 None	5-Major	iii ▲
Peer-to-Peer Authentication Settings	2 🔽	Block	Allow	🗶 Any	🗰 Any	🗰 Any	💻 None	5-Major	<u>Ē</u>
	3 🗖	Block IPv6	🔀 Block	≭ Any	≭ Any	🏟 Ethe	💻 None	10-Minor	萆
	4 🔽	Block IPv6 over IPv4 (Ter	🔀 Block	🗶 Any	🗶 Any	🙆 UDP:	None	10-Minor	E
	5 5	Block IPv6 over IPv4 (ISA	Block	Y Any	X Any	6 ID:1/11	- None	10-Minor	
	6 17	Allow fragmented nackets		Any Any	Any Any	100 ID:[41]	None	10-Minor	- 2 - 1
	7 7	Allow wireless FAPOI	Allow	Any Any	Any Any	G Etho	None None	10-Minor	
	8 17	Allow Local File Sharing t		* Anv	P Bowet		- None	10-Minor	
		Plock Local File Sharing t	O Allow	Ally Ally	Remot	A TOP	NULLE	10-Minor	- 2
	3 1	Alleus Baste	BIOCK	Any Any	Any	A UDD	X VVrite t	10-Willion	
	10	Allow Doolp	S Allow	T Ally	T Ally	işi ode	- None	10-Willion	*
	11 🔽	Allow UPnP Discovery fr	Allow	🔭 Any	Remot	🏟 UDP:	르 None	10-Minor	<u>ه</u>
	12 🔽	Block UPnP Discovery	🔀 Block	* Any	* Any	O UDP:	🕱 Write t	10-Minor	靈
	13 🔽	Allow Web Service requ	O Allow	* Any	Remot Remot Remot	ф тср: ф UDP:	None	10-Minor	Ē,
	14 🖂	Block Web Service reque	🔀 Block	🗶 Anv	X Anv	TCP:	🗴 Write t	10-Minor	Ē
	15 🔽	Allow LLMNR from privat	Allow	* Any	Remot	UDP:	None	10-Minor	Ē
					Remot				-
	•		11111		a manufi				
		Add Rule	Add Blar	nk Rule	Delete Rule		Move Up	Move Dov	wn
							ок	Cancel	Help

Select the Block Rule Right and in Action Select Block

Click OK

Firewall Policy				X		
	tules			Maximize Window		
	Rules Notifications					
Overview	irewall Rules					
Rules						
Built-in Rules	Firewali rules allow, block and log network traffic. You can add nigher priority rules in the table below.					
Protection and Steatth	☐ Inherit Firewall Rules from Parent Group					
Windows Integration	No En Name Action	Application Host	Service Log	Severity		
Peer-to-Peer Authentication Settings	1 Allow Admin O Allow	* Any 🗐 Remot	* Any None 5-	Major 🛒 📥		
	3 Ellock IBv6	W X Any	Any Mone p-	-Major E		
		× Any	🛱 LIDE: 🖃 None 10	D-Minor		
	5 Rick IPv6 over IPv4 (ISA S Ast	Any Any	🛱 007 🔤 None 🛛 10	3-Minor		
	6 Allow fragmented packets		P:[fr = None 10	D-Minor		
	7 V Allow wireless EAPOL		Ethe = None 10	D-Minor 📓		
	8 🔽 Allow Local File Sharing t 🧿	Remot	😳 TCP: 드 None 🛛 10	D-Minor 🚊		
	9 🔽 Block Local File Sharing 🧕 Dei	ne Rule * Any	🍄 TCP: 😰 Write t10	D-Minor 🙀		
	10 🔽 Allow Bootp 🧧 Cop	y Rule 🔭 Any	🗣 UDP: 🚍 None 🛛 10	D-Minor 📕		
	Pas	te Rule				
	Mov	re Up				
	11 🔽 Allow UPnP Discovery fr 🧿 Mov	e Down	🟟 UDP: 😑 None 🛛 10	D-Minor 🙀		
	Imp	ort				
	12 Block UPnP Discovery Exp	ort XAny	@ UDP: 🐮 Write t 10	D-Minor 🚊		
	13 Allow Web Service requ C Anow	Remot	OPTCP: Mone 10	D-Minor 🛒		
		Remot	₩ ₽ ° UDP:			
		Remot				
	14 🔽 Block Web Service reque 🔀 Block	🗶 Any 🔭 Any	🟟 TCP: 😰 Write t 10	D-Minor 🚊		
	15 🔽 Allow LLMNR from privat 🔘 Allow	🛪 Any 📃 Remot	🟟 UDP: 🚍 None 🛛 10	D-Minor 🙀		
		Remot				
		Remot		-		
	•			•		
	Add Rule Add Bla	nk Rule Delete Rule	Move Up	Move Down		
			ОК	Cancel Help		

Click OK