SYMANTEC CONFIGURATION GUIDE FOR WINDOWS

Once Symantec Endpoint Security is installed double click on the shield and Open Symantec Endpoint Protection. You will see the following STATUS screen where you will be able to see everything working normal.



Under Virus and Spyware Protection, Proactive Threat Protection, and Network Threat Protection you will see the Definitions Date. If the definitions are older than 3 days, click LiveUpdate on the left side of the screen.

This will automatically update all of the definitions library for your Symantec Installation.



Computing and Communication Services | September 2012

CHANGE SETTINGS

Under "Change Settings" you will see all of the options that are used to configure the Symantec client. You will have the option to configure each component individually, however most of these are set to their installation defaults.

UChange Settings - Syme	antec Endpoint Pro	lection	6 🗆 🗆 🛛
	Change	Settings	Help
Status Scan for Threats	You can change	e the following settings:	
Change Settings View Quarantine	.	Virus and Spyware Protection Protects against viruses, malware, and spyware	Configure Settings
LiveUpdate	2	Proactive Threat Protection Provides zero-day protection against unknown threats	Configure Settings
	.	Network Threat Protection Protects against Web and network threats	Configure Settings
		Exceptions Exceptions provide the capability to exclude files, folders, and processes from being scanned.	Configure Settings
Symantec.	Q	Client Management Provides functionality to manage this client.	Configure Settings

- Virus and Spyware Protection Preset to default for security and detection of viruses.
- Proactive Threat Protection Application control and heuristic scanning feature that is enabled. It scans files and detects virus according to anomalies and signatures. These are set to their most efficient settings by default.
- Network Threat Protection These include Intrusion Prevention, Firewall Settings, Notifications and Logs. They have been set by default for maximum protection and no need to configure them. To disable firewall or intrusion features just "uncheck" the box.

ewall	Intrusion Prevention	Microsoft Windows Networking	Notification	Logs
	able Firewall			
0.0.	- Rules			
E Fr	able Smart DHCP	Enable Smart	DNS	
Er	hable Smart WINS	Enable Stride	DINS	
Traffie	: Settings			
Er	hable NetBIOS protecti	ion		
	low token ring traffic			
Er	hable anti-MAC spoofin	9		
Er	hable network applicati	ion monitoring		
BI	ock all traffic until the fi	irewall starts and after the firewall s	tops	
	Allow initial DHCP ar	nd NetBIOS traffic		
Er	hable denial of service	detection		
Er	nable port scan detecti	on		
Unma	tched IP Traffic Settin	gs		
OAI	low IP traffic			
() AI	low only application tra	ffic		
E	Prompt before allowi	ng application traffic		
Active	e Response Settings			
₩ Ni	umber of seconds to a	utomatically block an attacker's IP	address:	900
Stealt	h Settings			
Cautio	on: There can be comp features after you hav	patibility issues when using these st e confirmed compatibility.	tealth setting	s. Only use
Er	hable TCP resequencin	ng 📃 Enable stealti	h mode Web	browsing
Er	hable OS fingerprint ma	isquerading		

Computing and Communication Services | September 2012

 Exceptions – These are exceptions from files and folders and processes that are excluded from being scanned. You have different options to exclude. Security Risk Exception relates to Files, Folders, Extensions, and Specific Web Domain URL's. Sonar Exclusion is a specific exclusion that will not be touched. DNS or Host File Change is specifically related to Applications.

Please See:

http://www.symantec.com/business/support/index?page=content&id=HOWT055204

	Exceptions		E
Chathan	User-defined Exceptions		
Status	Exception Item	Exception Type	Action
can for Threats	C:\Program Files\LogMeIn\x86\LMIGuardianSvc.exe	All Scans	Ignore
hange Settings	C:\Program Files\LogMeIn\x86\LogMeIn.exe C:\Documents and Sattings\laconsty.ba\My Documents\D	All Scans	Ignore
iow Quarantino	C:\Documents and Settings\jasonstrube\My Documents\D	SONAR	Ignore
ew Quarantine	C:\Program Files\LogMeIn*	SONAR	Ignore
View Logs	C:(Program Files)(maiwarebytes Anto-maiware)(* C:(Program Files)(uTorrept)*	SONAR	Ignore
	www.isohunt.com	Security Risk Scans	Ignore
LiveUpdate			
Securi SONA DNS o	vy Risk Exception + Delete + Exception + Host File Change Exception +		lose Help

• Client Management – These are the options for Management of the Symantec installation related to Tamper Protection and LiveUpdate.

VIEW QUARANTINE

View Quarantine displays any virus infections that Symantec detected and quarantined. If there is a file in Quarantine, it is locked and is safe from harming your computer. You must run another FULL SCAN to make sure the computer is clean and eliminate any other risks that may not have been detected. It is also safe to delete the files from quarantine.

	View Quar	antine			Help
Status Scan for Threats Change Settings	Files and registry entr	ies that are quarantined	l, backed up, or r Type	epaired are listed below. Original Location	Status
View Quarantine	Purge Opti	ions			
LiveUpdate	Quarantine Qua Length I Total fo	Trans Leaoup Items Repair ; rantined items will be deleted pe of time stored exceeds: Ider size exceeds:	riodically according to th	hese options.	
	K 11 Restore D	elete Rescan All	Cancel	Add Submit	:
Symantec.					

VIEW LOGS

Under "View Logs" you will have several options to view for actions that Symantec took in order to protect your computer from being infected. If you are unsure of something that was detected and actioned you will have the option of reviewing it here:

- Virus & Spyware Protection Scan Log/Risk Log/System Log
- Proactive Threat Protection Threat Log/System Log
- Network Threat Protection Traffic Log/Packet Log
- Client Management Control Log/Security Log/System Log/Tamper Protection Log

LIVE-UPDATE

Under "Live Update" is where you will update your Symantec Endpoint Protection. When you click on LiveUpdate another window will open up to automatically and start to download and install the most up to date definitions available for your computer to be protected. By default these options are set to download every 4 -8hrs. If new definitions are available they will be automatically updated.

You can setup LiveUpdate Schedule under "Change Settings, "Client Management" and LiveUpdate Tab.

Change Settings - Syma	ntec Endpoint Protection	
	Client Management Settings General Tamper Protection LiveUpdate Submissions	Help
Status Scan for Threats	Set the schedule for automatic updates via LiveUpdate.	
View Quarantine View Logs	Every 4 the hours Retry Window Vikeen trying for (in hours):	Configure Settings
LiveUpdate	Randomizet the start time for daily or weekly updates only.	Configure Settings
	Idle Detection Idle Detection Image: Delay scheduled LiveUpdates until the system is idle. Overdue sessions will eventually run unconditionally.	Configure Settings
	Proxy Options Configure Proxy Options	Configure Settings
Symantec	OK Cancel	Help Configure Settings