Symantec Endpoint Protection v12.1 Screencaptures

System: Xevo TQ-S, Windows 7, software test lab, Waters Wilmslow, 1st August 2016





Change Settings - Symant	Change	e Settings	Нер
Status	You can chan	ge the following settings:	
Change Settings View Quarantine	2	Virus and Spyware Protection Protects aganst 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
	2	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

Status	Activ	e Scan		Full Scan	
Scan for Threats	Scan o Infecta	riy the most commonly d areas.	Y	can run in the	badiground.
/lew Quarantine	Duration: I-2 m	inutes		Duration: 30-120 min	utes
View Logs			_		
	Scan Name	Enabled	Туре	When to Scan	Last Scan
	Monthly Scheduled Scan	Yes	Full Scan	Monthly	July 01, 2016 10:37 AM
	Weekly Scheduled Scan	Yes	Active Scan	Weekly	July 29, 2016 1:01 PM

1. Virus and Spyware Protection settings

O	utlook Auto-	Protect	Not	tes Auto-Protect	Early	Launch An	nti-Malware
Glob	oal Settings	Auto-Pro	tect	Download Insight	Interr	net Email A	uto-Protec
Sc	an Options						
Tł	nese <mark>config</mark> u	rations are	share	ed between manual s	scans ar	nd Auto-Pro	otect.
₽	🕖 Enable I	nsight for:		Symantec Truste	ed		÷
	What is	Insight?		1			
A	Enable E	loodhound BloodHour	l ™ he <u>nd?</u>	uristic virus detectio	n Auto	omatic	*
	Exceptions:	8				View Lis	t
Se	elect the time	e <mark>period to</mark> older than	retain	virus and spyware	protecti 4	on logs. days	*
Se In Sp	elect the time Delete logs Iternet Brow	e period to older than ser Protect dress to u	retain tion se as	virus and spyware	protecti 4	on logs. days rity risk ch	anges
Se In Sp vo	Delete logs ternet Brow becify the ac bur home par http://por	e period to older than ser Protec Idress to u ge. tal.waters.	retain tion se as	virus and spyware	4 🗼	on logs. days rity risk ch	anges

Click View List: no exceptions defined

Outlook Auto-	Protect	Not	tes Auto-Protect	Early Launch Anti-Malware
Global Settings	Auto-Pr	otect	Download Insight	Internet Email Auto-Protec
🔒 📝 Enable I	=ile Svsten	n Auto	-Protect	Artiene
File Types				Actions
🔒 🍥 All type	S			Notifications
🕐 Selecter	d:	E	Extensions	Advanced
	mine file t ents	ypes b	y examining file	
Options				
Scan fo	r security	risks		
Scan file	es on remo	ote con	nputers	
17 Only	where files	212.2272	concerning of	
1 7 1 9 1 1 2	when the	s are e	xecuted	
(E) Carry	when hie	s are e	xecuted	
	when me	s are e	xecuteo	
	when hie	saree	xecuted	
	when the	s are e	xecuteo	
	wrierr mes	s are e	xecuteo	
	Wrier rines	s are e	xecuteo	
	Writer r thes	s are e	xecuteo	
	Writer r thes	s are e	xecuteo	
	Writer r thes	s are e	xecuteo	
	Writer r thes	s are e	xecuteo	
	Writer r thes	s are e	xecuteo	
	Writer r thes	s are e	xecuteo	
	Writer r thes	s are e	xecuteo	
	Writeri i tiles	s are e	xecuteo	

click Notifications:

I Display a notification message when a risk is detected:	
Scan type: [LoggedBy] Scan	
Event: [Event]	-
Security risk detected: [SecurityRiskName]	-
File: [PathAndFileName]	
Location: [Location]	
Display the Auto-Protect results dialog	
mediation options	
Terminate processes automatically	
Stop services automatically	

Click Actions:

Virus Security Risks	Specify first and second ac What are the different typ	tions for detections of this to the set of risks?	type of risk.
- Dialer	First action:	Delete risk	-
Hack Tool Joke Program Misleading Application Parental Control Remote Access Security Assessment Tool Security Risk Spyware	If first action fails:	Quarantine risk	Ŧ
Remote Access Security Assessment Tool Security Risk Spyware			

click Advanced:

Changes requiring Auto-Protect reload	
Wait until the computer is restarted	
Stop and reload Auto-Protect	
Scan files when	
Scan when a file is accessed or modified	
Scan when a file is modified	
💟 Scan when a file is backed up	
👿 Do not scan files when trusted processes access the files	E.
Other options	
Always delete newly created infected files	
Always delete newly created security risks	
File cache	Risk Tracer
Enable the file cache	Enable Risk Tracer
	People the source computer IP address
Rescan the cache when new definitions load	
Automatic enablement	Poll for network sessions every:
When Auto-Protect is disabled, enable after:	10000 milliseconds
Backup options	
■ ☑ Back up files before attempting to repair them	
Additional advanced options Floppies Netwo	ork
	OK Cancel Help

Outlook Auto-Protect N			es Auto-Protect Ea		rly Launch Anti-Malwar	
Global Settings	Auto-Pro	tect	Download Insight	Inter	net Email Auto-Prote	
Enable Dow	nload Insig on file rep	ght to utatio	detect potential	(Actions	
What is	File Repu	tation	2	ſ	Notifications	
Specify downlo	ad sensiti	uitu le	wel	- N		
Select levels	au sensiu	VILY IC	.vei			
	/laximum)		Level 5 (Typi	ical)		
- 7 - 6(+ - 5(1 - 4 - 3 - 2 - 1(+	High) Fypical) Ainimum)		Allows only file: unknown reput considered mal considered unp false positive d	s that ation. icious, proven letectio	have a good or Some files are and some files are . The number of ons is low.	
Also detect files	s as malicio	ous ba	ased on their <mark>u</mark> se in th	ne Sym	nantec Community or fewer users	
Eiles kno	wn by use	rs for	; 2		or fewer days	
Intranet Setting	gs ally trust a	any fil	e downloaded from a	in intra	net website	

click Actions:

Specity file handling actio	ns for the following types of file	25.
Specify actions for ma	licious files:	
First action:	Quarantine risk	
If first action fails:	Leave alone (log only)	.7
Unproven files 🝺		
Specify action for unp	roven files:	
	Prompt	1.4

Outlook Auto-Prot	ect No	tes Auto-Protect	Early Launch Anti-Malware
Global Settings	uto-Protect	Download Insight	Internet Email Auto-Protec
🔒 📝 Enable Inte	rnet Email Ai	uto-Protect	Actions
File Types			Notifications
🔒 🎯 All types			Advanced
O Selected:	1	Extensions	
Send email t	o others:		Others

click Actions;

Security Risks	Specify first and second as What are the different ty	ctions for detections of this pes of risks?	s type <mark>of risk.</mark>
Dialer	First action:	Clean risk	*
Hack Tool Joke Program Misleading Application Parental Control Remote Access Security Assessment Tool Security Risk Spyware Trackware	If first action fails:	Delete risk.	*

click Notifications

Event: [Event]	
	[
Security risk detected: [SecurityRiskName]	
File: [PathAndFileName]	
ocation: [Location]	
Computer: [Computer]	
Jser: [User]	
Action taken: [ActionTaken]	

click Advanced:

📝 Scan files inside compress	ed files
Number of levels to expan compressed files:	d if there are compressed files within 3
Connection settings	
Incoming mail server (POP3):	110 Use Defaults
Outgoing mail server (SMTP)	25
Allow encrypted POP3 cor	nnections
Allow encrypted SMTP cor	nnections
Note: Messages sent over er	ncrypted connections cannot be scanned.
Mass Mailing Worm Heuristics	
Mass Mailing Worm Heuristics	5
Mass Mailing Worm Heuristics Mass Mailing Worm Heuristics Outbound worm heuristic First action:	s
Mass Mailing Worm Heuristics Mass Mailing Worm Heuristic Outbound worm heuristic First action: If first action fails:	s Quarantine threat * Delete threat *
Mass Mailing Worm Heuristics Mass Mailing Worm Heuristic First action: If first action fails: Progress notifications	s Quarantine threat * Delete threat *
Mass Mailing Worm Heuristics Outbound worm heuristic First action: If first action fails: Progress notifications Display a progress indicat	s Quarantine threat Delete threat Tor when email is being sent
Mass Mailing Worm Heuristics Cutbound worm heuristics First action: If first action fails: Progress notifications Display a progress indicat Display a notification area	s Quarantine threat Delete threat Tor when email is being sent a icon

Global Settings Auto-Pro	btect Download Insight	Internet Email Auto-Protec
Outlook Auto-Protect	Notes Auto-Protect	Early Launch Anti-Malware
🔒 📝 Enable Microsoft C	Outlook Auto-Protect	Actions
File Types		Notifications
All types		Advanced
O Selected:	Extensions	
Send email to othe	rs:	Others

click Actions:

Virus Security Risks	Specify first and second as What are the different ty	ctions for detections of this type of risk. <u>pes of risks</u> ?
Dialer	First action:	Delete risk 📼
Hack Tool Joke Program Misleading Application Parental Control Remote Access Security Assessment Tool Security Risk Spyware Trackware	If first action fails:	Quarantine risk 🔹

Click Notifications:

Scan type: [Logg	edBy] Scan	
Event: [Event]		
Security risk dete	cted: [SecurityRiskName]	
File: [PathAndFile	eName]	
Location: [Location	[nc	E
Computer: [Com	puter]	
User: [User]		
Action taken: [Ar	tionTakenl	

click on Advanced:

Compressed files options	
Scan files inside com	pressed files
Number of levels to compressed files:	expand if there are compressed files within 3

ciobal becalligs Had	Protect Download Insight	Internet Email Auto-Prote
Outlook Auto-Protec	t Notes Auto-Protect	Early Launch Anti-Malware
🔒 📝 Enable Lotus I	Notes Auto-Protect	Actions
File Types		Notifications
🕯 🎯 All types		Advanced
O Selected:	Extensions	
Send email to	others:	Others

Click on Actions

Virus Security Risks	Specify first and second a What are the different ty	ctions for detections of this to pes of risks?	/pe of risk.
Dialer	First action:	Delete risk	*
- Hack Tool Joke Program Misleading Application Parental Control Remote Access Security Assessment Tool Security Risk Spyware Trackware	If first action fails:	Quarantine risk	*

Click on Notifications;

Scan type	: [LoggedBy] Scan	
Event: [Ev	ent]	
Security ri	sk detected: [SecurityRiskName]	
File: [Path	AndFileName]	
Location:	Location]	
Computer	[Computer]	
User: [Use	r]	
Action tak	en: [ActionTaken]	

click on Advanced:

Compressed files options				
Scan files inside compre	ssed files			
Number of levels to exp compressed files:	and if there are com	pressed files v	vithin 3	

Global Settings Auto-P	rotect Download Insight	Internet Email Auto-Protect
Outlook Auto-Protect	Notes Auto-Protect	Early Launch Anti-Malware
Enable Symantec Ea	rly Launch Anti-Malware	
When Symantec Endpo	int Protection detects a pote	entially malicious driver
C Log the detection	as unknown so Windows all	ows the driver to load
() Use the default W	/indows action for the detec	tion
This feature requires W	indows 8.	
This feature requires W	indows 8.	
This feature requires W	indows 8.	
This feature requires W	indows 8.	
This feature requires W	indows 8.	
This feature requires W	indows 8.	
This feature requires W	indows 8.	

2. Proactive Threat Protection settings

SONAR	Suspicious Behavior Detection	System Change Detec	tion
≙	Enable SONAR		What is SONAR?
Action	ns for threat detection		
Speci	fy actions if SONAR finds a threa	it:	
🔒 Hiç	gh risk detection:	Remove	*
Lo	w risk detection:	Log	•
		Enable Aggressiv	ve Mode
W	nen detection found:	▲ ☑ Show alert upon	detection
		Prompt before te	erminating a process
		Prompt before st	topping a service
		ОК	Cancel Help

SONAR	Suspicious Behavior Detection	System Change Detection	
Action	n for threats in applications		
Speci	fy actions if SONAR finds a threa	t in applications:	
Hig	gh risk detection:	Block	•
Lo	w risk detection:	Ignore	•

ONAR	Suspicious Behavior Detection	System Change Detection	n
Action	ns for system changes		
Speci	fy actions when SONAR detects	the following system chang	ges:
DN	IS change detected:	Ignore	•
Ho	ost file change detected:	Ignore	•
Ex	ceptions:	View List]
		OK	Cancel Help

3. Network Threat Protection settings

rewall	Intrusion Prevention	Notifications	Logs		
Ena	able Firewall				
Built-in	Rules				
🗸 Ena	able Smart DHCP		😨 Enable Smart	DNS	
Ena	able Smart WINS				
Traffic	Settings				
Ena	able NetBIOS protect	ion			
Allo	ow token ring traffic				
Ena	able anti-MAC spoofin	ig			
Ena	able network applicat	ion monitoring			
Blo	ock all traffic until the f	îrewall <mark>s</mark> tarts an	d after the firewall s	tops	
V	Allow initial DHCP a	nd NetBIOS tra	fic		
Ena	able denial of service	detection			
Ena	able port scan detecti	ion			
Unmate	tched IP Traffic Settin	gs			
Allo	ow IP traffic				
🔿 Allo	ow only application tra	ffic			
	Prompt before allowi	ing application t	raffic		
Active	Response Settings				
Nur	mber of seconds to a	utomatically blo	ck an attacker's IP	address:	60
Stealth	n Settings				
Caution	n: There can be com	patibility issues	when using these s	tealth setting	s. Only use
these f	features after you hav	e confirmed co	mpatibility.	h mada Wab	-
	able TCF resequencin	ig 		T mode web	browsing
Ena	able US tingerprint ma	asquerading			
			ОК	Cancel	Help
ork Th	hreat Protection Se	ttinas			
					24
ewall	Intrusion Prevention	Notifications	Logs		

Firewall	Intrusion Prevention	Notifications	Logs
1	Display Intrusion Preve	ention notificatio	ons
	Use sound when r	otifvina users	

irewall	Intrusion Prevention Notifications	Logs		
Secur	ity Log File			
Maxim	ium log file size:	512	KB	Clear Log
Save	each log entry for:	14	days	A
Syster	n Log File			
Maxim	ium log file size:	512	KB	Clear Log
Save	each log entry for:	14	days	
Traffic	: Log File			52
Maxim	ium log file size:	512	KB	Clear Log
Save	each log entry for:	14	days	
Contro	ol Log File		<u></u>	
Maxim	ium log file size:	1024	KB	Clear Log
Save	each log entry for:	14	days	
_ Enat	ole Packet Log			
Packe	et Log File		-	
Maxim	ium log file size:	1024	KB	Clear Log
Cause	each log entry for:	14	days	

4. Exceptions

5. Client Manangement Settings

General	Tamper Protection	LiveUpdate	Submissions	
Displa	y Options			
V Sho	w Symantec security	icon in notific	ation area	
Proxy	Options			
	Configure Proxy Op	tions		
Reboo	ot Options			
	Configure Reboot Op	tions		
Locati	ion Options			
Curren	t location:		Default 🔹	
User I	information			
	Update User Informa	ation		
Applic	ation and Device	Control		
E	nable Application and	Device Cont	ol	

Proxy Options:

Proxy Configuration	
Select the proxy ser	rver option to use for all external communication except LiveUpdate
🔘 I do not use a p	roxy server
I want to use the second se	e proxy server specified by my client browser(default)
🔘 I want to use cu	ustom proxy settings
Host proxy:	
Port:	
Authenticati	on required
User name:	
Password:	

Reboot Options:

Restart Computer	
Immediately	
At this time:	Today ▼ 6:00:00 AM ▲
🔽 Randomize sta	art time Randomization Hours: 3
Restart Type	
💮 Do not restart (n	ot recommended)
No prompt	
Prompt with a co	untdown of: 5 👘 minutes
Promot and allow	u spooze up to: Scheduled Time
C Tranpe and allen	
Restart Message	
A security risk reme computer to restart	diation or a new content download requires this t.
Other Options	
I Lined contract	
Maru restart	polications will not be able to prevent this restart.
Third party a Unsaved use	r data could be lost.
Third party a Unsaved use	ely if the user is not logged in
Third party a Unsaved use Restart immediat If the user is option forces restart action	r data could be lost. ely if the user is not logged in not logged in when the restart request is sent, this an immediate restart and overrides other pending is.

General	Tamper Protection	LiveUpdate	Submissions	
Prot	ect Symantec securi	ty software fr	om being tampered with or s	hut down
A 147223	a ball of an analysis to	and the second to the	 Loop and a soluble and the state of the solution of solution. 	
Action I softwar	o take if an applicati e:	ion attempts t	o tamper with or shut down S	Symantec security
Action I softwar Block a	o take if an applicati e: ind do not log	ion attempts b	tamper with or shut down s	Symantec security

neral	Tamper Protection	LiveUpdate	Submissions	
Set	the schedule for aut	omatic update	s via LiveUpdate.	
	😨 Enable automati	c updates		
Fr	equency and Time			
	Every -		4 🗑 hours	
	Carlos Ma			
Re	etry Window			
3	🛚 Keep trying for (in l	nours):		2
Ra	andomization Options			
R	andomizes the start t	ime for daily o	or weekly updates only.	
E	Randomize the star	t time to be +	or - (in hours):	2
Id	le Detection			
	Delay scheduled Liv unconditionally.	eUpdates un	il the system is idle. Overdue	sessions will eventually run
Pri	oxy Options			
	Configure Proxy	Options		
10				

click Configure Proxy Options:

HTTP or HTTPS FTP	
HTTP or HTTPS Proxy Configur	ration
Select the type of configurat	tion for communications
💮 I do not use a proxy ser	ver for HTTP or HTTPS
I want to use my Window	ws Internet Ontions proxy settings (default)
 Twent to evolve any winder 	
Uset provide	THP or HTTPS setangs
HUSE PROXY,	
HTTP Port:	HTTPS Port:
Authentication requ	uired
Authentication Type	e
Basic Authentica	ation
User name:	
Password:	
🔘 NT LAN Manage	r Authentication
User name:	
Password:	
Domain name:	

HTTP or HTTPS FTP	
FTP Proxy configuration	
Select the type of con	figuration for communications
🗇 I do not use a prox	cy server for FTP
I want to use my V	Vindows Internet Options FTP settings (default)
I want to customize	
I want to customize	enty rife seconds
FTP host proxy:	
Porti	
	ीं

General	Tamper Protection LiveUpdate Submissions	
Subn	nissions help Symantec address threats in the fight aga	inst digital cybercrime.
V Le	t this computer automatically forward selected anonym	ous security information to Symantec
S	Select additional types of information to submit:	
π		
1		
1	Antivirus advanced heuristic detections	
1	SONAR detections	
	SONAR heuristic	
	If you disable any submission types, you preven providing the best protection for your dient com	t Symantec Endpoint Protection from puters.
A	llow Insight lookups for threat detection (recommended	0
	If you disable this option, you prevent Download In: computers. You also limit the protection that is provi The rate of false positives might increase.	sight from detecting threats on your dient ded by virus and spyware scans and SONAR.