Symantec Endpoint Protection

Small Business Edition 12

Best Practices

Bill Bowles Senior Technical Product Manager Endpoint Security

The latest version of this document can always be accessed via the following Symantec webpage:

http://www.symantec.com/business/support/overview.jsp?pid=55357

TABLE OF CONTENTS

TABLE OF CONTENTS2
INTRODUCTION3
What is SEP SBE 12? 3 General Note on Compatibility 4 System Requirements 4 Supported Platforms 5
INSTALLATION6
MIGRATION METHODOLOGY
WHAT TO EXPECT FROM THIS POINT ONWARD28
RECOMMENDED BEST PRACTICE CONFIGURATION29
MANAGER SETTINGS 29 Administrator Accounts 30 RECOMMENDED CLIENT PROTECTION POLICIES 31 Virus and Spyware Protection (AntiVirus) Policy 31 Firewall Policy 32 Intrusion Provention Policy 32
LiveUpdate Policy
LiveUpdate Policy

INTRODUCTION

This white paper focuses primarily on providing best practices guidance on how to successfully deploy Symantec Endpoint Protection Small Business Edition 12 (SEP SBE 12) Manager and Client protection components to Microsoft[®] Small Business Servers and create basic security policies.

It is recommended that the **getting_started.pdf**, **implementation_guide.pdf** and **Client_guide_sbe.pdf** be reviewed prior to deployment of SEP SBE 12. Pay particular attention to the sections entitled: "**Planning the Installation**" in the **getting_started.pdf** document as they will provide you with a roadmap for a successful SEP SBE 12 installation.

WHAT IS SEP SBE 12?

SEP SBE 12 combines Symantec Antivirus with advanced threat prevention to deliver unmatched defense against malware for laptops, desktops and servers. It seamlessly integrates essential security technologies in a single client and management console, increasing protection and helping lower total cost of ownership. It includes the following protection technologies:

- □ Antivirus and Antispyware
 - The Antivirus Email Protection feature is aimed at providing additional email protection to Clients. It is not necessary to install this function if added mail security is not necessary or if Email filtering has already been implemented in the environment
- □ Proactive Threat Protection (TruScan)
 - > This is currently not supported on server operating systems.
- Intrusion Prevention
- Firewall

The core components required to run in a centrally managed SEP SBE 12 Environment includes the following:

- Symantec Protection Center (SPC) (A web server also referred to as the "Manager" which utilizes Apache Tomcat)
- Database (An embedded database, based upon Sybase Adaptive Server Anywhere version 9)
- SEP SBE 12 Client (Runs on each machine you wish to protect, including the Manager)

□ Symantec Protection Center Remote Console (Optional Java-based console that can be run from anywhere with network access to the Manager)

GENERAL NOTE ON COMPATIBILITY

It is very possible to run a Symantec Protection Center and the SEP SBE Client on the same machine as a Microsoft Windows Small Business Server. By default, there are no technical conflicts between the two - <u>The key consideration is resource utilization on the target</u> <u>machine</u>, plus as a general best practice, good planning and preparation are also strongly recommended.

SYSTEM REQUIREMENTS

While every environment varies, below are some high-level guidelines on recommended hardware that will help to ensure the Windows Small Business Servers will run smoothly with SEP SBE 12 installed:

SEP SBE 12 Manager

- □ 32-bit processor: 1-GHz Intel Pentium III or equivalent minimum (Intel Pentium 4 or equivalent recommended)
- □ 64-bit processor : 2-GHz Pentium 4 with x86-64 support or equivalent minimum
 - > Intel Itanium processors are not currently supported
- □ 1 GB of RAM minimum (2 GB of RAM recommended)
- □ 4 GB or more of free disk space

SEP SBE 12 Client

- □ 32-bit processor: 1-GHz Intel Pentium III or equivalent minimum (Intel Pentium 4 or equivalent recommended)
- □ 64-bit processor: 2-GHz Pentium 4 with x86-64 support or equivalent minimum
 - > Intel Itanium processors are not currently supported
- **256 MB of RAM minimum (1 GB of RAM recommended)**
- □ 700 MB or more free disk space

SUPPORTED PLATFORMS

OPERATING SYSTEM	32-BIT	64-BIT
SPC SERVER		
Windows 2003	Х	Х
Windows XP	Х	Х
Windows 2000 (SP3 and later)	Х	
Windows 2008	Х	Х
Windows 2008 Small Business and Essential Business Servers		Х
DATABASE		
Embedded	Х	Х
CLIENT		
Windows Vista	Х	Х
Windows 2003	Х	Х
Windows XP	Х	Х
Windows 2000 (SP3 and later)	Х	Х
Windows 2008	Х	Х
Windows 2008 Small Business and Essential Business Servers		Х

INSTALLATION

MIGRATION METHODOLOGY

Phase I Planning and Preparation Considerations

- Review existing environment
- Identify recovery and support procedures
- > Obtain SEP SBE 12 Serial Number and Software
- Backup current Small Business Server environment

Phase II Management Server and Client Installation

- Install the SEP SBE Management server
- Migrate SAV/SCS Legacy Groups and Settings if applicable
- Migrate SAV/SCS Reporting if applicable
- Configure Management Server
 - (Groups, LiveUpdate Schedule, Notification Messages, Scheduled Reports, Administrator Accounts)
- Client Installation
 - If possible it is a good practice to test the client installation prior to production deployment

Phase III Post Installation Tasks

- > Register serial number and import site license
- Backup SBS Server environment

NOTE: Symantec provides notification messages, scheduled reports and protection policies out-of-the -box that can be leveraged for quick deployment if desired.

PHASE I PLANNING AND PREPARATION CONSIDERATIONS

- As a precaution, ensure you have a complete backup of your existing Microsoft Windows Small Business Server environment, and ensure the backup has been tested and confirmed to work.
- It is strongly recommend that you take some time to review the system resource utilization on your Small Business Server before beginning deployment of SEP SEB 12. Detailed below is the typical resource usage you should expect once SEP SBE12 is running.
 - Manager (including Database) Approximately 150MBs
 - Client Between 25MBs (idle) and 50MBs (running LiveUpdate or scheduled scan)
 - > Console (when in use) Approximately 80MBs
- □ If possible test the deployment of the Manager and Client first in a <u>non-production</u> test environment.
- □ It is highly recommended that you view the SEP SBE 12 instructional "Tours" located at the following links:
 - > Admin UI Tour:

http://www.symantec.com/redirects/symantec/support_symantec_com/sepsbe/tour/

Client Installation Tour:

http://eval.symantec.com/flashdemos/products/endpoint_protection/client_install_tour/

- □ It is recommended that installation be conducted at an off-peak time when there will be no users or applications interacting with the server.
- Ensure you have registered your company with Symantec Technical Support and have information on how to contact them to log a support case, so you're prepared for the unlikely event that you encounter issues.
- □ Ensure that you have obtained your SEP SBE 12 serial number to register and download your license file. You will then import your license file into the Manager.
- □ The SEP SBE 12 Software can be downloaded at the following link or can be obtained from your reseller:

https://fileconnect.symantec.com

- □ Installing the SEP SBE 12 Client with Network Threat Protection Technologies will require a reboot to enable the technology.
- □ Installing the Manager will not replace/upgrade an existing SAV 10 or 9 parent server nor will it install the Client.
- □ SEP SBE 12 Documentation can be found under the Documents folder on the installation CD.

IMPORTANT: If another vendor's antivirus or firewall product is currently running on the Windows Small Business Server it will need to be removed in advance of installing the SEP SBE 12 Manager. This also pertains to Clients that will have the SEP SBE 12 Client installed.

If you install the SEP SBE 12 Client on the SAV Parent Server it will remove the SAV Parent Server and will orphan existing SAV/SCS Clients. This is only recommended if you plan on migrating your SAV/SCS Clients at the time of the SEP SBE 12 Manager Client installation otherwise they will need to run parallel with one another as part of a phased migration until all Clients have been migrated.

The SEP SBE 12 Firewall is installed **disabled** and will not interfere with the Windows Firewall if enabled. Once the SEP SBE 12 Firewall has been enabled the Windows Firewall will be disabled and the SEP SBE 12 Firewall Policy will take effect.

If you have a Symantec System Center and/or SAV Reporting Server installed on the SBS machine, they must be relocated through Add/Remove Programs before continuing. A reboot is not required.

SEP SBE 12 does not support migration from SEP 11 SEPM to SEP SBE 12 SPC. The SEPM will have to be uninstalled prior to installing SEP SBE 12 SPC. If desired the SEP 11 policies can be exported and imported into the SEP SBE 12 SPC after installation.

PHASE II SYMANTEC PROTECTION CENTER INSTALLATION (SPC)

The installation of the Manager can be done within 20 minutes under normal circumstances. Symantec has streamlined the manager installation process for Small Business Environments requiring little input from the user during the Manager installation. To install the **Symantec Protection Center**:

Locate and execute the **Setup.exe** file located on Disc 1 of the installation files. The installation menu should appear. Select **Install Symantec Endpoint Protection**.



Select Next

🔂 Symantec Endpoint Protection Manager				
	Welcome to the Installation Wizard for Symantec Endpoint Protection			
	The Installation Wizard will perform the following steps:			
	 Install the management server and console Configure the management server Create the database Migrate from a previous version if required Install clients Click Next to begin. 			
Symantec.	WARNING: This program is protected by copyright law and international treaties.			
	< <u>Back</u> Cancel			

Select "I accept the terms in the license agreement" and then select Next

👘 Sym	nantec Endpoint Protection Manager	X
Licen Plea	ase read the following license agreement carefully.	
	SYMANTEC SOFTWARE LICENSE AGREEMENT	
SYMA LICEN WILL	INTEC CORPORATION AND/OR ITS AFFILIATES ("SYMANTEC") IS WILLING TO LICENSE THE NSED SOFTWARE TO YOU AS THE INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT BE UTILIZING THE LICENSED SOFTWARE (REFERENCED BELOW AS "YOU" OR "YOUR") (ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE	
AGRE	EEMENT ("LICENSE AGREEMENT"). READ THE TERMS AND CONDITIONS OF THIS LICENSE EEMENT CAREFULLY BEFORE USING THE LICENSED SOFTWARE. THIS IS A LEGAL AND DRCEABLE CONTRACT BETWEEN YOU AND SYMANTEC. BY OPENING THE LICENSED	
SOFT	WARE PACKAGE, BREAKING THE LICENSED SOFTWARE SEAL, CLICKING THE "I AGREE" OR "BUTTON, OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE	-
0 1 <u>0</u>	ccept the terms in the license agreement Enlish and encenter agreement	
Install5h	< <u>B</u> ack <u>N</u> ext > Cancel	

(Select "Change" if you need to change the path from the default and then select Next.



Select Install

🙀 Symantec Endpoint Protection Manager	×
Ready to Install the Program	mantec
The wizard is ready to begin installation.	mance.
Click Install to begin the installation.	
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the w	izard.
Instalishield	
< <u>B</u> ack	Cancel

Select Next

🖓 Symantec Endpoint Protection Manager 🛛 🛛 🔀				
Management Server and Console Installation Summary				
	The Installation Wizard has successfully installed Symantec Endpoint Protection Manager.			
	Install the management server and console Configure the management server			
	Create the database			
	Install clients			
	Click Next to configure the management server.			
Symantec.				
< <u>Back</u> Cancel				

Enter your **Company Name** and **Password**. The User name will default to Admin which can't be changed at this time. Enter an **Email address** of an administrator that will receive notification messages. Symantec provides multiple notification messages out-of-box that will send Security Status information to designated administrators. These messages can be reconfigured if desired from the management console. "**REMEMBER YOUR PASSWORD. IT WILL BE NEEDED TO LOG INTO THE MANAGEMENT CONSLE."**

🔍 Management Server Configu	ration Wizard	<u> </u>	
	Administrator Settings Specify a user name and password to create an administrator account. You use the account to log on to the management server.		
	Company name:	Symantec	
	User name:	admin	
	Password:	*****	
	Confirm password:	Minimum of 6 characters in length	
	Reports and Notificatio	ns	
	Important reports and notifications are sent to the email address that you specify below.		
	Email address:	administrator@symantec.local	
Symantec.	Chat with Symantec Supp	ort	
		<back next=""> Cancel</back>	

Verify that the **Email Server Name** and **Port Number** are correct and alter if necessary. If you do not know this information choose the defaults and select **Next**

🛑 Management Server Config	uration Wizard
	Email Server Communication Settings The management server uses these settings to communicate with your email server. Use the defaults if you do not know the values.
	Email Server Name: labsbs Port Number: 25
	Send Test Email
Symantec.	You can edit these settings at a later time from the Symantec Endpoint Protection Manager Console. <u>Chat with Symantee Support</u>
	< <u>Back</u> <u>N</u> ext > <u>Cancel</u>

Select Next

	Management Server Configuration Wizard				
~	Management Server Port Settings				
	The Install Wizard has automatically configured your remote access and client communications ports. The port numbers are important for remote access to the management console and for troubleshooting.				
	Server name: labsbs				
	Server port: 8443				
	Management console port: 9090				
	Client communications port: 8014				
	About the client communications port				
	Print a copy for your records (recommended).				
Symantec.	Chat with Symantec Support				
	< Back Next > Cancel				

Select Next



Select Next

🛑 Management Server Configuration Wizard			
	Database Creation Summary		
v	The database has been successfully created and initialized.		
	✓ Install the management server and console		
	 Configure the management server 		
	✓ Create the database		
	Migrate from a previous version if required		
	Install clients		
	Click Next to migrate from a previous version.		
Symantec			
Julianee			
	< Back	Cancel	

Select **Yes** if you wish to migrate the legacy SAV/SCS Group and settings into the SEP SBE 12 SPC. If you do not wish to do this at this time select **No**

Management Server Configu	ration Wizard
	Symantec AntiVirus Migration (optional) Do you want to migrate policy and client configurations from a previous version of Symantec AntiVirus or Symantec Client Security?
	You can run this wizard at a later time from the Start menu on this computer.
Symantec.	Chat with Symantec Support
	< Bac Cancel

NOTE: Refer to Chapter 6 of the **implementation_guide** for more information regarding the migration of legacy SAC/SCS groups and settings.

Select Next to complete the installation

Wanagement Server Configuration Wizard				
	Symantec Endpoint Protection Installation Complete			
	Next Steps:			
	Install protection on your computers. Use the Client Installation Wizard to install protection on multiple client computers and this server.			
	Activate your product within 30 days. Use the Licensing feature in the Admin section of the management console to activate your product.			
	Click Next to install the client to multiple computers.			
Symantec.	Chat with Symantee Support			
	< Back	<u>Cancel</u>		

The installation of the management server has been completed. The Client Installation Wizard will now appear. You can deploy the Clients at this time. If you wish to deploy the Clients at a later time select cancel and continue to Phase III Post Installation Tasks.

REMEMBER: If you install the SEP SBE 12 Client on the SAV Parent Server it will remove the SAV Parent Server and will orphan existing SAV/SCS Clients. This is only recommended if you plan on migrating your SAV/SCS Clients at the time of the SEP SBE 12 Manager Client installation otherwise they will need run parallel with one another as part of a phased migration until all Clients have been migrated.

If the Symantec System Center (SSC) is installed it will need to be removed prior to the installation of the SEP SBE 12 Client.

After the manager installation the LiveUpdate process will begin to run silently in the background, as an automated post-install task. Its purpose is to download the latest content (Antivirus and Antispyware definitions, etc) to the Manager. This process can run for varying lengths of time depending on the speed of the internet connection available. You do not need to wait for this process to complete before progressing to Phase 3, but you should be aware LiveUpdate is running in the background and will utilize resource, therefore may impact the user experience temporarily.

To install the Client on the Manager select Next

Client Installation Wizard		×
	Welcome to the Client Installation Wizard	
	The next steps will help you install protection onto the computers in your network.	
R.	Clickhere to watch a tutorial on how its done, or click Next to proceed.	
	You can run this wizard at a later time from the Symantec Protection Center.	
Symantec.	Chat with Symantec Support	
	<pre><box next=""> C ncel</box></pre>	

Select Servers from the dropdown list and select Next

🖲 Client Installation Wizard	X
Select Group and Protection Types	Symantec.
Select the group the new computers will join, and also the types of protection to install. Group: Servers Protection Types to install: Virus and Spyware Protection Include Email Protection	
Network Threat Protection (Includes Firewall and Intrusion Prevention)	
To continue, click Next	
< Bac Ne	xt> Ca zel

Select Custom Installation (advanced) and select Next



Select Next

🔘 Client Installation Wiza	rd	X
Install Package File Fo Select the file format for t	rmat he installation package.	Symantec.
Would you like to o separately? If you ⓒ Create a s	reate a single self-compressed SETUP.EXE file or generate all the files need to use an .MSI file, then you should generate all the files separately. ingle self-compressed SETUP.EXE	
C Generate a	II files separately	
Export folder:	c:ttemp\Symantec\ClientPackages Browse	
	< Back	ext > C ncel

Select Next



Click on the c:\temp\Symantec\ClientPackages link and Select Finish.



From the Packages directory select the 32-Bit folder and double click on the **Setup.exe** file to install the Client.

	🚞 C:\TEMP\Syma	ntec\ClientPac	:kages\Package_	_32-bit			
	<u>File E</u> dit <u>V</u> iew	F <u>a</u> vorites <u>T</u> o	ools <u>H</u> elp				
	🔇 Back 🝷 🕥 👻	🎓 🔎 Search	n 🜔 Folders 🛛 🖟	🖗 🌶 🗙 🎾 🖽	•		
	Address 🛅 C:\TEN	1P\Symantec\Clie	ntPackages\Packag	e_32-bit		-	🔁 Go
ľ	Name		Size	Туре	Date Modified	Attributes	
	Setup.exe		80,681 KB	Application	2/10/2009 10:28 PM	A	

Upon completion of the install you will see a yellow shield icon with a green circle appear in the bottom right corner of the system tray . You can also confirm the Client installation by opening the Manager, navigating to the Servers group under the Computer Tab and you will see your installed Client appear under the Computers Tab.

🕔 Symant	ec Protection Center	
Sym	antec Endpoint Pro	tection Small Business Edition
	Computers	Servers
Hama	🖃 📑 My Company	
Gome	- Call Lentens and Depktops	Computers Policies
	- 🕞 Servers	
1		This group contains the following computers:
Monitors		Computer Health State User Last Check-in
		🖳 labsbs 🔮 Ok Administrator 2/10/09 1:49 PM
<u>R</u> eports		
Policies		
Loncies		
28	Tasks	
	Add a computer	
Computers	Edit the group properties	

Note: The Antivirus and Antispyware protection component will typically be active before reboot. However the Network Threat Protection components require a reboot. It is normal to not see the Network Threat Protection technologies under the Client UI until a reboot has been performed.

PHASE III POST INSTALLATION TASKS

Once you have completed installation of the Manager and Client, you will need to register your serial number to obtain your license file and upload it to your Manager. Login to the Manager using the following credentials - **Username:** admin, **Password:** <specified earlier>

NOTE: The management console can optionally be run from a remote machine by installing the remote management console. To do this open a web browser on any machine with network access to the Manager, and connect to the following URL, <u>http://(SBS</u> <u>Hostname_or_IP):9090</u>. Follow the instructions to setup the remote console on your machine.

To register your serial number select **Activate your Product** from the Welcome Screen. You can also navigate to the **Admin Tab – Licensing Tab** and select **Register Serial Number** in the management console.



Enter your login credentials and select **Login** if you already have an account. If you do not have an account, select **Create An Account**. Once you have created an account a confirmation email will be sent to the email addressed specific during the account creation.

• E Ktps://ktensing.symantec.com/acctingit/undex.jsp		Dire Search
Edt Yew Fgvorkes Iools Help	1	D = 2 2 2
2 Gelicensing Portal		🚱 • 🖸 - 🕅 • 🖸 Bape • 🥥 To
symantee, Licensing Portal	>Help >FAQs >Symantec.com	
elcome to the Symantec Licensing	Portal.	
nsing Portal to register and activate newly purchased	Please Select Your Language	
ducts, manage existing license data and process software sion upgrade notifications.	English Français	
Veb users, to create a new account, please contact	Deutsch 0000	
mantec Customer Care or a super user.	Português DDD	
	Español 000	
ease Note: The following products require other ethods of activation and are not available to transac the Liceasing Partal. Sease active and install the license that activates the lowing products: Wilking Inducts: Wilking Artifician Search Search Search Search Gamer Search Search Vollowing IT ymantes Caleway Search Vollo Staries	To begin, please login or create an account. Login To Your Account Login ID: This may be your annal address Passent: Locat Cocat	

Select New Purchase



Input your Serial Number

Symantec. Licensing Portal	
Home Get a License Key Manage My Licenses Get Software My Account New Purchase Version Upgrade Moving an Existing License	
Get a License Key for a New Purchase Enter the Serial Number for the license you would like to register You can find the Serial Number on the associated License Certificate you received with your initial purchase.	
Enter One Serial Number: Serial Number Here Register more than one license ?	
Back SUBMIT	

Select the SEP SBE 12 license and select Next

5 s	ymantec.	Licensing Portal		We
lome	Get a License Key	Manage My Licenses Get S	Software My Accoun	1
iew Pui	chase version d	pgrade i Moving an Existing Licen		
Get a	a License I	Key for a New Purc	hase	
erify ease vine 'Nex	the serial numl erify that the serial t' button.	number below is related to the licer	Id like to register.	ister and click
1 Thi mu	s license can be reg Itiple licenses for th	jistered with other licenses for this p is product, please enter the serial n	product. If you would lik number and click the 'Ad	e to register d' button.
Add a Please Serial	nother license for enter the serial nur Number:	this product. mber below and click the 'Add' butto Add	n.	
Select	Licenses To Registe Serial #	er Together Description	Version	Order #
⊿	M1480799844	SEPSBE	12	16422918
			Ba	

Verify your account information and ensure that the correct email is listed to where the confirmation Email will be sent. Select **Complete Registration**.

ou will receive an emai omplete. Enter the emai mall.	I containing license key information when the reg ail addresses of the people you would like to copy	gistration process is y on the license key delivery
10:	hannan_galloway@symantec.com	
	Use commas to separate multiple email addresses.	
Subject :	Symantec license file for serial number M3437595077	7
Message :		
echnical Contact echnical contact(s) are	entitled to contact Symantec support services ac	ccording to the terms of you
echnical Contact echnical contact(s) are naintenance agreement First Name :	entitled to contact Symantec support services ac t described below. Hannah	ccording to the terms of you
echnical Contact echnical contact(s) are naintenance agreement First Name : Last Name :	entitled to contact Symantec support services ac t described below. Hannah Galloway	ccording to the terms of you
echnical Contact echnical contact(s) are naintenance agreemen First Name : Last Name : Email address : Phone Number :	entitled to contact Symantec support services ac t described below. Hannah Galloway hannah_galloway@symantec.com 3106140830	ccording to the terms of you
echnical Contact echnical contact(s) are naintenance agreement First Name : Last Name : Email address : Phone Number :	entitled to contact Symantec support services ac t described below. Hannah Galloway hannah_galloway@symantec.com 3106140830 Add another technical contact	coording to the terms of you
echnical Contact echnical contact(s) are naintenance agreement First Name : Last Name : Email address : Phone Number : Iser Comments	entitled to contact Symantec support services ac t described below. Hannah Galloway hannah_galloway@symantec.com 3106140830 Add another technical contact	coording to the terms of you

Download your license file by selecting **Download License Key File**. The license file will have a .slf extension.

ome Get a	License Key Manage My Lice Version Upgrade Moving an	nses Get Software My A	ccount
et a Lic	ense Key for a Ne	ew Purchase	
icense Con our registration he license(s) be electing the 'Ma	firmation and License Ke on is complete. License details slow have been added to your lic nage My Licenses' button on the	ey(s) have been sent to the email add ense catalog and can be accesse Licensing Portal Home Page	resses you specified. d at any time by
ownload the .sl Your Registere	f file to receive your license key d Licenses and Corresponding Li	file. Icense Keys	
ownload the .sl Your Registere Serial Number	f file to receive your license key d Licenses and Corresponding Li Description	file. Icense Keys License Key	License Key Required
ownload the .sl Your Registere Serial Number M3437595077	f file to receive your license key d Licenses and Corresponding Li Description SYMC MAIL SECURITY FOR MS EXCHANGE 6.0 WIN I/O BASIC MONTHS	file. icense Keys License Key 12 Download License Key (10914016.slf)	License Key Required

A confirmation Email will also be sent which will also contain the license file in Zip file format. You will need to extract the .slf file from the zip file prior to importing it into the Management Console.

Thank you for registering your Symantec	products. Your registration details are available below:
Serial Number: M3437593077 License Key: Download Attached Sym	antec License File(10914016ælp)
1 o download software for this purchase, §	0 00: https://iieconnect.symanice.com
License Information:	
Order Details Customer Name: Customer Number: Order Number: Quantity Purchased : Installed At Address 26900 PACIFIC COAST HIGHWAY MALIBU BEACH, CA 90265-9998 US	STARK INDUSTRIES 58864454 16422918 2
Instructions: IMPORTANT Your license file is contain contained within the .zip file is the actual Notepad or Wordpad as this will corrupt y	aed within the attached zip file. This file must be opened using a decompression utility such as Winzip or Winrar. The .slf file icenso file that must be implemented in your product to make it function. Do not attempt to edit the .slf file in a text editor such as your license file and prevent your product from working property.

Now that you have your license file you can import it to your management console. To do this navigate to the **Admin Tab – Licensing Tab** and select **Import License**

Symant	ec Endpoint Protection Small Business E	dition Console						l d x	
Sym	antec-Endpoint Prote	ection Sm	nall Business E	dition		Refresh	Help Lo	a Off	
dia	Licenses								
_		Serial Number	г Туре	Seats	Start Date	e Expir	ation Date		
Monitors		None	Triehvore	N/A	1/28/09	2/28/0	9		
eports									
Policies									
Computers									
	Tasks								
2	Register a serial number						Hide th	is page	
Aamin	Les import a identise tile	Please foll	ow the steps below t	o activate your current	license.				
?		Step 1:	Register Serial Number						
Support		Step :	lick Register Serial Numb sing your Symantec Lice Import License	er to register your product nging Portal account, or cr your license file into th	serial number. Log on to the eate a new account. Enter y e console.	Symantec Licensing Por our product serial numbr	tal Webste er, and		
	Administrators	Click Help fo	or more information on lic	enses.					
	System	To purchase For more inf	e additional licenses, Syr	nantec recommends conta	cting your preferred reseller.				
	Licenses	For more int	comation, prease visit the	A DESCRIPTION OF A DESC	State of the part was called S	85.			

Navigate to the location where you downloaded the license and select Import

🔘 Import L	icense				×
Look In:	💋 licenses	-	🙆 🙆	1	
PROD PROD PROD	10client-1renewal.slf 10client-1year.slf <mark>25client-1year.slf</mark>				
File <u>N</u> ame: Files of <u>I</u> yp	PROD_25client-1 year.slf e: Symantec License Files (*.slf)				_
			Import		Cancel

Congratulations you have now imported your site license. You can verify this by viewing your license information under the license list.

😲 Symantec Endpoint Protection Small Business Edition Console							
Sym	antec Endpoint Prot	ection Sma	all Business Edition	1		Refresh Help L	.og Off
Lone	Licenses Mi115694523 25 seits Expres: 11/13/09	Symantec Serial Number M1136804523	Endpoint Protection Type Intial loanse	Small Business Ec Seats 25	dition 12.0 Maintenanc Start Date 11/1208	e Registration Expiration Date 11/1309	
Eeports Eoloces Computers	Turka						
Admin Q Qupport	Import a renewed license file Detect bis Scense Register a serial number Import an additional license file	Picase follon Step 1: Re Clo usi dov Step 2: Clo	w the steps below to activ gister Serial Number In Register Serial Number to re rg your Symanitec Licensing P wiload the license file. Import License Ik Import License to Import you	ate your current license gister your product serial n ortal account, or create a n r license file into the consol	umber. Log on to the Symante evv account. Enter your produ le.	Hide - Licensing Portal Web ster ct serial number, and	this page
	Administrators	Click Help for r	nore information on licenses.				
	System	To purchase a	idditional licenses, Symantec i mation, please visit the Syma	recommends contacting you	ur preferred reseller.		
	Licenses	T GI IIIGI O PIIOP	ment have use and 52005		and hour address and a		

WHAT TO EXPECT FROM THIS POINT ONWARD

Now that SEP SBE 12 has been successfully deployed to your Microsoft Small Business Server, here are some general high-level guidelines on what to expect from this point onward:

- □ Auto-Protect, Intrusion Prevention and Proactive Threat Scanning have been enabled on your Client. Full scans will be conducted weekly at 8:00 PM.
- Content updates (such as Antivirus and Antispyware definitions) will be automatically and silently downloaded by the manager every 4 hours and distributed to the managed Symantec Endpoint Protection Clients. Clients will conduct their own LiveUpdate call daily at 9:45 PM.
- □ The database will automatically purge data as it becomes old or as the database fills up. In general, no database configuration or maintenance is required.
- □ A weekly *Executive Summary* report as well as notification messages will be delivered to the email specified during the installation. These reports and notification messages are configurable and additional Email addresses can be added as needed.

IMPORTANT: The Symantec Endpoint Protection Client firewall has been deployed to the client however is disabled. The firewall can only be enabled by enabling the policy and assigning it to a group or groups within the management console. If the Windows Firewall was deployed on the Client System it will continue to be enabled however will be disabled when the SEP SBE 12 Firewall is enabled.

RECOMMENDED BEST PRACTICE CONFIGURATION

The following guidance can be used as best practice configuration within Small Business Server environments. Symantec always recommends a design that ensures clients retrieve incremental updates (additional definitions since last download) when retrieving content. On average, three new content updates are posted daily. As clients connect to their manager, the default policy has them retrieve the latest definitions. This means that clients can receive up to three content updates a day. When a client connects to the manager, it will always request an incremental content update. If the Manager does not have the requested incremental update package for the Client the Manager will send a full definition package.

The default configuration of Manager is to retrieve content updates from Symantec every 4 hours. Clients are configured via their own LiveUpdate call daily at 9:55 PM to retrieve new content from Symantec. This will ensure that clients that are not connected to the network will receive daily updates directly from Symantec. These settings can be reconfigured if necessary for your environment. Keep in mind that the LiveUpdate process will require a connection to the Internet to receive and process these updates. For details on how to configure LiveUpdate for laptops refer to the section titled **"How clients receive content updates"** of **Chapter 10** in the **implementation_guide.pdf** document.

MANAGER SETTINGS

There are very few changes that typically need to be made on the server settings in the Symantec Protection Center console. It is necessary that the Manager have Internet connectivity with the appropriate Email Server and Proxy Server Settings. The Email Server and Proxy Server Settings are configured during installation however can be altered after installation within the Admin Tab of the Management Console. The following links can be referenced for information on how to configure Management server Email and Proxy Settings:

How to configure SMTP Settings

http://service1.symantec.com/support/entsecurity.nsf/854fa02b4f5013678825731a007d06af/8cf31c11c88a96ce652574c00072 b312?OpenDocument

How to configure Proxy Settings

http://service1.symantec.com/support/entsecurity.nsf/854fa02b4f5013678825731a007d06af/5a8f40b6478675438825733e007 163dd?OpenDocument

In addition, it is also important to ensure that you keep a backup of the SPC server certificate for easing recovery efforts. The SPC maintains a backup of the server certificate for you under the following directory:

C:\Program Files\Symantec\Symantec Protection Center\Server Private Key Backup

It is recommended that this folder be copied to a safe location in the event that this directory is corrupted.

After installation of the Manager it is recommended that LiveUpdate be ran to download the most current content. This can be accomplished by navigating to the *Common Tasks* drop down list in the upper right hand corner of the Homepage and selecting *Run LiveUpdate*.

You can optionally run LiveUpdate from the *Admin* Tab and also review the history of LiveUpdate content downloads.

ADMINISTRATOR ACCOUNTS

Symantec recommends that an additional administrator account be created for redundancy. This account can also be utilized to unlock the default Admin account if necessary. See the section titled **"Managing administrator accounts"** of **Chapter 16** in the **implementation_guide.pdf** document for more information.

RECOMMENDED CLIENT PROTECTION POLICIES

At a minimum Symantec recommends that Clients have AntiVirus/Antispyware, Proactive Threat Protection (TruScan) and Intrusion Prevention technologies installed on Clients. As an added layer of protection the SEP SBE 12 Firewall can be deployed to add additional network communication controls. The Firewall is recommend for Desktop and Laptop systems only and is not normally enabled on Server machines.

VIRUS AND SPYWARE PROTECTION (ANTIVIRUS) POLICY

In most cases, very few changes are required or recommended for virus protection policies. Symantec always recommends running SEP SBE 12 with Auto-Protect enabled along with scheduled scans. The frequency and depth of the scheduled scan is usually best determined by analyzing the results of the scan. It is typically recommended to start your deployment with a full weekly scan. If you notice that there are few infections being discovered via the on-demand scan, it is recommended to decrease the frequency and depth of the scan. In environments with low infection rates, it is common to find monthly full scan or weekly quick scans being performed. Symantec provides 3 scan tuning options each of which provides different levels of optimization during scans.

- Best Scan Performance Optimizes the performance of the scan which will take the scan less time to complete.
- Balanced Performance Balances the performance of the scan against the performance of other applications.
- Best Application Performance Optimizes the performance of applications that are running during the time of the scan. The scan will take longer however the results are the same. (This is the out-of-box default setting.)

Running a full scan while running on batteries will result in a faster depletion of the laptop battery. To combat this you want to consider enabling the **Delay scheduled scans when running on batteries** feature. Enabling this feature will typically increase end user satisfaction with the product. To further increase end user acceptance of the product, you may want to consider enabling the **Allow the user to stop a scan** feature. These settings can be found within the Virus and Spyware policy - Administrator-defined Scans -Advanced tab.

NOTE: If you notice a high amount of scans being stopped, switch to the **Allow user to pause or snooze a Scan**

SEP SBE 12 has three default virus and spyware protection policies: **Standard Policy**, **High Performance**, and **High Security**. Symantec recommends the default virus and spyware protection policy on most machines. On machines that are slow, have high resource utilization, or on machines where users typically complain of performance issues, Symantec recommends applying the **High Performance** policy. For machines that are mission critical and for machines/users that have a high infection rate (Bad Internet Hygiene), Symantec recommends applying the **High Security** policy.

Policies		Virus and Spyware Policies				
U N	virus and Spyware	Name	Description			
ا 🖗	ntrusion Prevention	Virus and Spyware policy	Recommended policy for most environments, providing a good balanc			
₩ L \$\$ ¢	Iveupdate Centralized Exceptions	Virus and Spyware policy - High Performa	Higher performance policy, but with reduced security. Relies on File S			

It is recommended to keep the defaults on for *Internet Email Auto-Protect Scanning* and leave *TruScan Proactive Threat Scans* turned on. Symantec only recommends installing Outlook/Lotus plug-ins when virus and spyware protection is absent on the Mail Server.

FIREWALL POLICY

The Symantec Endpoint Protection Small Business Edition 12 Client with default settings for the Virus/Spyware and Intrusion Prevention protection features provides a solid approach to security at the endpoint. As an added layer of protection, you might want to consider utilizing a firewall policy.

IMPORTANT: A poorly configured firewall on a host computer can cause disruptions in the daily activities of users by blocking "good" traffic such as access to internal network applications and resources or the Internet. Symantec recommends testing firewall rules prior to applying the policy to the production environment. For more detailed information regarding the SEP SBE 12 Firewall read the section titled "Managing firewall protection" of Chapter 14 of the implementation_guide.pdf document.

A well written firewall policy protects the host machine and network from malicious traffic that is transparent to the end user. Symantec has streamlined the SEP SBE 12 firewall to provide 4 options to be considered when applying a firewall policy.

Default – Allows all inbound and outbound IP-based network traffic, with the following exceptions:

- > Blocks inbound and outbound IPv6 traffic with all remote systems
- Restricts the inbound connections for a few protocols that are often used in attacks (for example, Windows File Sharing)
- Connections from the computers on internal networks are allowed.
 Connections from the computers on external networks are blocked.
 - The internal networks include 10.0.0/24, 172.16.0.0/16, 169.254.0.0/16, 192.168.0.0/16
- **Low** Allows all inbound and outbound traffic not covered by the default rules
- Medium Blocks inbound traffic and allows outbound traffic not covered by the default rules
- **High** Blocks all inbound and outbound traffic not covered by the default rules

Once your knowledge and comfort level with firewall rules increases, you may want to customize the policy to control traffic to/from host computers in your environment. Administrators have the ability to customize firewall settings as desired however Symantec recommends that you start with the default settings and then adjust from Low to Medium to High.

When customizing your firewall policy consider the following 4 configurations. Each configuration provides a different level of protection and changes the likelihood of encountering false positives and preventing legitimate applications from working.

Firewall Configuration	Level of Protection	False Positive	Complexity
Firewall Disabled	None	None	None
Block Known Trojan Ports	Low	Low	Low
Block all Inbound	Medium	Medium	Medium
Explicit Deny	High	High	High

Firewall Disabled

Disabling the firewall minimizes the potential for making a mistake with the configuration that can cause legitimate applications to cease working. Since every network environment is unique, some customers find it easier to keep this technology disabled until there is a need. In Symantec Endpoint Protection Small Business Edition 12, disabling the firewall but enabling Intrusion Prevention provides additional protection with minimal configuration and false positives.

Block Known Trojan Ports

Choosing to allow all network traffic with the exception of ports commonly associated with known Trojans will provide an additional level of security while minimizing the risk of creating a policy that might block a legitimate application. For a list of ports commonly associated with known hack tools/Trojans, please refer to <u>Appendix A</u>. Although this might provide some protection, the Intrusion Prevention Engine already provides signatures to detect and block most of these exploits. In this configuration, Administrators can choose to block specific applications without the need of knowing what is installed in the environment.

Block all Inbound Connections

In most enterprise organizations, it is uncommon to see Clients connecting to other Client machines. This is different in smaller organizations that use the concept of workgroups. Configuring the firewall to block all inbound connections greatly reduces the risk of an attacker gaining access to a Client's resources or data. Most applications that get installed on the box will still be allowed to initiate communications which will minimize some of the configuration settings that would need to be configured. This configuration will not stop all malicious code from being installed on the computer nor will it prevent the malicious code from communicating important data to a hacker. This configuration will also block some legitimate corporate applications like management utilities that expect to receive connections from a management server. It is highly recommended to test this configuration thoroughly prior to deployment. Some companies have found it easier to deploy this configuration that blocks all inbound connections except from the servers installed in the organization. This has minimized the number of changes that need to be made as new applications are installed and minimized the number of exceptions needed to the policy. This is also the type of configuration that the Windows firewall uses by default.

Explicit Deny

The last of the models is the *explicit deny* approach. In this configuration, the firewall is configured to block all communications except those settings that you choose to accept. This is the most secure approach to creating firewall policies. This means that any new code introduced to the environment (good or bad) will not be allowed to communicate until an administrator approves it. Although this provides the most secure architecture, constant changes are usually needed in the firewall as applications change, are added or removed.

INTRUSION PREVENTION POLICY

Symantec recommends always running Intrusion Prevention (IPS) on Client and Server machines. Symantec makes no recommendations on changing the default settings for IPS. If Administrators or individuals within the organization are running security tools and assessment tools, Symantec does recommend excluding those machines from the IPS detection as it may yield false positives. This is easily accomplished using the Centralized Exceptions Policy discussed in a later section.

LIVEUPDATE POLICY

The Symantec Endpoint Protection Small Business Edition 12 Client automatically downloads the definitions and other product updates from the Symantec Protection Center server. The out-of-box default LiveUpdate policy is configured to have Clients initiate their own LiveUpdate call to Symantec daily at 9:45 PM to retrieve signatures and definitions. This policy can be tuned as needed however Symantec recommends that laptop systems have this functionality enabled to ensure they receive signature and definition updates when not connected to the SPC. Please see the section titled **Updating the Client's protection** of **Chapter 4** in the **Client_guide_sbe.pdf** for more information on LiveUpdate and how it's used to protect computers from newly discovered threats.

CENTRALIZED EXCEPTIONS POLICY

The recommendation for exceptions is to add them as needed. Symantec Endpoint Protection Small Business Edition 12 automatically makes exceptions for certain applications, but it is best to add additional exceptions for Databases, Transactional Logs, VMware Images, and other items that have high transactional volume. It is also recommended to not allow employees the ability to add exceptions unless needed. For additional information on default exceptions and information on how to add exceptions, please reference the Symantec Online Knowledge Base through the following link:

How to add a security risk exception

http://service1.symantec.com/support/entsecurity.nsf/0/2e47fa3acc0706c6882573b5005b4458?OpenDocument

USEFUL ONLINE RESOURCES

Symantec Endpoint Protection Small Business Edition 12 – Product Documentation

http://www.symantec.com/business/support/documentation.jsp?pid=55357

Symantec Endpoint Protection Small Business Edition 12 – Support homepage (search the Knowledge Base from here)

http://www.symantec.com/business/support/overview.jsp?pid=55357

Symantec publicly accessible user forums

https://forums.symantec.com/syment/board?board.id=endpointcust

SEP SBE 12 Admin UI Tour

http://www.symantec.com/redirects/symantec/support_symantec_com/sepsbe/tour/

SEP SBE 12 Client Installation Tour

http://eval.symantec.com/flashdemos/products/endpoint_protection/client_install_tour/

Symantec Licensing

http://licensing.symantec.com

APPENDIX A: COMMON MALICIOUS CODE PORTS

21 Blade Runner, Doly Trojan, Fore, Invisible FTP, WebEx, WinCrash	23 Tiny Telnet Server	25 Email Password Sender, Haebu Coceda, Shtrilitz Stealth, Terminator, WinPC, WinSpy	31 Hackers Paradise	80 Executor	456 Hackers Paradise
555	666	1001	1011	1170	1234
Ini-Killer, Phase Zero, Stealth Spy	Satanz Backdoor	Silencer, WebEx	Doly Trojan	Psyber Stream Server, Voice	Ultors Trojan
1243	1245	1492	1600	1807	1981
SubSeven 1.0 - 1.8	VooDoo Doll	FTP99CMP	Shivka-Burka	SpySender	Shockrave
1999	2001	2023	2115	2140	2801
BackDoor 1.00-1.03	Trojan Cow	Ripper	Bugs	Deep Throat, The Invasor	Phineas Phucker
3024	3129	3150	3700	4092	4567
WinCrash	Masters Paradise	Deep Throat, The nvasor	Portal of Doom	WinCrash	File Nail 1
4590	5000	5000	5001	5321	5400
ICQTrojan	Bubbel	Sockets de Troie	Sockets de Troie	Firehotcker	Blade Runner 0.80 Alpha
5401	5402	5400	5401	5402	5569
Blade Runner 0.80 Alpha	Blade Runner 0.80 Alpha	Blade Runner	Blade Runner	Blade Runner	Robo-Hack
5742	6670	6771	6969	7000	7300
WinCrash	DeepThroat	DeepThroat	GateCrasher, Priority	Remote Grab	NetMonitor

7301 NetMonitor	7306 NetMonitor	7307 NetMonitor	7308 NetMonitor	7789 ICKiller	8787 BackOfrice 2000
9872 Portal of Doom	9873 Portal of Doom	9874 Portal of Doom	9875 Portal of Doom	9989 iNi-Killer	10067 Portal of Doom
10167 Portal of Doom	10607 Coma 1.0.9	11000 Senna Spy	11223 Progenic trojan	12223 Hack´99 KeyLogger	12345 GabanBus, NetBus
12346 GabanBus, NetBus	12361 Whack-a-mole	12362 Whack-a-mole	16969 Priority	20001 Millennium	20034 NetBus 2.0, Beta-NetBus 2.01
21544 GirlFriend 1.0, Beta-1.35	22222 Prosiak	23456 Evil FTP, Ugly FTP	26274 Delta	30100 NetSphere 1.27a	30101 NetSphere 1.27a
30102 NetSphere 1.27a	31337 Back Orifice	31338 Back Orifice, DeepBO	31339 NetSpy DK	31666 BOWhack	33333 Prosiak
34324 BigGluck, TN	40412.0 The Spy	40421 Masters Paradise	40422 Masters Paradise	40423 Masters Paradise	40426 Masters Paradise
47262 Delta	50505 Sockets de Troie	50766 Fore	53001 Remote Windows Shutdown	54321 SchoolBus .69-1.11, Back Orrifice	61466 Telecommando
65000 Devil					